COVID-19: A NECESSIDADE DE DISCIPLINA ADEQUADA À PROTEÇÃO DE DADOS SENSÍVEIS NO BRASIL

Ivo Corrêa

Mestre em Administração Pública pela Universidade de Harvard (EUA). Professor do Insper. Sócio do XVV Advogados.

Felipe de Paula

Doutor em Direito pela Universidade de São Paulo – USP e pela Universidade de Leiden (Holanda). Sócio do XVV Advogados.

Beatriz Bellintani

Bacharela em Direito pela Universidade de São Paulo – USP. Advogada do XVV Advogados.

Resumo: O presente artigo oferece uma reflexão sobre os desafios da implementação de uma disciplina adequada de proteção de dados sensíveis no Brasil. Desafios estes que, embora já existissem antes, foram colocados em evidência no contexto da crise atual, tendo em vista a proliferação de ferramentas de enfrentamento à pandemia de COVID-19 que utilizam tecnologias envolvendo o tratamento de dados pessoais. Para tanto, o artigo se propõe a analisar dois pontos essenciais da disciplina legal de dados sensíveis da Lei Geral de Proteção de Dados, a categoria de dados biométricos e o consentimento como principal base legal para o tratamento de dados, explicitando a divergência entre os regimes europeu e brasileiro, bem como os desafios decorrentes do caminho traçado pelo legislador nacional.

Palavras-chave: LGPD; Dados pessoais sensíveis; dados biométricos; consentimento; pandemia; Covid-19; *contact tracing*.

I Introdução

A pandemia causada pela disseminação do vírus SARS-CoV-2 (COVID-19) é um desafio sanitário de escala global e sem precedentes nas últimas décadas. Até que seja desenvolvida uma vacina comprovadamente eficaz, o enfrentamento do vírus passa pela rápida identificação dos infectados, pelo oferecimento do

melhor tratamento possível e por iniciativas de contenção do seu alastramento via contato social. Tais ações são complementadas por intenso investimento em pesquisa para compreender o comportamento do vírus sob diferentes condições, fatores de risco que elevam a letalidade da doença e inúmeros outros aspectos epidemiológicos.

Nesse sentido, muitos países têm adotado estratégias de enfrentamento à pandemia que incluem a utilização de tecnologias digitais para monitorar e controlar sua propagação – aplicativos de celular, dispositivos conectados, ferramentas de geolocalização etc. Embora essas tecnologias possam agregar muito valor sob a ótica da saúde pública, sua utilização muitas vezes envolve o tratamento de dados pessoais - inclusive dos chamados dados pessoais sensíveis[1] – em larga escala, acarretando riscos à privacidade dos cidadãos e gerando preocupação entre grupos, organizações e organismos que atuam na área de proteção de dados.

Tal cenário fez com que o debate sobre o uso adequado de dados pessoais no contexto da pandemia se tornasse um item prioritário na agenda pública em todo mundo, destacando-se especialmente os dados pessoais sensíveis. No Brasil, contudo, essa discussão ocorre simultaneamente com outras de caráter mais básico, como a definição do próprio arcabouço jurídico que rege a proteção de dados entre nós.

Apenas em 17 de setembro de 2020, com a conversão da Medida Provisória nº 959/2020 na Lei nº 14.058/2020 temos, após meses de incerteza,[2] a plena vigência da LGPD.

Também apenas recentemente foi promulgado o Decreto nº 10.474/2020,[3] que aprova a Estrutura Regimental e o Quadro Demonstrativo dos Cargos em Comissão e das Funções de Confiança da Autoridade Nacional de Proteção de Dados (ANPD). Contudo, o presidente e demais membros do corpo diretivo da ANPD ainda não foram nomeados, de modo que o Decreto ainda não se encontra em vigor, conforme disposto em seu Art. 6º.

---

1 No âmbito da legislação nacional, dentre os dados pessoais sensíveis figuram precisamente os dados relativos à saúde, conforme disposto no Art. 5º inciso II da LGPD.

2 No início da pandemia de COVID-19 foi editada a Medida Provisória (MP nº 959/2020), prorrogando a entrada em vigor da LGPD para maio de 2021. Após mais de quatro meses de incerteza sobre o adiamento da sua entrada em vigor, com diversas propostas diferentes de datas, finalmente, em setembro, a MP nº 959 foi convertida na Lei nº 14.058/2020, após aprovação no Senado e sanção presidencial. Também foi promulgado o Decreto nº 10.474/2020 aprovando a estrutura regimental da Autoridade Nacional de Proteção de Dados.

Mais sobre as sucessivas alterações do prazo para entrada em vigor da LGPD em: https://www.jota.info/big-data-venia/lgpd-em-vigor-reviravolta-no-senado-alvoroco-nas-empresas-e-anpd-no-planalto-27082020. Último acesso em: 24 set. 2020; https://www1.folha.uol.com.br/mercado/2020/08/reviravolta-sobre-prazo-da-lei-de-protecao-de-dados-no-senado-surpreende-empresas.shtml. Último acesso em: 24 set. 2020.

3 Decreto disponível em: https://www.in.gov.br/en/web/dou/-/decreto-n-10.474-de-26-de-agosto-de-2020-274389226. Último acesso em: 24 set. 2020.

Ou seja, ainda não há uma Autoridade em funcionamento e capaz de orientar a implementação da LGPD, cumprindo o papel de liderar esse debate fundamental sobre o tratamento de dados pessoais para fins de saúde. Mesmo com a LGPD em vigor, temas essenciais para essa discussão continuam sem resposta e dependem de sua correta interpretação ou regulamentação.

