RASTREAMENTO DE CONTATOS COMO FERRAMENTA DE COMBATE À TRANSMISSÃO DO SARS-COV-2: *BENCHMARK* INTERNACIONAL, SOLUÇÕES TECNOLÓGICAS E CONSIDERAÇÕES ÉTICAS

Antônio Glauter Teófilo da Rocha[1],
Marcos Cesar de Oliveira Pinto[2],
Marcelo Dias Varella[3],
Izabella Ribeiro Xavier[4]

RESUMO

A pandemia ocasionada pelo vírus humano Coronavírus SARS-CoV-2 tem se configurado em um dos maiores desafios à sociedade neste século. Dado que, no curto prazo, não há a perspectiva de vacinas ou tratamento para a doença, torna-se fundamental avaliar outras possibilidades que permitam desacelerar a sua transmissão. Este artigo investiga as soluções de rastreamento digital de contatos sendo exploradas em diferentes países, começando por um benchmark internacional, passando por um detalhamento do tipo de ferramenta sendo aplicada e avaliando as implicações éticas e relacionadas à privacidade ao se adotar tal estratégia. Conclui-se que as ferramentas podem trazer resultados positivos no combate à pandemia, mas que a estratégia de implementação deve ser feita de forma cuidadosa, tanto para garantir o bom funcionamento da ferramenta, como para afastar os temores que ela possa de alguma forma ferir direitos fundamentais ou invadir a privacidade dos cidadãos.

CONTACT TRACING AS A TOOL TO COMBAT THE TRANSMISSION OF SARS-COV-2: INTERNATIONAL BENCHMARK, TECHNOLOGICAL SOLUTIONS AND ETHICAL CONSIDERATIONS

ABSTRACT

The global health crisis caused by the SARS-Cov-2 virus is being considered one of the most challenges to civilization in the 21st century. Since the prospects for a vaccine or an effective therapeutic treatment in the short run are low, new strategies are needed to prevent the spread of the disease. This article compiles the international experience on digital contact tracing solutions, goes on the show the potential tools that are available and, finally, analyses the ethical and privacy implications of such a scheme. We conclude that there is clearly potential for digital contact tracing to be a relevant tool in combating the spread of SARS-Cov-2. However, the implementation strategy must be carefully drawn, in order not only to make sure that the app

[1] Engenheiro civil pela UFC. Doutor e Mestre em Enngenharia de Produção pela PUC/RIO. Doutorado Sanduíche e Especialização no Massachusetts Institute of Technology – MIT.
[2] Cientista da Computação formado na Universidade Estadual de Londrina e mestre em políticas públicas e desenvolvimento pelo IPEA - Instituto de Pesquisa Econômica Aplicada.
[3] Professor do Programa de Mestrado e Doutorado em Direito do UNICEUB. Doutor em Direito. Bolsista de Produtividade em Pesquisa do CNPq.
[4] Mestre em Direito pelo programa do UniCEUB. Advogada junto ao escritório Barroso Fontelles, Barcellos, Mendonça & Associados.

works properly, but also to prevent the fear that it might in any way hurt citizens' basic rights or invade their privacy.

1. INTRODUÇÃO

O recém-diagnosticado vírus humano Coronavírus SARS-CoV-2 está resultando em altas taxas de mortalidade e sobrecarga incapacitante nos sistemas de saúde, devido à COVID-19, doença por ele causada. Em todo o mundo, governos, autoridades de saúde, centros de pesquisa, empresas e ONGs estão trabalhando juntos para encontrar soluções para a pandemia, para proteger as pessoas e para colocar a sociedade em normalidade novamente.

Atualmente, não existe tratamento comprovado disponível. Tampouco há uma vacina para a doença – a opinião majoritária, refletida, entre outros, por Amanat e Kramer (2020), é que vacinas demorarão, no mínimo, de 12 a 18 meses para estarem disponíveis. Impedir o alastramento descontrolado da transmissão é, portanto, uma prioridade. As únicas abordagens atualmente à disposição das autoridades de saúde pública para interromper o surto são as do controle clássico de epidemias: isolamento de casos, rastreamento e quarentena de contatos, distanciamento físico e medidas de higiene.

Como a transmissão do Coronavírus SARS-CoV-2 ocorre rapidamente e antes dos sintomas se manifestarem, como argumenta Ferretti *et al* (2020), é altamente improvável que a epidemia seja contida apenas pelo isolamento de indivíduos sintomáticos. Assim, do ponto de vista do controle clássico de epidemias, de forma geral, restariam o rastreamento e quarentena de contatos, o distanciamento físico e as medidas de higiene como estratégias disponíveis para o combate à propagação descontrolada da epidemia.

Por esse motivo, logo na emergência dos primeiros casos da COVID-19, nas fases iniciais da epidemia, uma das principais ações implementadas pelos órgãos de saúde pública no Brasil, assim como em vários outros países, foi o trabalho de mapear cada pessoa doente e depois descobrir com quem interagiram recentemente. A técnica, chamada "rastreamento de contato" (*contact tracing*), ajuda a controlar surtos de doenças infecciosas. Como o Coronavírus SARS-CoV-2 pode ser transmitido pela proximidade a indivíduos afetados, as organizações de saúde pública, também nesse caso, elegeram o "rastreamento de contatos" como uma ferramenta valiosa para ajudar a conter sua disseminação.

O processo não é fácil. Quando uma pessoa fica doente, é entrevistada por autoridades de saúde pública para descobrir quem foi exposto a ela. Em seguida, as autoridades, a partir dessa lista, trabalham para conscientizar essas pessoas que monitorem com atenção o eventual aparecimento de sintomas e, caso necessário, que fiquem de quarentena. Se uma pessoa exposta estiver infectada, seus contatos recentes também serão rastreados. O processo continua até que todos que foram expostos estejam fora de circulação. O objetivo é tentar interromper a transmissão do vírus.

No início do surto do coronavírus no Brasil, como na maioria dos países afetados, as autoridades de saúde pública cuidadosamente examinaram o histórico recente de contatos de todos os casos recém-diagnosticados de COVID-19. Mas quando o número de casos começou a crescer, essa atividade se tornou impeditiva, não havia recursos

humanos suficientes para rastrear contatos para cada nova infecção – até porque a quantidade de pessoas a serem verificadas cresce geometricamente.

De fato, de acordo com estudos baseados em modelagens matemáticas[5] o rastreamento convencional de contatos, por meio de entrevistas, na prática, só pode melhorar a contenção do surto de forma limitada. É muito lento e não pode ser ampliado depois que a epidemia cresce além da fase inicial, principalmente devido à limitação de pessoal nas instituições de saúde pública.

Ferretti *et al* analisaram os principais parâmetros de propagação da epidemia da COVID-19 para estimar a contribuição de diferentes rotas de transmissão e determinar os requisitos para isolamento de casos e rastreamento de contatos necessários para interrompê-la. Concluiu que a disseminação viral do SARS-CoV-2 é rápida demais para ser contida pelo isolamento de casos ou pelo rastreamento convencional de contatos, mas poderia ser controlada se esse último processo fosse mais célere, mais eficiente e acontecesse em escala.[6]

Tomando como base os resultados obtidos usando um modelo matemático geral de infecciosidade do SARS-CoV-2 por eles desenvolvido, os autores acreditam que um aplicativo de rastreamento de contatos que crie uma memória de contatos de proximidade e notifique imediatamente contatos de casos positivos pode obter um controle relativamente satisfatório de uma epidemia dessa natureza, se usado por pessoas suficientes. Mesmo considerando a alta taxa de transmissibilidade do SARS-CoV-2, eles acreditam que com um aplicativo para celular implementando rastreamento instantâneo de contatos seria possível reduzir a transmissão o suficiente para sustentar a supressão epidêmica, impedindo a propagação do vírus.

No Brasil, desde o dia 13 de março de 2020, quando o Ministério da Saúde comunicou da necessidade de intensificação das medidas de distanciamento social, com o objetivo de promover o achatamento da curva epidêmica de propagação do coronavírus no Brasil, essa passou a ser a principal medida de controle epidemiológico utilizado pela maiorias dos estados e municípios, variando de caso a caso, dependendo da realidade de cada localidade. Trata-se da pandemia com maior mobilização dos entes públicos e privados e com maior mobilização de que se tem notícia no país, focada no isolamento.

Uma outra estratégia de saída da pandemia de coronavírus, discutida por alguns especialistas, pode ocorrer quando pessoas suficientes desenvolverem imunidade ao surto por infecção. Esse conceito controverso é conhecido como "*Herd immunity*". Está sendo usado na Suécia e foi adotado inicialmente como estratégia na Grã-Bretanha e na Holanda. Porém, esses dois últimos países mudaram recentemente de abordagem, após alertas de que esse método provavelmente sobrecarregaria seus sistemas de saúde e o número de mortos aumentaria.

Apesar de ainda haver alguma controvérsia, a maioria dos especialistas defendem que uma medida mais proativa, como o isolamento social, é a melhor maneira de se tentar conseguir esse achatamento da curva epidêmica no Brasil, mesmo sabendo que

[5] FRASER, C. *et al*. Factors that make an infectious disease outbreak controllable. Proc. Natl. Acad. Sci. U.S.A. 101, 6146– 6151. doi:10.1073/pnas.0307506101 Medline, 2004.
[6] FERRETTI, L. *et al.*. Quantifying SARS-CoV-2 transmission suggests epidemic control with digital contact tracing. Science 10.1126/science.abb6936, 2020

a subnotificação dos casos e a fila de exames podem impedir que a curva traduza de forma precisa o avanço da doença nas diversas localidades.

