Enap

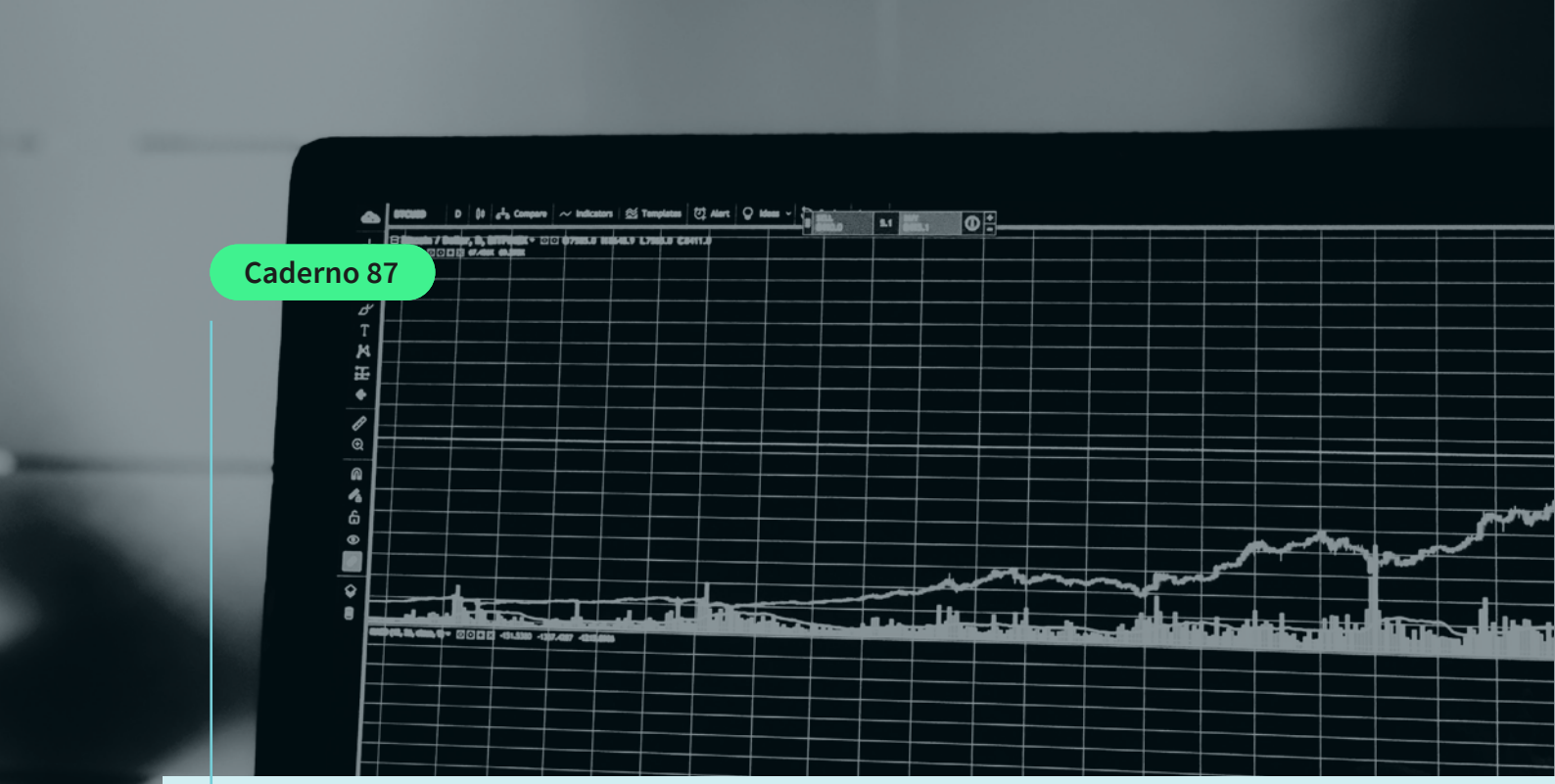
Cadernos

nº 87

# 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*



Caderno 87

**Coleção:**
*Covid -19 Fast Track*

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


**Autora**
Letícia Lobato Anicet Lisboa

**Parecerista convidada**
Karolyne Utomi


Este caderno é resultado dos conhecimentos gerados pelas pesquisas realizadas no âmbito do **Programa Cátedras Brasil**, desenvolvido com o objetivo de selecionar projetos de pesquisa que gerem subsídios para o entendimento ou enfrentamento à pandemia de Covid-19 pela Administração Pública. A presente publicação é uma das entregas previstas no Edital nº 69 de 2020.

## Conheça a autora

**Letícia Lobato Anicet Lisboa**
Autora

Doutora e mestre em direito empresarial pela Universidade do Estado do Rio de Janeiro (UERJ). Pós-doutoranda em direito e novas tecnologias pelo Mediterranea International Centre for Human Rights Research (MICHR). Professora Adjunta do curso de direito da Universidade Federal Rural do Rio de Janeiro. Advogada.

## Expediente

**Escola Nacional de Administração Pública – Enap**

**Presidente**
Diogo Costa

**Diretora-Executiva**
Rebeca Loureiro de Brito

**Diretora de Altos Estudos**
Diana Coutinho

**Diretor de Educação Executiva**
Rodrigo Torres

**Diretor de Desenvolvimento Profissional**
Paulo Marques

**Diretora de Inovação**
Bruna Santos

**Diretora de Gestão Interna**
Alana Regina Biagi Lisboa

**Revisão**
Roberto Araújo

**Projeto gráfico**
Amanda Soares
Letícia Lopes

**Edição eletrônica**
Amanda Soares

A Escola Nacional de Administração Pública (Enap) é uma escola de governo vinculada ao Ministério da Economia (ME).

Tem como principal atribuição a formação e o desenvolvimento permanente dos servidores públicos. Atua na oferta de cursos de mestrados profissionais, especialização lato sensu, cursos de aperfeiçoamento para carreiras do setor público, educação executiva e educação continuada.

A instituição também estimula a produção e disseminação de conhecimentos sobre administração pública, gestão governamental e políticas públicas, além de promover o desenvolvimento e a aplicação de tecnologias de gestão que aumentem a eficácia e a qualidade permanente dos serviços prestados pelo Estado aos cidadãos. Para tanto, desenvolve pesquisa aplicada e ações de inovação voltadas à melhoria do serviço público.

O público preferencial da Escola são servidores públicos federais, estaduais e municipais. Sediada em Brasília, a Enap é uma escola de governo de abrangência nacional e suas ações incidem sobre o conjunto de todos os servidores públicos, em cada uma das esferas de governo.

Ficha catalográfica elaborada pela equipe da Biblioteca Graciliano Ramos da Enap

L7692p Lisboa, Letícia Lobato Anicet

Políticas públicas e regulatórias para rastreamento de dados pessoais no Brasil para combate à Covid-19 / Letícia Lobato Anicet Lisboa. -- Brasília: Enap, 2021.

79 p. : il. -- (Cadernos Enap, 87; Coleção: Covid-19 Fast Track)

Inclui bibliografia

ISSN: 0104-7078

1. Políticas Públicas. 2. Saúde Pública. 3. Administração Pública. 4. Dados Abertos. 5. Primeiro Setor. 6. Ciência e Tecnologia. 7. Pandemia – Brasil. I. Título.

CDU 364:616-036.21(81)

Bibliotecária: Tatiane de Oliveira Dias – CRB1/2230



**Escola Nacional de Administração Pública (Enap)**
Diretoria de Altos Estudos
Coordenação-Geral de Pesquisa
SAIS – Área 2-A – 70610-900 — Brasília-DF, Brasil

# CÁTEDRAS FAST-TRACK

## Editorial

O ano de 2021 começou com a boa novidade das vacinas, permitindo às pessoas a revisão de suas expectativas quanto ao futuro. Expectativas são baseadas em informações e, para tomar boas decisões, é preciso que os indivíduos estejam bem informados.

A pesquisa científica, por exemplo, é um insumo informacional útil para gestores públicos e privados. Contudo, como ficou evidente neste último ano, a pesquisa leva tempo: seus resultados nem sempre são imediatos. Trata-se de um empreendimento árduo, mas necessário, principalmente quando a pesquisa tem por objetivo auxiliar na formulação de políticas públicas em um período tão atípico como o da pandemia de Covid-19.

É neste contexto que, em 2020, de forma inédita em sua história pela agilidade com a qual foi implementado, a Enap lançou uma chamada pública para seleção de projetos de pesquisas que gerem subsídios para o entendimento ou enfrentamento à pandemia de Covid-19 pela Administração Pública. Ficou conhecido como o edital Cátedras Covid-19 e os dez projetos de pesquisa selecionados foram concluídos até o final do ano de 2020.

O trabalho de Monique Menezes e coautores, sob a ótica das chamadas capacidades estatais, encontra uma heterogeneidade nas políticas públicas adotadas nas capitais brasileiras. A análise de documentos (conteúdo e discurso) mostrou uma articulação entre governos municipais e

estaduais. Além disso, um apanhado de “boas” e “más” práticas no combate à pandemia, por capitais brasileiras, é um interessante subproduto deste trabalho.

O modelo epidemiológico Suscetíveis-Infectados-Recuperados (SIR) microfundamentado foi usado por Geraldo Sandoval Goés e Luan Borelli para verificar o impacto da pandemia em cinco estados brasileiros: São Paulo, Amazonas, Ceará, Rio de Janeiro e Pernambuco. O objetivo foi comparar dois cenários: um no qual todos os estados seguem uma mesma política de contenção do vírus e outro no qual cada um adota uma política própria, conforme suas particularidades. As evidências das simulações favorecem a adoção de políticas públicas que respeitem as peculiaridades de cada estado.

Por meio de uma extensa base de dados municipais, Janaina Lopes Pereira Peres e coautoras encontram seis clusters de municípios espalhados de forma nada trivial pelo território brasileiro. As autoras criaram o termo comorbidade social para designar o “acúmulo de patologias sociais em um determinado território”, o que serviu de base teórica para seu trabalho. A pesquisa mostra evidências de que vários municípios das regiões Norte e Nordeste apresentavam grande quantidade de comorbidades sociais e também um desempenho ruim na pandemia (em termos de casos e óbitos por Covid-19).

Durante os primeiros meses da pandemia, vários governos estaduais buscaram um papel ativo na busca por soluções científicas. Este protagonismo foi detalhadamente estudado pela bolsista Silmary de Jesus Gonçalves Alvim, com um exaustivo e inédito levantamento de legislações com foco em políticas públicas estaduais de Ciência, Tecnologia e de Inovação (CT&I), no qual foram identificadas 118 políticas estaduais voltadas ao combate à Covid-19, sendo 19% delas caracterizadas pela parceria com o governo federal. Estimou-se que estes projetos movimentaram cerca de R$ 231 milhões em 2020.

O bolsista Anderson Castro Soares de Oliveira e coautora Lia Hanna Morita utilizaram dados diários do Ministério da Saúde (27 de março a 3 de outubro de 2020) e trabalharam com aproximadamente 1,5 milhão de observações utilizadas em vários modelos espaço-temporais (Poisson, Poisson Hurdle, Poisson Inflado de Zero, Binomial Negativa, Binomial Negativa Hurdle e Binomial Negativa Inflada de Zeros). O painel para a visualização dos resultados é outro subproduto desta pesquisa (https://lecdufmt.shinyapps.io/COVID/) e, já na 40ª semana epidemiológica, apontava para uma preocupante situação no estado do Amazonas.

Rafael Mesquita Pereira e seus coautores estudaram o impacto da pandemia no grupo de trabalhadores com mais de 60 anos de idade no período compreendido entre fevereiro e agosto de 2020. Em 18 de junho de 2020, a portaria conjunta do Ministério da Economia, da Saúde e da Agricultura, Pecuária e Abastecimento reconheceu a necessidade de se atribuir tratamento diferenciado geral aos trabalhadores do grupo de risco. O resultado foi uma diminuição nas horas trabalhadas por parte dos funcionários públicos nesta faixa etária, fato não observado no caso dos trabalhadores na mesma faixa etária no setor. Os autores ressaltaram os efeitos diferenciados da legislação que permitiu a funcionários públicos reduzirem suas jornadas de trabalho sem redução de rendimentos, ao passo que os trabalhadores do setor privado, em sua maioria, não puderam evitar o trabalho presencial visando minimizar as perdas em seus rendimentos.

O setor de transporte público municipal é alvo do trabalho de Gabriel Pabst. Segundo o autor, o setor já apresentava um déficit financeiro (projetado pelo autor em R$ 8 bilhões no final de 2020) e a pandemia gerou um conjunto de medidas restritivas de circulação diminuindo a quantidade de passageiros em circulação. Este é um setor cuja regulação carece de aperfeiçoamentos, como bem discute o pesquisador.

O trabalho infantil é objeto da pesquisa de Thauan Patrello e Ruth Knaak. Por meio de entrevistas envolvendo autoridades do setor no estado do Espírito Santo, os autores especulam que mudanças na política educacional seriam importantes para combater o trabalho infantil, indicando o ensino integral como exemplo de política pública interessante. Outra proposta apresentada pelos autores envolve a

garantia de algum tipo de auxílio emergencial às famílias das crianças e o reforço às medidas tradicionais de combate ao trabalho infantil.

Nos primeiros meses da pandemia, ainda em 2020, houve um debate importante acerca dos métodos de rastreamento de pessoas contaminadas - o chamado contact tracing - a partir de políticas adotadas em alguns países. Ferramentas criadas para o rastreamento levantam questões importantes sobre a privacidade dos dados dos cidadãos. No caso brasileiro, esta discussão encontra eco na nova Lei Geral de Proteção de Dados Pessoais (LGPD). A bolsista Letícia Lobato Anicet Lisboa fez um levantamento das políticas de rastreamento dos Estados Unidos, da União Europeia, da Alemanha, do Reino Unido e de Cingapura. As lições extraídas das políticas públicas destes países podem promover melhorias no arcabouço das políticas de saúde com base em evidências.

O pesquisador Júlio César Andrade de Abreu e coautores estudaram o uso de business intelligence (BI) pelos poderes públicos municipais no estado do Rio de Janeiro. Foi apontado que 21 municípios cariocas (aproximadamente 22.8% do total) fizeram uso de alguma ferramenta de BI no acompanhamento da evolução da Covid-19. Este baixo uso é preocupante, não apenas pelo cenário da pandemia no país. Trata-se, afinal, de uma ferramenta de gestão estratégica que pode - e deve - ter seu uso difundido na administração pública, visando informar o cidadão com o máximo de transparência possível dentro do marco da nova LGPD.

A pesquisa é um empreendimento fascinante. Cada projeto de pesquisa aqui resumido abordou o problema da pandemia no território brasileiro sob diferentes óticas teóricas, por meio do uso de abordagens empíricas distintas. A leitura mais atenta do conjunto destes trabalhos mostrará a emergência de alguns consensos e também novas hipóteses a serem pesquisadas.

**Diana Coutinho**
Diretora de Altos Estudos da Enap

# 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 datificação 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 de lei ou desconfiança 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 anominização 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 LPGD 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 2020[1] .

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 digitalização[2] 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.

**Clique aqui** para baixar
o **Sumário Executivo** separado.
Compartilhe!

[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.

## Resumo

O objetivo geral da pesquisa é analisar as 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 busca-se a compatibilização entre a nova regulamentação sobre proteção de dados pessoais 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 pessoais pode ser adequada aos processos de rastreamento; no entanto, há necessidade de maior incentivo e adesão da população às políticas públicas.

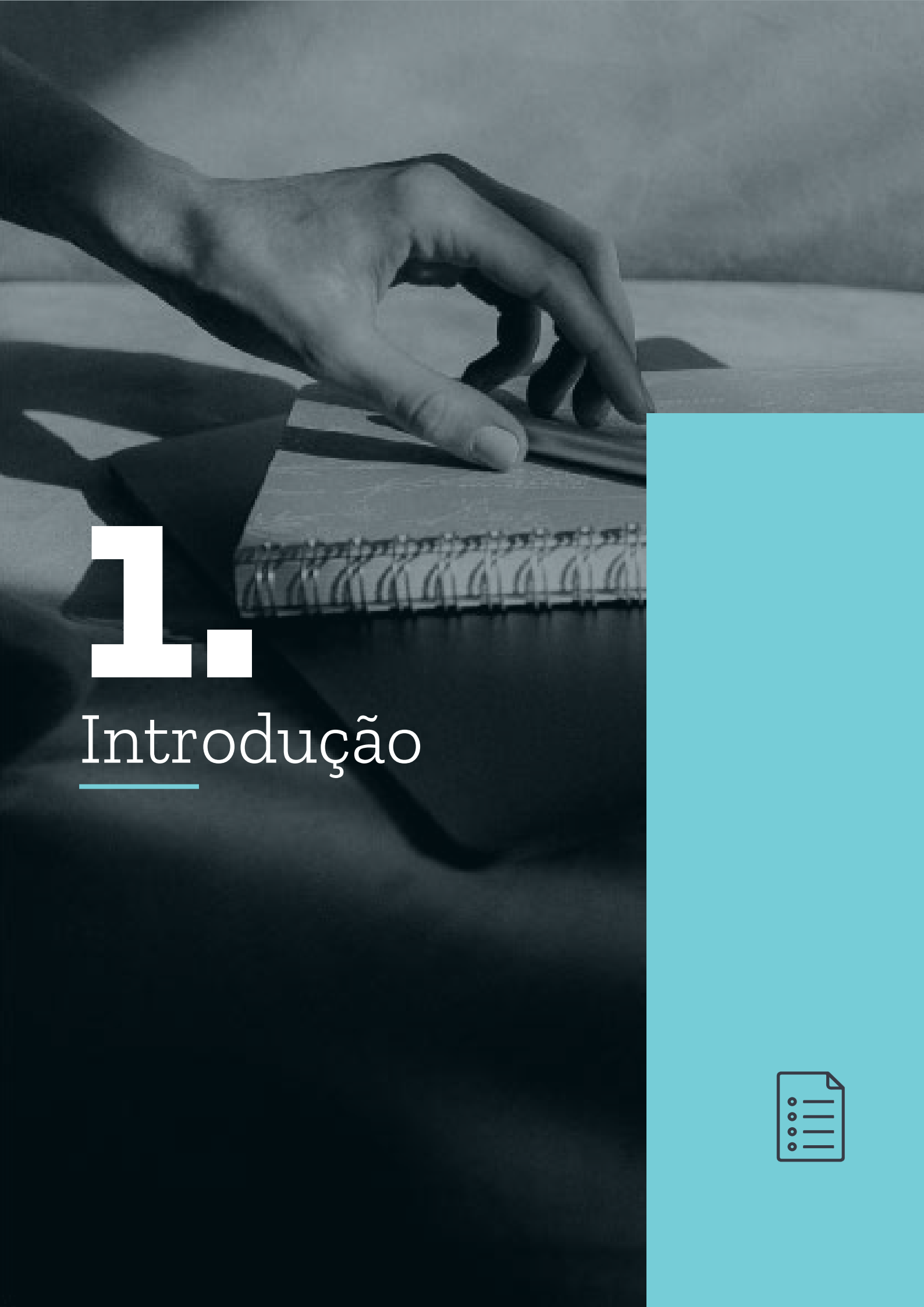

**Palavras-chave:** Rastreamento de dados, Covid-19, regulação, proteção de dados

## Abstract

The general objective of the research is to analyze public and regulatory policies for data tracking and contact tracing in Brazil with the mobile app´s use, with a focus on mitigating the Covid-19 contagion. This is a relevant issue because it seeks to make compatibility between the new regulations on data protection and the measures implemented by the public administration to monitor people, aiming at the harmonization of interests and the guarantee of legal security. The method used for the work was deductive and the research was developed in three chapters. Initially, the scenario resulting from the Covid-19 pandemic was presented, as well as the United States, European Union with study of Germany case, United Kingdom and Singapore. Then, data protection and the constitutional legal framework that must be observed by the public administration were investigated. Finally, possible compatibilities were developed, and it was possible to conclude that data protection may be adequate to the tracking processes, however there is a need for greater encouragement and adherence by the population to the public policies.