É preciso, portanto, dar clareza aos pressupostos básicos do debate nacional, ou à ausência deles. Embora esse seja um campo vasto, pensando no contexto do uso de dados pessoais como insumo de plataformas voltadas ao enfrentamento da pandemia, destacamos a relevância de tratar especificamente de dados pessoais sensíveis. Entender como a legislação brasileira que acaba de entrar em vigor almeja proteger os dados pessoais sensíveis e avaliar a capacidade institucional para eventuais respostas precedem o debate que já ocorre no contexto da pandemia.

Em que pese a explícita inspiração da lei brasileira no Regulamento Geral de Proteção de Dados da União Europeia ("GDPR"), há diferenças relevantes entre os contextos europeu e brasileiro. Os distintos pressupostos fáticos, institucionais e legais reforçam a necessidade de reflexão sobre a efetiva disciplina jurídica da proteção de dados sensíveis no Brasil.

O presente artigo pretende contribuir com essa tarefa e se propõe a analisar dois pontos essenciais da disciplina de dados sensíveis que explicitam a divergência entre os regimes europeu e brasileiro, bem como os desafios decorrentes do caminho traçado pelo legislador nacional.

O texto está estruturado da seguinte forma. Primeiro, apresentaremos como a pandemia e as respostas tecnológicas que lhe foram ofertadas impactaram o debate sobre a proteção de dados sensíveis no mundo. Em seguida, trataremos de como esse debate se desenvolveu no contexto brasileiro, considerada a recente entrada em vigor da lei e a ausência de efetiva implementação da ANPD. Depois, serão apresentados contornos gerais da disciplina oferecida à proteção de dados pessoais sensíveis pela LGPD, com destaque para diferenças em relação ao GDPR. Por fim, nos aprofundamos nas diferenças entre GDPR e LGPD no que diz respeito a dois temas: (i) o tratamento de dados biométricos; e (ii) a noção de consentimento qualificado como base legal para o tratamento de dados sensíveis.

II A pandemia e o tratamento de dados pessoais sensíveis

Muitas são as tecnologias digitais e ferramentas tecnológicas mobilizadas durante a pandemia que utilizam intensamente o tratamento de dados pessoais. Dentre as inúmeras medidas adotadas internacionalmente, algumas têm se destacado por sua relevância nas estratégias sanitárias de enfrentamento do vírus

e concomitantemente pelas preocupações que ensejam quanto ao uso abusivo ou indevido de dados pessoais, tais como (i) tecnologias de monitoramento de pessoas infectadas e de rastreamento de suas interações sociais, com vistas a controlar a propagação do vírus; (ii) tecnologias de monitoramento dos deslocamentos dos indivíduos, cuja finalidade é acompanhar e avaliar as políticas de distanciamento social impostas em vários países; e (iii) ferramentas de geolocalização de pessoas infectadas ou de suas residências, que também buscam compreender os padrões geográficos de incidência e propagação do vírus.

Em particular, uma parcela significativa do debate acerca da proteção de dados pessoais em tempos de pandemia foi gerado pela utilização de técnicas de *contact tracing*, em especial por meio de dispositivos tecnológicos ou de aplicativos de celular.[4] O mapeamento das pessoas que interagiram com indivíduos infectados é prática consagrada para o controle de qualquer doença infecciosa.[5] A sua realização através de tecnologias digitais, no entanto, aumenta exponencialmente o potencial do controle exercido, elevando sua eficiência sanitária e os riscos associados ao uso indevido das informações coletadas.

II.1 A proliferação de plataformas de *contact tracing* em meio à pandemia ao redor do mundo

Aplicativos de *contact tracing* desenvolvidos e utilizados por governos de outros países deram ensejo a esse importante debate[6] – até o início de julho de 2020, mais de 170 milhões de pessoas ao redor do mundo já haviam instalado algum *app* com essa finalidade em seu aparelho celular.[7]

---

4 CIDRI NETO, Oscar Carlos. *O Tratamento de dados pessoais e sensíveis frente ao contact tracing durante o COVID-19*. Grupo de Estudos de Direito Autoral e Industrial da Universidade Federal do Paraná. Junho, 2020. Disponível em: https://www.gedai.com.br/o-tratamento-de-dados-pessoais-e-sensiveis-frente-ao-contact-tracing-durante-o-covid-19/. Último acesso em: 14 jul 2020.

5 *Idem*.
TSANG, Amanda. *Here are the contact tracing apps being deployed around the world*. IAAP – The International Association of Privacy Professionals. 28/04/2020. Disponível em: https://iapp.org/news/a/here-are-the-contact-tracing-apps-being-employed-around-the-world/. Último acesso em: 14 jul. 2020.

6 *Idem*.
NORTON ROSE FULBRIGHT. *Contact tracing apps: a new world for data privacy*. Junho, 2020. Disponível em: https://www.nortonrosefulbright.com/en-sg/knowledge/publications/d7a9a296/contact-tracing-apps-a-new-world-for-data-privacy#Singapore. Último acesso em: 14 jul. 2020.
CHAVES, Luis Fernando Prado; VIDIGAL, Paulo. *Privacy implications of Coronavirus tracking mobile apps*. Disponível em: https://www.lexology.com/library/detail.aspx?g=498613c4-9587-4117-9ff2-de99d614ee99

7 MEDEIROS, Henrique. *Covid-19: 173 milhões de pessoas baixaram apps de rastreamento de contatos*. Mobile Time, 14/07/20. Disponível em: https://www.mobiletime.com.br/noticias/14/07/2020/covid-19-173-milhoes-de-pessoas-baixaram-apps-de-rastreio-de-contato/. Último acesso em: 16 jul. 2020.

