ESTUDO DAS REDES DE CONTATOS NO COMBATE   
AO SURTO DA COVID-19

*CONTACT NETWORKS STUDY IN COMBATING   
THE COVID-19 PANDEMIC*

|  |  |
| --- | --- |
| Fábio Corrêa Cordeiro | Doutorando  Escola de Matemática Aplicada  Fundação Getúlio Vargas (FGV) – Brasil  [fabiocorreacordeiro@gmail.com](mailto:fabiocorreacordeiro@gmail.com) |
| Raquel Corrêa Cordeiro | Doutoranda  Departamento de Artes & Design  Pontifícia Universidade Católica (PUC-Rio) – Brasil raquelcordeiro@aluno.puc-rio.br |

## Resumo

Com a pandemia da COVID-19, diversas áreas do conhecimento se depararam com enormes desafios. Esses desafios são primeiramente de ordem sanitária, mas devido às consequências de uma paralisação das atividades em escala global, também existem desafios econômicos, sociais, tecnológicos e éticos. Uma das estratégias mais defendida pelos pesquisadores é conhecida por TTIQ - Teste, Rastreio, Isolamento e Quarentena (*Test, Tracing, Isolate and Quarentine*). O rastreio dos contatos se mostrou uma ferramenta muito efetiva quando utilizada no início do surto. Entender o comportamento de uma pessoa infectada e quem ela teve contato nos remete ao estudo das redes, também conhecido como *Network Science*. Esse é um problema antigo, mas apresenta uma nova abordagem com a disponibilidade dos dados provenientes dos *smartphones*. Com a urgência da pandemia, muitos países, empresas e organizações lançaram aplicativos para coleta automática de informações, o que gerou um dilema ético entre conter a doença e renunciar à privacidade. Neste artigo, analisamos como é feito o rastreamento das redes de contatos, e avaliamos alguns dos principais aplicativos lançados por governos e empresas. Encontramos que há um desafio presente em todas as iniciativas, que é não apenas saber onde a pessoa passou, mas também o tipo de lugar, pois o contágio pode ser mais perigoso em lugares fechados. É necessária uma abordagem multidisciplinar, pois a simplificação de um território complexo e heterogêneo desconsidera elementos urbanísticos essenciais para se pensar em maiores ou menores propensões ao contágio. Alguns dos protocolos desenvolvidos mostraram que é possível conciliar anonimato e efetividade no rastreio, demonstrando que não é necessário existir um dilema entre saúde e privacidade. Desenvolvemos esse trabalho durante o desenrolar da pandemia, logo é necessário continuar avaliando o rastreio de contatos para acompanhar a evolução dos resultados alcançados.

**Palavras-chave:** COVID-19, Rastreamento de Contato, Privacidade, Políticas Públicas, Grafos.

## Abstract

With the COVID-19 pandemic, several areas of knowledge faced enormous challenges. These challenges are primarily healthy, but due to the consequences of a stoppage of activities on a global scale, there are also economic, social, technological, and ethical challenges. One of the strategies most defended by researchers is known as TTIQ - Test, Trace, Isolation, and Quarantine. Tracking contacts proved to be a useful tool when used at the beginning of the pandemic. Understanding the behavior of an infected person, and who had contact, leads us to the study of network science. It is an old problem, but it presents a new approach with the availability of data coming from smartphones. With the pandemic gravity, many countries, companies, and organizations launched applications for automatic information gathering, which created an ethical dilemma between holding the disease and giving up privacy. In this article, we analyze how to track a contact network and evaluate some of the main applications launched by governments and companies. We found that there is a challenge present in all initiatives, which is not only knowing where the person went but also the type of place, as contagion can be more dangerous in a closed environment. A multidisciplinary approach is necessary, as the simplification of a complex and heterogeneous territory ignores essential urban elements to a higher or lower propensity to transmission. Some of the protocols developed showed that it is possible to regulate anonymity and effectiveness in tracking, demonstrating that there is no need for a dilemma between health and privacy. We researched this work during the pandemic, so it is necessary to continue evaluating the tracking of contacts to follow the evolution of the results achieved.

**Keywords:** COVID-19, Contact tracing, Privacy, Public Policy, Graphs.

## 

## Introdução

Com o surto da pandemia da COVID-19, todas as áreas do conhecimento se depararam com enormes desafios, primeiramente de ordem sanitária, mas devido às consequências de uma paralisação das atividades em escala global, também existem enormes desafios econômicos, sociais, tecnológicos e éticos. As curvas e modelos epidemiológicos, que eram parte do dia a dia de um pequeno nicho de pesquisadores, passaram a ser acompanhadas diariamente nos jornais. Uma das estratégias mais defendida pelos pesquisadores é conhecida por TTIQ - Teste, Rastreio, Isolamento e Quarentena (*Test, Tracing, Isolate and Quarentine*) (TRONCOSO *et al.*, 2020). O rastreio dos contatos se mostrou uma ferramenta muito efetiva quando utilizada no início do surto, inclusive por países em desenvolvimento com menos recursos. Um bom exemplo é o Vietnã, apesar da baixa testagem per capita, é o país com a maior testagem por casos confirmados. Esses índices são os resultados de um extensivo rastreio das pessoas infectadas, e os testes - que eram raros no início da epidemia - foram direcionados para comunidades que tiveram contato com os infectados (POLLACK, THWAITES e RABAA, 2020).

Entender o comportamento de uma pessoa infectada e das pessoas com quem ela teve contato nos remete a uma modelagem de redes. Esse não é um problema novo, mas ganhou um novo elemento com a disponibilidade dos dados provenientes dos *smartphones*. Com a urgência da pandemia, muitos países, empresas e organizações lançaram aplicativos para coleta automática de informações, o que gerou um dilema ético quanto conter a doença e abrir mão da privacidade.

Nos próximos capítulos iremos desenvolver os conceitos de redes de contatos, questões de privacidade e a análise da seleção de aplicativos para o controle da doença. Discutiremos as tecnologias desenvolvidas e desafios encontrados.

