O monitoramento digital na pandemia:

como conciliar o direito à privacidade com a proteção da saúde coletiva?

João Pires Mattar

Medidas de restrição de circulação de pessoas e monitoramento da população são as principais ferramentas utilizadas pelas autoridades para controlar a transmissão do novo coronavírus. Já é possível ver o resultado em países que foram os primeiros a serem afetados pela pandemia e, por conseguinte, os primeiros a elaborar mecanismos para retomada gradual da normalidade, sendo incontestável a sua eficácia. Contudo, tais medidas tensionam a relação entre proteção da saúde pública e a garantia dos direitos e liberdades individuais. Até a ampla difusão da vacina contra a COVID-19, este será um debate corrente. Ponto chave desta controvérsia é o receio que mecanismos e leis criadas para o enfrentamento da pandemia perdurem mesmo quando já não houver riscos à saúde pública. Este texto irá abordar, em especial, a complicada harmonização entre a rastreamento digital de contatos e o direito à privacidade..

Entre as recomendações de epidemiologistas e autoridades sanitárias para retomada segura da atividade econômica está o contact tracing (SANCHE et al, 2020), isto é, mapeamento e identificação de pessoas que possam ter sido expostas ao vírus, a fim de isolá-las e impedir uma contaminação em sequência. A Organização Mundial da Saúde (OMS) ressalta que esta foi uma das medidas que tornou possível controlar o surto de ebola na África ocidental, entre 2013 e 2016 (WHO, 2014). Mas no caso do ebola, foi feito manualmente – uma vez diagnosticada, o infectado informa uma lista de pessoas com quem ele teve algum contato, e as autoridades, por sua vez, as contactam, testam e monitoram seus sintomas. Evidentemente, é impossível replicar para o caso do novo coronavírus, e o método está sujeito a falhas: como se reportaria cada pessoa que esteve próximo ao ir a um supermercado?

Logo, para realizar o *contact tracing* na atual conjuntura , os países estão empregando recursos digitais. A China foi o primeiro país a lançar um sistema de monitoramento em massa. O aplicativo "Alipay Health Code" gera um código que indica seu estado de saúde: verde (permite a circulação irrestrita), amarelo (sujeito a isolamento) e vermelho (quarentena obrigatória de 14 dias). Considerado o mais eficiente do ponto de vista sanitário, é também o menos transparente, pois o governo chinês não detalha quais informações e critérios são utilizados para atribuir as cores (GUROVITZ, 2020). O cidadão chinês é obrigado a apresentar o código constantemente, seja para usar o transporte público, seja para entrar em condomínios residenciais. Não surpreende que o aplicativo compartilhe os dados com a polícia (KROLIK; MOZUR; ZHONG, 2020), alimentando o já robusto sistema de vigilância chinês.

Já o modelo de *contact tracing* de Singapura tem se tornado uma referência no mundo – e difere do sistema chinês substancialmente. O governo lançou um site oficial exclusivo para detalhar o funcionamento de seu aplicativo "TraceTogether", apresentando uma série de garantias à privacidade. Primeiro, a instalação do aplicativo é voluntária e o consentimento pode ser revogado a qualquer momento. O software tampouco utiliza dados de localização, usando apenas o Bluetooth para detectar que um dispositivo com o app instalado se aproximou de outro (logo, não registra onde foi o encontro). Os dados são armazenados somente no aparelho, em outras palavras, não são compartilhados com o governo. Somente quando o usuário for diagnosticado com COVID-19 que lhe é solicitado a exportação desses dados para identificar outros usuários do TraceTogether que estiveram próximo a ele nos últimos dias (Government Technology Agency of Singapora, 2020a). A Austrália também lançou, no dia 26 de abril, seu próprio aplicativo – o "COVIDSafe" – com um sistema muito semelhante ao de Singapura. (Department of Health of the Australian Government, 2020).

O historiador israelense Yuval Harari, em artigo publicado na Financial Times, apresenta a questão entre saúde pública e privacidade pessoal em duas "escolhas" opostas: vigilância totalitária ou empoderamento do cidadão. Enquanto a primeira se sustenta em medidas coercitivas e vigilância centralizada, a segunda baseia-se em confiança das pessoas nas autoridades públicas, para criar uma população "auto-motivada e bem informada", disposta a monitorar a si mesma e contribuir voluntariamente com as autoridades.