Em março, por exemplo, o governo de Cingapura lançou o aplicativo chamado *Trace Together.* A partir do *login* individual, o aplicativo coleta o número de telefone e um ID aleatório anonimizado, mas não coleta dados de localização. Ele apenas capta sinais de *bluetooth* de proximidade entre celulares e, quando uma pessoa é diagnosticada com COVID-19, o Ministério da Saúde pode acessar os dados até então criptografados e notificar pessoas que tenham tido proximidade com o infectado. A plataforma ensejou diversas críticas e riscos à privacidade foram suscitados.[8]

Na Coreia do Sul também foram desenvolvidos dois aplicativos nesse sentido. Um deles, intitulado *Corona 100m*, foi desenvolvido pelo setor privado e alerta os usuários se eles chegam a um raio de até 100m de alguém diagnosticado com COVID-19. O aplicativo coleta dados como data do diagnóstico, nacionalidade, idade e gênero. Já o segundo aplicativo, *Corona Map*, traça as localizações de quem foi diagnosticado com COVID-19 para que outros possam evitá-las.

Por fim, vale citar o caso indiano, em especial pelas características do país que o aproximam do Brasil: sua numerosa população, sua grande extensão territorial e a ausência de uma legislação de proteção de dados em vigor.[9] Foi recentemente lançado o aplicativo de *contact tracing Aarogya Setu*, que angariou mais de 50 milhões de usuários em apenas 13 dias. Assim como o aplicativo de Cingapura, ele usa sinais de *bluetooth*, mas também usa dados de GPS e a coleta de informações dos usuários como nome, datas de nascimento e dados biométricos.

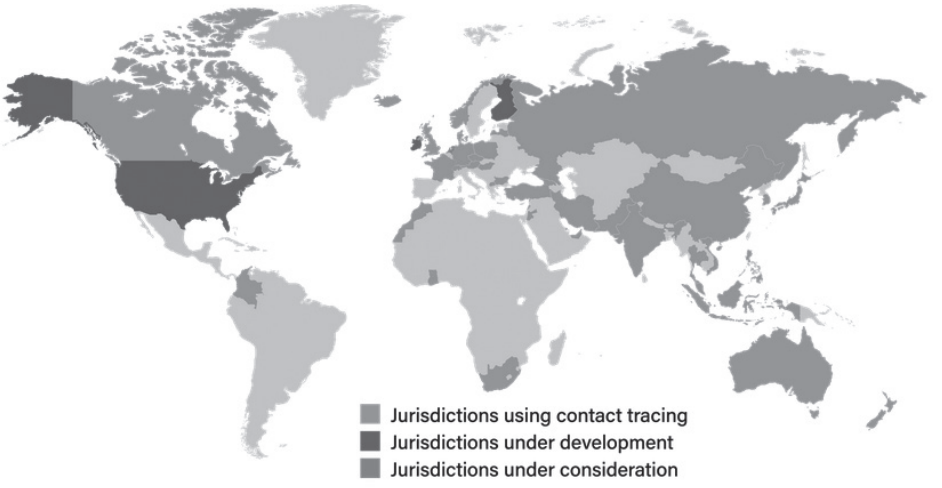
Contudo, diferentemente dos casos anteriores, a Índia ainda não possui uma legislação de proteção de dados em vigor. Por essa razão, mesmo que a política de privacidade do aplicativo tenha sido alterada para endereçar preocupações relativas à privacidade ao estabelecer, por exemplo, que o aplicativo usará IDs próprios para manter as informações anonimizadas e que os dados não serão utilizados por terceiros, a efetividade da fiscalização e do controle sobre isso é incerta, tendo em vista a ausência de uma autoridade específica e qualificada para tanto.

---

8 Mais sobre aplicativos de *tracing* em Cingapura: NORTON ROSE FULBRIGHT. *Contact tracing apps in Singapore*: a new world for data privacy. 11/06/2020. Disponível em: https://www.nortonrosefulbright.com/-/media/files/nrf/nrfweb/contact-tracing/singapore-contact-tracing.pdf?la=en-sg&revision=. Último acesso em: 14 ago. 2020.

9 Diferentemente do Brasil, que agora conta com uma legislação plenamente vigente, a Índia não possui qualquer legislação promulgada (havendo apenas um projeto de lei em tramitação). Nesse sentido, o governo indiano enfrenta dificuldade de agir sobre eventuais abusos ou violações de dados pessoais, como já reconhecido. *Vide* FTI Consulting Asia Pacific – Amit Jaju and Amol Pitale. A Review of India's Contact-tracing App, Aarogya Setu. Setembro, 2020. Disponível em: https://www.lexology.com/library/detail.aspx?g=f54419a1-4823-404c-92f3-c5e4f193b733. Último acesso em: 20 set. 2020.

Retrato global das plataformas de *contact tracing*[10]



Os casos acima apontados são apenas alguns exemplos da profusão de aplicativos de *contact tracing* que surgiram em resposta à pandemia, tendo havido inúmeros casos similares que também são objeto de críticas e questionamentos.

Nesse contexto, nos países que já contam com um arcabouço legal e institucional de proteção de dados pessoais mais consolidado, as respectivas autoridades se apressaram a publicar recomendações buscando equilibrar as demandas por informações essenciais à proteção da saúde pública e a tutela dos dados pessoais. De acordo com a entidade *Global Privacy Assembly*, até o início de julho de 2020 algumas dezenas de autoridades de proteção de dados ao redor do mundo já haviam se manifestado a respeito.[11]

Dentro desse universo, vale destacar o posicionamento do Comitê Europeu para a Proteção de Dados ("EDPB"), por sua influência global e pela já referida similaridade entre as legislações europeia e brasileira. O EDPB emitiu, dentre outras manifestações, duas *guidelines* sobre o assunto. A *Guideline* nº 03/2020 ofereceu esclarecimentos fundamentais acerca da interpretação de conceitos centrais presentes no GDPR, como "dados relativos à saúde" e "tratamento para efeitos de investigação científica". Além disso, apresentou os cuidados que precisariam ser tomados para o tratamento daqueles dados no contexto de investigação científica

[10] *Idem*.