Entretanto, o impacto econômico e social causado pelo isolamento social e fechamento dos estabelecimentos não essenciais é significativo e apresenta elevado risco de diminuir sua eficácia no médio prazo, se tiver que ser prolongada por meses consecutivos. Indivíduos com baixa renda, em especial, têm capacidade limitada para permanecer em casa, e o apoio a pessoas em quarentena requer recursos vultosos, hoje escassos no País. Ademais, em momentos de escassez de recursos as empresas tendem a perder a confiança ao longo do tempo, causando ciclos de feedback negativo na economia, gerando impactos psicológicos duradouros.

Portanto, mesmo considerando a potencial eficácia da estratégia do distanciamento social em larga escala no controle da epidemia, é imperativo que sejam desenhadas e testadas medidas complementares a ela, que possam ajudar a suavizar as medidas de isolamento nos momentos mais críticos e viabilizar uma saída gradual delas no momento adequado, definido pelas autoridades de saúde pública.

Assim, o objetivo deste artigo é explorar a possibilidade de soluções tecnológicas que eventualmente contribuam para desacelerar a disseminação do COVID-19 e acelerar o retorno da vida cotidiana, seja por meio de identificação de aglomerações, seja pelo rastreamento de contatos. Esta avaliação engloba diferentes prismas: na seção 2, estabelece-se o conceito de rastreamento digital de contatos e a experiência internacional recente no uso desse tipo de ferramenta. Na seção 3 buscou-se um aprofundamento quanto ao tipo de solução e de serviços oferecidos a serem considerados na construção de uma solução de rastreamento digital de contatos para o Brasil. Na seção 4, são discutidas as questões éticas envolvidas nesse tipo de intervenção, especialmente no que se refere à privacidade e à segurança dos cidadãos. Por fim, na seção 5, são apresentadas as considerações finais.

2. O rastreamento digital de contatos – experiências internacionais

O rastreamento digital de contatos pode desempenhar um papel importante na complementação e possível suavização das medidas de isolamento social hoje vigentes no país, sem diminuir sua efetividade no controle da epidemia. O método pode oferecer benefícios tanto para a sociedade quanto para os indivíduos, ao mesmo tempo em que seu uso adequado pode ajudar a reduzir o número de casos de infecção.

Ademais, a utilização eficaz do mesmo deve permitir que as pessoas retomem, gradualmente, suas vidas de maneira informada, segura e socialmente responsável. Seu uso adequado pode ajudar a conciliar os benefícios públicos do controle da epidemia com a necessidade de maior autonomia das pessoas.

De uma forma geral, e no Brasil em especial, o alcance de uma ferramenta dessa natureza não é pleno. Existem grupos da população que não seriam atingidos, seja por falta de acesso à tecnologia necessária (*smartphone*, conexão de internet, etc) ou por características pessoais, como faixa etária ou nível educacional. Contudo, por meio de modelagem matemática é possível explorar diferentes cenários de alcance da utilização desse tipo de ferramenta no contexto atual brasileiro, para diferentes estratégias de flexibilização, suavização ou saída gradual do isolamento social de larga escala.

Um aplicativo de celular pode fazer o rastreamento e a notificação de contatos instantaneamente após a confirmação do caso de infecção pelo SARS-CoV-2. Ao manter um registro temporário de eventos de proximidade entre indivíduos, pode alertar imediatamente os contatos próximos recentes dos casos diagnosticados e solicitar que eles se auto isolem, que procurem imediatamente as autoridades de saúde pública para orientações, ou ainda já transmitir automaticamente a eles as orientações das autoridades, por exemplo.

Em vários países do mundo já vem sendo realizado trabalho importante para desenvolver tecnologias digitais de rastreamento de contato. Há também desenvolvedores de *software* contribuindo com a elaboração de ferramentas técnicas para ajudar governos e agências de saúde a reduzir a propagação do vírus, buscando manter a privacidade e a segurança do usuário.

A seguir, de forma sucinta, são apresentadas algumas experiências internacionais no uso dessas tecnologias para o combate à pandemia da COVID19, com a ressalva que, devido ao fato da pandemia ser um fenômeno recente, ainda há poucos estudos acadêmicos que comprovem a eficácia de tais soluções – especialmente que tenham passado por processos de *peer review*.

2.1. Singapura

A cidade-estado lançou um aplicativo chamado *TraceTogether*, em 20 de março de 2020, ferramenta suplementar para seus esforços de rastreamento de contatos, que dependiam da recuperação e memória de indivíduos infectados. O método funciona por meio de telefones com o aplicativo instalado, onde estes trocam sinais Bluetooth de curta distância quando seus usuários estão próximos um do outro. Os registros desses encontros, incluindo a duração, são armazenados em seus respectivos telefones por 21 dias. Os dados do local não são coletados pelo Governo, permanecem no aparelho do cidadão. Se um usuário for diagnosticado com COVID-19, ele poderá permitir que o Ministério da Saúde de Cingapura acesse os dados do aplicativo para identificar pessoas que tiveram contato próximo com o indivíduo infectado.

Em Cingapura, quando uma pessoa é contatada, ela é obrigada por lei a ajudar o Ministério da Saúde a mapear com precisão seus movimentos e interações para minimizar o risco de infecção generalizada. Isso inclui o fornecimento de cronogramas de localização e *logs* físicos ou digitais que podem ser coletados pelos aplicativos.

De acordo com o Gabinete do Primeiro Ministro de Cingapura, a resposta ao aplicativo foi "amplamente positiva". Mais de 500.000 usuários com um número de celular registrado em Cingapura baixaram o aplicativo *TraceTogether* nas primeiras 24 horas de seu lançamento, ou seja, cerca de 10% da população.

O Governo de Cingapura promete disponibilizar livremente sua tecnologia de rastreamento de contatos aos interessados em adotar a tecnologia por trás do aplicativo, podendo usar ou adaptar o aplicativo para suas necessidades, sem custos (*open source*).

No caso de Cingapura, além do uso intensivo de tecnologia, nota-se uma sociedade com grande confiança no poder público, forte poder de mobilização social e fácil

isolamento social pelas características geográficas. O desenvolvimento e início do uso do aplicativo deu-se após apenas 80 casos e foi acompanhado da possibilidade de testagem em massa de toda a população e uso de máscaras. Assim, todos os infectados eram objeto de um rastreamento pretérito, e as pessoas com quem tiveram contato recente eram objeto de testagem e isolamento. A partir do conjunto de medidas, foi possível manter o isolamento parcial da sociedade, com a manutenção das empresas e shoppings abertos.

2.2. China

Para evitar um surto maciço da doença na China, o governo chinês adotou medidas abrangentes de prevenção, incluindo bloqueio e restrição de viagens em várias cidades. Embora essas medidas ajudem significativamente a prevenir a transmissão de doenças, também causam transtornos à vida das pessoas em geral. Durante esse período, várias tecnologias de informação pessoais e baseadas em telefones celulares foram desenvolvidas e amplamente utilizadas na China, ajudando a reduzir a transmissão do COVID-19 e manter a ordem social normal.

A primeira dessas tecnologias a se destacar foi o "Aplicativo do código de *status* de saúde" (*The application of health status code*) lançado em 11 de fevereiro de 2020, na cidade de Hangzhou, Zhejiang. Com base em tecnologias de *big data* e internet móvel, os residentes e aqueles que entram na cidade precisam se inscrever online e receber um código verde, vermelho ou amarelo. As cores são baseadas nas informações relatadas pelos cidadãos, incluindo seu estado de saúde, histórico de viagens e se eles mantiveram contato recente com pessoas de áreas epidêmicas. Indivíduos com código verde podem viajar pela cidade, já aqueles com código vermelho ou amarelo devem primeiramente passar de 7 a 14 dias em quarentena. De acordo com a classificação, o governo restringe a viagem de pessoas com possível infecção, mas permite que as saudáveis viajem livremente e retomem o trabalho. Com base em um resumo da experiência local, o governo chinês promoveu um sistema unificado de códigos de saúde em todo o país.

Outra importante tecnologia utilizada na China é o "Aplicativo de Casos Diagnosticados na Comunidade", que permite que as pessoas verifiquem a distribuição dos casos COVID-19 nas comunidades locais no mapa. O mapa abrange mais de 130 cidades chinesas e mostra o número e a localização do caso. Esse aplicativo ajuda as pessoas a gerenciar cuidadosamente suas viagens circundantes e a rever o potencial contato com os pacientes.

Com base nessas e outras experiências locais, a política de saúde pública da China foi implementada usando um aplicativo que não era obrigatório, mas era necessário para se move entre quadrantes/bairros (*quarters*) e entrar em espaços e transportes públicos. O aplicativo permite que um banco de dados central colete dados sobre o movimento do usuário e o diagnóstico de coronavírus, exibindo um código verde, âmbar ou vermelho para permitir ou impor restrições ao movimento. O banco de dados é analisado por um algoritmo de inteligência artificial que emite os códigos de cores. O aplicativo associado é um *plug-in* para os aplicativos WeChat e Alipay.