**Keywords:** Contact tracing, Covid-19, regulation, data protection

## Sumário



# 1. Introdução

# 1. Introdução

Desde o reconhecimento da pandemia de Covid-19 pela Organização Mundial da Saúde (OMS) em março de 2020, a dinâmica social foi substancialmente alterada diante das novas necessidades que o momento exigia. O cotidiano das pessoas foi afetado por medidas governamentais de isolamento e recomendações da OMS, contemplando a quarentena e suspensão de algumas atividades comerciais. No Brasil ocorreu a edição da Lei nº 13.979, de 06 de fevereiro de 2020, que trouxe as medidas de enfrentamento da emergência em saúde pública de importância internacional, decorrente da crise ocasionada pelo novo coronavírus.

Diante da crise sanitária, as ações governamentais (os atos normativos, de fiscalização, incentivo e planejamento) devem ser adotadas com base nos aspectos científicos e sociais, objetivando regulações eficientes. Nesse sentido, as ferramentas de "*data tracking*" ou rastreamento de dados, assim como o "*contact tracing*", foram utilizadas de forma estratégica por diversos governos para contenção do vírus e tomada de decisões administrativas.

O rastreamento de dados através de aplicativos em telefones móveis foi realizado em diversos países como Singapura e Alemanha, para controle do movimento de pessoas e notificações de exposição, indicando os resultados do isolamento social. Não obstante o tratamento dos dados para essa finalidade seja uma realidade, no Brasil, existem dúvidas sobre o conflito entre a Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais), o direito fundamental à privacidade (art. 5º, X da Constituição Federal) e o próprio interesse público.

A questão central a ser enfrentada nesse artigo é a análise das políticas públicas e regulatórias de rastreamento de dados no Brasil por intermédio de ferramentas digitais, com foco no ordenamento jurídico pátrio, para controle da emergência em saúde pública causada pela pandemia de Covid-19. A hipótese a ser respondida é se o rastreamento de dados ou *contact tracing* por aplicativos digitais é efetivo para a redução do contágio, assim como quais seriam as possibilidades para controle desses dados pela administração pública, de forma a não violar diretamente os direitos fundamentais das pessoas.

O método utilizado para o trabalho foi o dedutivo e a pesquisa realizada foi de caráter documental, além de envolver a análise de legislação, estudos doutrinários, jurisprudenciais e exame de artigos em periódicos. Esse método foi escolhido tendo em vista que a dedução se efetiva pelo desenvolvimento de um raciocínio lógico, que tem por ponto de partida uma ideia geral, uma verdade preestabelecida, da qual decorrerão preposições particulares. O raciocínio, neste caso, parte de uma ideia geral para conclusões particulares.

A ideia geral a partir da qual a pesquisa foi realizada baseou-se na eficácia ou não das políticas públicas de tratamento de dados pessoais com objetivo de contenção do contágio de Covid-19. Desenvolveu-se o objetivo em três capítulos, de maneira que a análise da legislação e políticas públicas de outros países foi fundamental. Para tanto, foram escolhidos os Estados Unidos da América, a União Europeia, Reino Unido e Singapura, como parâmetros para avaliação das políticas.

O primeiro capítulo tem como objetivo específico a investigação das políticas de rastreamento de dados para mitigação do coronavírus. Inicialmente o cenário da pandemia será apresentado, bem como a necessidade de utilização de dados pessoais pela administração pública na sociedade hodierna. Serão analisadas as experiências regulatórias dos EUA, União Europeia, Reino Unido e Singapura durante a pandemia em 2020.

O segundo capítulo versará sobre o conceito de proteção de dados pessoais, com foco nas relações sociais modernas, baseadas em novas tecnologias e utilização de dados. Assim, será investigado o arcabouço jurídico do Brasil acerca do direito à proteção de dados pessoais.

Consequentemente, o terceiro capítulo tratará sobre as políticas públicas e regulatórias no Brasil para o rastreamento de dados, o que poderia ser adequado das experiências estrangeiras e realidade dos dispositivos adotados. Também será analisada a jurisprudência do Supremo Tribunal Federal no tocante à ação direta de inconstitucionalidade nº 6.387 do Distrito Federal e possíveis soluções para a compatibilidade do interesse público de mitigação do contágio e a tutela da proteção de dados. Ao final, será apresentado um quadro comparativo sobre as políticas de rastreamento de dados desenvolvidas nos países estudados e recomendações para a Administração Pública brasileira.

# 2.

# Rastreamento de dados e enfrentamento à pandemia de Covid-19

## 2. Rastreamento de dados e enfrentamento à pandemia de Covid-19

A humanidade passa por uma revolução permanente em razão do constante desenvolvimento das tecnologias para melhoria de seu bem-estar. Após a segunda guerra mundial, vivenciou-se uma mudança no cenário político-social em razão das práticas capitalistas que desencadearam o consumo, as mudanças estatais e a ordem social. No entanto, as últimas décadas são reconhecidas como períodos com maiores características de variações sociais e tecnológicas, como infere Yuval Harari[1]:

> Nos últimos dois séculos, o ritmo das mudanças se tornou tão rápido que a ordem social adquiriu um caráter dinâmico e maleável. Agora existe em um estado de fluxo permanente.
> [...] Daí que qualquer tentativa de definir as características da sociedade atual é como tentar definir a cor de um camaleão. A única característica que podemos ter certeza é a mudança incessante. As pessoas se acostumaram a isso, e a maioria de nós pensa a ordem social como algo flexível, que podemos projetar e melhorar à vontade. (Harari, 2019)

[1] Harari, Yuval N. Sapiens. *Uma breve história da humanidade*. 48 ed., Porto Alegre: L&PM, 2019, p. 375-376.

Hodiernamente, vivencia-se uma era pós-industrial marcada por dinamismos sociais, econômicos e tecnológicos que impactam a realidade humana, suas relações intersubjetivas e a própria natureza. Acima de tudo, a sociedade pós-industrial também é conhecida pelo conhecimento e datificação[2], pois com o avanço das tecnologias para consumo, expansão dos métodos de comunicação e do uso da internet, os dados pessoais se tornaram ativos importantes para controladores sejam pessoas naturais ou jurídicas (empresários privados ou o poder público).

Diversos métodos de monitoramento de dados são realizados pelos controladores, como *big data analytics*[3] (análise de grandes dados), *data profiling*[4] e *data tracking* ou rastreamento de dados. A análise de grandes dados pode ser compreendida de forma ampla como toda operação com grandes dados para otimizá-los em informações úteis que serão utilizadas na tomada de decisões, sejam de pessoas naturais ou jurídicas[5]. Vários processos são compreendidos nessa lógica, como *data profiling* (perfilamento de dados, em português) ou o *data tracking* (rastreamento de dados).

A prática de *data profiling* foi descrita tecnicamente por Felix Naumann[6], em tradução livre, como "uma ampla variedade de métodos que analisam eficientemente um determinado conjunto de dados". Para Guilherme Martins, João Longhi e Faleiros Junior[7], quando tal técnica é utilizada para a concepção do indivíduo, pode gerar uma preconcepção comportamental da pessoa, com sua objetificação, inclusive para controle sanitário em políticas públicas:

[2] Cf. Nesse sentido, Bruno Bioni conceitua datificação como um fenômeno, "o ato de datificar – pôr em dados- praticamente toda a vida de uma pessoa". In: Bioni, Bruno R. *Proteção de dados pessoais*: a função e os limites do consentimento. Rio de Janeiro: Forense, 2019, p. 90.

[3] *Analytics* ou análise de dados significa o uso aplicado de dados, "permitindo que analistas, pesquisadores e usuários de negócios tomem decisões melhores e mais rápidas usando dados anteriormente inacessíveis ou inutilizáveis." IBM – Estados Unidos. *Big data analytics*. Disponível em: https://www.ibm.com/analytics/hadoop/big-data-analytics. Acesso em: 10 de junho de 2020.

[4] Cf. Ainda, de acordo com Bruno Bioni, a prática de *data profiling* é um risco para a sociedade, pois poderia gerar uma estigmação das pessoas, inclusive com práticas discriminatórias, "exemplos não faltam, valendo-se mais uma vez, do raciocínio dedutivo. Processos seletivos na área de recursos humanos, para a concessão de crédito, para a estipulação de prêmios securitários e até mesmo o risco de não embarcar em um avião, porque seus hábitos alimentares podem ser coincidentes com o perfil de um terrorista. In: Bioni, Bruno R. *Proteção de dados pessoais*: a função e os limites do consentimento. Rio de Janeiro: Forense, 2019.

[5] Kalyvas, James R.; Albertson, David R. A big data primer for executives. In: Kalyvas, James R; Overly, Michael R. (Coord). *Big data*: business and legal guide (e-book). Boca Raton. CRC Press. 2015, p. 3.

[6] Naumann, Felix. Data profiling revisited. *Acm SIGMOD Record*, Quatar Computing Research Institute, Doha, 2014, p 40-44.

[7] Martins, Guilherme Magalhães; Longhi, João Victor Rozatti; Faleiros Junior, José Luiza de Moura. A pandemia da covid-19 , o profiling e a Lei Geral de Proteção de Dados. In*: Portal Migalhas*, abril de 2020. Disponível em: https://www.migalhas.com.br/depeso/325618/a-pandemia-da-covid-19-o-profiling-e-a-lei-geral-de-protecao-de-dados. Acesso em: 21 de setembro de 2020.

> [...] reflete uma faceta inexorável da utilização dos algoritmos que, empregados nos processos de tratamento de grandes acervos de dados (Big Data), propiciam o delineamento do "perfil comportamental" do indivíduo, que passa a ser analisado e objetificado a partir dessas projeções.
> Essa situação é amplificada em tempos de pandemia, pois se almeja amplo controle populacional a partir da vigilância de dados (dataveillance). Com isso, iniciativas de monitoramento passam a ser festejadas e não mais repudiadas e exemplo disso já se notou anos atrás, em 2009, por ocasião da pandemia da Influenza H1N1, no Reino Unido, onde operadoras de telefonia móvel foram instadas a fornecer dados de geolocalização de seus usuários ao governo britânico. (Martins, Longhi e Faleiros Junior, 2020)

Outra proposta de utilização de dados, ocorre por meio de ações de rastreamento de dados, *data tracking* e *dataveillance* (vigilância)[8], em que os dados das pessoas naturais são monitorados por meio de sistemas de geolocalização, ou rastreamento, para diversas finalidades dos controladores. O objetivo do rastreamento pode ser para uso de um aplicativo móvel de locomoção, acompanhamento de trânsito de veículos, ou ainda pode ser utilizado para fins de consumo, análise de mercado ou para monitoramento da população em determinada área geográfica. O método de *data tracking* permite que o tratamento de dados pessoais seja realizado para algum tipo de política pública ou análise de comportamento, podendo ou não representar uma violação aos direitos fundamentais constitucionalmente garantidos.

O rastreamento pode também ser utilizado para monitoramento de contato, denominado *contact tracing*. De acordo com a Organização Mundial da Saúde, *"contact tracing* é o processo de identificar, avaliar e gerenciar pessoas que foram expostas a uma doença para prevenir a transmissão progressiva. Essas pessoas são chamadas de contatos[9]". Assim, os agentes públicos podem monitorar a locomoção das pessoas naturais, podendo verificar o contato com outras pessoas, a região em que o monitorado vive e trabalha, entre outras informações. A partir dessa investigação, esses cidadãos seriam aconselhados a isolarem-se, com intuito de limitar o número de possíveis contaminados, como demonstraram os estudos do centro europeu de prevenção e controle de doenças:

[8] *Dataveillance* não se trata necessariamente de um rastreamento de dados, está ligado à vigilância das pessoas naturais. Cf. Menezes Neto, Elias Jacob de; Morais, Jose Luis Bolzan de; Bezerra, Tiago José de Souza Lima. O Projeto de Lei de proteção de dados pessoais (PL5276/2016) no mundo do big data: o fenômeno da *dataveillance* em relação à utilização de metadados e seu impacto nos direitos humanos. In: *Revista Brasileira de Políticas Públicas*, v. 7, n. 3, Uniceub, Dez, 2017, p.185-199.

[9] OMS – Organização Mundial da Saúde. *Q&A*: Contact tracing for Covid-19**.** Disponível em: https://www.who.int/emergencies/diseases/novel-coronavirus-2019/question-and-answers-hub/q-a-detail/q-a-contact-tracing-for-covid-19. Acesso em: 22 de setembro de 2020.

> O rastreamento de contatos (*contact tracing*) é uma medida eficaz de saúde pública para o controle da Covid-19. A pronta identificação e o gerenciamento dos contatos dos casos Covid-19 permitem identificar rapidamente casos secundários que podem surgir após a transmissão dos casos primários. Isso permitirá a interrupção subsequente da transmissão. O processo de *contact tracing*, em conjunto com sistemas robustos de teste e vigilância, é central para controlar estratégias durante a descalcificação. O *contact tracing* tem sido uma parte essencial da resposta em vários países asiáticos que reduziram com sucesso o número de casos[10]. [Tradução livre]

Desse modo, as políticas públicas na sociedade digital podem utilizar hodiernamente a análise e o processamento de dados pessoais como fontes científicas para mitigação de contágio de Covid-19. Essa técnica foi utilizada mundialmente pelos governos, conforme será demonstrado no próximo item.

## 2.1. Impactos da pandemia de Covid-19

Em março de 2020, a Organização Mundial de Saúde anunciou o surto de Covid-19 como uma pandemia, em razão da escalada rápida da doença na Ásia e Europa, pois naquele momento havia um total de 114 mil casos confirmados em 114 países[11]. Nesse sentido, a pandemia é descrita pela própria organização como "a propagação mundial de uma nova doença[12]". Desse modo, identificou-se que Covid-19 havia se transfigurado em pandemia pela rápida expansão global, havendo a necessidade daquele anúncio para o desenvolvimento mundial de estratégias de contenção da doença e aceleração de esforços para seu controle.

A partir da predição, os Estados passaram a realizar, dentro de suas características e cenários próprios, medidas públicas para retardar ou prevenir a transmissão viral, como ações de distanciamento social, quarentena, fechamento de escolas,

[10] Cf. A redação original consiste em "Contact tracing is an effective public health measure for the control of Covid-19. The prompt identification and management of the contacts of Covid-19 cases makes it possible to rapidly identify secondary cases that may arise after transmission from the primary cases. This will enable the interruption of further onward transmission. Contact tracing, in conjunction with robust testing and surveillance systems, is central to control strategies during de-escalation. Contact tracing has been a key part of the response in several Asian countries that have successfully reduced case numbers". BAKA, Agoritsa; ANGELIS, Stefania De; DUFELL, Erika, *et. al. Contact tracing for Covid-19*: current evidence, options for scale-up and an assessment of resources needed. In: União Europeia. Centro Europeu de Prevenção e Controle de Doenças, 2020, p. 1. Disponível em: https://www.ecdc.europa.eu/sites/default/files/documents/COVID-19-Contract-tracing-scale-up.pdf. Acesso em: 14 de julho de 2020.

[11] Cf. OMS – Organização Mundial da Saúde. WHO announces Covid-19 outbreak a pandemic. In: *Coronavirus disease outbreak*, 12 de março de 2020. Recurso eletrônico. Disponível em: http://www.euro.who.int/en/health-topics/health-emergencies/coronavirus-covid-19/news/news/2020/3/who-announces-covid-19-outbreak-a-pandemic. Acesso em: 17 de março de 2020.

[12] Cf. OMS – Organização Mundial da Saúde. *Emergencies preparedness response*, 24 de fevereiro de 2010. Recurso eletrônico. Disponível em: https://www.who.int/csr/disease/swineflu/frequently_asked_questions/pandemic/en/. Acesso em: 17 de março de 2020

minimização do transporte público em horários de pico e controle fronteiriços. Considerando cada particularidade, houve a necessidade de criação de ações governamentais, por cada país, para o enfrentamento à Covid-19, de forma a equilibrá-las com possíveis impactos econômicos e sociais.

A pandemia de Covid-19 trouxe diversas mudanças mundiais no tocante à necessidade de criação de políticas públicas para mitigação e enfrentamento à doença, como regras de isolamento social, suspensão de atividades comerciais, quarentena e ações sanitárias. No entanto, tais ações devem ser baseadas em fundamentos técnicos e científicos, como a metodologia de análise de grandes dados, garantindo ações harmonizáveis com as boas práticas regulatórias. Dessarte, no próximo item serão investigadas as políticas para implementação de *contact tracing,* inclusive na experiência internacional.

## 2.2. As políticas públicas de enfrentamento com base em data tracking e aplicativos de contact tracing em nível global

O conceito de políticas públicas não foi elaborado de uma forma una pelos doutrinadores da ciência política. De maneira geral, parte-se da ideia do conjunto de ações e decisões tomadas pelos governos que irão produzir efeitos na população. O conceito mais conhecido foi formulado por Harold Lasswell[13], de modo que a política pública visa a responder às questões de quem ganha o quê, por quê e qual diferença faz. Em outras palavras, o significado de políticas públicas contempla as atividades governamentais, suas causas e seus efeitos.

Ainda, para o referido autor, o estudo da política é um estudo sobre influência e influentes. A ciência política prevê as condições, a filosofia da política justifica as preferências. Como afirma Harold Lasswell, em livre tradução, "os influentes são aqueles que obtêm o máximo do que existe para obter. Os valores disponíveis podem ser classificados como deferência, renda, segurança. Aqueles que obtêm mais são da elite; o resto é massa".

Conforme estabelece Enrique Saraiva[14], em uma visão moderna do tema, o processo de política pública busca gerenciar as incertezas decorrentes de mudanças de contexto, considerando a realidade socioeconômica. Desse modo, o autor conceitua política pública como:

[13] Lasswell, Harold. D. Politics: who gets what, when, how. In: *The political writings of Harold D. Lasswell*. Free press, Glencoe, Illinois, 1951. p. 295.

[14] Saravia, Enrique. Política Pública: introdução à teoria da política pública. In: Saravia, Enrique; Ferrarezi, Elisabete. *Políticas Públicas*; coletânea, v.1, 2006, p. 29. Brasília, Enap.