[11] GPA (GLOBAL PRIVACY ASSEMBLY). *COVID-19 Resources Library.* Disponível em: https://globalprivacyassembly.org/covid19/covid19-resources/. Último acesso em: 14 jul. 2020.

do COVID-19, alertando para a necessidade de cautela e do sopesamento entre privacidade e proteção de dados pessoais, de um lado, e de liberdade investigativa das ciências, de outro.[12]

A *Guideline* nº 04/2020, por sua vez, trouxe orientações específicas a respeito (i) do monitoramento sistemático, em grande escala, de localização de indivíduos e (ii) dos mecanismos de rastreio de contatos entre pessoas. Como salientado, tais mecanismos apresentam-se como fundamentais à construção de modelos da propagação do vírus e à avaliação da eficácia de medidas de isolamento e confinamento. A esse respeito afirma o Comitê:

> The systematic and large scale monitoring of location and/or contacts between natural persons is a grave intrusion into their privacy. It can only be legitimised by relying on a voluntary adoption by the users for each of the respective purposes. This would imply, in particular, that individuals who decide not to or cannot use such applications should not suffer from any disadvantage at all.[13]

O documento salienta a importância da definição clara do responsável pelo tratamento de dados no uso dessas ferramentas, priorizando que seja ele um órgão governamental e, caso haja intermediários, que os deveres e responsabilidades de cada um sejam previamente estabelecidos. Também ressalta que devem ser observados os princípios da finalidade e da necessidade – ou da minimização de dados, de modo a delimitar o uso dos dados a fins relacionados ao gerenciamento da crise sanitária e a restringir a coleta a dados efetivamente necessários para a consecução daquela finalidade.

Em síntese, as *guidelines*, alinhadas com as demais manifestações do Comitê,[14] postulam pela necessidade de agir dentro dos parâmetros legais pré-estabelecidos pelo GDPR.

---

[12] EDPB (EUROPEAN DATA PROTECTION BOARD). *Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak*. Adopted on21 April 2020. Disponível em: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202003_healthdatascientificresearchcovid19_pt.pdf. Último acesso em: 14 jul. 2020.

[13] EDPB (EUROPEAN DATA PROTECTION BOARD). *Diretrizes 4/2020 sobre a utilização de dados de localização e meios de rastreio de contactos no contexto do surto de COVID-19*. Adotadas em 21 de abril de 2020. Disponível em: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_20200420_contact_tracing_covid_with_annex_en.pdf. Último acesso em: 14 jul. 2020.

[14] Ver, dentre outros, os seguintes documentos: https://edpb.europa.eu/our-work-tools/our-documents/autre/statement-restrictions-data-subject-rights-connection-state_en https://edpb.europa.eu/our-work-tools/our-documents/ovrigt/statement-data-protection-impact-interoperability-contact_en; https://edpb.europa.eu/our-work-tools/our-documents/ovrigt/statement-processing-personal-data-context-reopening-borders_en

II.2 O debate sobre a proteção de dados sensíveis no Brasil na ausência de um arcabouço jurídico-institucional estabelecido

Embora no Brasil as plataformas de *contact tracing* não tenham ganhado a mesma proeminência vista em outros países, foram lançados no país aplicativos similares. Também aqui a pandemia suscitou o debate sobre a coleta e a proteção de dados pessoais.

Citamos, nesse sentido, iniciativas do poder público, tanto em nível federal como local, destinadas a viabilizar a prestação de serviços públicos, difundir informação e monitorar o quadro clínico dos cidadãos, tais como: (i) o aplicativo *Coronavírus SUS*,[15] desenvolvido pela Secretaria de Vigilância em Saúde do Ministério da Saúde; e (ii) o aplicativo *Coronavírus SP*,[16] bem como o Sistema de Monitoramento Inteligente ("SIMI"), ambos do Governo do Estado de São Paulo.[17] Tais mecanismos coletam diversos dados pessoais, incluindo dados sensíveis dos usuários.