As colocações do autor contribuem para o debate, mas são reducionistas. De fato, o modelo de Singapura trilha o caminho cujo Harari chama de "empoderamento do cidadão". O nome do aplicativo ("rastrear juntos") e o seu funcionamento estão fundamentados na colaboração voluntária, e o site, bem informativo e de fácil compreensão, busca convencer a população a baixar o aplicativo ("Proteja você mesmo, Proteja nossos entes queridos, Proteja nossa comunidade"). Mas nem tudo são flores: o aplicativo identifica seu usuário pelo número de telefone, e o governo poderia rastrear a movimentação de cada usuário do Trace Together simplesmente colocando receptores de Bluetooth espalhados pela cidade (CHO; IPPOLITO; YU, 2020).

Ademais, o modelo tem uma séria limitação. Não é capaz, por exemplo, de garantir que quem tenha sido diagnosticado cumpra o isolamento. Um interessante episódio na Coréia do Sul ilustra o problema. Ainda no início do contágio no país, uma mulher — conhecida como a paciente 31, por ser a 31º caso confirmado — se tornou uma superpropagadora do vírus ao ignorar as recomendações médicas para se testar e isolar. Do dia 20 de janeiro até meados de fevereiro, a Coreia do Sul havia rastreado e monitorado cada contato que os 30 primeiros diagnosticados haviam tido. Porém a situação saiu de controle quando a paciente 31, mesmo apresentando sintomas e sendo recomendada a se testar (e se isolar), prosseguiu com suas atividades, indo a duas missas na igreja local. Até o dia 18 de março, o grupo de infectados ligado a igreja — cerca de 5 mil — respondia por 60% de todos os casos do país, e a cidade de Daegu se tornou o epicentro da doença no país (HERNANDEZ; SCARR; SHARMA, 2020).

O caso impulsionou o desenvolvimento de um sistema de vigilância digital capaz de assegurar que os pacientes diagnosticados cumpram o isolamento. Para isso, utiliza, dentre outros, dados de cartão de crédito, localização por GPS e até mesmo reconhecimento facial das câmeras de segurança, sendo tão efetivo quanto invasivo (SANTIRSO, 2020). Yuval Harari, que cita a própria Coréia do Sul como país que deve sucesso a cooperação da população, se esquece de mencionar o sistema de vigilância draconiano e a quarentena compulsória. Para além disso, o caso da paciente 31 alerta para o dano que uma única pessoa é capaz de fazer ao não cooperar, mesmo em uma sociedade bem disciplinada e disposta a seguir as orientações.

Países ocidentais buscam lançar seus próprios aplicativos, e a tendência é que utilizem algo semelhante ao modelo de Singapura, que utiliza o Bluetooth ao invés de localização por GPS (THOMPSON, 2020). No momento de escrita desta análise, França, Alemanha e Grã-Bretanha se encontram em um impasse com Google e Apple: enquanto os países pressionam por uma flexibilização das políticas de privacidade, as empresas resistem. Diferente de Singapura, a intenção é que os dados pessoais sejam armazenados em um servidor central. Dessa forma, quando for feito o diagnóstico de alguém, o governo não dependerá, necessariamente, da permissão do usuário para notificar outras pessoas, pois estes dados já estariam com o Estado. Outro ponto é sobre o funcionamento do aplicativo em *background* (funcionamento "invisível"), não permitido pela Apple (REUTERS, 2020). Ambos foram apontados por Singapura como limitações do seu aplicativo TraceTogether (Government Technology Agency of Singapore, 2020b), o que expõe, novamente, dilema entre saúde coletiva e direito à privacidade.

Diante do bloqueio econômico e as mortes causadas pelo vírus, muitos afirmam que a privacidade é um preço pequeno a se pagar. Programas de vigilância ganham maior aceitabilidade na opinião pública, e debates que em circunstâncias normais se estenderiam por meses, são precipitados em face do estado de emergência. Deve-se considerar que, uma vez que o Estado adquira esse poder, dificilmente irá abdicar dele. Incorremos no risco de normalizar um estado de vigilância abusivo e torná-lo permanente

O filósofo italiano Giorgio Agamben, no livro "Estado de Exceção" publicado há quase vinte anos, chamava atenção para a transformação de medidas provisórias e excepcionais em técnicas de governo, em outras palavras, a exceção tornando-se regra. A crise do coronavírus indiscutivelmente coloca a sociedade diante da necessidade de monitorar infectados. O que Agamben alerta, é que "a necessidade, longe de apresentar-se como um dado objetivo, implica claramente um juízo subjetivo e que necessárias e excepcionais são [...] apenas aquelas circunstâncias que são declaradas como tais" (AGAMBEN, 2004, p. 46). Para fazer o *contact tracing* digital, por exemplo, há uma variedade de modelos, que possuem graus de violabilidade de nossa privacidade maiores e menores, assim como identificam riscos de contaminação de forma mais ou menos efetiva. Os epidemiologistas nos apresentam uma informação concreta: do ponto de vista sanitário, quanto mais monitoramento, melhor. Como conciliar isto com a proteção a nossa privacidade, isto está a cargo da sociedade avaliar e debater.