> sistema de decisões públicas que visa a ações ou omissões, preventivas ou corretivas, destinadas a manter ou modificar a realidade de um ou vários setores da vida social, por meio da definição de objetivos e estratégias de atuação e da alocação dos recursos necessários para atingir os objetivos estabelecidos. (SARAVIA, 2006)

As políticas públicas possuem componentes institucionais, decisórios, comportamentais e causais[15]. Consequentemente, são editadas por autoridades legalmente competentes, compostas por conjuntos de decisões para responder a problemas e necessidades, implicam em atos ou ausência desses, e, por fim, geram efeitos no sistema político e social. Nas palavras de Celina Souza[16], "as políticas públicas repercutem na economia e nas sociedades, daí por que qualquer teoria da política pública precisa também explicar as inter-relações entre Estado, política, economia e sociedade".

Diante desses cenários, durante a crise ocasionada pela Covid-19, restou constatada a necessidade de criação de políticas públicas e regulatórias para contenção da doença baseadas em informações científicas e técnicas. À vista disso, coube aos governos a tomada de decisões acerca das ações a serem adotadas nesse momento e se haveria a possibilidade de utilização de dados das pessoas naturais com intuito de decifrar os estágios da doença. Muitos países, então, utilizaram o monitoramento estatal dos dados das pessoas naturais para compreensão científica da doença, ou seja, a técnica de *contact tracing* foi realizada mediante uso de *big data* e inteligência artificial, denominado como *digital contact tracing*, como indica estudo da Jonhs Hopkins[17]no tocante aos estudos implementados nos Estados Unidos da América (EUA) sobre a utilização de aplicativos de rastreamento:

> A tecnologia de *contact tracing* e produtos de rastreamento de saúde relacionados (juntos DCTT) têm sido usados em vários países como parte de estratégias mais amplas de vigilância e contenção de doenças. Nos Estados Unidos, o DCTT foi proposto como parte integrante de alguns planos para "reabrir" o país. É quase certo que essas e outras tecnologias relacionadas não se tornarão apenas parte da resposta à Covid-19, mas de grandes ferramentas para a prevenção e controle de doenças em saúde pública no futuro. (KAHN, 2020)

O rastreamento de contatos ou *contact tracing* representa a identificação das pessoas contaminadas e seu monitoramento por 14 dias, com objetivo de reduzir

[15] Idem, p. 30.

[16] SOUZA, Celina. Políticas Públicas: uma revisão da literatura. In: *Revista Sociologias*, Porto alegre, p. 20-46, junho, 2006.

[17] KAHN, Jeffrey (Editor). Digital Contact Tracing for Pandemic Response. In: *Johns Hopkins Project on ethics and governance of digital contact tracing technologies*. Baltimore: Johns Hopkins University Press, 2020. p. 1.

a circulação do vírus, como ocorreu no período de disseminação de Covid-19 em diversos países, inclusive no Brasil. Nessa linha, descrevem Bethania Almeida , Danilo Doneda e outros[18]:

> Em termos gerais, estas soluções, que entram na classificação de sistemas de Contact Tracing, funcionam com a troca de identificadores anônimos entre telefones próximos via Bluetooth, após a instalação de um aplicativo disponibilizado pela autoridade de saúde nacional ou eventualmente pelo próprio sistema operacional, a depender de como opera a solução. Quando uma pessoa tiver resultado positivo para o coronavírus, ela irá fazer este registro no aplicativo, que o transmitirá para autoridades de saúde no seu respectivo país. Em seguida, as pessoas com as quais teve contato nos 14 dias anteriores serão alertadas que estiveram em contato com alguém que apresentou diagnóstico positivo para a doença. (Almeida *et al*., 2020)

Em Singapura, assim como em outros países asiáticos como na China, Israel e Coreia do Sul[19], houve a efetiva implementação de monitoramento de contatos e *contact tracing* por aplicativos com tratamento de dados pessoais, isso foi possível com a adoção de tais medidas pela administração pública e flexibilização da proteção de dados durante a crise[20]. No entanto, para fins de amostragem do presente estudo, será investigada a construção jurídico-prática dos aplicativos de rastreamento de dados em Singapura.

Na União Europeia, os estados-membros mostraram diferentes avaliações sobre eficácia, segurança, privacidade e proteção de dados nas soluções digitais para enfrentar a pandemia de Covid-19. Entre março e abril de 2020, a comunidade europeia vislumbrou que as tecnologias de rastreamento de dados poderiam desempenhar um papel fundamental em todas as fases da gestão da crise, especialmente no momento de suspensão gradual das medidas de distanciamento social, como será demonstrado nos próximos itens.

### 2.2.1. Experiência na Europa – União Europeia e Reino Unido

A União Europeia experimentou um grande impacto com consequências sanitárias, econômicas e sociais durante a pandemia de Covid-19. As estatísticas

[18] Almeida, Bethania*et al*. Preservação da privacidade no enfrentamento da Covid-19: dados pessoais e a pandemia global. In: *Ciência & Saúde Coletiva*, 25, 2020. Disponível em: https://www.scielo.br/pdf/csc/v25s1/1413-8123-csc-25-s1-2487.pdf. Acesso em: 14 de julho de 2020.

[19] União Europeia. Centro Europeu de Prevenção e Controle de Doenças. *Contact tracing for Covid-19*: current evidence, options for scale-up and an assessment of resources needed. Disponível em: https://www.ecdc.europa.eu/sites/default/files/documents/COVID-19-Contract-tracing-scale-up.pdf. Acesso em: 14 de julho de 2020.

[20] Singer, Natasha; Sang-Hun, Choe. As coronavirus surveillance escalates, personal privacy plummets. In: *The New York Times*, 23 de março de 2020. Disponível em: https://www.nytimes.com/2020/03/23/technology/coronavirus-surveillance-tracking-privacy.html. Acesso em: 24 de setembro de 2020.

da OMS[21] demonstram que a Europa apresentou o primeiro caso no final de janeiro de 2020, com um total aproximado de 6.500.000 de casos confirmados da doença e 250 mil mortes, em outubro de 2020.

Desde janeiro de 2020, diversas ações normativas, regulatórias e de pesquisa foram tomadas pela Comunidade Europeia, em conjunto com as suas agências, como a *European Centre for Disease Prevention and Control*, visando ao desenho de melhores estratégias e implementação de medidas para combate à Covid-19 na ótica comunitária. No entanto, em relação à proteção de dados e ao uso de aplicativos de *contact tracing*, as políticas comunitárias foram editadas paulatinamente e servirão futuramente como códigos de conduta sem um caráter vinculante aos membros.

Inicialmente, o Conselho Europeu de Proteção de Dados[22] manifestou-se em março de 2020, através do documento intitulado "*Statement on the processing of personal data in the context of the COVID-19 outbreak*". O órgão entendeu que as autoridades públicas europeias podem, no âmbito do Regulamento Geral de Proteção de Dados (GDPR), usar os dados das pessoas naturais, inclusive de geolocalização, para mitigação de contágio de Covid-19. Todavia, os princípios de tratamento devem ser respeitados (como necessidade, adequação e proporcionalidade), além de que os Estados-membros devem buscar a anonimização dos dados em suas políticas públicas de rastreamento[23].

Seguidamente, foi editado o instrumento "*Mobile applications to support contact tracing in EU´s fight against Covid-19*[24]", de 15 de abril de 2020, que é uma caixa de ferramentas para a consecução de dispositivos de rastreamento de dados na União Europeia, com o fim de assegurar a proteção de dados e privacidade dos cidadãos. O documento estabelece que, de forma majoritária, os Estados-membros irão desenvolver seus aplicativos e que devem estar de acordo com os procedimentos definidos pelas autoridades de saúde pública com potenciais implicações de privacidade e segurança avaliadas.

[21] OMS – Organização Mundial Da Saúde**.** *WHO Coronavirus Disease (Covid-19) Dashboard*, atualizado em 08 de outubro de 2020. Disponível em: https://covid19.who.int/table. Acesso em: 08 de outubro de 2020.

[22] O European Data Protection Board trata-se de ente independente, cujo objetivo é garantir a aplicação consistente do Regulamento Geral de Proteção de Dados (GDPR) e promover a cooperação entre as autoridades de proteção de dados da União Europeia e da European Data Protection Supervisor - EDPS.

[23] União Europeia. European Data Protection Board. *Statement on the processing of personal data in the context of the Covid-19 outbreak*, de 19 de março de 2020. Disponível em: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_statement_2020_processingpersonaldataandcovid-19_en.pdf. Acesso em: 08 de outubro de 2020.

[24] União Europeia. *Mobile Applications to support contact tracing in the Eu´s fight against Covid-19*, de 15 de abril de 2020. Disponível em: https://ec.europa.eu/health/sites/health/files/ehealth/docs/covid-19_apps_en.pdf. Acesso em: 08 de outubro de 2020.

Em 15 de julho de 2020, foi publicada a Decisão (EU) nº 2020/1023 que tratou sobre a utilização de aplicativos de *contact tracing* nos estados membros da UE para combate à Covid-19. Considerou-se que diversos membros desenvolveram seus aplicativos de rastreamento de dados para proteção coletiva, permitindo que os usuários fossem alertados quando expostos ao vírus, mas que a administração pública de tais governos deve cumprir e respeitar o GDPR (art. 7[25]). Seguidamente, em 02 de setembro de 2020, foi editado o documento "*European Proximity tracing*", como um código de conduta focado na arquitetura de interoperabilidade para aplicativos de *contact tracing*. Entre outras disposições, há instruções técnicas de segurança e criptografia; bem como o art. 8.2 estabelece que os aplicativos devem garantir: (i) tratamento de dados em conformidade com GDPR; (ii) mitigação de riscos para acessos não autorizados; e (iii) proteção dos direitos dos titulares de dados[26]. Considerando que membros, como a Alemanha, implementaram seus respectivos aplicativos de rastreamento de dados desde junho de 2020, se passa à análise dos casos concretos de avaliação do aplicativo.

O governo federal da Alemanha, em parceria com organizações do setor público e privado (a sociedade SAP de tecnologia da informação e a Robert Koch Institute), lançou em junho de 2020 o aplicativo "Corona Warn-App". Ele é baseado em *contract tracing*, porém, com a preservação de privacidade considerando a descentralização dos dados. Os dados coletados são criptografados e pseudoanonimizados, mantidos nos próprios celulares dos titulares, bem como a tecnologia utilizada no aplicativo utiliza dados de localização e *bluetooth* para determinar os dispositivos móveis próximos àquela pessoa, conforme explicam as informações do próprio aplicativo[27]:

> O Corona-Warn-App é um aplicativo que ajuda a rastrear cadeias de infecção de SARS-CoV-2 (relacionados à pandemia de COVID-19) na Alemanha. O aplicativo é baseado em tecnologias com abordagem descentralizada e notifica os usuários

[25] Cf. A redação do artigo in verbis: "(7) O tratamento de dados pessoais de utilizadores de aplicativos móveis de rastreio de contatos e de alerta, que é efetuado sob a responsabilidade dos Estados-membros ou de outras organizações públicas ou organismos oficiais dos Estados-membros, deve ser efetuado em conformidade com o Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho («Regulamento Geral sobre a Proteção de Dados») e a Diretiva 2002/58/CE do Parlamento Europeu e do Conselho. O tratamento de dados pessoais efetuado sob a responsabilidade da Comissão para efeitos de gestão e garantia da segurança do portal federativo deve cumprir o disposto no Regulamento (UE) 2018/1725 do Parlamento Europeu e do Conselho". In: União Europeia. *Decisão de execução (UE) 2020/1023 da Comissão*, de 15 de julho de 2020. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32020D1023&from=EN. Acesso em: 08 de outubro de 2020.

[26] União Europeia. *European proximity tracing*, de 02 de setembro de 2020. Disponível em: https://ec.europa.eu/health/sites/health/files/ehealth/docs/mobileapps_interop_architecture_en.pdf. Acesso em: 08 de outubro de 2020.

[27] Alemanha. *Corona Warn- App*. Open Source Project. Disponível em: https://www.coronawarn.app/en/. Acesso em: 08 de outubro de 2020.

> caso tenham sido expostos ao SARS-CoV-2. A transparência é a chave para proteger os usuários finais do aplicativo e para incentivar a adoção. (Alemanha, 2020).

O *download* do aplicativo pelos indíviduos é realizado de forma voluntária e ele indicará, por meio de notificações padronizadas de exposição (*API Exposure Notification framework*) e proximidade (*Rolling Proximity Identifier*), se o usuário poderá estar exposto ou não ao vírus. Inicialmente, o usuário poderá indicar se foi testado positivamente para o novo coronavírus e há a possibilidade de realizar a divulgação dos testes diretamente do laborátorio, caso tenha suporte eletrônico para tanto. Caso exista uma confirmação de contágio, todos os usuários com o qual o titular teve contato ou proximidade nos últimos 14 dias serão alertados, conforme informações do próprio Governo:

> No caso de um resultado de teste positivo, os usuários são solicitados a enviar voluntariamente suas chaves temporárias dos últimos 14 dias para o servidor. Para evitar o uso indevido, o back-end do Corona-Warn App verifica primeiro o resultado positivo do teste. Se confirmado, o servidor adiciona as chaves do usuário à lista de confirmados SARS-CoV-2, que é regularmente transmitida para todos os aplicativos. (Alemanha, 2020. Tradução livre)

O aplicativo alemão não oferece violação à proteção de dados e privacidade, pois há consentimento do usuário com o tratamento dos dados e todas as informações são criptografadas. Tanto o governo federal quanto os demais usuários do aplicativos recebem as informações através de chaves criptografadas, sem a possibilidade de identificação da pessoa natural. Esse processo não viola o Regulamento Geral de Proteção de Dados na forma do art. 4, item (5), que estabelece o conceito de pseudoanonimização como :

> [...] o tratamento de dados pessoais de forma que deixem de poder ser atribuídos a um titular de dados específico sem recorrer a informações suplementares, desde que essas informações suplementares sejam mantidas separadamente e sujeitas a medidas técnicas e organizativas para assegurar que os dados pessoais não possam ser atribuídos a uma pessoa singular identificada ou identificável[28]. (Alemanha, 2020). Tradução livre)

Por fim, entende-se que a maior preocupação a respeito da privacidade e proteção de dados do aplicativo seria a possibilidade de reversão dessa pseudoanonimização dos dados, com a completa indicação dos usuários, o que geraria violação às regras do GDPR, nas palavras de Cristoph Ritzer e outros:

[28] União Europeia. Regulamento (Ue) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:31995L0046&from=PT. Acesso em: 08 de outubro de 2020.

> Fácil reversão da pseudonimização e do manuseio inseguro do pseudônimo confidencial, já que o aplicativo não usa um navegador padrão, mas uma visualização da web incorporada que é insegura devido a ataques man-in-the-middle. O servidor RKI expõe funcionalidades adicionais, como uma interface de gerenciamento e administração, bem como uma API SOAP via Internet. Isso aumenta sua vulnerabilidade[29]. (Ritzer *et al*., 2020. Tradução livre)

Ocorre que, para fins de efetividade, o aplicativo "Corona Warn-App" não foi exaustivamente adquirido pelos cidadãos, pois, em outubro de 2020, apenas 18 milhões de *downloads* haviam sido realizados desde seu lançamento em julho[30], segundo dados do instituto Robert Koch. Portanto, no cenário da população alemã de aproximadamente 83 milhões, e por se tratar de país com altos níveis de desenvolvimento humano, verifica-se baixa adesão ao aplicativo de *contact tracing*.

Em relação às normas de proteção de dados, é importante notar que o Tratado da União Europeia (UE)[31], de 25 de março de 1957, consolidado até 2016, organiza o funcionamento desta, determina domínios e regras de exercício das competências. O referido Tratado explicita no art. 16 que todas as pessoas têm direito à proteção de dados de caráter pessoal que lhes digam respeito. Do mesmo modo, determinou que o Parlamento Europeu e o Conselho têm competência para deliberações sobre o tratamento de dados pessoais pelas instituições, órgãos e organismos da União Europeia e de seus membros.

Cooptando a maioria das disposições da norma antecedente, a Diretiva 95/46/CE, em 27 de abril de 2016, foi promulgado o Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho relativo à proteção das pessoas singulares, no que diz respeito ao tratamento de dados pessoais e à livre circulação destes (GDPR). O GDPR revogou a Diretiva, corrigiu diversas deficiências dela, alargou o seu âmbito de aplicação em toda União Europeia e inclusive fora dela, intensificando os requisitos existentes e introduzindo vários novos para as pessoas jurídicas, além de multiplicar os efeitos adversos por descumprimento e negligência.

[29] Ritzer, Cristoph *et al*. Contact tracing apps in Germany. In: *Norton rose Fulbright*, 23 de junho de 2020. Disponível em: https://www.nortonrosefulbright.com/-/media/files/nrf/nrfweb/contact-tracing/germany-contact-tracing.pdf?revision=ed379c1d-011d-4cd8-8e65-02c2664e2ba9. Acesso em: 05 de novembro de 2020.

[30] Alemanha. Instituto Robert Koch. *Principais dados sobre o Corona Warn-App*. Disponível em: https://www.coronawarn.app/en/. Acesso em: 08 de outubro de 2020.

[31] União Europeia. *Tratado sobre o funcionamento da União Europeia*. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:12012E/TXT&from=PT. Acesso em: 08 de outubro de 2020.

O Regulamento Geral de Proteção de Dados (GDPR) teve por objetivo reforçar e unificar a proteção de dados pessoais na União Europeia por meio de uma adaptação dos princípios à sociedade da informação, que cada vez mais realiza coleta e tratamento de dados pessoais físicos ou digitais, por meio da *internet* ou não.

O GDPR, por ser um regulamento, é diretamente aplicável a todos os membros da União Europeia, diferentemente do antigo diploma. Nessa lógica, o GDPR tem a força normativa necessária para a aplicação da proteção de dados a todos os Estados-membros. Mesmo com o caráter vinculante do regulamento, ele determina que os Estados-membros podem manter disposições específicas quanto à aplicação no regulamento, em razão do seu próprio tratamento de dados, na forma da segunda alínea do art. 6º. Isto é, podem editar atos normativos próprios às suas legislações sobre o tema.

Para além do nome, endereço de correio eletrônico, informações médicas, o GDPR indica que os dados pessoais de um indivíduo podem incluir fotos, áudio, formatos visuais em geral, transações financeiras, publicações em sítios de redes sociais, identificadores de dispositivos, endereço do computador, número de telefones celulares, dados de localização, credenciais do usuário (*login*), histórico de navegação, dados profissionais, e muito mais, além de informações genéticas.

O tratamento em si considera as atividades realizadas em dados pessoais de pessoas naturais, por meio automatizado ou não, como a coleta, o registro, a organização, estruturação, a conservação, a adaptação ou alteração, a recuperação, a consulta, a utilização, a divulgação, difusão ou qualquer outra forma de disponibilização, a comparação ou interconexão, a limitação, o apagamento ou a destruição.

Em relação à licitude, o tratamento só é lícito se: (i) o titular tiver dado seu consentimento para determinada finalidade; (ii) for necessário para execução de contrato de que o titular é parte ou diligências pré-contratuais a pedido do titular dos dados; (iii) for necessário para cumprimento de obrigação jurídica ou necessidades vitais do titular de dados ou outra pessoa natural; (iv) houver interesse público ou exercício da autoridade pública de que esteja investido o responsável; ou  por fim; (v) se for necessário para efeitos dos interesses legítimos de responsável pelo tratamento ou terceiros, exceto se prevalecerem interesses ou direitos e liberdades fundamentais do titular que exijam proteção de dados.