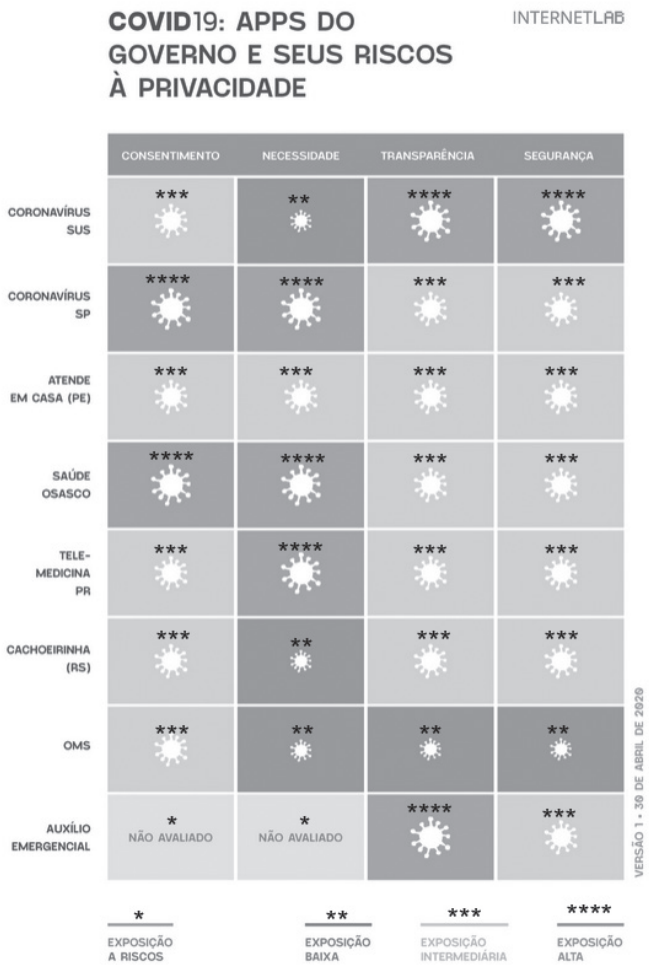
Na tabela abaixo, elaborada pelo InternetLab, centro de pesquisa independente de São Paulo, alguns destes aplicativos são avaliados conforme parâmetros distribuídos em quatro categorias – *consentimento, necessidade, transparência e segurança.* O trabalho avalia os riscos à privacidade oferecidos por cada aplicativo analisado, apontando também os eventuais mecanismos adotados para preservação dos direitos e mitigação de riscos embutidos no tratamento de dados pessoais - que em muitos casos poderiam ser considerados sensíveis.[18]

[15] O aplicativo solicita informações sobre o estado de saúde do indivíduo naquele momento de modo a subsidiar uma avaliação preliminar sobre o possível enquadramento como caso de COVID-19 e recomenda as medidas a serem adotadas pelo cidadão. Apesar dos dados solicitados terem potencialmente caráter sensível, conforme definição da LGPD, o aplicativo não apresentava, até abril deste ano, uma política de privacidade (BRASIL. Ministério da Saúde. *Coronavírus SUS*. Disponível em: https://www.gov.br/pt-br/apps/coronavirus-sus. Último acesso em: 14 jul. 2020).

[16] O aplicativo Coronavírus SP solicita do usuário dados como nome completo, data de nascimento, existência de sintomas e data de início desses sintomas, também sem qualquer esclarecimento prévio a respeito da utilização dessas informações, embora ofereça Política de Privacidade.

[17] O Governo do Estado de São Paulo, através do Instituto de Pesquisas Tecnológicas ("IPT"), também adotou o Sistema de Monitoramento Inteligente ("SIMI"), um sistema para avaliar os índices de isolamento social da população. O monitoramento é feito a partir de dados sobre a localização dos telefones celulares dos cidadãos, cujo acesso se deu por meio de acordo entre o Governo e as operadoras de telefonia móvel.

[18] A avaliação foi disponibilizada ao público no final de abril de 2020 e merece ser revista à luz de recentes alterações nos aplicativos, a exemplo da inclusão de política de privacidade no aplicativo Coronavírus SUS.



Fonte: InternetLab[19]

O estudo do InternetLab, bem como outros trabalhos,[20] mostram que apesar do uso reduzido dessas tecnologias no Brasil em comparação com outros países, o tema também é objeto de atenção pública e desperta preocupação.

[19] Disponível em: https://www.internetlab.org.br/pt/privacidade-e-vigilancia/covid-19-apps-do-governo-e-seus-riscos/

[20] *Vide*: https://www.uol.com.br/tilt/noticias/redacao/2020/05/12/contact-tracing-como-apple-e-google-querem-usar-bluetooth-contra-covid-19.htm; https://www.lgpdbrasil.com.br/contact-tracing-e-privacidade-em-tempos-de-pandemia/; https://www.migalhas.com.br/depeso/323077/contact-tracing-e-privacidade-em-tempos-de-pandemia

Destaca-se que um ponto crucial do debate, como demonstra o estudo conduzido pelo InternetLab, envolve a obtenção do consentimento dos titulares de dados. Nos aplicativos analisados no estudo o consentimento é um parâmetro que apresenta exposição intermediária a alta em todos eles.

Na contramão desses alertas, como já alertado anteriormente, a LGPD só entrou em vigor no mês setembro e, embora tenha sido promulgado o Decreto nº 10.474/2020 aprovando a estrutura regimental da ANPD, ela sequer teve sua efetiva implementação.

Consequentemente, há relevante lacuna de orientação centralizada e de interpretação sobre toda a norma, em geral, e sobre o tratamento de dados sensíveis, em especial, de modo que o embate no Brasil acerca da proteção de dados no contexto da pandemia tem tido como palco principal os tribunais e, em particular, o Supremo Tribunal Federal ("STF").

Nesse sentido, foram recentemente propostas perante o STF cinco Ações Diretas de Inconstitucionalidade ("ADIs") em face da Medida Provisória n. 954/2020,[21] que determinou o compartilhamento de dados não anonimizados de telefonia fixa e móvel e o endereço de seus usuários com a Fundação Instituto Brasileiro de Geografia e Estatística ("IBGE"). As ações questionam precisamente a constitucionalidade dessa determinação de compartilhamento, tendo em vista os riscos relevantes para a privacidade e proteção de dados dos cidadãos.

Embora as ações ainda aguardem julgamento final, já podem ser consideradas um marco no tema da proteção de dados no país. Isso porque, ainda em sede de decisão cautelar, o STF determinou a suspensão da medida provisória questionada com base no reconhecimento de que a Constituição Federal, além de proteger o direito à privacidade, acolhe também, de forma autônoma, os direitos fundamentais à proteção de dados pessoais e à autodeterminação informativa.[22]

Nesse contexto, a discussão travada em âmbito brasileiro tem diferenças significativas em comparação àquela desenvolvida no âmbito internacional. Na Europa e em diversos outros países, a discussão parte de um arcabouço jurídico e institucional minimamente consolidado em termos de proteção de dados. O Brasil, no entanto, sequer possui uma autoridade nacional em funcionamento.

