



Cadernos

nº 87

Sumário Executivo

Políticas públicas e regulatórias para rastreamento de dados pessoais no Brasil para combate à Covid-19

Letícia Lobato Anicet Lisboa

Coleção: Covid-19 Fast Track



Sumário Executivo

O objetivo geral da pesquisa é a análise das políticas públicas e regulatórias para rastreamento de dados pessoais e *contact tracing* no Brasil mediante o uso de aplicativos, com foco na mitigação de contágio de Covid-19. Trata-se de tema relevante, pois há necessidade de compatibilização entre a nova regulamentação sobre proteção de dados e as medidas implementadas pela administração pública para monitoramento das pessoas, considerando o interesse público e a garantia de segurança jurídica. O método utilizado para o trabalho foi o dedutivo e a pesquisa foi elaborada em três capítulos. Inicialmente, foi apresentado o cenário de singularidade em decorrência na pandemia de Covid-19, bem como foram examinadas as políticas de rastreamento de dados dos EUA, da União Europeia, onde, por amostragem, foi estudado o caso da Alemanha, Reino Unido e de Singapura. Seguidamente, investigou-se o direito à proteção de dados e o arcabouço jurídico constitucional que deve ser observado pela administração pública. Por fim, foram desenvolvidas proposições, sendo possível concluir que a proteção de dados pode ser adequada aos processos de rastreamento; no entanto, há necessidade de maior incentivo e adesão da população às políticas públicas.

O estudo da regulação das políticas públicas de rastreamento e proteção de dados, no intuito de avaliar a necessidade de sinergia

entre o interesse público e os direitos fundamentais, é um tema atual e relevante para a Escola Nacional de Administração Pública, pois é inovador e fundamental para a governança pública e boas práticas regulatórias baseadas em dados científicos.

Desse modo, a pesquisa realizada é relevante, uma vez que as novas operações tecnológicas e de tratamento de dados pela administração pública, notadamente em um cenário de crise, é essencial para a compreensão fática da realidade, com intuito de tornar as políticas públicas mais eficazes.

A pandemia de Covid-19 impactou severamente a sociedade moderna global, seja em relação à crise nas áreas de saúde e sanitária, bem como econômico-socialmente e nas estruturas da administração pública. A pesquisa demonstrou a fragilidade da adesão popular às medidas governamentais para enfrentamento das crises em diversas economias, bem como a necessidade de governança pública e, sobretudo, estudos técnico-científicos para formulação de políticas públicas eficazes.

Nessa ótica, constatou-se que diversos países adotaram a estratégia de *contact tracing*, ou, em livre tradução, rastreamento de contatos, como uma estratégia governamental para contenção do contágio. O método de *contact tracing* consiste no monitoramento das pessoas que tiveram resultados positivos de testes para Covid-19, bem como das pessoas que tiveram contato próximo com elas nos últimos 14 dias. Essa estratégia é reconhecida pela OMS, porém, não é necessariamente realizada pelo meio digital.

A operação *contact tracing* já era realizada muitas vezes por meio de tratamento de dados pessoais, mas de forma orgânica e/ou manual. Contudo, com a propagação da digitalização na sociedade pós-industrial e das análises de *big data*, a operação de *contact tracing* passou a ser realizada digitalmente, inclusive com o uso de aplicativos em dispositivos móveis, os quais permitem o rastreamento dos usuários e seus contatos próximos.

Foram investigadas as políticas públicas adotadas pela Alemanha, Reino Unido, EUA e Singapura, para realização de *contact tracing* com uso de aplicativos em celulares móveis, para fins comparativos com as políticas do Brasil. Foi possível depreender que a Alemanha, Reino Unido e Singapura possuíam leis específicas para a proteção de dados (GDPR, Data Protection Act do Reino Unido e Personal Data Protection Act de Singapura) e que elas não representavam um empecilho para as políticas de rastreamento de dados. No caso dos EUA, apesar de não existir uma lei federal específica sobre proteção de dados, nem uma política

federal de *contact tracing*, a estratégia adotada por Nova Iorque com o aplicativo “Covid Alert NY” também foi compatível com a lei estadual “Personal Privacy Protection Law”.

O caso mais relevante de *contact tracing* digital investigado no presente trabalho foi adotado por Singapura. Isso porque a maioria absoluta da população adquiriu o aplicativo TraceTogether lançado pelo Ministério da Saúde (2,5 milhões de *downloads*). Ressalte-se que a eficácia do *contact tracing* digital depende, sobretudo, da adesão da população à política pública, pois o aplicativo é voluntário, assim como a divulgação dos testes, em conformidade com a tutela da proteção de dados. Todavia, verificou-se que esse país adotou um segundo aplicativo destinado apenas aos empresários, visando a realização de *check-in* pelos consumidores em seus estabelecimentos, sendo possível assim monitorar os contatos nessas localizações. Esse aplicativo é denominado Safe Entry e é obrigatório para os empresários; portanto, tal medida garante o *enforcement* da política pública de rastreamento.