## 1 Rastreio das redes de contatos

Antes de tratar o rastreio de contatos como uma rede, vamos definir o que é uma rede, ou no jargão matemático, um grafo. Grafo é uma coleção de vértices e arestas (NEWMAN, 2010). No caso do rastreio de pessoas infectadas, cada pessoa é um vértice e a existência de contato entre duas pessoas (ou seja, entre dois vértices) é uma aresta. Na Tabela 1 temos alguns outros exemplos de grafos. Dados os vértices i e j, uma aresta entre esses dois vértices é representada como (i,j). Consequentemente, podemos representar uma rede como uma lista de arestas. Uma representação mais comum de uma rede é através de uma matriz de adjacência Aij, onde Aij = 1 se existe uma aresta entre i e j, e Aij = 0 caso não exista.

|  |  |  |
| --- | --- | --- |
| **Rede** | **Vértice** | **Aresta** |
| Internet | Computador ou roteador | Cabos ou conexões |
| *World Wide Web* | *Web Pages* | *Hyperlink* |
| Rede de citações | Artigos, patentes e casos legais | Citação |
| Rede de distribuição de energia | Geradores e subestações | Linhas de transmissão |
| Rede de amizade | Pessoas | Amizade |
| Rede metabólica | Metabólito | Reação metabólica |
| Rede neural | Neurônio | Sinapses |
| Cadeia alimentar | Espécies | Predação |

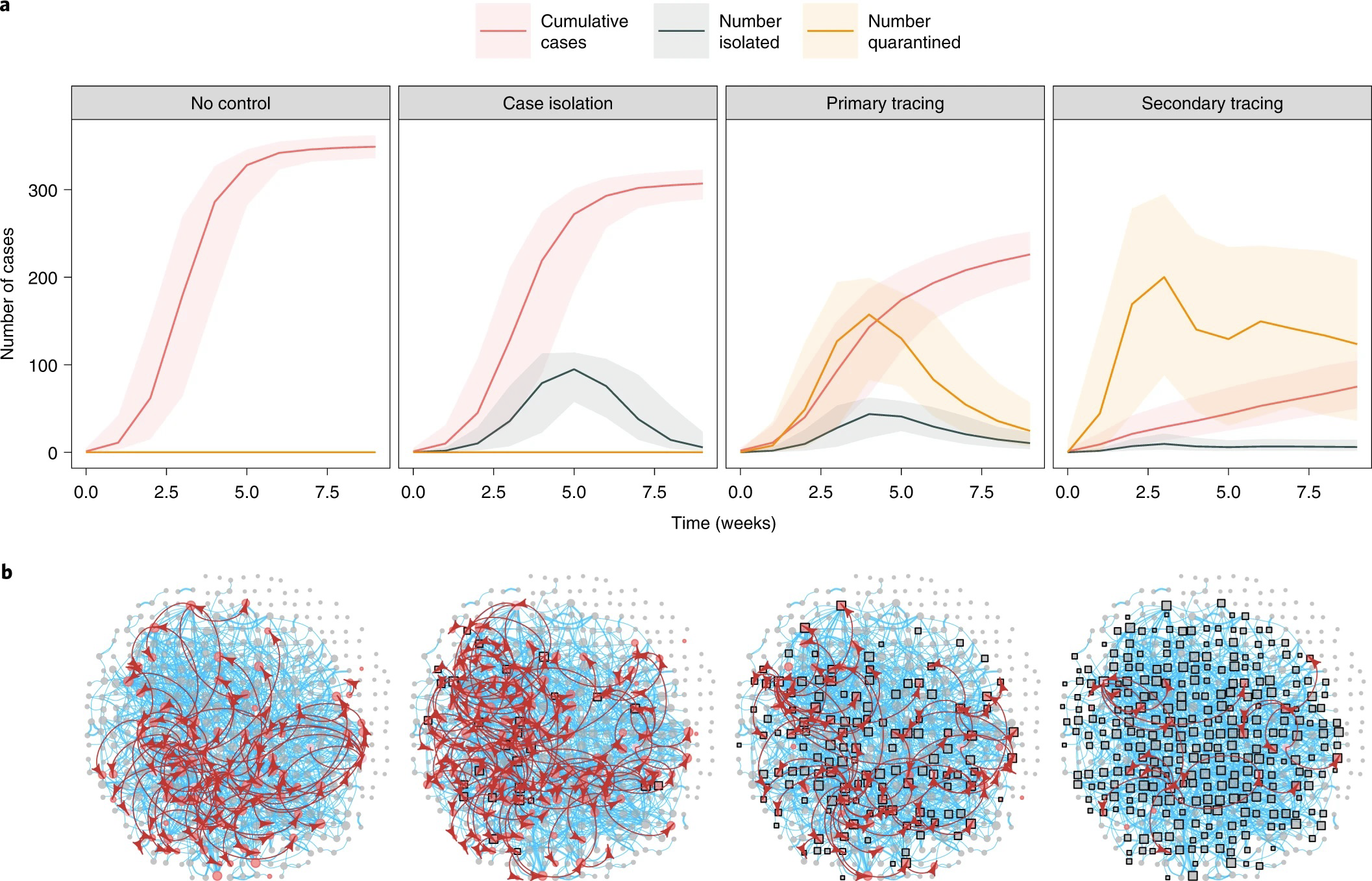
**Tabela 1** - Exemplos de grafos

**Fonte**: NEWMAN, 2010

Outros atributos que podemos analisar em uma rede é o peso e direção das arestas, a existência de ciclos, os caminhos, a centralidade e a clusterização dos vértices. Uma modelagem mais simples considera apenas se a conexão entre os vértices existe ou não. Em alguns, casos podemos qualificar melhor essas conexões acrescentando pesos e direção. No caso do rastreamento de contato, por exemplo, a direção do vértice pode representar a direção da infecção, e os pesos representam a duração e o tipo de contato. Podemos analisar a estrutura do grafo, que pode ter formato de árvores ou podem existir ciclos. Para muitos casos, é muito importante identificar possíveis caminhos, incluindo os caminhos mais curtos, entre dois vértices.