Em face dessa enorme fragilidade jurídico-institucional, e embora se compreenda o debate acerca da utilização de dados sensíveis por ferramentas governamentais no contexto da COVID-19, entendemos ser necessário dar um passo

[21] Ações Diretas de Inconstitucionalidade nºs 6387, 6388, 6389, 6390 e 6393.

[22] MENDES, Laura Schertel. Decisão histórica do STF reconhece direito fundamental à proteção de dados pessoais. *Jota,* 10/05/2020. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/decisao-historica-do-stf-reconhece-direito-fundamental-a-protecao-de-dados-pessoais-10052020. Último acesso em: 06 jul. 2020.

atrás. A contribuição para o debate sobre a proteção de dados pessoais no contexto de uma crise de saúde pública passa necessariamente pela discussão acerca do quanto já estabelecido pela LGPD, suas lacunas e interpretações, bem como os espaços para avanços. É neste contexto que se desenvolve o presente artigo.

III A disciplina dos dados pessoais sensíveis no Brasil: origem e consolidação da LGPD

A classificação de dados pessoais em categorias ou subcategorias em razão do maior grau de vulnerabilidade que a própria condição do sujeito – como no caso de crianças e adolescentes – ou a maior probabilidade de que o tratamento gere consequências negativas para o seu titular – como é o caso dos dados sensíveis – é adotada em grande parte dos países que possuem legislações em vigor ou em desenvolvimento sobre proteção de dados pessoais.

O fundamento jurídico para tanto é o reconhecimento de que o tratamento de algumas categorias de dados acarreta maior risco à personalidade, sobretudo em termos de práticas discriminatórias. Em outras palavras, o tratamento, armazenamento e compartilhamento desses dados apresentavam maior propensão a favorecer práticas de exclusão, segregação e desigualdade, exigindo assim maiores cuidados.

A legislação brasileira já havia incorporado esse tipo de precaução por ocasião da formulação da Lei nº 12.414, de 2011, a chamada Lei do Cadastro Positivo.[23] A LGPD seguiu na mesma direção, adotando a categoria dos "dados pessoais sensíveis", a qual atribuiu disciplina específica.

Embora tenha havido inúmeras discussões prévias e algumas mudanças posteriores pontuais, a essência da disciplina foi estabelecida ainda no âmbito do Projeto de Lei nº 4.060/2012, por meio do parecer substitutivo apresentado pelo Deputado Orlando Silva (PCdoB-SP). Nele, o Deputado ressalta a importância do consentimento qualificado:

> Como há duas categorias de dados, os dados pessoais ('gerais') e, nessa categoria, o subconjunto dos dados sensíveis, resolvemos por discriminar os tipos de consentimentos. Para a primeira categoria de dados, o consentimento é livre, informado e inequívoco. Já para a

[23] Um dos incisos do Art. 3º da Lei de Cadastro Positivo já trazia a proibição da anotação de informações sensíveis nos bancos de dados ali regulados, entendidas como "aquelas pertinentes à origem social e étnica, à saúde, à informação genética, à orientação sexual e às convicções políticas, religiosas e filosóficas".

> segunda categoria, explicitamos, no Art. 11, que esse consentimento deverá ser específico e em destaque para finalidades específicas, adicionais às contidas no consentimento referente ao tratamento de dados pessoais 'gerais'. Dessa maneira, a necessidade de se obter consentimento em destaque é, assim, a camada adicional de proteção para este tipo de dados.

Findo o processo legislativo, a redação da LGPD define dados sensíveis em seu Art. 5º, inciso II, da seguinte forma:

> O dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural.

Esses dados ficam ainda sujeitos às determinações dispostas nos arts. 11 a 13 da LGPD. E é aquele primeiro que trata especificamente das bases legais para o tratamento dos dados sensíveis, que diferem da disciplina geral aplicável aos demais tipos de dados pessoais.

A lei apresenta dois caminhos possíveis. O primeiro exige que para o tratamento de dados sensíveis haja consentimento específico e destacado do titular ou responsável legal, para finalidades específicas – o chamado c*onsentimento qualificado.* Nessa primeira alternativa não há restrição adicional à finalidade para a qual o dado sensível será utilizado, contanto que haja consentimento nos termos definidos.

Não obstante, embora tanto a lei brasileira como o regime europeu adotem o consentimento qualificado como base primordial para o tratamento de dados pessoais sensíveis, atribuindo exigências adicionais em relação ao consentimento exigido para o tratamento dos demais dados, os termos em que o fazem são diferentes. Esta particularidade será tratada adiante em tópico específico.

O segundo caminho, por seu turno, permite a dispensa do consentimento do titular para finalidades expressa e taxativamente previstas. Também nesse ponto assemelha-se à legislação europeia, embora com peculiaridades locais. A lei oferece as seguintes hipóteses:

1) cumprimento de obrigação legal ou regulatória pelo controlador;
2) tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos;
3) realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis;
4) exercício regular de direitos;

5) proteção da vida ou da incolumidade física do titular ou de terceiro;
6) tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária;
7) garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos.