Há que se falar que Singapura detém um quadro normativo-regulatório (*Data Protection Act* de 2012 e *Infectious Disease Act* de 1976) que permite a utilização de *contact tracing* e o tratamento de dados pessoais para a finalidade de atenção à saúde, interesse coletivo e mitigação da propagação de doenças infectocontagiosas e, portanto, não ocorreu uma edição de nova lei ou desconfiância por parte da população em relação a tais políticas.

Em relação ao ordenamento jurídico pátrio, constatou-se que a Lei nº 13.709, de 14 de agosto de 2018, denominada Lei Geral de Proteção de Dados (LGPD), representa um marco legal sobre o tratamento de dados pessoais no Brasil. O tratamento de dados pessoais é considerado toda operação realizada pelas pessoas naturais ou jurídicas de direito público ou privado, inclusive a coleta, armazenamento, uso e exclusão de dados de pessoas naturais. Dessa forma, o rastreamento de dados e o *contact tracing* utilizam dados das pessoas naturais para monitoramento de contatos e tomada de decisões pelos órgãos e entidades da Administração Pública, sendo, portanto, formas de tratamento. Por outro lado, se os dados forem anonimizados, inclusive por meio de criptografia, e não puderem identificar as pessoas naturais, a LGPD não será aplicável (art. 12 da LGPD).

Foi possível concluir que a LGPD permite o tratamento de dados pela administração pública quando houver necessidade de proteção da vida ou da incolumidade física, inclusive sem a necessidade de consentimento prévio, na forma do art. 7º, VII. Consequentemente, entende-se que a pandemia de Covid-19 é uma ameaça

à vida e à incolumidade física dos cidadãos, além de gerar impactos à economia e saúde financeira dos países e seus povos. Portanto, o tratamento de dados pessoais, inclusive *contact tracing*, é uma medida de suma importância para a implementação de políticas públicas e regulatórias de enfrentamento à crise com base em dados científicos.

Todavia, ainda que o tratamento de dados possa ser realizado pela administração pública, existem contrapesos e limites expressos na Constituição Federal e na própria LGPD, com objetivo de tutelar a privacidade das pessoas (art. 5º, X da Constituição Federal) e o direito à proteção de dados pessoais. Desse modo, as políticas públicas de tratamento de dados pessoais, como o *contact tracing*, devem respeitar os princípios gerais de proteção de dados, como a finalidade específica, adequação e proporcionalidade. Outrossim, a administração pública deve criar medidas de segurança informática, sempre que possível adotar a anonimização e, todas as operações devem ser realizadas com responsabilidade e transparência.

Nessa perspectiva, a Medida Provisória nº 954, de 2020, que tornava mandatório o repasse de dados pessoais detidos por empresas de telefonia para o IBGE, não estava em conformidade com LGPD e seus princípios, bem como não apresentava qualquer caráter de finalidade específica, transparência e proporcionalidade. Por este motivo, foi considerada inconstitucional pelo Supremo Tribunal Federal na Ação Direta de Inconstitucionalidade nº 6387, de 2020¹.

Sob outra ótica, o Ministério da Saúde desenvolveu, entre março e julho de 2020, o aplicativo Coronavírus-Sus, cuja aquisição e compartilhamento de informações são voluntários pelo titular, atendendo à hipótese de tratamento de dados por meio do consentimento (art. 7º, I da LGPD). Nesse dispositivo, os dados pessoais são criptografados, não há uso de geolocalização, mas de dispositivos de notificação por proximidade. O aplicativo, apesar de cumprir, em certa medida, regras gerais da LGPD como a finalidade, o consentimento, a anonimização, não se mostrou eficaz como uma política pública de combate à Covid-19 porque há baixa adesão da população e há burocracia no compartilhamento dos testes pelos usuários.

Diante do desenvolvimento pelo Ministério da Saúde do aplicativo Coronavírus-Sus, existe uma ferramenta de rastreamento de dados no Brasil baseada em consentimento e aquisição voluntária pelos titulares. Desse modo, a primeira

.....
¹ STF- Supremo Tribunal Federal. *Ação Direta de Inconstitucionalidade nº 6387*. Ministra Relatora Rosa Maria Pires Weber. Disponível em: <http://portal.stf.jus.br/processos/detalhe.asp?incidente=5895165>. Acesso em: 10 de junho de 2020.

proposição a ser realizada em relação aos aplicativos ou ferramentas de *contact tracing* é que esses devem respeitar o princípio constitucional de privacidade e o direito à proteção de dados, na forma da LGPD.