O Brasil se encontra em uma situação delicada em virtude do adiamento da Lei Geral de Proteção dos Dados (LGDP), que deveria entrar em vigor em agosto próximo. A Agência Nacional de Proteção de Dados, órgão previsto para regulamentação e fiscalização da lei, tampouco foi implementada, sendo essa uma das justificativas para ampliação do prazo da LGPD. Se houver um mínimo de comprometimento do governo federal em conter a pandemia, medidas de contact tracing serão elaboradas. Contudo, o tratamento de dados sem uma legislação própria que o regula coloca os cidadãos em posição muito vulnerável, o que torna ainda mais indispensável o debate sobre o tema no Brasil.

A questão entre direitos individuais e proteção da saúde pública não se trata de uma dicotomia, em que se escolhe um ou outro, mas tampouco significa que harmonizá-los é uma tarefa simples, como busquei expor neste texto. Nesse sentido, gostaria de concluir apresentando algumas orientações, ponderações e princípios que devem ser considerados ao elaborar políticas públicas de monitoramento digital. Os pontos a seguir foram sintetizados a partir de textos e documentos escritos por jornalistas (BIDDLE, 2020. GUROVITZ, 2020), *think tanks* (Laboratório de Políticas Públicas e Internet, 2020), acadêmicos (CHO; IPPOLITO; YU, 2020. ABELER, BÄCKER; BUERMEYER, 2020), instituições (Banco Interamericano de Desarollo, 2020) e, por fim, pela declaração conjunta assinada por uma centena de organizações da sociedade civil (Rede Intervozes, *Civil Liberties Union for Europe, Human Rights Watch*, Access Now, dentre outras). Entre eles há o consenso de que é possível proteger a saúde coletiva enquanto são respeitados os direitos individuais, desde que se atente-se aos pontos abaixo:

1. Qualquer programa deve ter um objetivo claro e bem delimitado, para que a coleta de dados seja proporcional e a mínima possível para atingir esta meta;

2. As autoridades de saúde devem ser aquelas responsável pela definição e condução da coleta de dados;

3. Os dados devem ser usados com fim exclusivamente sanitário, ou seja, não podem ser utilizados por outras agências do governo mesmo que apresentem utilidade, seja para prender um criminoso, deportar um imigrante irregular ou cobrar sonegadores de impostos;

4. Os códigos do software devem ser públicos e auditáveis por técnicos e membros da sociedade civil;

5. Qualquer programa/ferramenta deve estar limitado a uma data de validade rigorosa;

6. A anonimização deve ser a maior possível e recursos computacionais e protocolos de criptografia devem ser empregados;

7. Por fim, deve-se considerar que programas de monitoramento digital excluem populações sem acesso a tecnologia, e a saúde de grupos marginalizados deve ser contemplada por outras políticas.

Referências

ABELER, Johannes; BÄCKER, Matthias; BUERMEYER, Ulf. Corona-Tracking & Datenschutz: kein notwendiger Widerspruch. **NETZPOLITIK.ORG.** Disponível em: https://netzpolitik.org/2020/corona-tracking-datenschutz-kein-notwendiger-widerspruch. Acesso em: 01 de mai. de 2020.

AGAMBEN, Giorgio. **Estado de Exceção.** 2ª Edição. São Paulo: Boitempo, 2004.

Banco Interamericano de Desarrollo. **¿Es la privacidad de los datos el precio que debemos pagar para sobrevivir a una pandemia?** Documento para discussión n. IDB-DP-00764, abr. de 2020. Disponível em: https://publications.iadb.org/publications/spanish/document/Es_la_privacidad_de_los_datos_el_precio_que_debemos_pagar_para_sobrevivir_a_una_pandemia.pdf. Acesso em: 01 de mai. de 2020.

BIDDLE, Sam. Privacy experts say responsible coronavirus surveillance is possible. **The Intercept,** 2 de abr. de 2020. Disponível em: https://theintercept.com/2020/04/02/coronavirus-COVID-19-surveillance-privacy/. Acesso em: 01 de maio de 2020.

CHO, Hyunghoon; IPPOLITO, Daphne; YU, Yu William. **Contact Tracing Mobile Apps for COVID-19: Privacy Considerations and Related Trade-offs.** 30 de mar. de 2020. Disponível em: https://arxiv.org/pdf/2003.11511.pdf**.** Acesso em: 01 de mai. de 2020.