Em paralelo, houve total bloqueio da região com maior número de casos. Ademais, funcionários de edifícios residenciais foram convocados para irem nos

apartamentos, medir a temperatura dos cidadãos e preencher dados em um aplicativo indicado pelo governo, de forma a alcançar os mais resistentes à acatar as medidas governamentais.

A China continental fora da província de Hubei recebeu significativamente mais entradas de Wuhan do que em qualquer outro lugar, devido à movimentação de pessoas em torno do Ano Novo Chinês e o início do bloqueio de Wuhan. Apesar disso, a supressão epidêmica sustentada foi alcançada na China: menos de 150 novos casos por dia foram relatados de 2 a 23 de março, abaixo dos milhares informados a cada dia no auge da epidemia. Em grande parte, isso foi conseguido usando tecnologia associada à recomendação da quarentena.

2.3. Israel

Após a decisão de rastrear os locais visitados pelos pacientes com coronavírus, o Governo de Israel lançou aplicativo de código aberto para avisar usuários de casos de coronavírus. O aplicativo israelense, chamado "The Shield" ("HaMagen", em hebraico), pode informar instantaneamente aos usuários se eles cruzaram o caminho com alguém já anteriormente notificado com infecção pelo coronavírus.

O aplicativo utiliza os dados de localização do telefone do usuário e os compara com as informações nos bancos de dados sobre os históricos de localização de casos confirmados, do Ministério da Saúde, para os 14 dias anteriores ao diagnóstico. Se o aplicativo não detectar que o usuário foi exposto, ele os informa que "de acordo com os dados coletados até o momento, nenhum ponto de interseção foi encontrado com pacientes infectados com coronavírus".

Nas palavras do Ministro Benjamin Netanyuahu:

> "We will dramatically increase the ability to locate and quarantine those who have been infected. Today, we started using digital technology to locate people who have been in contact with those stricken by the Corona. We will inform these people that they must go into quarantine for 14 days. These are expected to be large – even very large – numbers and we will announce this in the coming days. Going into quarantine will not be a recommendation but a requirement and we will enforce it without compromise. This is a critical step in slowing the spread of the epidemic."[7]

Até aquele momento, os movimentos de pessoas diagnosticadas com coronavírus eram publicados no site do ministério e em seu canal Telegram - mas avaliar se alguém poderia ter entrado em contato com uma pessoa infectada envolvia horas percorrendo as informações. O aplicativo - disponível para telefones Apple e Android – passou a fazer isso instantaneamente.

O aplicativo é *open source*, seu código já foi disponibilizado para especialistas na área e, em breve, será disponibilizado ao público em geral. Além disso, houve a alteração normativa, para permitir o uso de tecnologia anti-terrorismo, com a finalidade de

[7] https://techcrunch.com/2020/03/18/israel-passes-emergency-law-to-use-mobile-data-for-covid-19-contact-tracing/, acesso em 24.04.2020

realizar o rastreamento massivo de toda a população, por 30 dias, para conter a propagação do vírus.

2.4. Suíça

A Suíça vem monitorando os dados do celular dos cidadãos para determinar se há necessidade de bloqueios. De fato, hoje as autoridades suíças estão usando esses dados para determinar se é necessário implantar bloqueios mais rigorosos, tendo em vista que diversas medidas de isolamento já foram impostas até o momento. Os dados dos telefones estão sendo rastreados para verificar se as pessoas estão ficando em casa e se optam por não se reunir em grupos. Se essas medidas não estiverem sendo seguidas, restrições mais extremas são definidas pelo governo. Exemplo disso ocorreu no dia 20 de março de 2020, quando o governo suíço implementou novas restrições, convidando as pessoas a ficarem em casa e proibindo grupos de mais de cinco pessoas sob a ameaça de uma punição, em princípio, na forma de multas.

Em seguida, anunciou que medidas mais extremas seriam adotadas, em duas etapas. A primeira é impor toque de recolher a partir das 18h diariamente, exigindo que todos fiquem em suas casas, a menos que saiam com uma desculpa válida, como fazer compras ou visitar um centro médico. O governo continuará a monitorar os metadados do telefone celular para determinar se isso está sendo cumprido. Caso contrário, toque de recolher completo, semelhante ao observado na Itália e na França, seria um possível passo adicional.

2.5. Coreia do Sul

O governo sul-coreano está mapeando os movimentos de portadores de coronavírus, por meio de um "registro de viagem do paciente com vírus". Na prática, faz isso utilizando informações dos movimentos das pessoas antes de serem diagnosticadas com o vírus - refazendo suas etapas usando ferramentas como rastreamento por GPS de telefone, registros de cartão de crédito, vídeo de vigilância e entrevistas pessoais com os pacientes. A partir dessas informações, informa ao público, através de um site central e de mensagens de texto regionais, se eles cruzaram com pessoas infectadas, cujos nomes não são divulgados.

Devido a experiência com a crise do MERS no passado, a Coréia do Sul já havia revisado suas leis para conceder maior acesso às informações pessoais de pessoas infectadas. Agora, qualquer pessoa considerada culpada de mentir sobre detalhes considerados necessários para a contenção de infecções pode estar sujeita a um máximo de dois anos de prisão.

A Coréia do Sul conseguiu uma supressão epidêmica sustentada: 76 novos casos, em 24 de março, abaixo do pico de 909, em 29 de fevereiro. Esse resultado, em parte, está relacionado ao uso de um aplicativo de celular para recomendar quarentena. Por esse motivo, outros países da Ásia adotaram rapidamente sua própria versão do mapeamento de infecções da Coréia do Sul.

2.6 Google/Apple (Projeto da "Ferramenta de rastreamento de coronavírus")

As empresas Apple e Google anunciaram a "Plataforma de rastreamento de contatos COVID-19", seu projeto conjunto para ajudar governos e sociedade no combate a pandemia mundial. A plataforma poderá alertar as pessoas se elas forem expostas ao novo coronavírus. Diferentemente de outros métodos – como daqueles que usam dados de GPS – essa ferramenta, baseada em tecnologia Bluetooth, não rastreia a localização física das pessoas. Basicamente, capta os sinais de telefones próximos em intervalos de 5 minutos e armazena as conexões entre eles em um banco de dados. Se uma pessoa apresentar resultado positivo para o novo coronavírus, ele poderá dizer ao aplicativo que foi infectado e notificar outras pessoas cujos telefones passaram a curta distância nos dias anteriores.

Pelo anunciado até o momento nos documentos de especificação disponibilizados pelas empresas, tecnicamente a plataforma funcionaria da seguinte maneira:

- Se você testar positivo para COVID-19 e relatar ao aplicativo, o sistema deve enviar seus últimos 14 dias de "chaves" anônimas para um servidor. Os telefones de outras pessoas baixarão automaticamente as listas de chaves e, se tiverem uma "chave" correspondente no histórico, receberão uma notificação de exposição. O aplicativo precisará garantir que as pessoas estejam realmente infectadas. Atualmente, os testes COVID-19 são administrados por profissionais e registrados nas autoridades de saúde, portanto, talvez a Apple e o Google precisarão trabalhar em estreita cooperação com as autoridades de saúde locais para validar os testes. De qualquer forma, o planejado pelas empresas é que o compartilhamento das chaves deve ser voluntário.
- Se as pessoas compartilharem os dados conforme descrito acima, o telefone verificará a lista uma vez por dia e procurará as principais correspondências e notificará se encontrar alguma. O exemplo de alerta do aplicativo seria bastante simples, por exemplo: "Você foi exposto recentemente a alguém que testou positivo para COVID-19" e oferece um link com mais informações. Essas informações serão fornecidas pela autoridade de saúde que esteja oferecendo o aplicativo a seu critério, provavelmente explicando os sintomas do COVID-19 e as diretrizes da auto-quarentena.

Vale ressaltar que a exposição não é um processo binário simples: quanto mais tempo você passa com uma pessoa infectada, maior o risco. A documentação inclui referências à duração medida em intervalos de 5 minutos. Teoricamente, essas informações poderiam ser enviadas diretamente aos usuários ou oferecer uma avaliação geral dos riscos sem um número exato, o que proporcionaria um maior nível de anonimato.

3 Alternativas técnicas

Com base na experiência internacional e aplicando-a à realidade brasileira, cabe fazer uma análise sobre as possíveis soluções a serem implementadas. Esta análise pode ser dividida em duas grandes linhas: **tipo de solução e serviços oferecidos.** No processo de implementação, será necessária uma análise de custo-benefício que aponte quais serviços e tecnologias serão de fato aplicadas na solução brasileira.

3.1. Solução tecnológica

Antes de mais nada, todas as soluções discutidas no capítulo anterior são baseadas em informações coletadas pelos aparelhos celulares dos próprios cidadãos. Alguns países (notadamente a China) têm também adotado soluções de controle baseadas em dispositivos instalados nas residências ("Internet das Coisas") – por exemplo, sensores que informam se o portão da casa de alguém em quarentena é aberto. No entanto, além das implicações de privacidade, esta solução, em um primeiro momento, teria questões operacionais, tecnológicas e orçamentárias que, no caso brasileiro, a inviabilizam. Assim, voltando para a premissa que o telefone celular do cidadão é a ferramenta principal de rastreamento disponível, há duas possibilidades de coleta de informações:

- por meio dos dados obtidos pelas operadoras de telefonia celular; ou
- por meio de aplicativos instalados nos aparelhos dos cidadãos.