Para fins de estudo e amostragem, o Reino Unido, que desde janeiro de 2020 se retirou da União Europeia[32], lançou, entre setembro e outubro de 2020, o aplicativo "NHS Covid-19 App[33]". O disposito de *contact tracing* foi uma iniciativa do Serviço Nacional de Saúde (United Kingdom National Health Service – NHS) e desenvolvido pelas corporações Apple e Google. Ele utiliza ferramentas de bluetooth, localização, *"check-in"*, além de que foi adequado às normas de privacidade da União Europeia. O aplicativo pode ser adquirido pelos titulares de dados de forma voluntária e também foi pensado previamente pelas autoridades de forma a garantir a proteção de dados dos cidadãos.

O aplicativo NHS Covid-19 é descentralizado, mantendo as informações nos celulares dos titulares, que podem ou não compartilhar seus testes. Por fim, as informações mantidas são igualmente pseudoanonimizadas, similarmente à experiência alemã. Caso um titular decida compartilhar que seu teste de Covid-19 é positivo, os demais dispositivos que tiveram contato com ele serão notificados, mas sem qualquer informação a respeito da identificação daquele. Isso mantém a conformidade com o Data Protection Act do Reino Unido de 2018[34], segundo indicações do próprio aplicativo[35]:

> Se você teve um resultado de teste de coronavírus positivo (Covid-19) e decidir compartilhar essas informações para que outras pessoas possam ser alertadas, IDs únicos aleatórios são usados como parte da tecnologia de rastreamento de contato. Nenhum dado pessoal é compartilhado entre o seu telefone e o telefone de outra pessoa,
>
> A lei de proteção de dados estabelece uma estrutura clara de medidas de proteção que seguimos para garantir que o aplicativo seja legalmente compatível e atenda aos padrões esperados para manter todos os dados seguros e confidenciais. Além dessas medidas, garantimos que a privacidade e a identidade dos usuários do aplicativo sejam protegidas de outros usuários do aplicativo, do NHS e do governo. (Reino Unido, 2018. Tradução livre)

Considerando a preocupação do Estado no tocante à proteção de dados, na União Europeia há um complexo normativo-regulatório que visa à proteção dos cidadãos europeus, notadamente com o GDPR. Nesse sentido, verificou-se que houve a criação de aplicativos de *contact tracing* pelos Estados-membros, investigando-se a Alemanha. E no contexto europeu, por amostragem, analisou-

[32] União Europeia. *Counsel decision (EU) 2020/135 of 30 January 2020*. Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32020D0135. Acesso em: 04 de novembro de 2020.

[33] Reino Unido. *NHS Covid-19 APP*. Disponível em https://www.covid19.nhs.uk/privacy-and-data/you-choose-what-data-you-share.html. Acesso em 12 de outubro de 2020.

[34] Reino Unido. *Data Protection Act*, de 23 de maio de 2018. Disponível em: https://www.legislation.gov.uk/ukpga/2018/12/introduction/enacted. Acesso em: 04 de novembro de 2020.

[35] Idem.

se o caso do Reino Unido; porém, ambos os casos foram concebidos previamente com respeito ao GDPR e demais regulamentos de proteção de dados.

### 2.2.2. Experiência nos Estados Unidos da América (EUA)

Os EUA foram amplamente afetados pela expansão do contágio de Covid-19. A OMS estima que em outubro de 2020 houve, aproximadamente, 7.700.000 casos confirmados e 213 mil mortes, indicando que se trata do país com maior contágio da doença, em relação aos números citados. O primeiro caso foi reportado em fevereiro de 2020 e, consequentemente, o governo federal estadunidense implementou diversos atos para contenção da epidemia e redução dos efeitos econômicos, como o "*Coronavirus Preparedness and Response Supplemental Appropriations Act",* de 06 de março de 2020, e o *"Families First Coronavirus Response Act"*, de 18 de março de 2020.

Nessa linha, o desencadeamento de ações de rastreamento de dados, notadamente pelos aplicativos de celulares, foi realizado de forma estadual nos EUA. Desse modo, a título de amostragem, o Estado de Nova Iorque lançou, em outubro de 2020, seu aplicativo "Covid Alert NY[36]", de forma pioneira no país. O aplicativo foi desenvolvido pelo governo estadual em parceria com as corporações Apple e Google e também segue os padrões europeus de atendimento aos princípios de privacidade e proteção de dados.

O aplicativo pode ser obtido voluntariamente por qualquer cidadão e, assim como na União Europeia, utiliza a tecnologia de bluetooth para identificar os dispositivos celulares próximos. Portanto, os usuários do aplicativo serão alertados caso tenham contato próximo com alguém cujo teste tenha sido positivo para o novo coronavírus. A tecnologia também é descentralizada, bem como o aplicativo pode ser apagado a qualquer momento e mantém os dados anônimos, uma vez que não identifica qualquer indivíduo pelo uso de chaves criptografadas. Finalmente, os dados pessoais são compartilhados voluntariamente pelo titular, mas apenas serão divulgados ao Departamento de Saúde do Estado de Nova Iorque, conforme informações do próprio aplicativo[37]:

> O aplicativo coleta as informações fornecidas por você, caso você escolha como o município em que você mora, seu sexo, sua faixa etária, sua etnia e seus sintomas, bem como os dados gerados pelo próprio aplicativo. Esses dados são registrados

[36] Perrigo, Billy. Us States are rolling out Covid-19 contact tracing apps. Months of evidence from Europe shows they ´re no silver bullet, 09 de outubro de 2020. In**:** *Time*. Disponível em: https://time.com/5898559/covid-19-contact-tracing-apps-privacy/. Acesso em: 13 de outubro de 2020.

[37] Estados Unidos. Estado de Nova Iorque. *Covid Alert NY*: what you need to know. Disponível em: https://coronavirus.health.ny.gov/covid-alert-ny-what-you-need-know. Acesso em: 13 de outubro de 2020.

> anonimamente e qualquer um deles poderá ser compartilhado com o Departamento de Saúde do Estado de Nova Iorque, porém não poderá ser usado para identificá-lo ou a qualquer outro indivíduo que use o aplicativo.
> Se você ativou o registro, o recurso de Notificação de Exposição dentro do Sistema Operacional do seu telefone irá coletar os códigos aleatórios de outros smartphones que estão dentro de 6 pés de seu telefone por mais de 10 minutos. Se você estiver em contato próximo com alguém com teste positivo para Covid-19, o aplicativo irá compartilhar a data mais recente em que você esteve em contato direto com essa pessoa. (Estados Unidos, 2020. Tradução livre)

A proteção de dados nos EUA é regulamentada nos níveis estadual e federal em diversas leis esparsas. Ou seja, não existe um núcleo ou lei única sobre essa temática, como ocorre na União Europeia ou no Brasil. A legislação federal é aplicável de forma setorial (como o *Fair Credit Reporting Act*[38] e *Privacy Act*[39]), pois foi criada e é aplicável aos diferentes segmentos de atuação empresarial, enquanto as leis estaduais são mais voltadas para os consumidores, para as pessoas residentes naqueles estados, conforme estabeleceu Shawn Boyne[40]:

> Os Estados Unidos seguem uma abordagem setorial para proteção de privacidade de dados. Não existe uma legislação federal abrangente que garanta a privacidade e a proteção de dados pessoais. Em vez disso, a legislação a nível federal protege principalmente os dados dentro de contextos específicos de cada setor. Em contraste com a abrangente Diretiva de Proteção de Dados da Europa, os Estados Unidos contam com uma combinação de leis nos níveis federal e estadual, regulamentos administrativos e diretrizes de autorregulação específicas da indústria. As garantias de proteção e de privacidade são específicas de cada setor e estão localizadas em uma miríade de instrumentos legislativos e na jurisprudência. Essas regras aplicam-se apenas a setores específicos como serviços de saúde, educação, comunicações e serviços financeiros ou, no caso de coleta de dados on-line, a crianças. (Boyne, 2018. Tradução livre)

As leis federais dos Estados Unidos regularam a proteção de dados e privacidade das pessoas em uma lógica setorial, com foco em serviços financeiros e fornecedores de serviços de saúde. Complementarmente, as leis federais impõem obrigações aos agentes econômicos, geralmente com o intuito de proibir o uso abusivo das informações dos consumidores, considerando alguns critérios de segurança,

[38] Fair Credit Reporting Act (FCRA) de 1970, considerada a primeira lei sobre privacidade nos Estados Unidos. O referido diploma estabeleceu proteção aos consumidores mediante notificação sobre o registro de seus dados.

[39] *Privacy Act de 1974* que regulou os bancos de dados do governo dos Estados Unidos. Trata-se de um código de boas práticas sobre informações pessoais que são mantidas em sistemas de registros em agências federais. Além disso, o *Privacy Act* estabeleceu que o direito à privacidade é um direito fundamental protegido pela Constituição dos Estados Unidos, o que foi um marco na legislação desse país.

[40] Boyne, Shawn Marie. Data protection in the United States. In: *The American Journal of Comparative Law*, v. 66, p. 299-343, 2018. Oxford University Press..

emprego, crédito e para regular as telecomunicações. Essas leis foram baseadas na premissa de que um indivíduo possui uma expectativa de privacidade, exceto se essa foi de alguma forma restringida ou eliminada por algum acordo, contrato, lei ou consentimento.

Em relação às leis estaduais, é possível citar a Lei de Proteção à Privacidade Pessoal de Nova Iorque[41], que é prevista na Lei Estadual de Nova Iorque, de 1903, especificamente no artigo 6-A, nas Seções 91 a 99. Ela regula o acesso e direito de impugnação relativa às informações contidas nos registros dos órgãos e entidades do poder público do Estado de Nova Iorque, não havendo impacto sobre o uso para *contact tracing*, como prevê a Seção 92:

> Agência. O termo "agência" significa qualquer conselho estadual, agência, comitê, comissão, conselho, departamento, autoridade pública, corporação de utilidade pública, divisão, escritório ou qualquer outra entidade governamental que desempenhe uma função governamental ou proprietária para o estado de Nova York, exceto a Judiciário ou a Assembleia Legislativa ou qualquer unidade do governo local e não deve incluir escritórios de promotores distritais.
> (2) Comitê. O termo "comitê" significa o comitê de governo aberto constituído de acordo com a subdivisão um da seção 89 deste capítulo.
> (3) Assunto dos dados. O termo "pessoa em causa" significa qualquer pessoa singular sobre quem as informações pessoais foram coletadas por uma agência.
> (4) Divulgação. O termo "divulgar" significa revelar, liberar, transferir, disseminar ou de outra forma comunicar informações ou registros pessoais oralmente, por escrito ou por meio eletrônico ou de qualquer outro meio que não seja para o titular dos dados[42]. (Estados Unidos da América, 2019. Tradução livre)

Destaque-se também a Lei de Privacidade do Consumidor da Califórnia (California Consumer Privacy Act CCPA), de 2018, que tratou sobre a proteção de dados pessoais naquele estado e estabeleceu princípios como: (i) o direito de um consumidor ter conhecimento de que um controlador coletou seus dados, bem como o modo de tratamento e a finalidade; (ii) direito de exclusão do banco de

[41] Estados Unidos da América. New York State Senate. *Personal Privacy Protection Law*. Disponível em: https://www.nysenate.gov/legislation/laws/PBO/93. Acesso em: 14 de abril de 2019.

[42] *Ibidem*. Na redação original: “Section 92. Definitions. (1)Agency. The term "agency" means any state board, bureau, committee, commission, council, department, public authority, public benefit corporation, division, office or any other governmental entity performing a governmental or proprietary function for the state of New York, except the judiciary or the state legislature or any unit of local government and shall not include offices of district attorneys. (2) Committee. The term "committee" means the committee on open government as constituted pursuant to subdivision one of section eighty-nine of this chapter. (3) Data subject. The term "data subject" means any natural person about whom personal information has been collected by an agency. (4) Disclose. The term "disclose" means to reveal, release, transfer, disseminate or otherwise communicate personal information or records orally, in writing or by electronic or any other means other than to the data subject”.

dados e interrupção do tratamento; (iii) direito de revogação do consentimento de tratamento de dados; e (iv) não discriminação[43].

Conclui-se que os EUA estabeleceram a privacidade em sua legislação em nível federal (diversos atos setoriais que tangenciam o tema) e estadual. Não existe diploma legal específico sobre a proteção de dados e tratamentos pessoais de forma unificada no país, o que torna a estrutura frágil. Em relação ao *contact tracing*, pelo uso de aplicativos, também a iniciativa tem sido realizada de forma pulverizada e de forma pioneira pelo Estado de Nova Iorque. Contudo, não há um arcabouço legal de proteção de dados para desenvolvimento ou regulação dos aplicativos de rastreamento de dados.

### 2.2.3. Experiência em Singapura

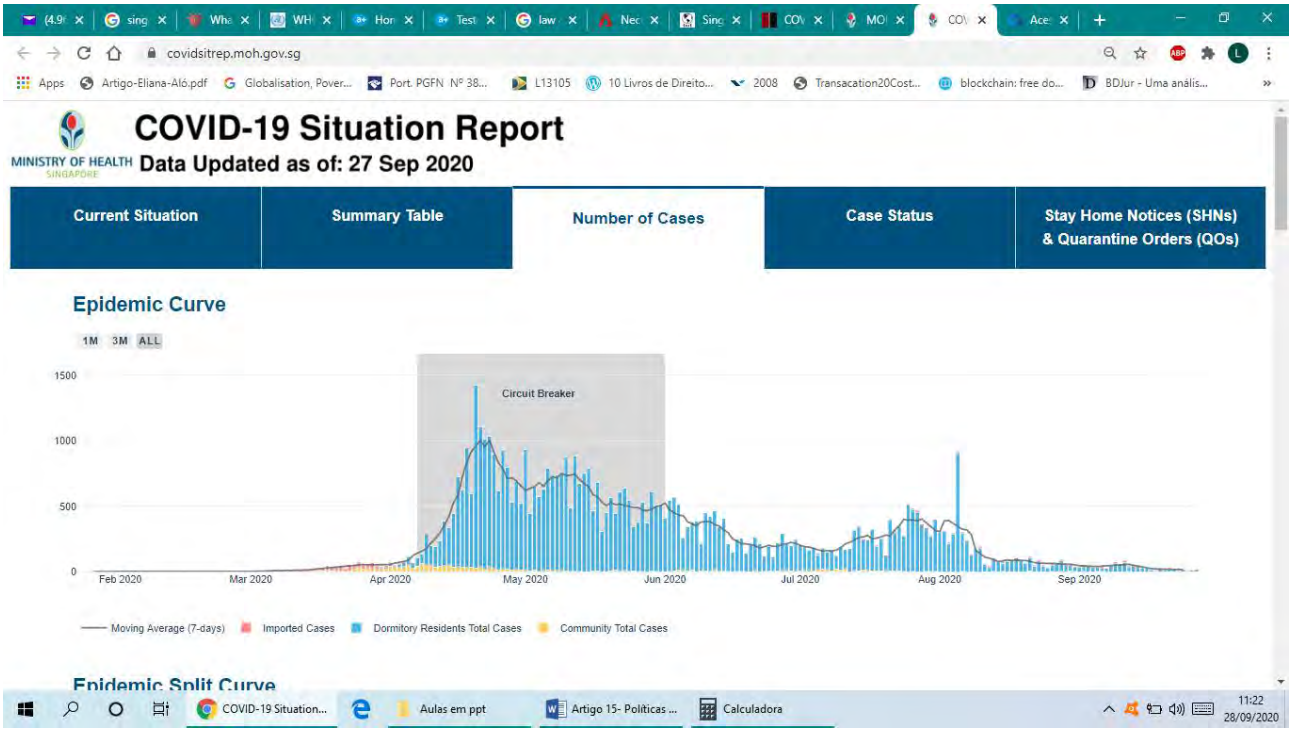
Singapura foi um dos estados, quantitativamente, pouco afetados pela pandemia de Covid-19, de acordo com as estatísticas apresentadas pela OMS.
Conforme relatório da OMS, em setembro de 2020, esse estado apresentou apenas 57 mil casos de Covid-19 e 27 mortes decorrentes da doença. Apresentando um total de 0,01% da população com a confirmação da doença e apenas 0,000000474% de mortes em relação àquela. Isso considerando a densidade demográfica de aproximadamente 7.900 habitantes por km²[44].

Conforme explicitam os relatórios da OMS os primeiros casos de coronavírus reportados por Singapura ocorreram em janeiro de 2020, porém a expansão deles ocorreu no início de abril de 2020 quando os números de infectados passaram a duplicar diariamente. Ao final de abril e início de maio os números já apresentavam queda, ou seja, no dia 23 de abril o país apresentou 1397 novos casos e, em 1º de maio, 636, conforme gráfico a seguir:

[43] Estados Unidos da América. Califórnia legislative information. Civil Code. *California Consumer Privacy Act of 2018*. Disponível em: http://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5. Acesso em: 13 de outubro de 2020.

[44] Comparativamente, o Brasil possui em 2020, aproximadamente, 211 milhões de habitantes em 2020 em 8.516.000 km² de território, com uma densidade demográfica de aproximadamente 25 habitantes por km². Por sua vez, apresentou-se, até outubro de 2020, 4.800.000 casos reportados da doença, além de 142.000 mortes confirmadas, de acordo com a OMS. Ou seja, no Brasil há um percentual de aproximadamente 0,022% da população infectada e 0,000672% de mortes, o que demonstra que as políticas públicas adotadas por Singapura foram potencialmente mais eficientes que as brasileiras, porque o percentual de infectados no Brasil corresponde ao dobro de Singapura, e, em relação às mortes, o percentual é quase 140 vezes maior. Caso seja considerado que o novo coronavírus é transmitido pelo vetor humano, seja por contato direto ou indireto.

**Figura 1– Relatório sobre curva epidêmica da Covid-19 em Singapura**




Fonte: Ministério da Saúde de Singapura, 2020[45].

Após a eclosão da epidemia em Singapura, o governo agiu com eficiência, editando diversos atos e políticas regulatórias para sua repressão. Inicialmente, formou-se uma força tarefa ministerial composta pelos Ministérios da Saúde e do Desenvolvimento Social, que elaboraram protocolos para *contact tracing,* baseados nos processos utilizados anteriormente na crise de SARS em 2003. Adicionalmente, a resposta do governo de Singapura à Covid-19 envolveu diversas medidas regulatórias e restrições à população. Houve a imposição de restrições de viagens, quarentena de duas semanas para viajantes e, em 23 de março, o governo proibiu viagens de curta duração. Em abril de 2020, foi editado o Ato Covid-19 (Medidas Temporárias) de 2020, ou, na linguagem original, "*Covid-19 (Temporary measures) Act 2020*", conforme assevera, em livre tradução, Kevin Y. L Tan[46]:

> [...] Restrições à movimentação local da população foram impostas no início de abril, em uma série do que o governo chamou de medidas de "*circuit breaker*". Para implementar essas medidas, o Parlamento de Singapura aprovou o Ato Covid-19 (Medidas Temporárias)

[45] Singapura, Ministério da Saúde. *Covid-19 Interactive Situation Report***.** Disponível em: https://www.moh.gov.sg/covid-19/situation-report. Acesso em: 28 de setembro de 2020.