Uma análise importante é tentar qualificar os vértices. Existe uma série de medidas de centralidade que tentam atribuir graus de importância para os nós de uma rede. A contagem do número de arestas de um vértice é uma forma simples de atribuir pesos para um nó. Outras medidas de centralidade são a centralidade de autovetor, centralidade de Katz e o sistema *PageRank*. Essas análises podem auxiliar a identificação de *hubs* e "autoridades". *Hubs* são vértices altamente conectados e "autoridades" são aqueles com muito peso. Podemos considerar que os trabalhadores de serviços essenciais são *hubs*, por se manterem ativos e com muitos contatos mesmo em períodos de quarentena; já os passageiros de avião podem ser "autoridades", devido ao potencial de espalhar o vírus para regiões não afetadas de forma muito rápida. Por fim, podemos analisar a rede de forma mais ampla identificando agrupamentos e similaridades entre os vértices e arestas.

Apesar da recente tendência de análises de redes sociais, essa área de estudo teve início na década de 30 do século passado com o psiquiatra Jacob Moreno, seus estudos deram origem a sociometria (NEWMAN, 2010). Um interessante uso de redes de relacionamento é a amostragem bola de neve. Essa é uma forma de amostragem utilizada para identificar grupos escondidos em uma população que dificilmente seriam encontrados através de uma amostragem aleatória. Por exemplo, em pesquisas com usuários de drogas é difícil ou muito caro encontrar o público alvo através de uma pesquisa com o público geral. Nesse caso, pode ser interessante iniciar a pesquisa com usuários em tratamento, descobrir seus companheiros de uso e contactá-los. Ao avançar nessa rede de contatos é mais fácil de descobrir a comunidade alvo do estudo. O rastreamento de contatos de pessoas portadoras de doenças infecciosas é um caso especial de amostragem bola de neve (Figura 1).



**Figura 1** - Modelo de predição do surto em diversos cenários de rastreio de contato. A) Número de casos acumulados, número de pessoas isoladas e número de pessoas quarentenadas até um certo ponto em cada cenário. Linhas e áreas sombreadas representam a mediana e o percentil 5–95, respectivamente, para 1.000 simulações. B) Exemplo de uma rede para uma única simulação para cada cenário no 20º dia do surto.

**Fonte:** FIRTH, 2020

Um caso interessante de uso de modelos epidemiológicos de populações junto com modelos de redes é o simulador Global Epidemic and Mobility Model (GLEAM) (CHINAZZI, 2020). Este simulador divide cerca de 200 países e territórios em 3200 subpopulações. Essas populações estão centradas e conectadas por *hubs* de transporte, em geral aeroportos. Os dados demográficos e de viagem são provenientes de fontes oficiais e são bem próximos da realidade. Os modelos epidemiológicos tradicionais são aplicados em cada subpopulação, e o intercâmbio de pessoas é modelado de acordo com as viagens entre os *hubs* (*long-range*) ou pelas fronteiras (*short-range*) (Figura 2).



**Figura 2** - Camadas do Global Epidemic and Mobility Model (GLEAM)

**Fonte:** PASTORE Y PIONTTI *et a.l*, 2019

A urgência de se acompanhar cada pessoa infectada, seus contatos, locais por onde passou e viajou, adicionado pela automatização da coleta de informação, acende um alerta para a má implementação dessas atividades. O monitoramento em larga escala é um risco para o vazamento de informações dos cidadãos, bem como para o uso indevido por empresas e governos. Há a preocupação de que governos com viés autoritário use a pandemia como desculpa para monitoramento da população. Como vários dos protocolos já demonstraram, não é necessário renunciar à privacidade para implementar um aplicativo de rastreamento de contato. Ou seja, o dilema entre saúde e privacidade é um falso dilema. A transparência é sempre uma boa prática para minimizar o uso indevido dos dados coletados.

## 2 Privacidade

Os dados podem revelar informações sensíveis sobre a população, segundo Cottrill (2020) algumas questões de privacidade são críticas, como georreferenciamento ou outro tipo de dado de localização, apesar de representarem insumos valiosos. A coleta de dados de localização de *smartphones* pode ser altamente reveladora e usada para detalhar rotas de comportamento de um indivíduo.

Por isso o conceito de privacidade é importante, que para Cavoukian (2017) é sinônimo de controle pessoal do uso dos seus dados pessoalmente identificáveis. Com o avanço de tecnologias e novas capturas de dados, algumas legislações tiveram que ser criadas e atualizadas, como a *General Data Protection Regulation* (GDPR) na Europa e a Lei Geral de Proteção de Dados (LGPD) no Brasil.

O conceito de *Privacy-by-design,* desenvolvido por Cavoukian (2009), é outra iniciativa caracterizada por ser pró-ativa e antecipar invasões de privacidade. Ela se baseia em sete princípios:

1. **Pró-ativo não reativo;** **Preventivo não remedial:** Antecipa e prevê eventos antes de acontecerem. Por exemplo, uma empresa disponibilizaria um contrato mais amplo do que as próprias leis, com alto padrão de privacidade;
2. **Privacidade como Padrão:** O usuário não precisa agir para proteger a privacidade. O propósito de cada informação coletada é especificado, mantendo durante o tempo necessário e apagando-o depois de usá-lo.
3. **Privacidade Integrada no Projeto:** Abordagem sistemática de privacidade em todas as etapas do projeto, com documentação e publicação dos impactos e riscos de privacidade.
4. **Funcionalidade Total:** Não é necessário diminuir as funcionalidades para ter privacidade, nem ter que escolher outros interesses; todos os objetivos devem ser claramente documentados.
5. **Segurança de ponta a ponta:** Privacidade no ciclo total, ou seja, antes do primeiro dado ser coletado até o descarte. Assumir responsabilidade pela segurança da informação pessoal, ter padrões para garantir confidencialidade, integridade e disponibilidade.
6. **Visibilidade e Transparência:** Deve haver responsabilidade pela privacidade, abertura das informações e acordo sobre o acesso e o pedido dos dados.
7. **Respeito pela Privacidade do Usuário:** Priorizar opções centradas no usuário, empoderando-o para gerenciar o próprio dado.