As duas abordagens têm vantagens e desvantagens: a solução via operadoras não demanda esforço por parte dos cidadãos, e pode ser aplicada para qualquer tipo de aparelho. Por outro lado, os dados de localização oferecidos pelas operadoras são obtidos por meio de triangulação de estações rádio-base, e, portanto, são bem imprecisos.

A solução via aplicativos, por sua vez, depende dos cidadãos de fato instalarem o mesmo e darem as devidas permissões para o seu funcionamento. Ela não tem resultado com usuários que ainda usam os chamados feature phones (aparelhos que não permitem a instalação de aplicativos). Haveria a necessidade de um processo muito rápido de desenvolvimento e teste do alicativo, que precisará funcionar em uma variedade imensa de aparelhos com especificações técnicas variadas para ter a efetividade desejada.

Na ausência de um mecanismo de coerção que assegure o uso do aplicativo ou o isolamento de quem estiver infectado, recomenda-se, também, campanhas publicitárias encampadas pelo governo federal em rede nacional, de esclarecimento e de reforço da eficácia do uso do aplicativo, bem como da imperatividade – em prol do coletivo – de se cumprir a quarentena.

3.2 Escopo dos serviços

Com base na experiência internacional e considerando-se as especificidades do Brasil, é possível identificar as seguintes soluções a serem implementadas no contexto de uma *toolbox* para isolamento social por meio de tecnologia celular:

Identificação de multidões: uso dos dados das operadoras para identificar, em tempo real, aglomerações acima do aceitável de acordo com parâmetros dos órgãos de saúde e vigilância sanitária da região. Importante identificar se a aglomeração ocorre em local aberto ou fechado, já que os últimos aumentam significativamente o risco de contaminação.

Estatísticas de isolamento: análise da taxa de isolamento de determinada área geográfica (quanto maior a granularidade possível, melhor) com base nos dados de operadoras ou, se possível, nos dados de aplicativo para *smartphones* desenvolvido para tal tarefa. A priori não precisa ser em tempo real – sugere-se uma análise diária.

Rastreamento de contatos: uso de aplicativos para identificar pessoas que tiveram contato com infectados, de modo a recomendar a quarentena e a atenção aos sintomas.

Preservação de quarentena: uso de aplicativos para verificar se pessoa infectada / suspeita está cumprindo a quarentena. Nesse caso, seria necessária uma solução para verificar periodicamente se o usuário está se mantendo no mesmo lugar – idealmente por meio de biometria.

As soluções com base em dados de operadoras têm a vantagem de ser de implementação mais rápida e, portanto, podem ser adotadas primeiramente. Para a solução de rastreamento de contatos, possivelmente o caminho mais rápido de implementação seria usar a solução já em desenvolvimento pela Google e pela Apple, mas de todo modo é importante a análise dos órgãos competentes quanto às alternativas disponíveis, inclusive com a eventual realização de pilotos.

Por outro lado, é importante também estabelecer os mecanismos de estímulo para que a população mais idosa (60 anos ou mais), de maior risco para a COVID-19, instale os aplicativos, sendo aspecto fundamental implementar sistemas de *zero rating* com as operadoras, de modo que o tráfego de Internet gerado pelos aplicativos não onere os cidadãos . Além disso, outra medida a ser adotada pode ser determinado programa de estímulo à substituição de *feature* phones por *smartphones* – de acordo com a pesquisa CETIC.br[8], o uso de Internet por celulares nessa faixa etária é o mais baixo.

Por último, uma possível solução de preservação de quarentena é potencialmente a mais complexa de ser implementada. O grande desafio é identificar um mecanismo que, sem ser excessivamente intrusivo, evite que o cidadão simplesmente deixe o celular em casa e continue circulando. Idealmente seria necessária uma verificação biométrica a ser realizada de forma periódica, o que esbarra tanto na inconveniência do processo como em limitações tecnológicas, ainda mais considerando-se a grande variedade de aparelhos disponíveis no mercado, com diferentes especificações. Ademais, há uma questão logística/operacional complexa: caso o *ap*licativo detecte que o cidadão "não respeitou" a quarentena, quais são as consequências? Ele seria multado? Procurado pela polícia ou por profissionais de saúde? Em suma, esta solução, embora desejável, necessita de uma avaliação mais acurada sobre sua efetividade.

4 Ética, privacidade e bem comum

Um dos principais marcos do *direito à privacidade* é o trabalho de Warren (ex-juiz da Suprema Corte dos Estados Unidos) e Brandeis[9], no final do século XIX. O contexto da discussão teria sido o suposto vazamento não autorizado de fatos íntimos a respeito do casamento da filha de Warren, ou seja, tratava-se de verdadeira preocupação com a tutela da personalidade humana. Contemporaneamente, o também ex-Juiz da Suprema Corte Thomas Cooley cunhou a expressão *right to be let alone*, em clara preocupação com o fato de que fotografias instantâneas e empresas de comunicação teriam devassado a privacidade do lar. Já àquela época, falava-se na ameaça de numerosos dispositivos tecnológicos: "aquilo que é sussurrado na alcova deve ser berrado no

[8] https://cetic.br/tics/domicilios/2018/individuos/C16/
[9] WARREN, Samuel D.; BRANDEIS, Louis, D. Right to privacy. Harvard Law Review, v. IV, n. 5, December, 1890. Disponível em: <http://faculty.uml.edu/sgallagher/Brandeisprivacy.htm>. Acesso em: 28. jul. 2019.

telhado". A fofoca – anteriormente, mero vício ocioso – teria se tornado um verdadeiro instrumento de barganha, um produto comercializável[10]. Passados quase 150 anos, a preocupação parece não ser muito diferente da externada na presente análise, exceto pela escala dos danos.

A Declaração Universal dos Direitos Humanos (1948) afirma que "ninguém sofrerá intromissões arbitrárias na sua vida privada, na sua família, no seu domicílio ou na sua correspondência, nem ataques à sua honra e reputação. Contra tais intromissões ou ataques toda a pessoa tem direito a proteção da lei".

O desenvolvimento da tecnologia de coleta e sensoriamento implicou exponencial crescimento do recolhimento, processamento, utilização e circulação das informações. O contexto, portanto, é de verdadeira universalização da necessidade de tutela da privacidade[11]. No Brasil, a onda democrática trazida pela CF/88 optou por não utilizar o termo *privacidade*: a opção do legislador constituinte foi pelos termos *vida privada* e *intimidade*. De uma ou outra forma, o cerne ainda é o mesmo: trata-se da tutela de uma liberdade da pessoa, uma verdadeira necessidade do homem. Ou seja, a privacidade é interna ao homem, uma manifestação de sua personalidade em aspecto íntimo, que contribui para sua formação como humano. Não se trata, portanto, de mera segmentação entre público e privado, mas de verdadeira defesa da autodeterminação psicossocial, o núcleo essencial[12] da pessoa. A conduta protegida aqui é o recorte de quais aspectos da vida pessoal – justamente por se referirem apenas ao pessoal – podem ser conhecidos ou acessados por terceiros. A privacidade é a faculdade de fazer concessões no terreno mais reservado de sua existência[13].

De modo geral, contudo, há certo consenso no que se tutela pela vida privada: convívio pessoal e familiar do indivíduo, círculo próximo da pessoa e importante forma de desenvolvimento de relações sociais e valores essenciais. O elemento central da vida privada seria a intimidade. Essa é a proteção da Constituição Federal e da própria legislação infraconstitucional, alçando o direito à privacidade ao patamar de um direito da personalidade e verdadeiro direito fundamental. Aliás, essa vem sendo a regra em outros países:

> "O direito à privacidade começou a ser incluído na legislação civil – enquanto direito da personalidade – sendo, ao final, reconhecido como direito fundamental protegido em sede constitucional. Dentre as constituições atuais, observa-se que algumas Cartas preveem a privacidade apenas de forma genérica; em outras, a privacidade nos meios de comunicação e, por fim, há aquelas que protegem a privacidade sob esses dois aspectos e também a privacidade informacional, como as de Portugal, Hungria, Eslovênia e Rússia. Ainda

[10] CANCELIER, Mikhail Vieira de Lorenzi. *O Direito à Privacidade hoje: perspectiva histórica e o cenário brasileiro*. Sequência (Florianópolis), Florianópolis, n. 76, p. 213-239, 2017.
[11] DONEDA, Danilo. Considerações iniciais sobre os bancos de dados informatizados e o direito à privacidade. 2000. Disponível em: <http://www.egov.ufsc.br/portal/sites/default/files/anexos/8196-8195-1-PB.htm>. Acesso em: 28.jul. 2019.
[12] MACHADO, Joana de Moraes Souza. Caminhos para a tutela da privacidade a sociedade da informação: a proteção da pessoa em face da coleta e tratamento de dados pessoais por agentes privados no Brasil. 2014. 186 p. Tese (Doutorado) - Fundação Edson Queiroz, Universidade de Fortaleza, Centro de Ciências Jurídicas, Programa de Pós-Graduação em Direito Constitucional, 2014. Disponível em: <http://uolp.unifor.br/oul/ObraSiteLivroTrazer.do?method=trazerLivro>. Acesso em: 28.jul. 2019.
[13] ARDENGHI, Régis Schneider. Direito à vida privada e direito à informação: colisão de direitos fundamentais. Revista da ESMESC. [S.l.], v. 19, n. 25, p. 227-251, 2012. Disponível em: <http://revista.esmesc.org.br/re/article/view/57>. Acesso em: 28. jul. 2019.