No caso europeu, além do texto propriamente legal, o GDPR também traz uma série de considerandos – ou *recitals*, no idioma original. Os *recitals* 51 a 54 do GDPR abordam em mais detalhes as chamadas categorias especiais de dados pessoais, aquelas "especialmente sensíveis do ponto de vista dos direitos e liberdades fundamentais". O *recital* 52 toca diretamente o tratamento de dados pessoais sensíveis para a prevenção e controle de doenças transmissíveis:

> Derogating from the prohibition on processing special categories of personal data should also be allowed when provided for in Union or Member State law and subject to suitable safeguards, so as to protect personal data and other fundamental rights, where it is in the public interest to do so, in particular processing personal data in the field of employment law, social protection law including pensions and for health security, monitoring and alert purposes, the prevention or control of communicable diseases and other serious threats to health.[24]

No Brasil, entretanto, em face da ausência de regulamentação e da ANPD, não há interpretação consolidada para previsões similares. Na ausência de orientação clara e de estruturas de *enforcement*, agentes públicos e privados têm tratado o tema cada um ao seu modo, com os desafios e riscos vistos acima.

Na busca de um arcabouço nacional que contemple o assunto, observamos – especialmente em trabalhos acadêmicos – a tendência a reproduzir diretamente os conceitos e construções de matriz europeia, tendo em vista a sabida inspiração da LGPD no GDPR e mesmo algumas similaridades nos textos, como já indicado neste artigo.[25]

[24] Recital nº 52. Disponível em: https://www.privacy-regulation.eu/en/recital-52-GDPR.htm. Último acesso em: 16 jul. 2020.

[25] Nos deparamos com perspectivas que afirmam que "a LGPD conceituou de forma semelhante, senão idêntica, ao GDPR, o conceito de dados pessoais sensíveis, sendo certo que a lei brasileira é bastante inspirada no regulamento europeu" ou que "ao se proceder a uma comparação com o GDPR, constata-se uma identidade de hipóteses de caracterização com os dados sensíveis na LGPD" (NEGRI, Sérgio Marcos Carvalho de Ávila; KORKMAZ, Maria Regina Detoni Cavalcanti Rigolon. A normatividade dos dados sensíveis na Lei Geral de Proteção de dados: ampliação conceitual e proteção da pessoa humana. *Rev. de Direito, Governança e Novas Tecnologias*, v. 5 n. 1, p. 63-85. Goiânia, Jan./Jun. 2019 (p. 74). Disponível em: https://indexlaw.org/index.php/revistadgnt/article/view/5479/pdf >

Ao nosso ver o regime jurídico atribuído aos dados sensíveis na legislação brasileira guarda muitas semelhanças com o GDPR, porém apresenta algumas distinções importantes que não podem ser desconsideradas. Tais diferenças tocam temas centrais como os próprios elementos que integram a definição de dados sensíveis, os requisitos exigidos para que o consentimento do titular seja considerado válido quando relativo a esses dados, ou mesmo as bases legais admitidas para além do consentimento.[26]

Nesse sentido, o restante do texto abordará duas dessas distinções, selecionadas por sua relevância normativa e possível impacto direto nas práticas de tratamento de dados sensíveis com finalidades relacionadas à pandemia causada pela disseminação do vírus da COVID-19. O primeiro caso diz respeito ao tratamento de uma importante categoria de dados sensíveis, os chamados dados biométricos – incluídos expressamente tanto na LGPD como no GDPR, porém apenas este último diploma traz uma definição do termo e orientações de como interpretá-lo. O segundo caso se refere à própria forma de obtenção de consentimento do titular para tratamento de dados sensíveis, como veremos a seguir.

IV Dados biométricos

Os dados biométricos estão no centro do debate acerca das ferramentas tecnológicas de enfrentamento à pandemia. Dentre múltiplos mecanismos mobilizados para a contenção de doenças contagiosas, destacam-se ferramentas que utilizam tecnologias de reconhecimento facial.[27] Conforme reconhecido pela OCDE:

> Facial recognition has been one of the most frequently used biometrics in a number of countries to monitor the spread of COVID-19. (...) However, the use of biometrics (including facial recognition) in response to COVID-19 raises a number of privacy and security concerns, particularly

[26] A LGPD inova, por exemplo, ao trazer como base legal para o tratamento de dados pessoais sensíveis a hipótese de *prevenção à fraude e segurança do titular*.

[27] CIDRI NETO, Oscar Carlos. *O Tratamento de dados pessoais e sensíveis frente ao contact tracing durante o COVID-19*. Grupo de Estudos de Direito Autoral e Industrial da Universidade Federal do Paraná. Junho, 2020. Disponível em: https://www.gedai.com.br/o-tratamento-de-dados-pessoais-e-sensiveis-frente-ao-contact-tracing-durante-o-covid-19/. Último acesso em: 14 jul. 2020.

> when these technologies are being used in the absence of specific guidance or fully informed and explicit consent.[28]

A definição e a natureza legal dos dados biométricos foi intensamente debatida na Europa antes de sua efetiva incorporação na legislação por meio da GDPR. Os primeiros documentos tratando do tema datam do início dos anos 2000 e demonstram grande hesitação sobre seu *status* e classificação adequada.

Em 2003, o Grupo de Trabalho Artigo 29[29] publicou o primeiro documento consistente sobre a aplicação das regras de proteção de dados pessoais aos sistemas biométricos.[30] Contudo, nesse momento, ainda não havia conceito de dados biométricos nem definição clara de quando seriam eles considerados dados pessoais. Apenas em 2007 a entidade elaborou novo documento em que trazia o conceito, segundo o qual dados biométricos seriam "propriedades biológicas, características psicológicas, traços ou ações replicáveis em que tais características ou ações sejam tanto únicas de determinado indivíduo como mensuráveis".[31]

Como bem aponta Jasserand,[32] é a partir desse momento que a discussão avança para a definição atual. Passa-se a considerar que a definição técnica de dados biométricos não exige necessariamente uma conexão das características com um indivíduo específico, mas precisa de tal vinculação para ser considerado um dado pessoal. Em outras palavras, dados biométricos só serão dados pessoais – e, portanto, passíveis de proteção – na medida em que as características físicas, psicológicas e comportamentais de um determinado indivíduo puderem ser utilizadas para a identificação singular daquele indivíduo.