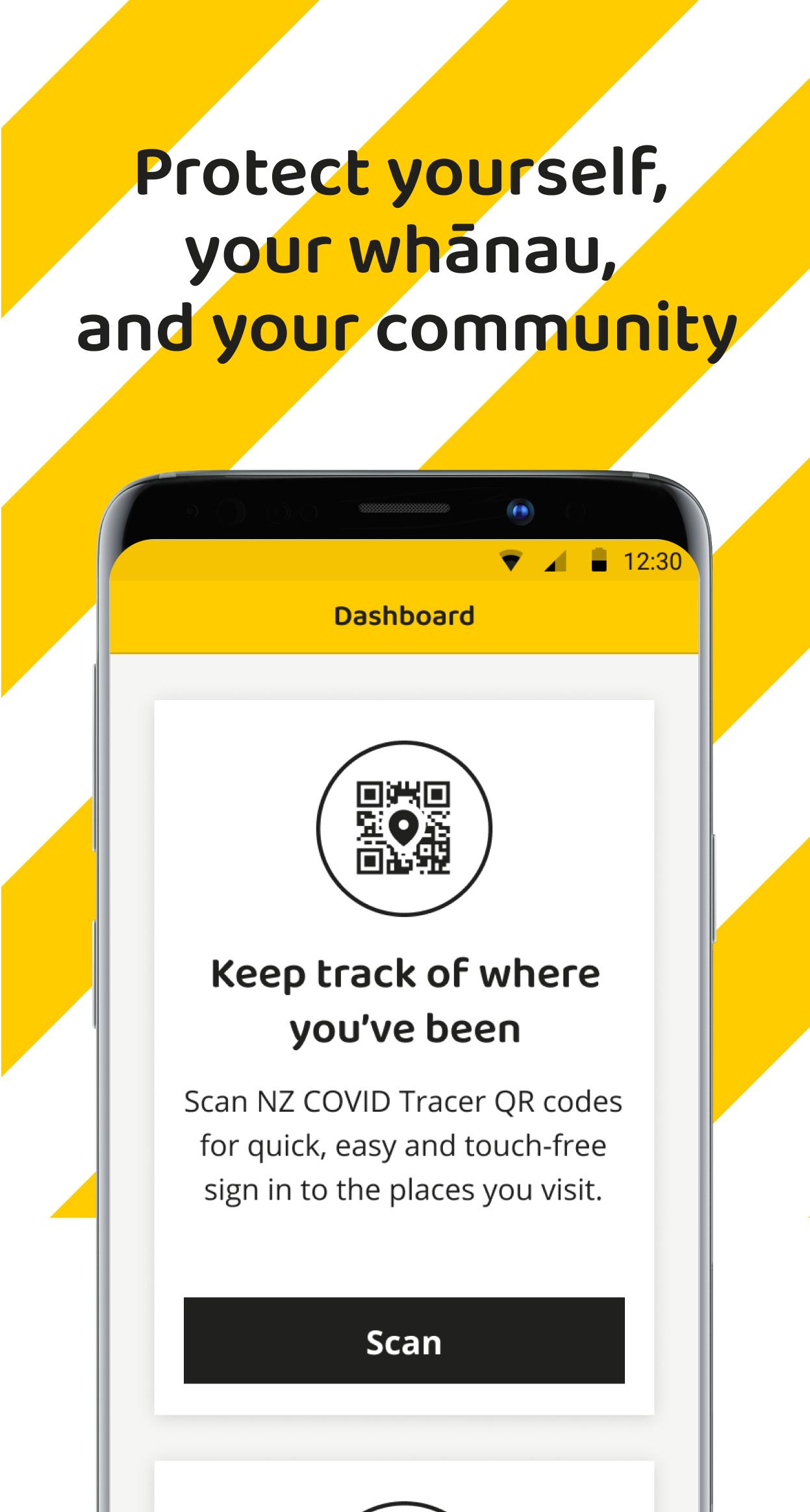
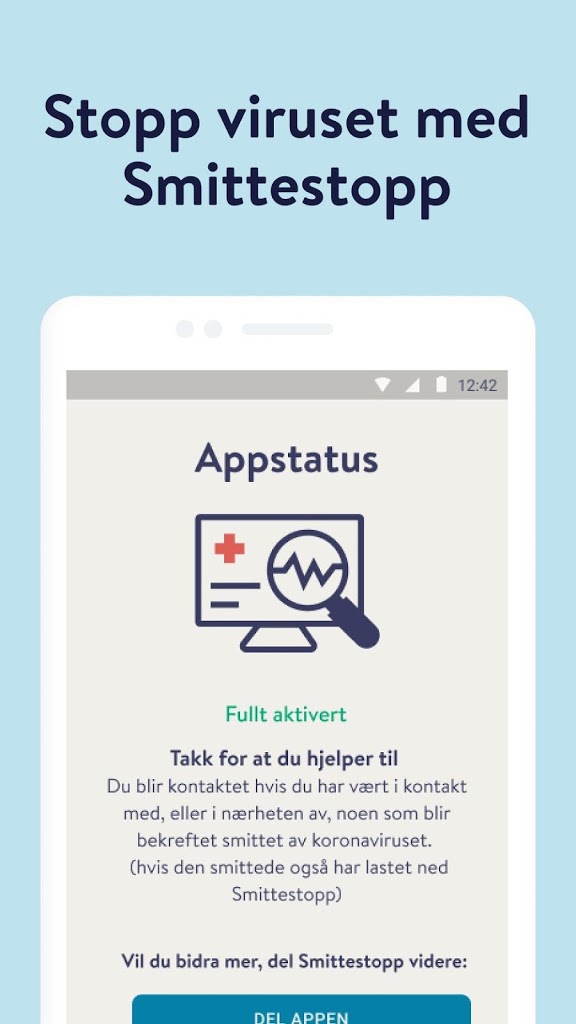
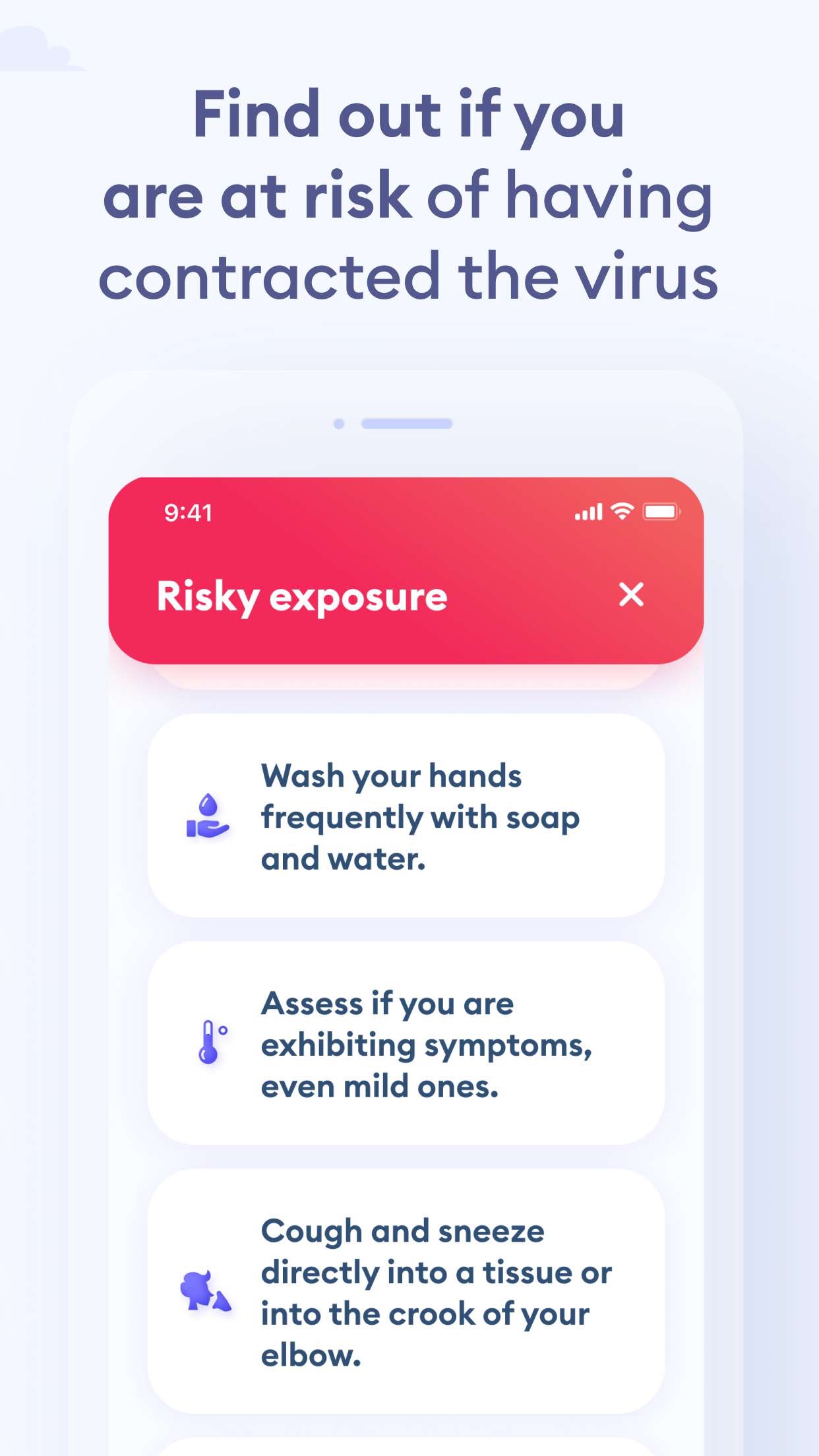
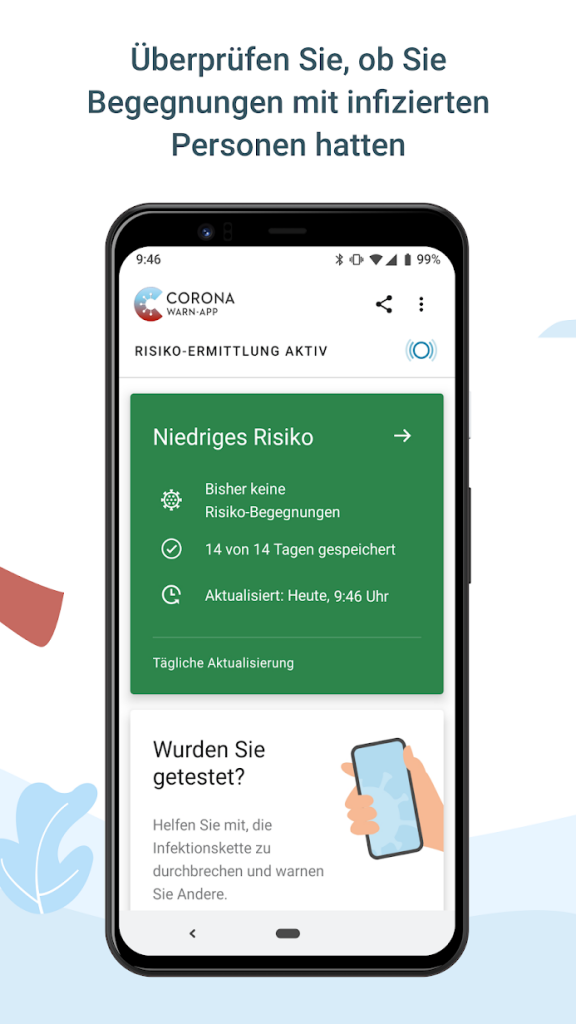
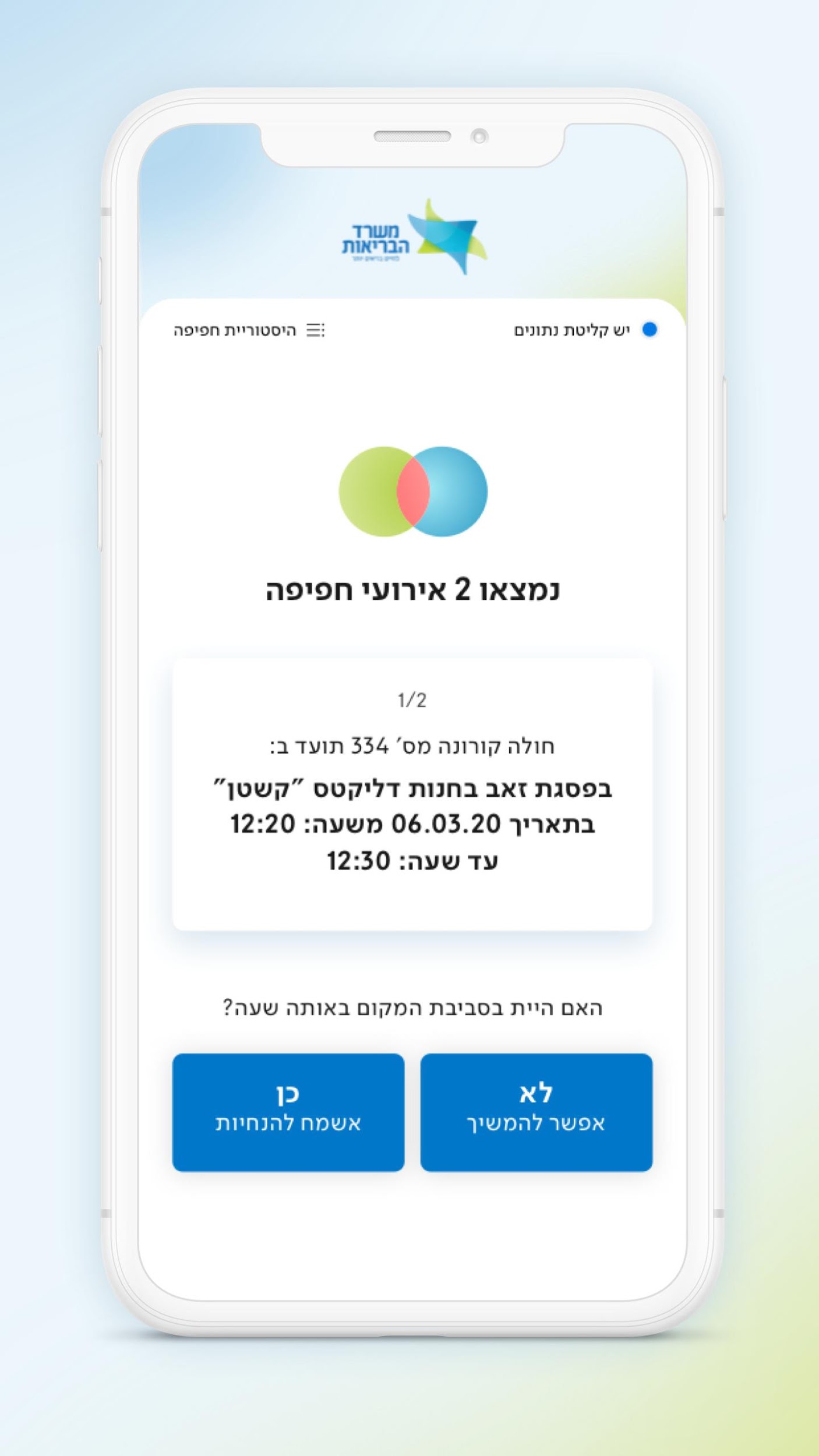
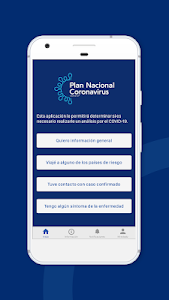
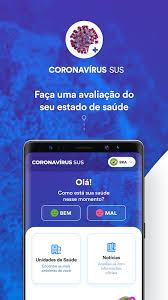
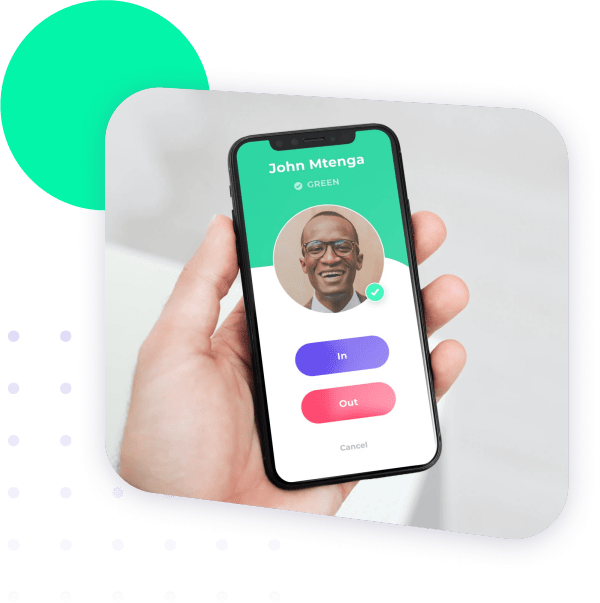
Como as leis que regulamentam o uso de dados são muito novas, ou inexistente em vários países, as empresas e instituições ainda estão adaptando os seus sistemas. Mesmos com algumas leis já em vigor, muitos aplicativos ainda coletam dados sem observar os princípios listados. Neste trabalho, analisamos como os aplicativos desenvolvidos para rastrear as redes de contato das pessoas com COVID-19 tratam os dados do usuário.