[46] Tan, Kevin Y. L. Singapore's Regulatory Response to Covid-19. In: *The regulatory review*. Penn Programme of Regulation, jun, 2020. Disponível em: https://www.theregreview.org/2020/06/15/tan-singapore-regulatory-response-covid-19/. Acesso em: 28 de setembro de 2020.

> em 7 de abril. Entre outras coisas, essa lei suspendeu as obrigações contratuais, proporcionou alívio às partes em dificuldades financeiras, estabeleceu novas práticas para a realização de reuniões e introduziu medidas para manter os tribunais funcionando usando tecnologia de comunicação remota. A lei também permitiu que funcionários do governo restringissem certas atividades para evitar a propagação do vírus. (TAN, 2020. Tradução livre)

O Ato Covid-19 estabelece na "parte 7" as ordens de controle. De acordo com o artigo 34, o ministro da Saúde poderá regular e editar normas no intuito de prevenir, proteger, retardar e controlar a incidência de transmissão do vírus. Dessa forma, as normas e ordens de controle poderiam: (i) restringir a movimentação das pessoas; (ii) restringir contatos entre pessoas ou limitar atividades em grupo; (iii) limitar o uso das pessoas a determinados locais em determinados horários ou exigir o fechamento de instalações[47].

Cumpre ressaltar que em Singapura vigora desde 1976 o *Infectious Disease Act*, que é a principal lei que regula a prevenção e controle de doenças infecciosas. Essa regulação é realizada pelo Ministério da Saúde e pela Agência Nacional de Meio Ambiente. O artigo segundo define contato como "qualquer pessoa que foi exposta ao risco de infecção daquela doença". Em adição, ações de *contact tracing* são conceituadas como "quaisquer medidas para facilitar o rastreamento de contatos de uma doença infecciosa[48]".

O artigo 19-A da referida lei estatui que quaisquer medidas de *contact tracing* poderão ser autorizadas pelas autoridades, caso haja necessidade de prevenir a propagação ou surto de qualquer doença infecciosa. Consequentemente, as autoridades podem notificar e/ou direcionar pessoas para realização de rastreamento ou permitir que agentes de saúde (*Health officers*) conduzam as ações de vigilância em locais de risco.

Igualmente, *o Infectious Diseases Act* estabelece no art. 7 que as autoridades poderão instituir programas de vigilância e investigações epidemiológicas de maneira a determinar a existência da epidemia. O artigo 16 versa ainda que as pessoas suspeitas ou confirmadas de exposição a doenças infectocontagiosas devem ser controladas e vigiadas pelas autoridades por período estabelecido por elas. Caso haja um descumprimento às medidas de vigilância ordenadas pelas autoridades, sem justo motivo, haverá uma ofensa criminal, que será punida

[47] SINGAPURA. *Covid-19 (Temporary measures act)*. Disponível em: https://sso.agc.gov.sg/Act/COVID19TMA2020. Acesso em: 28 de setembro de 2020.

[48] SINGAPURA. *Infectious diseases act*. Disponível em: https://sso.agc.gov.sg/Act/IDA1976#pr19A-. Acesso em: 28 de setembro de 2020.

conforme o Código de Processo Penal daquele país.

Em relação aos dados pessoais, a lei disciplina que as autoridades podem, diante de um surto de epidemias ou da necessidade de mitigação de eventuais contágios, ter acesso e disponibilizarem às demais autoridades competentes e entes responsáveis dados e informações, nos termos do art. 10:

> Art. 10 (1) O Diretor pode, com a finalidade de investigar qualquer surto ou suspeita de surto de uma doença infecciosa, prevenir a propagação ou possível surto de uma doença infecciosa, ou tratar qualquer pessoa que seja, ou suspeite de ser, um caso ou portador ou contato de uma doença infecciosa - (a) exigir que qualquer profissional de saúde obtenha de seu paciente as informações que o Diretor possa razoavelmente exigir para esse fim e transmita essas informações ao Diretor; e (b) com a aprovação do Ministro competente, editar normas, criar medidas ou procedimentos gerais ou específicos para esse fim para cumprimento por qualquer profissional de saúde, hospital, clínica médica, laboratório clínico ou estabelecimento de saúde[49]. (Singapura, 2020)

O governo de Singapura lançou, em março de 2020, um aplicativo para realização de *contact tracing* denominado "TraceTogether", que, juntamente com o aplicativo "Safe Entry", realizam rastreamento de dados de pessoas e monitoram a circulação de pessoas em estabelecimentos. O aplicativo TraceTogether[50] é voluntário, consiste no uso de tecnologia bluetooth em aplicativo de celular ou *token* e é centralizado no próprio celular do usuário por 21 dias, podendo ser acessado pelas autoridades governamentais, caso ele ofereça consentimento para encaminhamento ao servidor central, como preveem Stella Cramer e outros[51]:

> O governo de Singapura lançou um aplicativo de *contact tracing* (TraceTogether) em 20 de março de 2020. Igualmente, o Safe Entry também foi lançado pelo governo de Singapura. O Safe Entry é um sistema nacional de check-in digital que registra carteiras nacionais de identidade e os números de celular de indivíduos que visitam hotspots, locais de trabalho e de serviços, bem como locais públicos para prevenir e controlar a transmissão de Covid-19 por meio de atividades como rastreamento e identificação de clusters. Os indivíduos fazem check-in/out do Safe Entry em pontos de entrada ou saída por meio de (1) aplicativo SingPass Mobile com código QR ou a partir de uma lista de locais próximos usando a função 'Check-in SafeEntry', (2) tendo uma identificação com um código de barras (por exemplo carteira de identidade, passe de estudante ou carteira de trabalho) ou (3) escaneamento de um código QR

[49] Idem.

[50] Cf. O aplicativo foi desenvolvido pelo Serviço Digital do Governo de Singapura e pode ser acessado no site https://www.tracetogether.gov.sg/.

[51] Cramer, Stella*et al*. *Contract tracing apps in Singapore*. In: Norton Rose Fulbright, 11 de junho de 2020. Disponível em: https://www.nortonrosefulbright.com/-/media/files/nrf/nrfweb/contact-tracing/singapore-contact-tracing.pdf?la=en-sg&revision=. Acesso em: 28 de setembro de 2020.

> exibido no local para envio de dados pessoais. (Cramer *et al*., 2020. Tradução livre)

Ademais, o aplicativo Safe Entry[52] é obrigatório para estabelecimentos comerciais, escritórios, escolas, locais públicos, taxis e demais instalações que estejam operando com público. Stella Cramer e outros, sobre esse tema, ainda adiantam que "para o Safe Entry, os dados coletados são criptografados e armazenados em um servidor centralizado do governo, mas acessados apenas pelas autoridades quando forem necessários para a finalidade de prevenir ou controlar a transmissão de COVID-19".

Em síntese, os aplicativos utilizados em Singapura utilizam dados pessoais, identidades, dados sensíveis de saúde e geolocalização para monitorar os casos suspeitos, bem como rastrear possíveis contatos com os quais o indivíduo contaminado se reuniu naquele período. Mas, de acordo com as autoridades competentes que gerenciam os aplicativos, não há uma violação à proteção de dados e privacidade porque eles são criptografados. Desse modo, em consonância com as instruções do próprio aplicativo Trace Together[53]: (i) os dados armazenados são limitados ao número do telefone e uma identidade de usuário anonimizada; (ii) é utilizada tecnologia bluetooth de aproximação; (iii) os dados de dispositivos próximos são armazenados no próprio celular do usuário e apenas serão utilizados pelo Ministério da Saúde se o titular testar positivamente para Covid-19; (iv) os dados apenas serão utilizados para rastreamento sobre Covid-19, por período limitado de tempo; e (v) o usuário poderá solicitar a exclusão dos dados.

Finalmente, mesmo que os citados aplicativos efetivamente estejam em conformidade com os princípios gerais de proteção de dados, como finalidade, livre acesso e segurança, há que se destacar que a própria lei de proteção de dados singapuriana autoriza a utilização dos dados pessoais pelos órgãos públicos sem a necessidade de consentimento do seu titular, conforme preceitua o artigo 1 do quarto anexo do *Personal Data Protection Act* de 2012[54]:

> DIVULGAÇÃO DE DADOS PESSOAIS SEM CONSENTIMENTO
> 1. Uma organização pode divulgar dados pessoais sobre um indivíduo sem o seu consentimento nas seguintes circunstâncias: (a) a divulgação é necessária para qualquer finalidade que seja claramente do interesse do indivíduo, se o consentimento para sua divulgação não puder ser obtido em tempo hábil; (b) a

[52] Cf. Igualmente, o aplicativo Safe Entry foi desenvolvido pelo Serviço Digital do Governo de Singapura e pode ser acessado no site https://www.safeentry.gov.sg/.

[53] SINGAPURA. *TraceTogether Privacy Safeguards*. Disponível em: https://www.tracetogether.gov.sg/common/privacystatement. Acesso em: 28 de setembro de 2020.

[54] Singapura. *Personal Data Protection Act, 2012*. Disponível em: https://sso.agc.gov.sg/Act/PDPA2012#pr44-. Acesso em 28 de setembro de 2020.

> divulgação é necessária **para responder a uma emergência que ameace a vida, saúde ou segurança dele** ou de outro indivíduo;
> (c) **sujeito às condições do parágrafo 2, existem motivos razoáveis para acreditar que a saúde ou segurança deste indivíduo ou de outro indivíduo será seriamente afetada e o consentimento para a divulgação dos dados não pode ser obtido em tempo hábil;** (SINGAPURA, 2012. Tradução livre e grifos do autor)

Ante tais circunstâncias investigadas, o quadro normativo-regulatório de Singapura admite 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, independentemente da edição de novas leis e decretos para contenção da Covid-19. Em relação à efetividade, verifica-se que 2,4 milhões de cidadãos de Singapura[55] realizaram o download do aplicativo ou resgataram seu token, em uma população de 5,5 milhões, o que representa ampla divulgação e incentivos pelo governo.

Ante à pesquisa sobre o rastreamento de dados no cenário internacional, no próximo capítulo serão analisados os critérios da proteção de dados no Brasil, para ao final propor medidas comparativas para a implementação de programas de rastreamento no país.

[55] SINGAPURA. *TraceTogether App*. Disponível em: https://www.tracetogether.gov.sg/. Acesso em: 28 de setembro de 2020.

# 3.
# Fundamentos da proteção de dados no Brasil

# 3. Fundamentos da proteção de dados no Brasil

Como visto no capítulo anterior as políticas públicas de rastreamento de dados com base na utilização de informações sanitárias e de saúde dos cidadãos, têm como possível entrave e limitação, os próprios direitos fundamentais à privacidade e proteção de dados.

Nesse capítulo serão analisados os fundamentos da proteção de dados no ordenamento jurídico brasileiro, para em ato contínuo, investigar as políticas adotadas pela administração pública federal brasileira sobre rastreamento de dados para combate e prevenção à pandemia de Covid-19.

## 3.1. A proteção de dados e sua positivação do ordenamento jurídico brasileiro (estado da arte)

A Lei nº 13.709, de 14 de agosto de 2018, denominada Lei Geral de Proteção de Dados (LGPD), conceituou o tratamento de dados pessoais, inclusive em meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com objetivo de proteger os direitos fundamentais e o livre desenvolvimento da personalidade da pessoa natural.

Com a promulgação da LGPD[1], criou-se um marco para a disciplina da proteção de dados[2]. A nova legislação foi baseada nas normas estadunidenses e europeias, especialmente no Regulamento Geral de Proteção de Dados da União Europeia (RDPG), de 14 de abril de 2016, bem como nas diretrizes da Organização para Cooperação e Desenvolvimento Econômico[3] de 2013, notadamente após a repercussão mundial acerca de vazamento de dados e ciberataques mundiais[4].

A proteção de dados foi fomentada pelo próprio princípio fundamental da privacidade, previsto na Constituição Federal; porém, passa a ser um princípio com autonomia própria, aplicado em âmbito público ou privado, conforme indicou Danilo Doneda[5]:

> Através da proteção de dados pessoais, as garantias que a princípio eram relacionadas com a privacidade passam a ser vistas através de ótica mais abrangente, pela qual outros interesses devem ser considerados, compreendendo as diversas formas de controle tornadas possíveis com a manipulação de dados pessoais. Esses interesses devem ser observados pelo operador do direito por tudo que representam, e não somente pelo seu traço visível – a violação de privacidade – para uma completa apreciação do problema. (Doneda, 2006, p. 204)

A LGPD estabeleceu os padrões e procedimentos de como os dados pessoais devem ser coletados, armazenados, disseminados e tratados de modo geral, em meio digital ou físico. Além disso, por intermédio da emenda realizada pela Lei nº 13.853, de 08 de julho de 2019, foi estabelecida a criação de uma autoridade para fiscalização dessas ações, a Autoridade Nacional de Proteção de Dados (ANPD).

[1] Os artigos 55-A, 55-B, 55-C, 55-D, 55-E, 55-F, 55-G, 55-H, 55-I, 55-J, 55-K, 55-L, 58-A e 58-B entraram em vigor em 28 de dezembro de 2019, enquanto os artigos 52, 53 e 54 entrarão em vigor em agosto de 2021, e os demais entraram em vigor em agosto de 2020. In: Brasil. *Lei nº 13.709, de 14 de agosto de 2018*. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 27 de outubro de 2020.

[2] Cf. Patricia Peck Pinheiro informa: "A Lei nº 13.709/2018 é um novo marco legal brasileiro de grande impacto, tanto para as instituições privadas quanto para as públicas, por tratar dos dados pessoais dos indivíduos em qualquer relação que envolva o tratamento de informações classificadas como dados pessoais, por qualquer meio, seja por pessoa natural ou jurídica". In: Pinheiro, Patricia Peck. *Proteção de Dados Pessoais***.** Comentários à Lei nº 13.709/2018 (LGPD). São Paulo: Saraiva, 2018, p. 15.

[3] OCDE. *Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data***,** de 11 de julho de 2013**.** Disponível em: http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf. Acesso em: 13 de abril de 2020.

[4] Entre os casos mais famosos, estão o vazamento de dados dos usuários da rede social Facebook para a organização de marketing político Cambridge Analytica em 2018 e o ciberataque mundial que atingiu diversas organizações públicas e privadas em 2017, exigindo resgate em dinheiro em razão de possível inutilização do sistema de dados. In: *O Globo*. São Francisco. Dados de 87 milhões foram usados pela Cambridge Analytica, diz Facebook. 04 de abril de 2018. Recurso eletrônico. Disponível em: https://oglobo.globo.com/economia/dados-de-87-milhoes-foram-usados-pela-cambridge-analytica-diz-facebook-22556605. Acesso em: 27 de outubro de 2020; e *O Globo*. G1. Ciberataques em larga escala atingem empresas no mundo e afetam Brasil. Recurso eletrônico. Disponível em: <https://g1.globo.com/tecnologia/noticia/hospitais-publicos-na-inglaterra-sao-alvo-cyber-ataques-em-larga-escala.ghtml Acesso em: 27 de outubro de 2020.

[5] Doneda, Danilo. *Da privacidade à proteção de dados*. Rio de Janeiro: Renovar, 2006, p. 204.

A finalidade da lei é possibilitar a regulação da proteção de dados, com a coesão das iniciativas dos agentes, fiscalização, responsabilidades e instituição de princípios, proporcionando controle dos riscos envolvidos no tratamento de dados e segurança jurídica para as pessoas, agentes econômicos e poder público. Nessa ótica, de acordo com o art. 2º da LGPD, a disciplina da proteção de dados pessoais tem por fundamentos: (i) o respeito à privacidade; (ii) a autodeterminação informativa; (iii) a liberdade de expressão, de informação, de comunicação e de opinião; (iv) a inviolabilidade da intimidade, da honra e da imagem; (v) o desenvolvimento econômico e tecnológico e a inovação; (vi) a livre iniciativa, a livre concorrência e a defesa do consumidor; e (vii) os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.

Os princípios gerais do tratamento de dados foram disciplinados no art. 6º da Lei nº 13.709, de 2020. Além da boa-fé, as partes devem respeitar: (i) a finalidade, ou seja a realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular; (ii) a adequação, isto é a compatibilidade do tratamento com as finalidades informadas ao titular; (iii) a necessidade ou proporcionalidade que é a limitação e pertinência do tratamento ao mínimo necessário para a realização de suas finalidades; (iv) o livre acesso; (v) a qualidade que significa garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados; (vi) a transparência; (vii) a segurança, através do uso de medidas técnicas e administrativas aptas a proteger os dados pessoais; (viii) a prevenção pela adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais; (ix) a não discriminação; e (x) a responsabilização e prestação de contas.

Em relação às definições, note-se que o titular é a pessoa natural a quem se referem os dados pessoais objeto do tratamento (art. 5º, V); já os dados pessoais são "as informações relacionadas a uma pessoa natural identificada ou identificável[6]" (art. 5º, I). Não há qualquer limitação legal à natureza, forma ou especificação dessas informações, seja automatizada ou não, patrimonial ou existencial. Contudo, há a diferenciação sobre dados pessoais sensíveis que são relacionados à questão racial ou étnica, convicção religiosa, opinião política, filiação a sindicato

[6] Brasil. *Lei 13.709, de 14 de agosto de 2018*. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm. Acesso em: 30 de outubro de 2020. Art. 5º Para os fins desta Lei, considera-se: I - dado pessoal: informação relacionada a pessoa natural identificada ou identificável; [...]

ou a organização de caráter religioso, filosófico ou político, referente à saúde ou à vida sexual, dado genético ou biométrico (art. 5º, II).

Consequentemente, o tratamento dos dados (art. 5º, X) considera todas as operações realizadas com manuseio de dados, contemplando, mas não se limitando, coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

As pessoas envolvidas no tratamento, denominadas agentes de tratamento, são o controlador, operador e o encarregado. O controlador é a pessoa natural ou jurídica, de direito público ou privado, a quem competem decisões sobre tratamento de dados. Caso exista uma pessoa que irá tratar os dados em seu nome, será considerado operador. Por sua vez, o encarregado é a pessoa indicada pelo controlador, que atuará como intermediador na comunicação entre controlador, titulares dos dados e a ANPD com competência para zelar, implementar e fiscalizar o cumprimento da lei. Ele também é denominado como *data protection officer*, considerando a influência do GDPR que estatui no art. 37 sua designação, *in verbis*:

> 1. The controller and the processor shall designate a data protection officer in any case where:
>
> (a) the processing is carried out by a public authority or body, except for courts acting in their judicial capacity;
>
> (b) the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale; or
>
> (c) the core activities of the controller or the processor consist of processing on a large scale of special categories of data pursuant to Article 9 and personal data relating to criminal convictions and offences referred to in Article 1. […][7]
>
> (União Europeia, 2016)

A lei é extensiva a qualquer operação de tratamento realizada por pessoa natural ou por pessoa jurídica de direito público ou privado, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados, desde que ou (i) a operação de tratamento seja realizada no território nacional, ou (ii) tenha por objetivo a oferta ou o fornecimento de bens, serviços ou o tratamento de dados de indivíduos localizados no território nacional, ou (iii) os dados pessoais objeto do tratamento tenham sido coletados no território nacional.