A LGPD não deve significar um empecilho ao tratamento de dados pessoais pela administração pública, mas uma norma de incentivo, balizadora das ações governamentais, para que não ocorram violações aos direitos individuais dos cidadãos. Destarte, a segunda proposição seria relativa à implementação de ferramentas para tratamento de dados pessoais de forma geral, como o rastreamento, operação e o uso, seja para mitigação de Covid-19 ou de outras crises para a coletividade, que sejam compatíveis com a LGPD e principalmente com a Constituição Federal. Desde a sua concepção (*privacy by design*), as ferramentas devem cumprir os princípios do tratamento de dados como a finalidade específica, a adequação, a necessidade e a segurança.

A Autoridade Nacional de Proteção de Dados (ANPD), nesse cenário, tem papel regulatório fundamental para o *enforcement* da LGPD, inclusive com atribuições de fiscalização e aplicação de sanções às organizações privadas e públicas no tocante ao tratamento de dados, inclusive relativas ao *contact tracing* (Art. 55-J da LGPD). Nessa senda, a terceira proposição é a efetiva operacionalização da ANPD pelo poder público. Ela é essencial, pois também poderia fazer um papel de incentivo a tais políticas, colaborando com órgãos e entes, bem como promovendo estudos e relatórios de impacto à proteção de dados (art.55-J, XIII da LGPD).

Ultrapassada a análise da legislação sobre a proteção de dados, em relação às políticas públicas praticadas pelo Poder Executivo para o rastreamento de dados, verificou-se que há baixa adesão da população. Dessa maneira, são necessárias medidas de governança pública que coadunem os interesses da população aos do gestor público. A governança também implica a assimilação de todas as tecnologias de informação e comunicação às políticas públicas, no intuito de introduzir agilidade e eficiência à interação entre o Estado e a sociedade. Como estimuladora da cooperação entre o setor privado e o público, a governança visa a estabelecer novos acessos das pessoas (reguladas) à decisão, implementação e fiscalização públicas, logo, resultando em transparência e participação. Portanto, a quarta proposição é a necessidade de criação de ações governamentais para aderência da população e redução de assimetrias, como comunicação transparente aos cidadãos e *marketing* no setor público.

Finalmente, última proposição é relativa à criação ou a atualização de uma agenda executiva que priorize a introdução de novas tecnologias e digitalização² para os órgãos e entidades da Administração Pública. Essa proposta é fundamental para a realidade da sociedade brasileira pós-industrial. Ao investigar-se as demais economias que utilizaram dispositivos digitais de *contact tracing*, entre elas Singapura, foi possível identificar que os órgãos e entidades desses países dispõem de informações pessoais, empresariais, identificadoras e governamentais centralizadas em bancos digitais. Tal situação torna o processo de obtenção de informações de saúde, por exemplo, ou de *check-in* em estabelecimentos comerciais, mais eficaz e célere.

Conclui-se que há muitas falhas nas políticas públicas e regulatórias de rastreamento de dados no Brasil. Há a necessidade de processos mais acurados de governança pública no tocante à sua edição, ou seja, avaliação do contexto atual e estimativas sobre providências cabíveis a serem adotadas com base na realidade coletiva dos indivíduos e empresas, adequação às tecnologias disponíveis e redução de assimetrias informacionais. No caso dos aplicativos de rastreamento de dados e *contact tracing*, a observância do quadro normativo-regulatório na concepção dos projetos é essencial. Além disso, os dispositivos móveis são meras ferramentas tecnológicas; portanto, cabe à administração pública a criação de mecanismos de adesão da população às políticas, com maior transparência e respeito aos direitos fundamentais.

.....
² Cf. A Estratégia de Governo Digital para o período de 2020 a 2022 foi estabelecida no Decreto nº 10.332, de 29 de abril de 2020. O objetivo é realizar políticas públicas e serviços de melhor qualidade, mais simples, acessíveis a qualquer hora e lugar e a um custo menor para o cidadão, mediante transformação digital de serviços, unificação de canais digitais e interoperabilidade de sistemas. In: BRASIL. Decreto nº 10.332, de 28 de abril de 2020. Disponível em: <https://www.in.gov.br/web/dou/-/decreto-n-10.332-de-28-de-abril-de-2020-254430358>. Acesso em: 04 de novembro de 2020.