## 3 Aplicativos para o controle do covid-19

O atual surto gerou uma onda de desenvolvimento de aplicativos para rastreamento de contato automatizado. Ao invés das tradicionais pesquisas por telefone ou por agentes de saúde, a hipótese desses aplicativos é que os dados sobre localização dos celulares geram informações valiosas para as autoridades sanitárias. Em 2018, o Facebook já havia depositado uma patente para rastreio de contato (SATHYA e RASKAR, 2018). Em maio de 2020, a Apple e Google se uniram para lançar um protocolo único de rastreio - *Exposure Notification* - que está disponível nos dois principais sistemas operacionais que abrange a maioria dos celulares do planeta (GOOGLE, 2020). Devido ao risco à privacidade, alguns consórcios desvinculados das grandes empresas de internet também lançaram os seus protocolos. Dois exemplos são o *Pan-European Privacy-Preserving Proximity Tracing* (PEPP-PT) (PEPP-PT, 2020) e o *Decentralized Privacy-Preserving Proximity Tracing* (DP-3T) (TRONCOSO, 2020).

Cada protocolo tem as suas especificidades, mas em geral seguem os seguintes procedimentos: cada aplicativo gera um identificador aleatório que periodicamente é alterado para garantir o anonimato; Esses códigos são trocados com os celulares próximos via *Bluetooth,* tecnologia com um alcance mais curto, o que indicaria uma proximidade maior entre os usuários; Caso um dos usuários tenha o diagnóstico confirmado para COVID-19, os seus identificadores e todos os códigos lidos dos celulares próximos são disponibilizados em um servidor central; Os aplicativos observam constantemente o servidor central, e caso um dos identificadores gerados apareça no servidor, indica a existência de contato com uma pessoa diagnosticada com o vírus; Nesse momento, são passadas as primeiras informações sobre isolamento e indicação de como contatar as autoridades de saúde e realizar o teste.