[7] União Europeia. *Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho*, de 27 de abril de 2016. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:31995L0046&from=PT. Acesso em: 08 de outubro de 2020.

Ultrapassadas as considerações acima, a LGPD autoriza o tratamento de dados apenas na situações descritas no rol do *caput* do art. 7º, quais sejam: (i) com o consentimento do titular; (ii) para o cumprimento de obrigação legal ou regulatória; (iii) pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas respaldados em leis, regulamentos ou contratos; (iv) para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais; (v) quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados; (vi) para o exercício regular de direitos em processo judicial, administrativo ou arbitral, esse último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem); (vii) para a proteção da vida ou da incolumidade física do titular ou de terceiro; (viii) para a tutela da saúde, em procedimento realizado por profissionais da área da saúde ou por entidades sanitárias; (ix) quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais; (x) ou para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente.

Em relação à esfera íntima que compreende a dignidade da pessoa humana, cumpre destacar que, no direito brasileiro, a privacidade é um direito fundamental constitucionalmente garantido. O *caput* do art 5º da Constituição Federal do Brasil de 1988[8] dispõe que todas as pessoas são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e estrangeiros residentes no país a inviolabilidade do direito à vida, liberdade, igualdade, segurança e propriedade. Não obstante, o inciso X desse artigo estabelece que "são invioláveis a intimidade, a vida privada[9], a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação[10]".

A Constituição Federal estabeleceu a segurança e a propriedade como direitos fundamentais e assegurou que o Estado deve garantir a inviolabilidade da intimidade e da vida privada das pessoas, além da própria privacidade necessária

[8] Brasil. *Constituição Federal*. Disponível em: http://www.planalto.gov.br/ccivil_03/Constituicao/Constituicao.htm. Acesso em: 03 de abril de 2019.

[9] Cf. José Afonso da Silva, neste sentido, entendeu que o direito à privacidade é a representação de todos aqueles direitos fundamentais, em sua síntese: "Por isso, preferimos usar a expressão direito à privacidade, num sentido genérico e amplo, de modo a abarcar todas essas manifestações da esfera íntima privada e da personalidade, que o texto constitucional em exame consagrou. Toma-se, pois, a privacidade como o conjunto de informação acerca do indivíduo que ele pode decidir manter sob seu exclusivo controle, ou comunicar, decidindo a quem, quando onde e em que condições, sem a isso poder ser legalmente sujeito". In: Silva, José Afonso da. *Curso de Direito Constitucional Positivo*. 35.ed. São Paulo. Malheiros. 2012. p. 206.

[10] Brasil. *Constituição Federal*, Idem.

diante de novas tecnologias. Destarte, a esfera de proteção da privacidade, de inviolabilidade da pessoa, de acordo com o texto constitucional, é ampla, podendo envolver seu nome, endereço, imagem, pensamentos, planos, família, modo de vida, enfim todas as características externas e internas da pessoa, patrimoniais, existenciais.

A privacidade também representa um direito da personalidade, previsto na Lei nº 10.406, de 10 de janeiro de 2002 (Código Civil), no Capítulo II do Título I, uma vez que o art. 21 do Código Civil defende a inviolabilidade da vida da pessoa natural, bem como que o juiz, mediante requerimento desse indivíduo, adotará as providências necessárias para impedir ou cessar eventuais violações.

Diante do exposto, infere-se que o rastreamento de dados das pessoas naturais, ainda que realizado pela administração pública, se constitui como uma operação de tratamento de dados, motivo pelo qual a LGPD deverá ser aplicada ao caso concreto, inclusive no tocante às políticas de *contact tracing*. No tocante à esfera íntima e vida privada, em sentido subjetivo, os cidadãos possuem a privacidade como um direito fundamental constitucionalmente estabelecido, sendo certo que as ações do poder público devem ser pautadas em tais concepções, conforme será investigado a seguir.

## 3.2. Tratamento de dados pela administração pública

Investigou-se anteriomente que o tratamento de dados pessoais é qualquer procedimento como a coleta, armazenamento, uso e exclusão, realizado dentro ou fora do território nacional, desde que a operação ou a oferta de produtos e serviços ocorra neste local. Além disso, o controlador é considerado "a pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais[11]" (art. 5º, VI da LGPD). Nessa ótica, entende-se que a lei aplica-se à administração pública, na forma do art.1º da LGPD, vinculando a "administração pública direta (União, Estados, DF e Municípios), as pessoas jurídicas de direito público (autarquias e fundações estatais de direito público), de direito privado (empresas públicas, sociedades de economia mista e fundações estatais de direito privado e da administração indireta[12]".

Consequentemente, a LGPD reservou regras específicas para o tratamento de dados realizado pela administração pública que foram estabelecidas no Capítulo

[11] Brasil. *Lei 13.709, de 14 de agosto de 2018*. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm. Acesso em: 30 de outubro de 2020

[12] Bucar, Daniel; Oliveira, Rafael Carvalho Rezende. A Lei Geral de Proteção de Dados e a Administração Pública. In: Pozzo, Augusto Neves dal; Martins, Ricardo Marcondes. *LGPD e Administração Pública – Uma análise ampla dos impactos*, São Paulo, Thomson Reuters Brasil, 2020, p. 904.

IV. Entretanto, elas não se aplicam às empresas estatais em regime concorrencial de mercado, que se submetem ao regime geral da LGPD (art. 24 da LGPD).

Inicialmente, o tratamento de dados realizado pelas "pessoas jurídicas de direito público será realizado para atendimento da finalidade pública, na persecução do interesse público, com o objetivo de executar as competências legais ou cumprir atribuições legais do serviço público" (art. 23 da LGPD)[13]. Porém, também caberá à administração pública o atendimento aos princípios estabelecidos no art. 6º da Lei nº 13.709, de 2020, assim como as possibilidades de tratamento de dados (art. 7º) e o cumprimento das regras relativas aos dados sensíveis, inclusive informações sobre a saúde dos titulares. Outrossim, no tratamento de dados pela administração pública, devem ser fornecidas informações claras sobre a previsão legal, finalidades e operações que serão executadas, além de que deve ser indicado um encarregado (*data protection officer).*

Conforme estabelece o art. 25 da LGPD, os dados devem ser mantidos pelos órgãos e entidades controladores "em formato interoperável e estruturado para o uso compartilhado, com vistas à execução de políticas públicas, a prestação de serviços públicos, à descentralização da atividade pública e à disseminação e ao acesso das informações pelo público em geral". Cabe ressaltar que o uso compartilhado de dados pessoais pelo poder público deverá atender às finalidades específicas de execução de políticas públicas e atribuição legal pelas organizações, respeitados os princípios de proteção de dados (art. 26 da LGPD)[14].

Pelo exposto, a administração pública poderá realizar o tratamento de dados pessoais para a tomada de decisões, notadamente para atendimento às demandas de governança pública. Contudo, diante da autonomia da disciplina de proteção de dados[15], há a necessidade de compatibilização das operações com dados.

[13] Cf. Patricia Peck Pinheiro então esclarece que "Da mesma forma que as instituições privadas devem apresentar uma finalidade clara e transparente para a realização do tratamento de dados pessoais, a pessoa jurídica de direito público deve adotar a finalidade público e o interesse público para a realização do tratamento de dados". In: Pinheiro, Patricia Peck. Idem, 2016, p. 86.

[14] Brasil. *Lei 13.709, de 14 de agosto de 2018*. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm. Acesso em: 30 de outubro de 2020

[15] Cf. estabelece Bruno Bioni, o direito à proteção de dados "é um direito que opera fora da lógica binária do público e privado, bastando que a informação esteja atrelada a uma pessoa – conceito de dado pessoal – para deflagrá-lo. Nesse sentido, os direitos de acesso e retificação transitam na esfera pública e não na privada, na medida em que se busca apenas tutelar que o dado pessoal projete fidedignamente seu titular". In: Bioni, Bruno R. *Proteção de dados pessoais*: a função e os limites do consentimento. Rio de Janeiro: Forense, 2019, p. 99.

# 4.

# As políticas públicas no Brasil para rastreamento de dados


# 4.
## As políticas públicas no Brasil para rastreamento de dados

No Brasil, os primeiros casos da doença foram confirmados em fevereiro de 2020 e, com a rápida expansão deles, houve a necessidade de criação de normas para medidas de enfrentamento em saúde pública. Com isso, foi editada a Lei nº 13.979, de 06 de fevereiro de 2020, que dispõe sobre as ações, em prol da coletividade, a serem adotadas para enfrentamento ao surto de coronavírus (art. 1º)[1].

O art. 3º da referida lei, alterada pela Lei nº 14.035, de 2020, estatui que as autoridades poderiam adotar, no âmbito de suas competências, medidas de isolamento, quarentena, realização de exames, uso obrigatório de máscaras, investigações epidemiológicas, restrições temporárias de rodovias, portos e aeroportos, requisição de bens e serviços, entre outras.

Destaque-se que o parágrafo primeiro do art. 3º da Lei nº 13.979, de 2020, estabelece que as medidas previstas "somente poderão ser determinadas com base em evidências científicas e em análises sobre as informações estratégicas

[1] BRASIL. *Lei nº 13.979, de 6 de fevereiro de 2020*. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/lei/l13979.htm. Acesso em: 22 de novembro de 2020.

em saúde e deverão ser limitadas no tempo e no espaço ao mínimo indispensável à promoção e preservação em saúde pública[2]". Do mesmo modo, a Lei nº 13.989, de 2020, define em seu art. 6º que "é obrigatório o compartilhamento entre órgãos e entidades da administração pública federal, estadual, distrital e municipal de dados essenciais à identificação de pessoas infectadas ou com suspeita de infecção pelo coronavírus, com a finalidade exclusiva de evitar a sua propagação[3]".

Em síntese, a referida norma permitiu o tratamento de dados pessoais, sobretudo de rastreamento de dados e compartilhamento entre órgãos e entidades da administração pública. Contudo, sempre visando a beneficiar a coletividade na forma do art. 1º, I da lei. Portanto, verificou-se que, com o rápido avanço da doença no Brasil, foi necessário o estabelecimento de políticas públicas de *contact tracing*, baseadas no tratamento de dados pessoais de saúde, visando a mitigação do contágio de Covid-19.

## 4.1. Inconstitucionalidade da Medida Provisória nº 954, de 17 de abril de 2020

Diante do cenário de expansão da pandemia de Covid-19 no Brasil, em abril de 2020 foi publicada a Medida Provisória (MP) nº 954, que versava sobre o compartilhamento de dados por empresas de telecomunicações com o Instituto Brasileiro de Geografia e Estatística (IBGE) em razão da pandemia. A referida MP foi submetida à Presidência da República pelo Ministério da Economia, sob a justificativa de que o IBGE necessitava de acesso às informações de número de telefone, endereço residencial dos consumidores de serviços de telecomunicações, pessoas naturais ou jurídicas para realização da Pesquisa Nacional por Amostra de Domicílios Contínua (PNAD Contínua) e monitoramento da pandemia no território nacional, conforme exposição de motivos[4]:

> Submeto à apreciação proposta de Medida Provisória que dispõe sobre o compartilhamento de dados de empresas de telecomunicações para fins de suporte à produção estatística oficial, com vistas ao levantamento de dados para as pesquisas estatísticas do IBGE, incluindo o monitoramento da pandemia associada à Covid-19.
>
> É mister frisar que a edição da referida Medida Provisória coloca-se como urgente diante de três fatos objetivos, quais sejam: 1) a necessidade da produção tempestiva de dados para o monitoramento da pandemia de COVID-19; 2) a necessidade de

[2] Idem.

[3] Idem.

[4] Brasil. *Exposição de motivos da Medida Provisória nº 954, de 17 de abril de 2020*. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/mpv/mpv954.htm. Acesso em: 20 de outubro de 2020.

> garantir a continuidade da PNAD Contínua, com a natural preservação de suas séries históricas básicas, úteis à gestão e avaliação de políticas públicas em âmbito nacional; 3) a tempestividade necessária para a obtenção dos dados requeridos junto às empresas de telecomunicações, supondo-se que uma Medida Provisória terá eficácia mais significativa se comparada a quaisquer outras normas ou instrumentos de solicitação dos dados. (Brasil, 2020)

Ademais, a MP previa que "as empresas de telecomunicação prestadoras do Serviço Telefônico Fixo Comutado (STFC) e do Serviço Móvel Pessoal (SMP) deverão disponibilizar ao IBGE, em meio eletrônico, a relação dos nomes dos números de telefone e dos endereços dos consumidores, pessoas físicas ou jurídicas" (art. 2º).

Considerando o tratamento de dados na forma do art. 1º da LGPD, bem como a possível violação de privacidade do art. 5º, X, o Conselho Federal da Ordem dos Advogados do Brasil (CFOAB) propôs a Ação Direta de Inconstitucionalidade nº 6.387[5] contra a sua eficácia diante da obscuridade em relação à utilização dos dados e contradição com princípios constitucionais.

Por meio de relatoria da Ministra Rosa Weber, o Tribunal Pleno, por maioria de votos referendou, no dia 7 de maio de 2020, a medida cautelar para suspender a eficácia da MP nº 954. O Supremo Tribunal Federal identificou que a referida norma gerava uma violação à privacidade e ao sigilo de dados dos titulares, assim como havia ausência dos requisitos da finalidade, proporcionalidade e adequação que garantissem o direito à proteção de dados dos indivíduos, conforme trecho da decisão[6]:

> Nessa ordem de ideias, não emerge da Medida Provisória n. 954/2020, nos moldes em que posta, interesse público legítimo no compartilhamento dos dados pessoais dos usuários dos serviços de telefonia, considerados a necessidade, a adequação e a proporcionalidade da medida. E tal dever competia ao Poder Executivo ao editá-la. Nessa linha, ao não definir apropriadamente como e para que serão utilizados os dados coletados, a MP n. 954/2020 não oferece condições para avaliação da sua adequação e necessidade, assim entendidas como a compatibilidade do tratamento com as finalidades informadas e sua limitação ao mínimo necessário para alcançar suas finalidades. Desatende, assim, a garantia do devido processo legal (art. 5º, LIV, da Lei Maior), em sua dimensão substantiva. (STF, 2020)

Em perspectiva diversa, o Estado de São Paulo também utilizou a ferramenta de *contact tracing*, oriunda dos celulares da população, para contabilizar os

[5] Cf. Além da ADI nº 6387

[6] 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.

resultados do isolamento social. O órgão especial do Tribunal de Justiça do Estado de São Paulo, por meio de acórdão no Mandado de Segurança nº 2069736-76.2020.8.26.0000 impetrado contra o governador do estado[7], denegou a ordem por entender que o governo paulista utilizava dados anonimizados e agregados. Portanto, o uso de dados na forma anônima e agregada, com a finalidade específica de apurar regiões com maior movimentação de pessoas, não configuraria violação à privacidade, locomoção ou intimidade.

A LGPD estabelece as diretrizes para o tratamento de dados de pessoais, como as hipóteses para o tratamento de dados (art. 7º), os princípios gerais (art. 6º), os direitos do titular, as responsabilidades dos agentes de tratamento (artigos 37 e seguintes), além das sanções cabíveis por violação às disposições. A intenção da administração pública é a vigilância dos dados pessoais para a execução de políticas públicas previstas em leis, que inclusive é hipótese de tratamento prevista no artigo 7º, III, da LGPD. No entanto, a Autoridade Nacional de Proteção de Dados (ANPD) (artigo 55-A da Lei nº 13.709, de 2018), ente responsável pela centralização das informações e controle, na data da MP, não estava operando, deixando uma lacuna para uma potencial violação ao direito fundamental da privacidade pela violação da autodeterminação informativa dos cidadãos pelo aparato estatal, como asseverou Danilo Doneda[8]:

> [...] a Autoridade Nacional de Proteção de dados poderia, neste contexto, desempenhar papel fundamental, ao estabelecer diretrizes, esclarecer limites e, em sua atuação geral, favorecer a utilização de dados pessoais neste contexto ao mesmo tempo em que estabelece limites e salvaguardas de forma concreta e dinâmica.
> Lembrando que a LGPD, no que toca à sua criação, já se encontra em vigor, caracterizando justamente a mora e inação do Poder Executivo na criação de um órgão que, ainda que previamente à entrada em vigor da lei, já seria capaz de proporcionar um debate e direcionamento fundamentais neste momento. A omissão

[7] Cf. Ementa: MANDADO DE SEGURANÇA. Impetração contra ato do Governador do Estado de São Paulo, impugnando "ACORDO DE COOPERAÇÃO" celebrado com as operadoras Vivo, Claro, OI e TIM, para monitorar o isolamento durante a quarentena, devido a pandemia Covid 19. Uso de dados na forma anônima e agregada, tão só para apuraras regiões com maior movimentação de pessoas. Inexistência de violação à privacidade, locomoção ou intimidade. Ademais, o processo de exclusão do monitoramento, implicaria a identificação do impetrante, aí sim, resultado não desejado. Inteligência do Regulamento Sanitário Internacional, acordado na 58ª Assembleia Geral da OMS, em 23.05.05, incorporado ao ordenamento jurídico interno pelo Dec. nº 10.212/2020, Lei nº 13.979/2020 e art. 72, § 2º da Lei Geral de Telecomunicações. Precedentes do E. STJ. Denegada a ordem. 1. Trata-se de mandado de segurança preventivo (fls. 01/17) impetrado por CAIO JUNQUEIRA ZACHARIAS contra ato do Governador do Estado de São Paulo, impugnando "ACORDO DE COOPERAÇÃO" celebrado com as operadoras Vivo, Claro, OI e TIM, para monitorar o isolamento durante a quarentena com informações geradas a partir de dados de aparelhos, devido a pandemia Covid 19. In: São Paulo. Tribunal de Justiça. Órgão Especial. *Mandado de Segurança nº 2069736-76.2020.8.26.0000*. Relator Desembargador Evaristo dos Santos. DJ: 24.06.2020.

[8] Doneda, Danilo. *A proteção de dados em tempos de coronavírus*. In: Jota, Opinião e análise, 25 de março de 2020. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/a-protecao-de-dados-em-tempos-de-coronavirus-25032020. Acesso em: 03 de novembro de 2020.