Department of Health of the Australian Government. **COVIDSafe app**, Camberra, 29 de abr. de 2020. Disponível em: https://www.health.gov.au/resources/apps-and-tools/COVIDsafe-app#resources-COVIDsafe-app. Acesso em: 29 de abr. de 2020.

Government Technology Agency of Singapora. **TraceTogether Privacy Safeguards**, 2020a. Disponível em: https://www.tracetogether.gov.sg/. Acesso em: 28 de abr. de 2020.

Government Technology Agency of Singapore. **BlueTrace: A privacy-preserving protocol for community-driven contact tracing across borders,** 2020b. Disponível em: https://bluetrace.io/static/bluetrace_whitepaper-938063656596c104632def383eb33b3c.pdf. Acesso em: 29 de mar. de 2020.

GUROVITZ, Helio. É possível rastrear sem invadir. **G1,** 13 de abr.. de 2020. Disponível em: https://g1.globo.com/mundo/blog/helio-gurovitz/post/2020/04/13/e-possivel-rastrear-sem-invadir.ghtml. Acesso em: 29 de abr. de 2020.

HARARI, Yuval Noah. Yuval Noah Harari: the world after coronavirus. **Financial Times,** Londres, 20 de mar. de 2020. Disponível em: https://www.ft.com/content/19d90308-6858-11ea-a3c9-1fe6fedcca75. Acesso em: 28 de abr. de 2020.

HERNANDEZ M.; SCARR S.; SHARMA M. The Korean clusters: How coronavirus cases exploded in South Korean churches and hospitals. **Reuters,** Londres, 20 de mar. de 2020. Disponível em: https://graphics.reuters.com/CHINA-HEALTH-SOUTHKOREA-CLUSTERS/0100B5G33SB/index.html. Acesso em: 29 de abr. de 2020.

Joint civil society statement: States use of digital surveillance technologies to fight pandemic must respect human rights. 02 de abr. de 2020. Disponível em: https://intervozes.org.br/wp-content/uploads/2020/04/Documento_vigil%C3%A2ncia.pdf. Acesso em: 01 de maio de 2020.

KROLIK, Aaron; MOZUR, Paul; ZHONG, Raymond. In Coronavirus Fight, China Gives Citizens a Color Code, With Red Flags. New York Times, Hangzhou, 1 de mar. de 2020. Disponível em: https://www.nytimes.com/2020/03/01/business/china-coronavirus-surveillance.html. Acesso em: 28 de abr. de 2020.

Laboratório de Políticas Públicas e Internet. Relatório LGPD em tempos de COVID-19: balanço do webinário realizado com especialistas em proteção de dados pessoais. Abr. de 2020. Disponível em: https://9977a902-e455-46d9-8a7b-0ac71f155f93.filesusr.com/ugd/77388c_920893a510034484bab422ee3c889384.pdf. Acesso em: 01 de maio de 2020.

Laboratório de Políticas Públicas e Internet. Relatório Vigilância Digital contra COVID-19: um mal necessário? Abr. de 2020. Disponível em: https://9977a902-e455-46d9-8a7b-0ac71f155f93.filesusr.com/ugd/77388c_f164b66b78d94c769b8d749547c7d00e.pdf. Acesso em: 01 de maio de 2020.

REUTERS. France, Germany in standoff with Silicon Valley on contact tracing, Londres, 24 de abr. de 2020. Disponível em: https://www.reuters.com/article/us-health-coronavirus-europe-tech/france-germany-in-standoff-with-silicon-valley-on-contact-tracing-idUSKCN2262LM. Acesso em: 29 de abr. de 2020.

SANCHE S, et. al.. High contagiousness and rapid spread of severe acute respiratory syndrome coronavirus 2. Journal of the Centers for Disease Control and Prevention, V. 26, No. 7, Jul. 2020.

SANTIRSO, Jaime. Coreia do Sul: contra o coronavírus, tecnologia. El País, Pequim, 15 de mar. de 2020. Disponível em: <https://brasil.elpais.com/internacional/2020-03-15/coreia-do-sul-contra-o-coronavirus-tecnologia.html>. Acesso em: 28 de abr. de 2020.

THOMPSON, Derek. The Technology That Could Free America From Quarantine. The Atlantic, 07 de abr. de 2020. Disponível em: https://www.theatlantic.com/ideas/archive/2020/04/contact-tracing-could-free-america-from-its-quarantine-nightmare/609577/. Acesso em: 29 de abr. de 2020.

World Health Organization. Contact Tracing During an Outbreak of Ebola Virus Disease. Brazzaville, WHO Regional Office for Africa, set. 2014. Disponível em: https://www.who.int/csr/resources/publications/ebola/contact-tracing-during-outbreak-of-ebola.pdf. Acesso em: 29 de abr. de 2020.