> mais inovadora se apresenta a Constituição espanhola que além de garantir o direito à intimidade e à vida privada, à privacidade do domicílio, à privacidade das comunicações, ainda limita o uso da informática para garantir a intimidade pessoal e familiar (artigo 18). […]. Hoje, a maior parte dos países democráticos tutela a privacidade na própria Constituição, exceto alguns países da raiz *common law*, como o Reino Unido, que reconhece o direito à privacidade mediante jurisprudência"[14].

Nesse sentido, transplantando essa lógica aos tempos atuais, a relevância de se falar sobre privacidade, bem como sua aderência à realidade são notórias: recentemente acompanhamos na mídia os inúmeros escândalos envolvendo o *Facebook* e a comercialização de dados de usuários para empresas de análise comportamental que, alegadamente, influenciaram o resultado das eleições da maior economia do mundo. Ou seja, para além de mera publicidade comportamental, nossos dados podem estar sendo usados para manipulação de democracias. A discussão parece ganhar ainda mais relevo quando cuidamos de *aplicativos públicos ou de utilidade pública*, onde, ao menos em tese, apenas o interesse público deve prevalecer, alinhado à prestação cômoda do serviço à população.

Aqui, é fundamental ter em mente que o Marco Civil da Internet estabelece, como um direito básico do usuário de internet e como requisito para a guarda de dados, que o consentimento seja ***livre***, ***expresso*** e ***informado***, e que o dado guardado tenha relação direta de pertinência com a finalidade à qual foi dado o consentimento[15]. Também nesse caminho corre a Lei Geral de Proteção de Dados[16], evidenciando que o ordenamento jurídico atual confere posição privilegiada ao consentimento.

Nesse contexto, registra-se que os provedores de aplicações veem no consentimento a materialização da *autodeterminação informativa* dos titulares dos dados. Ou seja, vê-se no consentimento uma forma de transferência integral da responsabilidade sobre com o que se concorda para os titulares das respectivas informações. Trata-se, portanto, de verdadeiro *disclaimer*, pois, partindo dessa premissa, os provedores de aplicações acabam explorando a posição vulnerável em que se encontra o usuário – e consumidor – do aplicativo, sob a ótica **jurídica** (não compreende a relevância do seu consentimento dentro daquele contrato), **técnica** (não compreende o que está sendo feito com seus dados), **econômica** (não tem poder de discutir as cláusulas contratuais, que são

[14] VIEIRA, Tatiana Malta. O direito à privacidade na sociedade da informação: efetividade desse direito fundamental diante dos avanços da tecnologia da informação. 2007. 297 p. Dissertação (Mestrado) - Universidade de Brasília, Faculdade de Direito, Programa de Pós-Graduação em Direito, Estado e Sociedade, 2007. Disponível em: <http://repositorio.unb.br/bitstream/10482/3358/1/2007_TatianaMalta-Vieira.pdf>. Acesso em: 28. jul. 2019.

[15] Art. 7º O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos: (...) VII - não fornecimento a terceiros de seus dados pessoais, inclusive registros de conexão, e de acesso a aplicações de internet, **salvo mediante consentimento livre, expresso e informado ou nas hipóteses previstas em lei**; (...) IX - **consentimento expresso** sobre coleta, uso, armazenamento e tratamento de dados pessoais, que deverá ocorrer de forma destacada das demais cláusulas contratuais. Nesse mesmo sentido, o art. 16, também do MCI, dispõe: "Na provisão de aplicações de internet, onerosa ou gratuita, é vedada a guarda: I - dos registros de acesso a outras aplicações de internet sem que o titular dos dados tenha consentido previamente, respeitado o disposto no art. 7º; ou II - de dados pessoais que sejam excessivos em relação à finalidade para a qual foi dado consentimento pelo seu titular".

[16] Confiram-se os arts. 8º e 9º da LGPD.

nitidamente de adesão) e **informacional** (submete-se unicamente às informações unilateralmente disponibilizadas pelo provedor, sem mecanismos de controle efetivo)[17].

Em alguns países, a discussão da privacidade se torna mais preocupante, porque já existe uma centralização dos mecanismos de identificação do cidadão. A simplificação da prestação de serviços públicos por meio de plataformas com identificação única permite da mesma forma a integração e disponibilização de todos os dados dos cidadãos, além do que pretendiam.

Na União Europeia, a preocupação com o tema parece estar bem acima dos demais países. Houve uma série de regulações sobre direito à privacidade, como a Convenção nº 108 do Conselho da Europa, sobre a proteção de pessoas em relação ao tratamento automatizado de dados de caráter pessoal; o Regulamento (UE) 2016/679, do Parlamento Europeu e do Conselho, relativo à proteção de pessoas físicas em relação ao tratamento de dados de caráter pessoal e a livre circulação destes dados; o Regulamento (UE) 910/2014 do Parlamento Europeu e do Conselho de 23 de julho de 2014 sobre a identificação eletrônica e os serviços de confiança para as transações eletrônicas no âmbito do mercado interior; o Regulamento de Execução (UE) 2015/102 da Comissão, que fixa as especificações técnicas e os procedimentos mínimos relativos aos níveis de garantia de meios de identificação eletrônica, entre outros. Ao mesmo tempo, houve a criação de uma autoridade que fiscaliza a proteção dos dados pessoais.

Em maio de 2019, o Governo francês publicou um decreto criando um novo mecanismo de identificação eletrônica, chamado Aplicativo de Leitura de Identidade do Cidadão em Mobilidade (AliceM), disponível em internet. O usuário do telefone informa seu número de celular, que recebe uma confirmação. Há um cadastro e verificação da biometria do usuário, com reconhecimento fácil estático, ou seja, com uma foto, ou dinâmico, com um vídeo do usuário mexendo o rosto. O usuário também cadastra uma senha pessoal. A proposta é que todas as pessoas com passaporte eletrônico ou cartão de estrangeiro possam baixar o aplicativo, fazer uma autenticação biométrica usando seu telefone e passar a usar serviços públicos.

Note-se que neste caso, além da possibilidade do reconhecimento facial, o cruzamento das informações disponíveis levaria a certeza da sua localização e hábitos, por meio de tecnologia de big data.

A Comissão Nacional de Informática e Liberdades da França foi incumbida de avaliar o projeto AliceM, que prevê o rastreamento de pessoas a partir do reconhecimento facial, usando múltiplas câmeras de segurança e que poderia ser expandida para várias finalidades, inclusive o combate a pandemia.

No tocante ao uso para múltiplos fins, a Comissão considerou que haveria abusos, pois não é possível acessar os serviços públicos sem realizar o reconhecimento facial e esse seria objeto de tratamento de dados do cidadão. A própria negação dos termos de acesso apenas pode ser realizada após o cadastramento. Na opinião da Comissão, se o não consentimento de tratamento de dados impede a pessoa de ter acesso a determinado serviço público, então há violação das normas europeias. Como os cidadãos não

[17] BIONI, Bruno R. Autodeterminação informacional: Paradigmas inconclusos entre os direitos da personalidade, regulação dos bancos de dados eletrônicos e a arquitetura da internet. Dissertação de Mestrado. Faculdade de Direito da Universidade de São Paulo, 2016.

têm outra alternativa para obter a identidade digital, além da leitura fácil e checagem de dados, haveria uma violação de direitos. Seria preciso dar a alternativa ao cidadão de validar sua identidade pessoalmente em algum órgão público, em vez de alimentar o sistema com mais dados e possibilitar à Administração o tratamento destes dados para outras finalidades.[18]

Considerou que a autorização dada pelo cidadão para criar sua identidade digital é muito genérica. O Estado pode usar os dados quando "necessário por motivos de interesse público Importantes". Assim, fez sugestões à minuta de decreto, para a melhoria do serviço antes da sua implementação, de tal forma a garantir que o usuário tenha a real possibilidade de não autorizar o tratamento de dados, sobretudo com o reconhecimento facial, sem que seja privado do acesso aos serviços públicos.

Contudo, no tocante ao COVID-19, discute-se inclusive o aperfeiçoamento do sistema, para a identificação da proximidade com uma pessoa contaminada por meio de bluetooth. Nesse caso, sequer seria necessário o rastreamento. O celular dispararia um alarme quando o seu possuidor se aproximasse de alguém com outro celular identificado como sendo de posse de um contaminado.