> do poder público quanto à sua estruturação acaba por se acumular, portanto, a diversas outras que se fazem sentir de maneira particularmente clamorosa neste momento. (Doneda, 2020)

Pelo exposto, a questão central a ser enfrentada é que o tratamento de dados pela administração pública durante o estado de emergência em saúde pública deve ter a finalidade de preservação da coletividade e da vida (artigo 1º, § 1º, da Lei nº 13.979, de 2020, e artigo 1º, III, da Constituição Federal ). Além disso, ainda que exista inércia do Poder Executivo na operacionalização da ANPD, os princípios dispostos no artigo 6º da LGPD devem ser observados, o que não foi vislumbrado na MP nº 954, de 2020, conforme também informou a Ministra Rosa Weber em seu voto[9]:

> [...] Não se subestima a gravidade do cenário de urgência decorrente da crise sanitária nem a necessidade de formulação de políticas públicas que demandam dados específicos para o desenho dos diversos quadros de enfrentamento. O seu combate, todavia, não pode legitimar o atropelo de garantias fundamentais consagradas na Constituição.
>
> [...]a adequada tutela do direito à intimidade, privacidade e proteção de dados pessoais é estruturada pela característica da inviolabilidade. Vale dizer, uma vez afrontada a norma de proteção de tais direitos, o ressarcimento se apresenta como tutela insuficiente aos deveres de proteção. (STF, 2020)

Concomitantemente à declaração de inconstitucionalidade da Medida Provisória nº 954, de 2020, o Ministério da Saúde desenvolveu, entre março e julho de 2020, um aplicativo nos moldes das ferramentas digitais de Singapura e da Alemanha, conforme será analisado no próximo item.

## 4.2. Aplicativo Coronavírus-SUS do Ministério da Saúde

Em março de 2020, o Ministério da Saúde criou o aplicativo "Coronavírus-SUS". Inicialmente o aplicativo visava a conscientizar a população sobre a epidemia de Covid-19 no país, divulgando informações sobre os sintomas da doença, medidas de prevenção e indicação de mapas com as unidades de saúde próximas em caso de suspeita. Ocorre que, em julho de 2020, o Ministério da Saúde adotou o modelo de aplicativo baseado em *API Exposure Notification framework*[10], desenvolvido

[9] 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.

[10] Brasil. Ministério da Saúde**.** *Coronavírus-SUS: aplicativo alerta contatos próximos de pacientes com Covid-19*. Disponível em: https://www.gov.br/casacivil/pt-br/assuntos/noticias/2020/agosto/coronavirus-sus-aplicativo-alerta-contatos-proximos-de-pacientes-com-covid-19. Acesso em: 29 de outubro de 2020.

pelas companhias Apple e Google, isto é, a mesma ferramenta utilizada pelo Reino Unido, Alemanha e o Estado de Nova Iorque.

O aplicativo é voluntário e descentralizado, pois os dados são armazenados no próprio dispositivo móvel do usuário. Para mais, ele não coleta informações pessoais que poderiam identificar o titular, como nome, sobrenome data de nascimento, endereço, número de telefone e *e-mail*, bem como todos os dados são criptografados.

De acordo com as próprias informações de sua política de privacidade, o aplicativo não coleta dados de geolocalização, apenas envia sinais de *bluetooth* para reconhecimento de contatos próximos, durante um tempo mínimo de tempo, desde que os contatos possuam o aplicativo instalado durante 14 dias. Ou seja, caso um usuário tenha obtido teste positivo para Covid-19 e optou por alertar o aplicativo, todas as pessoas que tiveram contato próximo a ele nos últimos 14 dias serão notificadas.

A política de privacidade informa que as informações compartilhadas pelos titulares, como testes, nome, data de nascimento e dados de saúde não são divulgadas, pois esses dados são criptografados[11] e apenas chaves são disponibilizadas, mantendo os dados anonimizados, conforme trecho do documento:

> A Controladora fica autorizada a tomar decisões referentes ao tratamento e a realizar o tratamento dos seguintes dados pessoais do Titular:
> Chave identificadora do telefone móvel;
> Além disso, a Controladora fica autorizada a tomar decisões referentes ao tratamento e a realizar o tratamento da identificação através de chaves privadas, fornecidas pela Apple e / ou Google, impessoais, fornecidas pelas empresas mencionadas, com a intenção de obter a monitoração e presença junto a outras pessoas que, poderiam estar contaminadas ou serem contaminadas em momentos de aproximação. Como por exemplo, descobrir que está contaminado e o Controlador poder contactar com os equipamentos que estiveram próximos ao usuário[12]. (Brasil, 2020)

[11] Brasil. Ministério da saúde**.** *Aplicativo Coronavírus-SUS vai alertar contatos próximos de pacientes com Covid-19*. Disponível em: https://web.archive.org/web/20200919141547/https://www.saude.gov.br/noticias/agencia-saude/47292-aplicativo-coronavirus-sus-vai-alertar-contatos-proximos-de-pacientes-com-covid-19. Acesso em: 29 de outubro de 2020.

[12] Brasil. Valida Coronavírus-Sus. Políticas de Privacidade. *Termo de Consentimento para Tratamento de Dados*. Disponível em: https://validacovid.saude.gov.br/politica-privacidade. Acesso em: 29 de outubro de 2020.

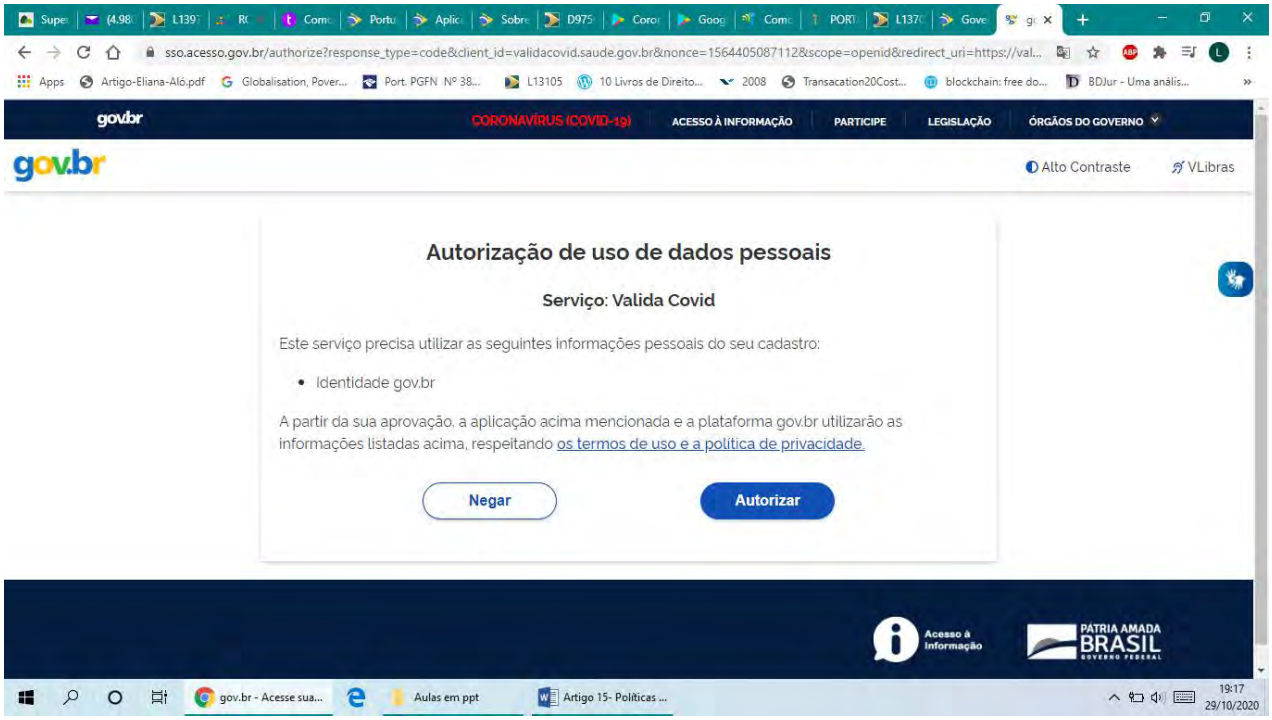
Em um primeiro momento, o tratamento de dados com a ferramenta API desenvolvida pela Apple e Google é eficiente porque utiliza apenas bluetooth e notificações de exposição sem identificar diretamente o usuário e, consequentemente, não caracteriza descumprimento ao direito de proteção de dados, nos termos da LGPD notadamente dos Arts. 11 e 12. No entanto, a disponibilização dos dados pelo próprio usuário pode gerar um possível vazamento e há um descompasso entre as informações vinculadas nas políticas de privacidade para uso do Coronavírus-SUS e o compartilhamento dos dados no aplicativo, não obstante ele ocorra com o consentimento do titular.

Sucede que, ao compartilhar um teste positivo no aplicativo, o usuário deve validá-lo no portal do Governo Federal ("gov.br"), o qual realizará uma pesquisa no banco de dados do Ministério da Saúde. Esse banco de dados é obtido por meio do programa "e-SUS Notifica". Nesse sentido, a Portaria nº 464, de 20 de maio de 2020, do Ministério da Saúde, estabelece no art. 1º, parágrafo único, o compartilhamento dos resultados dos testes obtidos nas unidades básicas de saúde do Sistema Único de Saúde[13]. Logo, verifica-se que há tratamento de dados pessoais não anonimizados, ou exposição de dados identificadores do titular.

Entende-se que esse processo de acesso de dados por meio do "gov.br" pode gerar uma incompatibilidade com os direitos do titular de dados (art. 9º da LGPD), pois existe a expressa divulgação no aplicativo de que apenas as chaves criptografadas do celular serão armazenadas. A título de visualização, a figura a seguir demonstra como os dados são coletados:

[13] Brasil. Ministério da Saúde**.** *Portaria nº 464, de 20 de maio de 2020*. Disponível em: https://www.in.gov.br/en/web/dou/-/portaria-n-464-de-20-de-maio-de-2020-258043581#:~:text=Inclui%20exames%20para%20o%20diagn%C3%B3stico,%C3%9Anico%20de%20Sa%C3%BAde%20(SUS). Acesso em: 29 de outubro de 2020.

**Figura 2 – Mensagem do aplicativo Coronavírus-SUS para utilização de identidade**




Fonte: Brasil, Governo Federal, 2020[14].

Analisou-se que a eficácia do dispositivo é duvidosa, pois não é possível a inclusão manual dos resultados dos testes pelos usuários, apenas mediante sincronização com dados do Ministério da Saúde. Tal situação gera grande burocracia e entraves sobre a acurácia das informações.

Não há divulgação do *site* do Ministério da Saúde sobre as estatísticas de *downloads* do aplicativo, o que representa falta de transparência do órgão. Todavia, em agosto de 2020, o órgão divulgou que 10 milhões de pessoas o adquiriram[15], correspondendo a 4% da população brasileira, demonstrando baixa adesão ao aplicativo que depende de informações voluntárias para plena eficácia.

## 4.3. Quadro comparativo entre políticas de contact tracing

Considerando a investigação realizada nas seções anteriores relativa às políticas de *contact tracing* e ferramentas digitais realizadas pelas jurisdições da Alemanha, Reino Unido, EUA, Singapura e a análise crítica do aplicativo Coronavírus-SUS, é possível realizar a comparação resumidamente com a seguinte figura:

[14] Brasil. Governo Federal. *Coronavírus – SUS App*. Disponível em: https://www.gov.br/pt-br/apps/coronavirus-sus. Acesso em: 29 de outubro de 2020.

[15] Brasil. Ministério da Saúde. *Coronavírus-SUS*: aplicativo alerta contatos próximos de pacientes com Covid-19. Disponível em: https://www.gov.br/casacivil/pt-br/assuntos/noticias/2020/agosto/coronavirus-sus-aplicativo-alerta-contatos-proximos-de-pacientes-com-covid-19. Acesso em: 29 de outubro de 2020.

## Figura 3 – Tabela comparativa entre os aplicativos digitais de *contact tracing*

| **Países - Comparativo** | **Alemanha/EU** | **Reino Unido** | **Estados Unidos da América** | **Singapura** | **Brasil** |
|---|---|---|---|---|---|
| Aplicativo | Corona Warn-App | NHS Covid-19 App | N/A, exceto no Estado de Nova Iorque (Covid Alert NY) | TraceTogether e Safe Entry | Coronavírus-SUS |
| Data de implementação | Julho de 2020 | Setembro de 2020 | Outubro de 2020 | Março de 2020 | O app foi criado em Março de 2020, mas a funcionalidade de *contact tracing* em julho de 2020. |
| Tecnologias utilizadas | *Bluetooth* com objetivo de notificação a exposição (API Exposure Notification framework) | *Bluetooth* com objetivo de notificação a exposição (API Exposure Notification framework) | *Bluetooth* com objetivo de notificação a exposição (API Exposure Notification framework) | *Bluetooth*, GPS, *Check-in* e *tokens* com objetivo de rastreamento de dados (Digital Contact Tracing) | *Bluetooth* com objetivo de notificação a exposição (API Exposure Notification Framework) |
| Armazenamento de dados | Descentralizado e pseudoanonimizado | Descentralizado e pseudoanonimizado | Descentralizado e pseudoanonimizado | Descentralizado e pseudoanonimizado. No entanto, em caso de teste positivo, o Ministério da Saúde terá acesso aos dados pessoais para realização de *contact tracing*. | Descentralizado. No entanto, no Brasil, ocorre a validação dos dados por *e-mail* do e-SUS, gerando a centralização dos testes na base de dados do Ministério da Saúde. |
| Participação dos titulares de dados (Voluntária ou Mandatória) | Voluntário | Voluntário | Voluntário | Voluntário em relação ao TraceTogether e Mandatório para Safe Entry. | Voluntário |

| **Países - Comparativo** | **Alemanha/EU** | **Reino Unido** | **Estados Unidos da América** | **Singapura** | **Brasil** |
|---|---|---|---|---|---|
| Há regulação/ normas próprias para rastreamento de dados por aplicativos durante a pandemia? | Sim, baseado nas normas da EU, Decisão (EU) nº 2020/1023 e o código de conduta "Mobile Applications to support contact tracing in the Eu´s fight against Covid-19" | Sim, foi realizada Análise de Impacto de Proteção de Dados (Data protection impact assessment) sobre o aplicativo. | Não | Não, mas o Infectious Disease Act de 1976 prevê a possibilidade de qualquer política de *contact tracing,* para mitigação das epidemias. | Não, mas a Lei nº 13.979, de 2020, prevê o uso de dados entre órgãos públicos para mitigação de Covid-19 |
| Há violação à norma geral de proteção de dados no país? | Não, os aplicativos foram criados com base GDPR e na Lei Geral de Proteção de Dados alemã de 2017 (Bundesdatenschutzgesetz) | Não, os aplicativos foram criados com base na Lei Geral de Proteção de Dados do Reino Unido de 2018 | Não. No caso de Nova Iorque, existe o Personal Privacy Protection Law. | Não, em Singapura há a Lei Geral de Proteção (Personal Data Protection Act) de Dados de 2012. | Indeterminado. No Brasil, existe a LGPD que dispõe sobre o tratamento de dados pessoais. No entanto, pela investigação, há transferência de dados pessoais sensíveis ao Ministério da Saúde que não consta na política de privacidade. |
| Adesão da população | 18 milhões de *downloads* (23% da população) entre julho e setembro de 2020) | 19 milhões de *downloads* (28% da população) entre Setembro e Outubro de 2020 | Não houve tempo hábil para avaliar estatisticamente. | 2,5 milhões de *downloads* (45% da população) entre março e outubro de 2020. | 10.000.000 de *downloads* (4% da população), entre março e agosto de 2020. |

Fonte: Elaboração própria, com base em Brasil, Ministério da Saúde, 2020.

Ante o exposto, inferiu-se que as economias estudadas desenvolveram os aplicativos de *contact tracing* digital em consonância com as suas normas pátrias sobre proteção de dados. Destarte, considerando que todos os aplicativos investigados são baixados mediante consentimento do usuário, a proteção de dados dos titulares de dados foi preservada nesse primeiro ponto, sobretudo em consideração ao *design* e estrutura dos aplicativos. Entretanto, a utilização dos aplicativos é voluntária e a eficácia da notificação de contágio depende do compartilhamento de testes e ativação de rastreio pelos titulares.

Desse modo, a maior ou menor adesão dos aplicativos de *contact tracing* pela população não ocorre pelo cumprimento das normas de proteção de dados, mas pelas políticas públicas conexas. Por conseguinte, o próximo item versará sobre proposições de políticas públicas para incentivo e expansão do uso dessas ferramentas no Brasil.

## 4.4. Proposições para as políticas de rastreamento de dados no Brasil

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 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.

Os dados pessoais, em momentos de emergência pública, notadamente de saúde, são fundamentais para compreensão e desenvolvimento das políticas públicas, pois são evidências fáticas e científicas para a tomada de decisões. Portanto, a LGPD não significa um empecilho a tais políticas, mas uma norma de incentivo, balizadora das ações da administração pública para que não ocorram violações aos direitos individuais dos cidadãos, na explicação de Danilo Doneda:

> Em uma crise aguda como a da atual pandemia do Covid-19, os dados pessoais são elementos essenciais para modelar e executar políticas públicas de contenção e controle do vírus, bem como para tornar possível que a pesquisa científica proporcione os melhores resultados possíveis no menor período de tempo. Ao mesmo tempo, o papel das legislações de proteção de dados na proteção de liberdades individuais e coletivas ganha relevância fundamental, diante do risco de que novos usos de dados derivem para interesses não relacionados ao combate à doença[16]. (DONEDA, 2020)

[16] DONEDA, Danilo. Idem, 2020. sp.

A segunda proposição seria relativa à implementação de ferramentas de rastreamento, operação, uso ou tratamento de dados pessoais, 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*[17]), as ferramentas devem cumprir os princípios do tratamento de dados, como a finalidade específica, a adequação, a necessidade e segurança.[18]

Por isso, não obstante o consentimento ou voluntariado por parte da população seja importante para adesão dos titulares, analisou-se que, caso exista uma emergência pública, os dados poderão ser tratados pela administração pública "para a proteção da vida ou da incolumidade física do titular ou de terceiro" (art. 7º, VII da LGPD).

A ANPD[19], 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 operacionalização da ANPD pelo poder público é essencial e a terceira recomendação, pois a autoridade poderia fazer um papel de incentivo a tais políticas, colaborando com órgãos e entes da administração pública, 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 adotadas para o rastreamento de dados, verificou-se que há baixa adesão social. Dessa forma, são necessárias medidas de governança

[17] Cf. É uma metodologia na qual a proteção de dados é pensada desde a concepção de sistemas, práticas comerciais, projetos, produtos ou qualquer outra solução que envolva o manuseio de dados pessoais. In: Cavoukian, Ann. *Privacy by Design*. The 7 Foundational Principles. Informational and Privacy Commissioner of Ontario. Ontario. Janeiro. 2011. Disponível em: https://www.ipc.on.ca/wp-content/uploads/resources/7foundationalprinciples.pdf. Acesso em: 11 de setembro de 2020.

[18] Neste sentido, Ronaldo Lemos asseverou que: "Em outras palavras, os dados autorizados mesmo em emergências devem ser usados apenas para essa exclusiva finalidade. Tão logo a emergência seja superada, tais dados colhidos e usados em situação excepcional devem ser apagados, e a prática de uso dos dados sem consentimento, descontinuada. Além disso, técnicas como anonimização e agregação de dados devem ser aplicadas sempre que possível". In: Lemos, Ronaldo. A proteção de dados e a Covid-19. In: *Folha de São Paulo*, 30 de março de 2020. Disponível em: https://www1.folha.uol.com.br/colunas/ronaldolemos/2020/03/a-protecao-de-dados-e-a-covid-19.shtml. Acesso em: 04 de novembro de 2020.