Neste artigo apresentamos o resultado de uma pesquisa secundária (*desk-research*), realizada no mês de junho de 2020, com informações sobre aplicativos de diversos países para combater a pandemia (Figura 3). Uma parte deste estudo será publicada na revista *Strategic Design Research Journal,* em edição especial sobre contribuições para a emergência global da COVID-19 (CORDEIRO *et al.*, 2020, no prelo). Foram escolhidos 10 exemplos de diferentes continentes, com o objetivo de rastrear a população ou informar sobre possíveis contaminações do vírus.



**Figura 3**. Tela dos aplicativos: Covi-ID (África do Sul), Coronavirus SUS (Brasil), Coronavirus UY (Uruguai), Aarogya Setu Mobile App (Índia), HaMagen (Israel), TraceTogether (Singapura), Covid-Warn-App (Alemanha), Immuni (Itália), Smittestopp (Noruega) e NZ Covid Tracer app (Nova Zelândia)

Os aplicativos escolhidos possuem abrangência nacional, por isso não foram selecionados exemplos dos EUA, em que as iniciativas partiram de cada estado. Também se buscou fontes oficiais de divulgação; dessa forma, não foram selecionados aplicativos da China e Coreia do Sul que não disponibilizaram informações em inglês, o que impossibilitou a nossa análise.

Analisamos como os apps estão sendo utilizados no período da pesquisa, ainda que não seja algo permanente, pois o cenário muda rapidamente e algumas atualizações não puderam ser cobertas. Para fazer essas análises buscou-se informações nos sites oficiais dos desenvolvedores e governo, nas lojas da Apple e Google de cada país, e no site da OMS.

## 4 Análise e discussão

Dentre os aplicativos escolhidos há tecnologias diversas para captação da localização: 2 usam *QR code*, 2 GPS e 6 *bluetooth*. Desses, 3 usam tecnologia *Exposure Notifications* e 7 são *open source*. No caso do Brasil, o aplicativo já existia, mas foi adaptado para informações atualizadas (Tabela 2).

Depois que a Apple e Google anunciaram parceria para desenvolver a tecnologia *Exposure Notification*, alguns países lançaram seu aplicativo ou atualizaram para essa nova tecnologia. Apesar disso, *bluetooth* ainda é uma tecnologia pouco eficiente e muito questionada, pois não consegue identificar andares diferentes, paredes separando pessoas, o tipo de estabelecimento, ou se é um lugar fechado ou aberto, por exemplo.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Ícone** | **App** | **País** | **Geolocalização** | ***Open  Source*** | **Tempo dos dados salvos** |
|  | Covi-ID | África  do Sul | *QR Code* | Não | O tempo que for necessário |
|  | Coronavirus SUS | Brasil | GPS para identificar unidade mais perto e sinal do celular para saber áreas de aglomeração | Sim | Não é especificado |
|  | Coronavirus UY | Uruguai | *Bluetooth*  *(Exposure Notifications)* | Sim | 15 dias |
|  | Aarogya Setu Mobile App | Índia | *Bluetooth* | Sim | Teste negativo:  30 dias  Teste positivo:  60 dias |
|  | HaMagen | Israel | GPS | Sim | Localização:  7 anos  Outros dados: 30 dias |
|  | Trace Together | Singapura | *Bluetooth* | Sim | 25 dias |
|  | Covid-Warn-App | Alemanha | *Bluetooth*  *(Exposure Notifications)* | Sim | Teste negativo:  14 dias  Teste positivo:  21 dias |
|  | Immuni | Itália | *Bluetooth*  *(Exposure Notifications)* | Sim | Até no  máximo 31/12/2020 |
|  | Smittestopp | Noruega | *Bluetooth* e GPS | Não | 30 dias |
|  | NZ Covid Tracer app | Nova Zelândia | *QR Code* | Não | 31 dias |

**Tabela 2** - Tabela resumo com os aplicativos

Os aplicativos podem ser divididos em dois grupos: centralizados, aqueles com processamento de dados em servidores na nuvem; e descentralizados, com processamento dentro dos próprios dispositivos. No modelo centralizado, as autoridades de saúde têm maior controle, enquanto os descentralizados oferecem mais segurança para a privacidade dos cidadãos, modelo apoiado pela Apple e Google. Na Alemanha, ressaltam que a filosofia do projeto é a descentralização da tecnologia para que a população tenha mais confiança e o governo não concentre o armazenamento dos dados.

Nove dos dez aplicativos disponibilizam informações claras sobre a política de privacidade e o destino dos dados no próprio site oficial de divulgação. No Brasil, a política de privacidade só foi encontrada mediante *download*.Oito aplicativos especificam por quanto tempo o dado ficará armazenado, e que será automaticamente apagado sem nenhuma ação do usuário. Os únicos que não especificam são África do Sul e Brasil. Em Israel, mesmo aqueles dados de localização considerados irrelevantes ficarão armazenados por sete anos.

Sete aplicativos disponibilizam o código *open source* e convida a população a participar e inspecionar a segurança do código. Os únicos que não mencionam serem *open source* são Nova Zelândia, Noruega e África do Sul.

Alguns países, como Índia, Israel, Alemanha e África do Sul, têm parceria com diversas empresas e órgãos governamentais, às vezes de países diferentes, logo, com legislação diferente. Dessa forma, precisam ser responsáveis pelos dados em todos os processos, o que pode ser mais difícil. Além disso, nem todos explicam de forma clara como o usuário pode requisitar seus dados, como no caso de Israel, Itália e Brasil.

Outra questão de ética e privacidade é o caso da África do Sul, em que comerciantes ficam responsáveis por escanear os *QR codes* e verificar quem está livre para entrar. Essa dinâmica pode ser invasiva e constrangedora, ainda mais em um país com histórico de segregação racial.