Nota-se neste caso específico a importância de órgãos de controle para identificar até que ponto a pessoa que baixa um aplicativo – ou independente disso – pode ser exposta. Em geral, os cidadãos não param para avaliar os termos de consentimento, sendo que este trabalho é necessariamente realizado por ONGs ou por entidades governamentais.[19]

Como evidenciado na seção 2, vários países têm usado dados de telefone celular - de forma consensual ou não - para rastrear a circulação de cidadãos, a fim de verificar se as restrições impostas por conta do surto do coronavírus estão sendo mantidas ou para cumprir outras funções no combate à epidemia. É nesse ambiente que emerge o debate sobre as questões éticas envolvidas nesse tipo de intervenção, especialmente no que se refere à privacidade e à segurança dos cidadãos, usuários desses aparelhos.

No contexto desta proposta, em primeiro lugar, ressaltamos que a privacidade pessoal é importante e deve ser respeitada, mesmo durante uma pandemia. Contudo, não podemos nos alienar de que, durante um período de crise de saúde pública aguda, como a atual, se faz necessária alguma flexibilização a esse respeito - consciente, responsável e provisória. Saúde pública e privacidade individual precisam ser avaliadas de forma articulada, pesadas e ponderadas conjuntamente, sem perder de vista o bem comum.

Como relatamos na seção 1, quando apareceram os primeiros casos da doença no Brasil, uma das melhores ferramentas à disposição dos funcionários da saúde pública foi descobrir dos suspeitos de infecção onde estiveram recentemente e rastrear todos com quem estiveram em contato. Em prol do bem comum, não tiveram como evitar exigir informações privadas dessas pessoas. Mais ainda, possivelmente, precisaram

[18] COMISSION Nationale de l´Informatique et des libertés. Délibération no 2018-342 du 18 octobre 2018 portant avis sur projet de décret autorisant la création d'un traitement automatisé permettant d'authentifier une identité numérique par voie électronique dénommé «Application de lecture de l'identité d'un citoyen en mobilité» (ALICEM) et modifiant le code de l'entrée et du séjour des étrangers et du droit d'asile demande d'avis no 18008244

[19] GONÇALVES, T. C. N. M. e VARELLA, M. D. Os desfaios da administração pública na disponibilização de dados sensíveis *in* Revista DireitoGV, v. 14, n.2, 2018.

compartilhar algumas dessas informações, incluindo informações sobre a saúde de alguém.

Não houve aí nenhuma ilegalidade ou mesmo quebra de conduta ética. O sistema de saúde pública é configurado com permissões, proteções e obrigações legais diferentes das de um consultório médico normal e, por natureza, se relaciona de forma diferente no que diz respeito à privacidade do paciente. Nesse caso, era responsabilidade desses profissionais de saúde pesarem as questões de sigilo de informação dos indivíduos infectados contra os riscos e possíveis danos às pessoas por eles contatadas e ao restante da população. Precisaram coletar a quantidade mínima necessária de informação para atingir uma meta de saúde pública, usando-a apenas para essa atividade.

Os especialistas da área alertam ainda que o equilíbrio entre proteger a privacidade individual e coletar informações críticas para o bem comum muda ao longo da evolução de uma epidemia. Da mesma forma, a quantidade de dados que as autoridades de saúde pública precisam coletar e divulgar também mudam ao longo da trajetória do surto. Além disso, quanto maior a incerteza em relação à doença, maior a necessidade de se obter e distribuir informações dos pacientes. No caso da COVID-19, médicos e cientistas ainda estão no escuro sobre diversas nuances da doença. A coleta de informações detalhadas sobre saúde é, portanto, mais útil e mais importante nesse caso.

As informações de rastreamento digital são hoje onipresentes e podem facilitar a coleta de dados para uso das autoridades de saúde pública. Como vimos na seção 2, em Cingapura, na Suíça, na China, em Israel e na Coreía do Sul há uma extensiva coleta, utilização e disponibilização ao público de informações, por exemplo, de onde estão e onde já foram as pessoas com casos confirmados de COVID-19, por meio de aplicativo e outros dispositivos digitais. Quando se utiliza esses tipos de ferramentas, os mesmos princípios de saúde pública devem ser aplicados.

Assim como era antes, quando um oficial de saúde pública souber, por exemplo, para onde uma pessoa foi e, em nome do bem comum, precisar compartilhar essa informação, isso deve ser feito, nos limites do ordenamento legal e ético. Isso não é diferente do que acontece com as informações de rastreamento digital. O que acontece nesse caso é que se tornou muito mais fácil, rápido e barato coletar, tratar e distribuir essas informações, mas isso não o torna mais ético ou menos ético. Em resumo, rastrear para onde as pessoas vão e com quem interagem é algo que as autoridades de saúde pública fazem normalmente, com parte de seu ofício. É apenas mais fácil, mais rápido e mais efetivo com informações digitais.

Contudo, a privacidade individual e os riscos que podem advir da divulgação de informações pessoais de saúde - como estigma associados a certas enfermidades - ainda são preocupações críticas para as autoridades de saúde pública. Mesmo em casos de crises como a da COVID-19, há limites legais e éticos de privacidade que as autoridades devem respeitar ao obter e disponibilizar informações sobre a saúde das pessoas, principalmente se for sem seu consentimento. Quando se trata de rastreamento digital de contato, da mesma forma, não se pode deixar de respeitar esses limites.

Por último, um aspecto importante, do ponto de vista da privacidade e proteção aos dados pessoais, é garantir que as medidas de vigilância excepcionais não se tornem perenes, ou seja, que elas sejam descontinuadas após o final da pandemia. Dar esta

garantia aos cidadãos desde o início será um fator importante para tranquilizá-los e facilitar a adesão massiva ao programa.

As questões éticas levantadas pela vigilância em saúde só aumentarão. Como alerta Calvo[20], muitas vezes, elas são vistas como uma troca de soma zero entre segurança e privacidade. Mas, como sugere o autor, existe uma alternativa produtiva: quando ambos os lados endossam o bem-estar como objetivo valorizado em conjunto, a vigilância em saúde pode ser um jogo de soma positiva, eficaz e escolhida livremente.

A Lei nº 13.460/2017 introduziu ao ordenamento jurídico a ideia de participação, proteção e defesa dos direitos do usuário dos serviços públicos da Administração Pública. Para além do fato de não afastar a incidência das normas protetivas dispostas no Código de Defesa do Consumidor (CDC), a legislação reforça os princípios já dispostos na Lei nº 8.789/95 e dispõe que "*os serviços públicos e o atendimento do usuário serão realizados de forma adequada, observados os princípios da regularidade, efetividade, segurança, atualidade, generalidade, transparência e cortesia*".

A lei elenca algumas diretrizes que devem ser adotadas pelos prestadores de serviços públicos, tal como a adoção de medidas visando a proteção à saúde e a segurança dos usuários, assim como a aplicação de soluções tecnológicas que visem a simplificar processos e procedimentos de atendimento ao usuário e a propiciar melhores condições para o compartilhamento das informações.

No que se refere aos direitos básicos do usuário, destacam-se: (i) obtenção e utilização dos serviços com liberdade de escolha entre os meios oferecidos e sem discriminação; (ii) acesso e obtenção de informações relativas à sua pessoa constantes de registros ou bancos de dados, observado o disposto no inciso X do caput do art. 5º da Constituição Federal e na Lei nº 12.527/2011; e (iii) proteção de suas informações pessoais, também nos termos da Lei nº 12.527/2011.

Partindo-se da análise dos supracitados direitos, vê-se que, especificamente no que se refere à temática aqui tratada, ao usuário do serviço público deve ser concedida a proteção de suas informações pessoais, o que sugere, portanto, que a prestação dos respectivos serviços por meio de aplicativos móveis também deve contribuir para tal proteção, inegavelmente.

No entanto, há a hipótese de rastreamento digital, automático, sem o consentimento das pessoas. Haveria certas ponderações entre direitos fundamentais a serem realizadas:

a) Seria possível avisar as pessoas que estão aglomeradas e isso as coloca em risco, mesmo sem ter sido solicitado?

b) O contaminado teria direito à privacidade ao ponto de impedir que fosse exposto caso não mantenha o isolamento e exponha a risco outras pessoas?

c) Seria possível realizar rastreamento de toda a população, independente do consentimento?

[20] Calvo, R *et al*. Health surveillance during covid-19 pandemic: How to safeguard autonomy and why it matters. BMJ 2020;369:m1373 doi: 10.1136/bmj.m1373, 2020.

Cabe então considerar se a proposta em discussão estaria no âmbito da Lei Geral de Proteção de Dados – LGPD. Embora atualmente a mesma não esteja em vigência, é bem possível que tenha a validade tenha se iniciado quando eventual solução de rastreamento esteja em fase de implementação. O primeiro aspecto a ser considerado é se o tratamento de dados a ser realizado está de acordo com alguma das hipóteses de tratamento previstas no art. 7º.

> *Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:*
>
> .....
>
> *III - pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei;*
>
> .....
>
> *VIII - para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária;*

Claramente, é possível enquadrar as atividades de rastreamento tanto no inciso III), como também no inciso VIII. Cabe ressaltar que para ambos os incisos não é necessário o consentimento do cidadão. Adicionalmente, redação similar à do inciso VIII pode ser encontrada no art. 11, inciso II, alínea f, que trata dos casos em que, no tratamento de dados sensíveis, não é necessário consentimento. Cabe aqui ressaltar que informações de saúde são consideradas dados sensíveis, de acordo com o art. 5º, inciso II da mesma Lei.