[19] Nesse sentido, Flávio Garcia Cabral disserta: "a ANPD, uma que seu papel regulatório será fundamental para esclarecer os termos da legislação, bem como conferir operacionalidade a ela, além da circunstância de que sua competência sancionatória, a depender de como for exercida, permitirá a efetividade da LGPD sem que haja desrespeito aos direitos e garantias fundamentais. De igual maneira, a independência técnica financeira política e administrativa será pressuposto fundante para a efetiva proteção de dados no Brasil". Cabral, Flávio Garcia. O princípio da boa administração pública e a LGPD. In: Pozzo, Augusto Neves dal; Martins, Ricardo Marcondes. *LGPD e Administração Pública* – Uma análise ampla dos impactos. São Paulo: Thomson Reuters Brasil, 2020, p. 75 e 76.

pública[20] 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. Nesse sentido afirma Layon Cezar:

> [... a comunicação pública atualmente tem um papel central para garantir tanto a possibilidade de troca quanto o engajamento social nos espaços de deliberação pública. [...]
> Por meio da comunicação pública, as campanhas e estratégias de marketing tornam-se conhecidas pelos cidadãos, podendo esses participarem até mesmo de sua construção por meio de feedbacks contínuos.[21] (Cezar, 2019)

Finalmente, última proposição é relativa à criação ou à atualização de uma agenda executiva que priorize a introdução de novas tecnologias e digitalização[22] para os órgãos e entidades da administração pública. Ressalte-se que o processo de digitalização deve ser aplicado conjuntamente com medidas de segurança da informação aptas a proteger os dados pessoais e evitar incidentes de vazamento de dados.

A implementação de processos de digitalização e avanço tecnológico 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.

[20] Saravia, Enrique. Governança social no Brasil contemporâneo. In: *Revista Governança Social* – IGS, Belo Horizonte, ano 3, n. 7, p. 21, dez. 2009/mar. 2010.

[21] Cezar, Layon Carlos. *Comunicação e marketing no setor público*: diferentes abordagens para a realidade brasileira. Brasília: Enap, 2019. p. 20.

[22] 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.

# 5. Conclusão

## 5. Conclusão

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*, denominado de rastreamento de contatos, como 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. Contudo, com a propagação da datificação na sociedade pós-industrial e das análises de big data, a operação de *contact tracing* passou a ser realizada por meio de tratamento de dados pessoais, por intermédio

de dispositivos em celulares móveis, que realizam 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 de comparativo 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 de lei ou desconfiança 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 que evidencia o direito à proteção 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 *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. 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 anominização 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 LPGD e seus princípios, bem como não apresentava qualquer caráter de finalidade específica, transparência e proporcionalidade. Por esse motivo, foi considerada inconstitucional pelo Supremo Tribunal Federal na Ação Direta de Inconstitucionalidade nº 6387, de 2020.

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 pessoais 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.

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 edição de políticas, ou seja, de avaliação do contexto atual, para estimar as providências cabíveis a serem adotadas com base na realidade coletiva dos indivíduos e empresas, 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 são meras ferramentas tecnológicas; portanto, cabe à administração pública criar mecanismos de adesão da população às políticas, com maior transparência e respeito aos direitos fundamentais.

## REFERÊNCIAS


ALEMANHA. *Corona Warn- App*. Open Source Project. Disponível em: https://www.coronawarn.app/en/. Acesso em: 08 de outubro de 2020.

ALEMANHA. Instituto Robert Koch. *Principais dados sobre o Corona Warn-App*. Disponível em: https://www.coronawarn.app/en/. Acesso em: 08 de outubro de 2020.

ALMEIDA, Bethania *et al*. Preservação da privacidade no enfrentamento da Covid-19: dados pessoais e a pandemia global. In: *Ciência & Saúde Coletiva*, 25, 2020. Disponível em: https://www.scielo.br/pdf/csc/v25s1/1413-8123-csc-25-s1-2487.pdf. Acesso em: 14 de julho de 2020.

BIONI, Bruno R. *Proteção de dados pessoais*: a função e os limites do consentimento. Rio de Janeiro: Forense, 2019.

BOYNE, Shawn Marie. Data protection in the United States. In: *The american journal of comparative Law*, v. 66. Oxford University Press, 2018.

BRASIL. *Constituição Federal*. Disponível em: http://www.planalto.gov.br/ccivil_03/Constituicao/Constituicao.htm. Acesso em: 03 de abril de 2019.

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.

BRASIL. *Exposição de motivos da Medida Provisória nº 954, de 17 de abril de 2020*. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/mpv/mpv954.htm. Acesso em: 20 de outubro de 2020.

BRASIL. Governo Federal. *Coronavírus – SUS App*. Disponível em: https://www.gov.br/pt-br/apps/coronavirus-sus. Acesso em: 29 de outubro de 2020.

BRASIL. *Lei nº 13.709, de 14 de agosto de 2018*. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 27 de outubro de 2020.

BRASIL. *Lei nº 13.979, de 6 de fevereiro de 2020*. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/lei/l13979.htm. Acesso em: 22 de novembro de 2020.

BRASIL. Ministério da saúde. *Aplicativo Coronavírus-SUS vai alertar contatos próximos de pacientes com Covid-19*. Disponível em: https://web.archive.org/web/20200919141547/https://www.saude.gov.br/noticias/agencia-saude/47292-aplicativo-coronavirus-sus-vai-alertar-contatos-proximos-de-pacientes-com-covid-19. Acesso em: 29 de outubro de 2020.

BRASIL. Ministério da Saúde**.** *Coronavírus-SUS: aplicativo alerta contatos próximos de pacientes com Covid-19*. Disponível em: https://www.gov.br/casacivil/pt-br/assuntos/noticias/2020/agosto/coronavirus-sus-aplicativo-alerta-contatos-proximos-de-pacientes-com-covid-19. Acesso em: 29 de outubro de 2020.

Brasil. Ministério da Saúde**.** *Portaria nº 464, de 20 de maio de 2020*. Disponível em: https://www.in.gov.br/en/web/dou/-/portaria-n-464-de-20-de-maio-de-2020-258043581#:~:text=Inclui%20exames%20para%20o%20diagn%C3%B3stico,%C3%9Anico%20de%20Sa%C3%BAde%20(SUS). Acesso em: 29 de outubro de 2020.

Brasil. Valida Coronavírus-SUS. Políticas de privacidade. *Termo de Consentimento para Tratamento de Dados*. Disponível em: https://validacovid.saude.gov.br/politica-privacidade. Acesso em: 29 de outubro de 2020.

Bucar, Daniel; Oliveira, Rafael Carvalho Rezende. A Lei Geral de Proteção de Dados e a Administração Pública. In: Pozzo, Augusto Neves dal; Martins, Ricardo Marcondes. *LGPD e Administração Pública* – Uma análise ampla dos impactos. São Paulo: Thomson Reuters Brasil, 2020.

Cabral, Flávio Garcia. O princípio da boa administração pública e a LGPD. In: Pozzo, Augusto Neves dal; Martins, Ricardo Marcondes. *LGPD e Administração Pública* – Uma análise ampla dos impactos. São Paulo: Thomson Reuters Brasil, 2020.

Cavoukian, Ann. *Privacy by Design*. The 7 foundational principles. Informational and Privacy Commissioner of Ontario. Ontario. Janeiro. 2011. Disponível em: https://www.ipc.on.ca/wp-content/uploads/resources/7foundationalprinciples.pdf. Acesso em: 11 de setembro de 2020.

Center For Public Impact. BCG Foundation. *Building a digital government in Singapore*. 12 de abril de 2016. Disponível em: https://www.centreforpublicimpact.org/case-study/building-digital-government-singapore/. Acesso em: 04 de novembro de 2020.

Cezar, Layon Carlos. *Comunicação e marketing no setor público*: diferentes abordagens para a realidade brasileira. Brasília: Enap, 2019.

Cramer, Stella *et al*. *Contract tracing apps in Singapore*. In: Norton Rose Fulbright, 11 de junho de 2020. Disponível em: https://www.nortonrosefulbright.com/-/media/files/nrf/nrfweb/contact-tracing/singapore-contact-tracing.pdf?la=en-sg&revision=. Acesso em: 28 de setembro de 2020.

Doneda, Danilo. A proteção de dados em tempos de coronavírus. In: *Jota, Opinião e análise*, 25 de março de 2020. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/a-protecao-de-dados-em-tempos-de-coronavirus-25032020. Acesso em: 03 de novembro de 2020.

Doneda, Danilo. *Da privacidade à proteção de dados*. Rio de Janeiro: Renovar, 2006.

Estados Unidos. Estado de Nova Iorque. *Covid Alert NY*: what you need to know. Disponível em: https://coronavirus.health.ny.gov/covid-alert-ny-what-you-need-know. Acesso em: 13 de outubro de 2020.

Estados Unidos da América. Califórnia legislative information. Civil Code. *California Consumer Privacy Act of 2018*. Disponível em: http://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5. Acesso em: 13 de outubro de 2020.

Estados Unidos da América. New York State Senate. *Personal privacy protection law*. Disponível em: https://www.nysenate.gov/legislation/laws/PBO/93. Acesso em: 14 de abril de 2019.

Harari, Yuval N. Sapiens. *Uma breve história da humanidade*. 48 ed. Porto Alegre: L&PM, 2019.

IBM – Estados Unidos. *Big data analytics*. Disponível em: https://www.ibm.com/analytics/hadoop/big-data-analytics. Acesso em: 10 de junho de 2020.

Kahn, Jeffrey (Editor). Digital contact tracing for pandemic response. In: *Johns Hopkins Project on Ethics and Governance of Digital Contact Tracing Technologies*. Baltimore: Johns Hopkins University Press, 2020.

Kalyvas, James R.; Albertson, David R. A Big Data primer for executives. In: Kalyvas, James R; Overly, Michael R. (Coord). *Big Data*: business and legal guide (e-book). Boca Raton. CRC Press. 2015.

Lasswell, Harold. D. Politics: who gets what, when, how. In: *The political writings of Harold D. Lasswell*. Free press, Glencoe, Illinois, 1951.

Lemos, Ronaldo. A proteção de dados e a Covid-19. In: *Folha de São Paulo*, 30 de março de 2020. Disponível em: https://www1.folha.uol.com.br/colunas/ronaldolemos/2020/03/a-protecao-de-dados-e-a-covid-19.shtml. Acesso em: 04 de novembro de 2020.

Martins, Guilherme Magalhães; Longhi, João Victor Rozatti; Faleiros Junior, José Luiza de Moura. A pandemia da covid-19 , o profiling e a Lei Geral de Proteção de Dados. In: *Portal Migalhas*, Abril de 2020. Disponível em: https://www.migalhas.com.br/depeso/325618/a-pandemia-da-covid-19-o-profiling-e-a-lei-geral-de-protecao-de-dados. Acesso em: 21 de setembro de 2020.

Menezes Neto, Elias Jacob de; Morais, Jose Luis Bolzan de; Bezerra, Tiago José de Souza Lima. O Projeto de Lei de proteção de dados pessoais (PL5276/2016) no mundo do big data: o fenômeno da dataveillance em relação à utilização de metadados e seu impacto nos direitos humanos. In: *Revista Brasileira de Políticas Públicas*, v. 7, n. 3, dez. 2017. Uniceub.

Naumann, Felix. Data profiling revisited. *Acm SIGMOD Record*. Quatar Computing Research Institute, Doha, 2014.

OCDE. *Guidelines governing the protection of privacy and transborder flows of personal data*, de 11 de julho de 2013. Disponível em: http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf. Acesso em: 13 de abril de 2020.

O Globo. G1. Ciberataques em larga escala atingem empresas no mundo e afetam Brasil. Recurso eletrônico. Disponível em: <https://g1.globo.com/tecnologia/noticia/hospitais-publicos-na-inglaterra-sao-alvo-cyber-ataques-em-larga-escala.ghtml> Acesso em: 27 de outubro de 2020.

O Globo. São Francisco. Dados de 87 milhões foram usados pela Cambridge Analytica, diz Facebook. 04 de abril de 2018. Recurso eletrônico. Disponível em: https://oglobo.globo.com/economia/dados-de-87-milhoes-foram-usados-pela-cambridge-analytica-diz-facebook-22556605. Acesso em: 27 de outubro de 2020.

OMS – Organização Mundial da Saúde. *Emergencies preparedness response*, 24 de fevereiro de 2010. Recurso eletrônico. Disponível em: https://www.who.int/csr/disease/swineflu/frequently_asked_questions/pandemic/en/. Acesso em: 17 de março de 2020.

OMS – Organização Mundial da Saúde. *Q&A*: contact tracing for Covid-19. Disponível em: https://www.who.int/emergencies/diseases/novel-coronavirus-2019/question-and-answers-hub/q-a-detail/q-a-contact-tracing-for-covid-19. Acesso em: 22 de setembro de 2020.

OMS – Organização Mundial da Saúde. WHO announces Covid-19 outbreak a pandemic. In: *Coronavirus disease outbreak*, 12 de março de 2020. Recurso eletrônico. Disponível em: http://www.euro.who.int/en/health-topics/health-emergencies/coronavirus-covid-19/news/news/2020/3/who-announces-covid-19-outbreak-a-pandemic. Acesso em: 17 de março de 2020.

OMS – Organização Mundial da Saúde. *WHO Coronavirus Disease (Covid-19) Dashboard*, atualizado em 08 de outubro de 2020. Disponível em: https://covid19.who.int/table. Acesso em: 08 de outubro de 2020.

Perrigo, Billy. *Us States are rolling out Covid-19 contact tracing apps*. Months of evidence from Europe shows they ´re no silver bullet, 09 de outubro de 2020. In: *Time*. Disponível em: https://time.com/5898559/covid-19-contact-tracing-apps-privacy/. Acesso em: 13 de outubro de 2020.

Pinheiro, Patricia Peck. *Proteção de dados pessoais*. Comentários à Lei nº 13.709/2018 (LGPD). São Paulo. Saraiva. 2018.

Reino Unido. *Data protection act*, de 23 de maio de 2018. Disponível em: https://www.legislation.gov.uk/ukpga/2018/12/introduction/enacted. Acesso em: 04 de novembro de 2020. REINO UNIDO. *NHS Covid-19 APP*. Disponível em: https://www.covid19.nhs.uk/privacy-and-data/you-choose-what-data-you-share.html. Acesso em: 12 de outubro de 2020.

RITZER, Cristoph *et al*. Contact tracing apps in Germany. In: *Norton Rose Fulbright*, 23 de junho de 2020. Disponível em: https://www.nortonrosefulbright.com/-/media/files/nrf/nrfweb/contact-tracing/germany-contact-tracing.pdf?revision=ed379c1d-011d-4cd8-8e65-02c2664e2ba9. Acesso em: 05 de novembro de 2020.

SARAVIA, Enrique. Governança social no Brasil contemporâneo. In: *Revista Governança Social* – IGS, Belo Horizonte, ano 3, n. 7, dez. 2009/mar. 2010.

SARAVIA, Enrique. Política Pública: introdução à teoria da política pública. In: SARAVIA, Enrique; FERRAREZI, Elisabete. *Políticas Públicas*; coletânea, v.1, Brasília, ENAP, 2006.

SÃO PAULO. Tribunal de Justiça. Órgão Especial. *Mandado de Segurança nº 2069736-76.2020.8.26.0000*. Relator Desembargador Evaristo dos Santos. DJ: 24.06.2020.

SILVA, José Afonso da. *Curso de Direito Constitucional Positivo*. 35. ed. São Paulo: Malheiros, 2012.

SINGAPURA. *Covid-19 (Temporary measures act)*. Disponível em: https://sso.agc.gov.sg/Act/COVID19TMA2020. Acesso em: 28 de setembro de 2020.

SINGAPURA. *Infectious diseases act*. Disponível em: https://sso.agc.gov.sg/Act/IDA1976#pr19A-. Acesso em: 28 de setembro de 2020.

SINGAPURA, Ministério da Saúde. *Covid-19 Interactive Situation Report*. Disponível em: https://www.moh.gov.sg/covid-19/situation-report. Acesso em: 28 de setembro de 2020.

SINGAPURA. *Personal Data Protection Act, 2012*. Disponível em: https://sso.agc.gov.sg/Act/PDPA2012#pr44-. Acesso em: 28 de setembro de 2020.

SINGAPURA. *TraceTogether App*. Disponível em: https://www.tracetogether.gov.sg/. Acesso em: 28 de setembro de 2020.

SINGAPURA. *TraceTogether Privacy Safeguards*. Disponível em: https://www.tracetogether.gov.sg/common/privacystatement. Acesso em: 28 de setembro de 2020.

SINGER, Natasha; SANG-HUN, Choe. As coronavirus surveillance escalates, personal privacy plummets. In: *The New York Times*, 23 de março de 2020. Disponível em: https://www.nytimes.com/2020/03/23/technology/coronavirus-surveillance-tracking-privacy.html. Acesso em: 24 de setembro de 2020.

SOUZA, Celina. Políticas Públicas: uma revisão da literatura. In: *Revista Sociologias*, Porto Alegre, junho, 2006.

TAN, Kevin Y. L. Singapore's Regulatory Response to Covid-19. In: *The Regulatory Review*. Penn Programme of Regulation, jun. 2020. Disponível em: https://www.theregreview.org/2020/06/15/tan-singapore-regulatory-response-covid-19/. Acesso em: 28 de setembro de 2020.

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.

União Europeia. Centro Europeu de Prevenção e Controle de Doenças. *Contact tracing for Covid-19*: current evidence, options for scale-up and an assessment of resources needed. Disponível em: https://www.ecdc.europa.eu/sites/default/files/documents/COVID-19-Contract-tracing-scale-up.pdf. Acesso em: 14 de julho de 2020.

União Europeia. *Counsel decision (EU) 2020/135 of 30 January 2020*. Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32020D0135. Acesso em: 04 de novembro de 2020.

União Europeia. *Decisão de execução (UE) 2020/1023 da Comissão*, de 15 de julho de 2020. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32020D1023&from=EN. Acesso em: 08 de outubro de 2020.

União Europeia. European Data Protection Board. *Statement on the processing of personal data in the context of the Covid-19 outbreak*, de 19 de março de 2020. Disponível em: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_statement_2020_processingpersonaldataandcovid-19_en.pdf. Acesso em: 08 de outubro de 2020.

União Europeia. *European proximity tracing*, de 02 de setembro de 2020. Disponível em: https://ec.europa.eu/health/sites/health/files/ehealth/docs/mobileapps_interop_architecture_en.pdf. Acesso em: 08 de outubro de 2020.

União Europeia. *Mobile Applications to support contact tracing in the Eu´s fight against Covid-19*, de 15 de abril de 2020. Disponível em: https://ec.europa.eu/health/sites/health/files/ehealth/docs/covid-19_apps_en.pdf. Acesso em: 08 de outubro de 2020.

União Europeia. *Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho*, de 27 de abril de 2016. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:31995L0046&from=PT. Acesso em: 08 de outubro de 2020.

União Europeia. *Tratado sobre o funcionamento da União Europeia*. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:12012E/TXT&from=PT. Acesso em: 08 de outubro de 2020.

Enap

# Cadernos

**Caderno nº 86**

***Coleção:*** *Covid-19 Fast Track*