No Brasil, a falta de transparência dos dados e a utilidade clara do aplicativo são desafios, pois o conteúdo não precisaria ser implementado em um aplicativo; o usuário poderia acessar por outros meios. Essa falta de utilidade clara acrescida à questão da privacidade também traz uma dúvida da relevância desses produtos digitais. No caso da Noruega, o aplicativo já foi descontinuado porque recebeu uma notificação sobre o uso de dados pessoais do instituto de proteção de dados do país. Eles acreditam que os casos baixos de COVID-19 não justificam a invasão de privacidade.

Um desafio é além de saber onde a pessoa andou também conhecer o tipo de lugar, pois lugares fechados podem ser mais contagiosos. Segundo Marino *et al*. (2020), uma abordagem multidisciplinar é necessária para não haver uma simplificação de um território complexo e heterogêneo, desconsiderando elementos urbanísticos para se pensar em maiores ou menores propensões ao contágio. Outro desafio é ter transparência e a população confiar para viabilizar sua participação. Segundo Kitchin *et al*. (2015), quando o cidadão tem um papel central na coleta de dados espera-se por métodos objetivos com dados transparentes, imparciais e livres de vieses. Para Carugati (2020), uma possível solução para tecnologias mais justas é criar um comitê de cidadãos que regule os algoritmos. Para resolver problemas sociais, muitas vozes precisam ser ouvidas e assim ter uma melhor governança cidadã.

## 5 Considerações Finais

Podemos identificar diversos usos da teoria dos grafos ao atacar os desafios apresentados por uma epidemia da escala do atual surto da COVID-19. Podemos observar a rede de contatos em uma escala tão pequena quanto as pessoas em suas relações diárias, ou em uma escala global no qual todas as populações do planeta estão interconectadas em uma grande teia. A estratégia de rastrear os infectados vem se demonstrando bastante eficiente, mas como tudo nessa pandemia, pode gerar efeitos adversos não esperados.

Como dito anteriormente, essa pesquisa foi um recorte de um período. O estudo realizado teve uma limitação de tempo, e não foi possível avaliar o ciclo total do produto, como ele foi elaborado e concluído. Por isso, seria interessante analisar os aplicativos depois da pandemia, entender se eles continuarão sendo utilizados, se os dados serão apagados ou manipulados para outros fins, e se esse tipo de aplicação foi relevante nesse contexto.

O resultado pode trazer algumas contribuições para outros pesquisadores, como informações sobre questões de privacidade em manipulação de dados dos cidadãos, uma visão das tecnologias disponíveis e alguns desafios encontrados. As comunicações oficiais são limitadas e parciais, necessitando uma maior transparência. Como é um recorte temporal, as tecnologias podem mudar, os aplicativos podem ser atualizados ou surgir outros. No entanto, os conceitos analisados nessa pesquisa são mais amplos, e podem ser discutidos e aplicados em outras iniciativas, não apenas no contexto de pandemia.

## Referências

CARUGATI, F. A Council of Citizens Should Regulate Algorithms. **Wired**. 12 jun. 2020. Disponível em: <https://www.wired.com/story/opinion-a-council-of-citizens-should-regulate-algorithms/?ct=t%28News+TB+%23706%29> Acesso em 5 jul. 2020.

CAVOUKIAN, A. Privacy by Design - The 7 foundational principles - Implementation and mapping of fair information practices. **Information and Privacy Commissioner of Ontario, Canada**, p. 5, 2009. DOI 10.1007/s12394-010-0062-y. Disponível em: <https://www.iab.org/wp-content/IAB-uploads/2011/03/fred_carter.pdf%5Cnwww.privacybydesign.ca>.

CAVOUKIAN, A. “Global privacy and security, by design: Turning the ‘privacy vs. security’ paradigm on its head.” **Health and Technology**, vol. 7, no. 4, p. 329–333, 12 Dec. 2017. DOI 10.1007/s12553-017-0207-1. Disponível em: <http://link.springer.com/10.1007/s12553-017-0207-1>.

CHINAZZI, M. et al. The effect of travel restrictions on the spread of the 2019 novel coronavirus (COVID-19) outbreak. **Science**, 2020.

CORDEIRO, R. C.; MONT’ALVÃO, C.; QUARESMA, M. Citizen data-driven design for pandemic monitoring. **Strategic Design Research Journal**, 2020. No prelo.

COTTRILL, C. D. MaaS surveillance: Privacy considerations in mobility as a service. **Transportation Research Part A: Policy and Practice**, vol. 131, no. September 2019, p. 50–57, 2020. DOI 10.1016/j.tra.2019.09.026. Disponível em: <https://doi.org/10.1016/j.tra.2019.09.026>.

FIRTH, J.A. et al. CMMID COVID-19 Working Group. Using a real-world network to model localized COVID-19 control strategies. **Nature Medicine**, 2020.

GOOGLE. Notificações de Exposição: tecnologia a serviço das autoridades de saúde pública no combate à COVID-19, 2020.

KITCHIN, R.; LAURIAULT, T. P.; MCARDLE, G. Knowing and governing cities through urban indicators, city benchmarking and real-time dashboards. **Regional Studies, Regional Science**, vol. 2, no. 1, p. 6–28, 2015. <https://doi.org/10.1080/21681376.2014.983149>.

MARINO, A., *et al*. (2020). Simplificação da leitura do comportamento da epidemia no território dificulta seu enfrentamento. Disponível em: <http://www.labcidade.fau.usp.br/simplificacao-da-leitura-do-comportamento-da-epidemia-no-territorio-dificulta-seu-enfrentamento/>. Acesso em: 5 jul. 2020.

NEWMAN, M. **Networks**. Oxford University Press, 2010.

PASTORE Y PIONTTI, A. et al. Charting the Next Pandemic: Modeling Infectious Disease Spreading in the Data Science Age**. Springer International Publishing**, 2019.

PEPP-PT. Pan-European Privacy-Preserving Proximity Tracing, 2020.

POLLACK, T., THWAITES, G. e RABAA, M. Emerging COVID-19 success story: Vietnam’s commitment to containment. Our World in Data**.** 2020. Disponível em: <https://ourworldindata.org/covid-exemplar-vietnam>.

SATHYA, S. S. e RASKAR, R. Proximity-based trust, 2018.

TRONCOSO, C. *et al*. Decentralized Privacy-Preserving Proximity Tracing. arXiv:2005.12273 [cs], 2020.