Cabe ressaltar, porém, que o fato da Lei autorizar o tratamento não significa que não há uma série de requisitos a serem cumpridos, exatamente para salvaguardar a privacidade dos usuários, evitando o uso indevido das informações a serem tratadas. Primeiramente, é fundamental atender aos princípios elencados no art. 6º - de particular importância é o da finalidade – ou seja, os dados a serem tratados serão usados apenas para a finalidade específica informada aos cidadãos. No caso concreto, é uma premissa fundamental para conquistar a confiança da população, especialmente porque as informações coletadas (de localização e de contato) poderiam ser potencialmente utilizadas para outros fins – por exemplo, de segurança pública.

A importância da confiança pode ser demonstrada por um caso ocorrido em outra pandemia, a do vírus Ebola, em 2015: um jovem foi assassinado em uma guerra de gangues em Monrovia, capital da Libéria. O cadáver testou positivo para Ebola, o que levou à necessidade de se rastrear todas pessoas que entraram em contato com ele – inclusive os próprios assassinos. Assim, o governo do país, com a ajuda de profissionais do CDC – Center for Disease Control – dos Estados Unidos, que estavam no país monitorando a evolução da doença, tiveram que rastrear os contatos e conquistar a confiança deles para que ficassem em isolamento, garantindo que não seriam perseguidos pela polícia no processo.[21]

[21] https://www.washingtonpost.com/national/health-science/a-corpse-tests-positive-for-ebola-and-an-unusual-murder-investigation-ensues/2016/12/16/8fec6004-c224-11e6-9a51-cd56ea1c2bb7_story.html

Ainda nessa linha, um aspecto fundamental para se conquistar a confiança da população é por meio da transparência. Nesse aspecto, a LGPD estabelece uma série de provisões que devem ser seguidas, tais como a elaboração de relatórios de impacto à proteção de dados pessoais (art. 5º, XVII) e a necessidade de se informar as hipóteses em que o tratamento de dados é realizado pela administração pública (art. 23, I).

Por último, é fundamental garantir que a solução técnica seja robusta e que minimize a possibilidade de ataques de qualquer tipo. É o que preconiza o art. 46 da respectiva lei:

Art. 46. Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.

Ademais, o art. 50, que trata da necessidade do estabelecimento de melhores práticas de governança para o trato com os dados pessoais torna fundamental a adoção dos conceitos de *privacy by design* e *security by design* – ou seja, os temas de privacidade e segurança da informação devem estar imbricados em todo o processo de desenvolvimento da solução, e não apenas uma mera adequação posterior da ferramenta.

Em suma, e à luz do que preconiza a LGPD, considera-se possível adotar uma solução em favor da coletividade, mas limitando o impacto à privacidade do cidadão individual. Uma pessoa contaminada pratica um ilícito penal caso não se mantenha em quarentena.[22] De forma a evitar a prática de crime, não seria um abuso à Lei Geral de Dados Pessoais exigir a informação sobre a contaminação e rastrear o celular das pessoas infectadas. O direito dos demais indivíduos de serem alertados sobre riscos à sua saúde se sobrepõe ao direito de privacidade da pessoa contaminada que não cumpre a quarentena e pratica um ilícito penal.

Por último, cabe uma discussão além da letra fria da Lei sobre a necessidade do consentimento do cidadão envolvido. A eficácia de uma solução de rastreamento de contatos é proporcional à parcela da população participante – o que poderia indicar que a adoção de uma solução sem consentimento dos cidadãos seria justificada pelo privilégio ao coletivo ao invés do individual. Por outro lado, como já mencionado antes, construir confiança é aspecto fundamental para o sucesso de uma iniciativa como estas. A possiblidade do usuário consentir (ou recusar o consentimento) de parte ou de todas as funcionalidades da aplicação pode ser uma forma de deixá-lo mais seguro quanto à utilização da ferramenta. É uma discussão complexa, da qual pode depender o sucesso da iniciativa.

[22] **Infração de medida sanitária preventiva**
Art. 268 - Infringir determinação do poder público, destinada a impedir introdução ou propagação de doença contagiosa:
Pena - detenção, de um mês a um ano, e multa.
Parágrafo único - A pena é aumentada de um terço, se o agente é funcionário da saúde pública ou exerce a profissão de médico, farmacêutico, dentista ou enfermeiro.
Omissão de notificação de doença
Art. 269 - Deixar o médico de denunciar à autoridade pública doença cuja notificação é compulsória:
Pena - detenção, de seis meses a dois anos, e multa.

5 Considerações Finais

Acreditamos que as evidências apresentadas justificam a realizações de estudos, por parte do governo brasileiro, para a eventual utilização das novas tecnologias digitais de combate à COVID-19. Os recursos para isso existem. As tecnologias são viáveis e estão disponíveis, inclusive com código aberto (*open source*). O *know-how*, o como fazer, as experiências supracitadas mostram. E, principalmente, já há indicações preliminares de bons resultados da implementação dessas tecnologias, conforme apresentado.

A utilização dessas soluções tecnológicas, especialmente do rastreamento digital de contato, pode contribuir em todas as fases da curva epidêmica. A solução tecnológica e o escopo dos serviços utilizados variarão em importância de acordo com a fase da curva em que cada localidade se encontre, por isso, é imperativo que o desenvolvimento das soluções contemple uma multiplicidade de serviços, utilizando-se das diversas tecnologias disponíveis.

Na fase em que a maioria das localidades se encontram atualmente, faixa mais à esquerda da curva, de crescimento exponencial ou acelerado da epidemia, as autoridades de saúde – além do esforço hercúleo de fornecer o atendimento médico-hospitalar para os infectados e fortalecer o sistema de saúde - se concentram em reduzir o ritmo de crescimento de novas infecções, para promover o chamado "achatamento da curva", impedindo que o número de casos ultrapasse a capacidade de atendimento do sistema de saúde, evitando seu colapso.

Nessa etapa, o rastreamento deve atuar como mecanismo de apoio às atuais medidas de distanciamento ou isolamento social adotadas em vários estados e município do País. Para tanto, deve estar preparado para oferecer, de imediato, os serviços de "Identificação de multidões" e de "Estatísticas de isolamento", abordados na seção 3. A maneira, menos precisa, mas de mais rápida implementação é o uso de informações das operadoras de celular para identificar e dispersar grandes aglomerações de pessoas. Estes serviços permitirão que as autoridades aperfeiçoem seu planejamento – por meio da análise da taxa de isolamento de determinada área geográfica - e, principalmente, atuem para inibir aglomerações acima do aceitável pelos parâmetros dos órgãos de saúde e vigilância sanitária da região, seja por meio da criação de multas, ação policial ou endurecimento das medidas de isolamento. Cabe ressaltar que já existe uma solução desenvolvida pelas operadoras de telefonia celular, que estão dispostas a cedê-la ao governo federal gratuitamente, como já tem sido feito com alguns estados.

Situação diferente ocorre na parte descendente da curva, impondo a necessidade de implementação de outros serviços. Os especialistas mostram que, assim como a fase de crescimento de uma epidemia é exponencial, a parte final da curva - diminuição da taxa de crescimento dos novos casos - também o será, afinal, quanto menos pessoas se infectam por dia, menor o número de doentes. Segundo os especialistas, o decaimento é também exponencial, iniciando quando o número de curados por dia for maior que o número de novos infectados por dia. Entretanto, mesmo quando isso ocorrer, ainda não será a hora de abandonar as medidas de controle, mas de incrementá-las ou substituí-las por soluções mais adequadas a essa nova realidade.

Se medidas adequadas não forem adotadas também nessa fase, poderão ocorrer subsequentes ondas da epidemia, defendem os especialistas. Estudos mostram que

uma segunda onda de epidemia pode acontecer, por exemplo, quando se alcança o pico da curva não porque saturou o número de infectados e o número de pessoas suscetíveis está baixo, mas porque as medidas de distanciamento ou isolamento social fizeram efeito. Assim, no caso em que o decaimento exponencial é alcançado graças à eficiência do isolamento social, se as pessoas forem colocadas novamente em contato, abre-se a possibilidade de um segundo pico epidêmico.

Para que isso não aconteça, os novos infectados precisam continuar sendo identificados e devidamente isolados do resto da população que ainda está suscetível a ser infectada. Nesse momento, de saída gradual do isolamento, o rastreamento convencional de contatos utilizado no início do surto é claramente ineficiente, devido ao contraste entre escala de pessoas a serem rastreadas e o efetivo de pessoal disponível para realizar a tarefa. Nesse contexto, o rastreamento digital de contato vai se mostrar imprescindível.

Assim, nessa segunda fase da epidemia, além dos serviços mais imediatos de "Identificação de multidões" e de "Estatísticas de isolamento", deve-se ainda contar com os serviços de "Rastreamento digital instantâneo de contatos" - para identificar pessoas que tiveram contato com infectados, de modo a recomendar a atenção aos sintomas, teste e eventual quarentena - e de "Preservação de quarentena" - para verificar se pessoa infectada ou suspeita de infecção está cumprindo a quarentena.

Estes serviços demandam o desenvolvimento (ou adaptação) e disponibilização para a população de aplicativo projetado especificamente para esse fim. Nessa fase, não apenas os aspectos técnicos são mais desafiadores, mas também é de fundamental importância levar em consideração aspectos de respeito à privacidade dos cidadãos. Embora esteja clara a supremacia do interesse público na questão em monta, é fundamental para o sucesso da implementação que os cidadãos confiem no aplicativo, tanto do ponto de vista técnico (ou seja, ele terá mínimo efeito na *performance* do seu celular, e não incorrerá em custos na sua utilização), como também do ponto de vista da privacidade (eventuais dados coletados serão usados apenas para os fins de combate à pandemia). Assim, estabelecer uma relação de confiança com a sociedade e implementar uma solução tecnológica que maximize a confiabilidade, a segurança e o bom desempenho da aplicação são aspectos fundamentais para o sucesso da iniciativa.

Por último, cabe ressaltar que esta foi apenas uma observação preliminar das soluções sendo adotadas em outros países, e suas potenciais implicações. Mais estudos são necessários, não apenas para o desenvolvimento de uma solução técnica adequada às peculiaridades do Brasil, mas também contemplando aspectos como a estratégia de implantação da ferramenta, o uso de elementos de economia comportamental para ampliar a adesão da população, além da própria medição dos potenciais resultados por meio de testes controlados em públicos vulneráveis, como profissionais de saúde.

REFERÊNCIAS BIBLIOGRÁFICAS

Amanat, F., & Krammer, F. (2020). SARS-CoV-2 vaccines: status report. Immunity.

ARDENGHI, Régis Schneider. Direito à vida privada e direito à informação: colisão de direitos fundamentais. Revista da ESMESC. [S.l.], v. 19, n. 25, p. 227-251, 2012. Disponível em: <http://revista.esmesc.org.br/re/article/view/57>. Acesso em: 28. jul. 2019.

BIONI, Bruno R. Autodeterminação informacional: Paradigmas inconclusos entre os direitos da personalidade, regulação dos bancos de dados eletrônicos e a arquitetura da internet. Dissertação de Mestrado. Faculdade de Direito da Universidade de São Paulo, 2016.

Calvo, R et al (2020). Health surveillance during covid-19 pandemic: How to safeguard autonomy and why it matters. BMJ 2020;369:m1373 doi: 10.1136/bmj.m1373 (Published 6 April 2020

CANCELIER, Mikhail Vieira de Lorenzi. O Direito à Privacidade hoje: perspectiva histórica e o cenário brasileiro. Sequência (Florianópolis), Florianópolis, n. 76, p. 213-239, 2017.

COMISSION Nationale de l´Informatique et des libertés. Délibération no 2018-342 du 18 octobre 2018 portant avis sur projet de décret autorisant la création d'un traitement automatisé permettant d'authentifier une identité numérique par voie électronique dénommé «Application de lecture de l'identité d'un citoyen en mobilité» (ALICEM) et modifiant le code de l'entrée et du séjour des étrangers et du droit d'asile demande d'avis no 18008244

DONEDA, Danilo. Considerações iniciais sobre os bancos de dados informatizados e o direito à privacidade. 2000. Disponível em: <http://www.egov.ufsc.br/portal/sites/default/files/anexos/8196-8195-1-PB.htm>. Acesso em: 28.jul. 2019.

Fraser, C. et al (2004). Factors that make an infectious disease outbreak controllable. Proc. Natl. Acad. Sci. U.S.A. 101, 6146– 6151. doi:10.1073/pnas.0307506101 Medline

Ferretti, L. et al (2020). Quantifying SARS-CoV-2 transmission suggests epidemic control with digital contact tracing. Science 10.1126/science.abb6936.

GONÇALVES, T. C. N. M. e VARELLA, M. D. Os desfaios da administração pública na disponibilização de dados sensíveis in Revista DireitoGV, v. 14, n.2, 2018.

Hellewell, J. et al (2020). Feasibility of controlling COVID-19 outbreaks by isolation of cases and contacts. Centre for the Mathematical Modelling of Infectious Diseases COVID-19 Working Group, Lancet Glob. Health 8, e488–e496. doi:10.1016/S2214-109X(20)30074-7 Medline.

MACHADO, Joana de Moraes Souza. Caminhos para a tutela da privacidade a sociedade da informação: a proteção da pessoa em face da coleta e tratamento de dados pessoais por agentes privados no Brasil. 2014. 186 p. Tese (Doutorado) - Fundação Edson Queiroz, Universidade de Fortaleza, Centro de Ciências Jurídicas, Programa de Pós-Graduação em Direito Constitucional, 2014. Disponível em: <http://uolp.unifor.br/oul/ObraSiteLivroTrazer.do?method=trazerLivro>. Acesso em: 28.jul. 2019.

Peak, C. M. et al (2017). Buckee, Comparing nonpharmaceutical interventions for containing emerging epidemics. Proc. Natl. Acad. Sci. U.S.A. 114, 4023–4028. doi:10.1073/pnas.1616438114 Medline.

VIEIRA, Tatiana Malta. O direito à privacidade na sociedade da informação: efetividade desse direito fundamental diante dos avanços da tecnologia da informação. 2007. 297 p. Dissertação (Mestrado) - Universidade de Brasília, Faculdade de Direito, Programa de Pós-Graduação em Direito, Estado e Sociedade, 2007. Disponível em:

<http://repositorio.unb.br/bitstream/10482/3358/1/2007_TatianaMaltaVieira.pdf>. Acesso em: 28. jul. 2019.

WARREN, Samuel D.; BRANDEIS, Louis, D. Right to privacy. Harvard Law Review, v. IV, n. 5, December, 1890. Disponível em: <http://faculty.uml.edu/sgallagher/Brandeisprivacy.htm>. Acesso em: 28. jul. 2019.

FONTES DAS INFORMAÇÕES SOBRE AS EXPERIÊNCIAS INTERNACIONAIS:

Apple/Google:

"Apple and Google partner on COVID-19 contact tracing technology". https://blog.google/inside-google/company-announcements/apple-and-google-partner-covid-19-contact-tracing-technology. Acessado em 14/04/2020.

"Privacy-Preserving Contact Tracing". https://www.apple.com/covid19/contacttracing/. Acessado em 14/04/2020.

"How you'll use Apple and Google's coronavirus tracking tool". https://www.theverge.com/2020/4/10/21216715/apple-google-coronavirus-covid-19-contact-tracing-app-details-use. Acessado em 14/04/2020.

"What is contact tracing? Google and Apple announced today that they'll use Bluetooth to track COVID-19 cases". https://www.theverge.com/2020/4/10/21216550/contact-tracing-coronavirus-what-is-tracking-spread-how-it-works. Acessado em 14/04/2020.

"Apple and Google are building a coronavirus tracking system into iOS and Android: Potentially a huge step forward in the fight against COVID-19". https://www.theverge.com/2020/4/10/21216484/google-apple-coronavirus-contract-tracing-bluetooth-location-tracking-data-app. Acessado em 14/04/2020.

"Answering the 12 biggest questions about apple and google's new coronavirus tracking Project: What the technical documents tell us about the project's privacy and security measures". https://www.theverge.com/2020/4/11/21216803/apple-google-coronavirus-tracking-app-covid-bluetooth-secure. Acessado em 14/04/2020.

Cingapura:

"Singapore says it will make its contact tracing tech freely available to developers". https://www.cnbc.com/2020/03/25/coronavirus-singapore-to-make-contact-tracing-tech-open-source.html. Acessado em 15/04/2020.

China:

Pan, Xiao-Ben (2020). Application of personal-oriented digital technology in preventing transmission of COVID-19, China. Irish Journal of Medical Science (1971 -) https://doi.org/10.1007/s11845-020-02215-5.

"China's coronavirus health code apps raise concerns over privacy". https://www.theguardian.com/world/2020/apr/01/chinas-coronavirus-health-code-apps-raise-concerns-over-privacy. Acessado em 15/04/2020.

Coréia do Sul:

A 'travel log' of the times in South Korea: Mapping the movements of coronavirus carriers". https://www.washingtonpost.com/world/asia_pacific/coronavirus-south-korea-tracking-apps/2020/03/13/2bed568e-5fac-11ea-ac50-18701e14e06d_story.html. Acessado em 15/04/2020.

Israel:

"Israel Unveils Open Source App to Warn Users of Coronavirus Cases". https://www.haaretz.com/israel-news/israel-unveils-app-that-uses-tracking-to-tell-users-if-they-were-near-virus-cases-1.8702055. Acessado em 15/04/2020.

Suíça:

"Switzerland monitoring mobile phone data to determine further lockdowns: Report". https://www.thelocal.ch/20200324/further-lockdowns-in-switzerland-to-be-determined-by-mobile-phone-data. Acessado em 15/04/2020.

"Switzerland bans gatherings of more than five people but curfew avoided". https://www.thelocal.ch/20200320/switzerland-bans-gatherings-of-more-than-five-people-but-curfew-avoided. Acessado em 15/04/2020.

'Help is coming': What you need to know about Switzerland's new emergency coronavirus measures". https://www.thelocal.ch/20200320/help-is-coming-what-you-need-to-know-about-the-swiss-governments-new-emergency-coronavirus-measures. Acessado em 14/04/2020.