---

[28] OCDE. *Leveraging biometric data adds both benefits and challenges*, 2020. Disponível em: http://www.oecd.org/coronavirus/policy-responses/tracking-and-tracing-covid-protecting-privacy-and-data-while-using-apps-and-biometrics-8f394636/#section-d1e194. Último acesso em: 14 jul. 2020.

[29] O Article 29 Data Protection Working Party foi um conselho formado por representantes das autoridades de proteção de dados de cada um dos países da União Europeia, do European Data Protection Supervisor e do European Data Protection Board (EDPB). Em maio de 2018 o A29WP foi substituído pelo EDPB. A função do A29WP, agora assumida pelo EDPB era de: (i) Fornecer aconselhamento técnico aos Estados-membro da UE sobre temas relacionados a proteção de dados; (ii) promover a aplicação consistente das diretivas de proteção de dados em toda a UE; (iii) fornecer à Comissão Europeia opiniões sobre lei da Comunidade Europeia que afetem o direito à proteção de dados pessoais; (iv) fazer recomendações ao público em temas relacionados a proteção de dados pessoais e privacidade. Disponível em: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=59485

[30] ARTICLE 29 DATA PROTECTION WORKING PARTY. *Working document on biometrics*. 01/08/2003 Disponível em:. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2003/wp80_en.pdf. Último acesso em: 14 jul. 2020.

[31] ARTICLE 29 DATA PROTECTION WORKING PARTY. *Opinion 4/2007 on the concept of personal data*. 20/06/2007. Disponível em: https://www.clinicalstudydatarequest.com/Documents/Privacy-European-guidance.pdf. Último acesso em: 14 jul. 2020.

[32] JASSERAND, Catherine. *Legal nature of biometric data: from 'generic' personal data to sensitive data*. University of Groningen Faculty of Law Research Paper Series n. 24/2018. Junho de 2016.

O resultado desse processo foi a definição e a disciplina fornecidas pelo GDPR. Em seu Art. 4 (14) o GDPR define dados biométricos da seguinte forma:

> 'biometric data' means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data.

Embora tal definição mencione a "possibilidade de identificar ou confirmar a identidade", o Art. 9 (1) da lei especifica que só são dados sensíveis os dados biométricos utilizados "para identificar uma pessoa de forma inequívoca". Nesse sentido, embora todo dado biométrico que possibilite a identificação de uma pessoa seja um dado pessoal, ele só será um dado sensível na medida em que efetivamente for utilizado para realizar a identificação do indivíduo.

A identificação[33] é o processo por meio do qual se estabelece a identidade de um indivíduo a partir da comparação e da correspondência entre os dados biométricos em uma base de dados prévia.[34] Tal interpretação – construída ao longo de anos – está registrada tanto no julgamento de casos concretos como em *recitals* e *guidelines*.

Nesse sentido, a *Information Commissioner's Office* ("ICO"), autoridade de proteção de dados britânica, elenca como exemplos do que se configura como dado biométrico para fins de identificação – e, portanto, dado sensível – o reconhecimento facial, a verificação de impressão digital, reconhecimento de voz e análise de assinatura manual.

Esse extenso acúmulo gerado no âmbito da União Europeia poderia (e deveria) ter sido aproveitado para o caso brasileiro. Porém, embora a LGPD também inclua os dados biométricos como dados sensíveis, ela (i) não traz uma definição para o termo, (ii) não explicita que apenas aqueles que permitam a identificação

[33] "(…) l'identification d'une personne, qui vise à retrouver une personne au sein d'un groupe d'individus, dans un lieu, une image ou une base de données. Dans ce cas, le système doit effectuer un test sur chaque visage capté pour générer un gabarit biométrique et vérifier si celui-ci correspond à une personne connue du système. Cette fonctionnalité repose ainsi sur la comparaison d'un gabarit avec une base de données de gabarits. Par exemple, elle permet de lier un «état civil» (nom, prénom) à un visage, si la comparaison est faite avec une base de photographies associées à un nom et un prénom. Elle peut aussi consister à suivre la trajectoire d'une personne dans une foule, sans nécessairement faire le lien avec l'état civil de la personne" (COMMISSION NATIONALE INFORMATIQUE & LIBERTÉS (CNIL). *Reconnaissance Faciale: pour un débat à la hauter des enjeux*. Novembro, 2019. Disponível em: https://www.cnil.fr/sites/default/files/atoms/files/reconnaissance_faciale.pdf. Último acesso em: 17 jul. 2020.

[34] JASSERAND, Catherine. *Legal nature of biometric data: from 'generic' personal data to sensitive data.* University of Groningen Faculty of Law Research Paper Series n. 24/2018. Junho de 2016 (p. 9).

do indivíduo são dados pessoais, muito menos que (iii) apenas quando o tratamento desses dados tiver a finalidade de identificação única do indivíduo é que ele será caracterizado como dado sensível.

A falta de maior contextualização no texto da LGPD pode dar margem a interpretações extremamente restritivas e inadequadas, que poderiam, inclusive, levar ao questionamento futuro da proteção prevista na lei.

IV.1 O exemplo do tratamento de imagens e do reconhecimento facial

Um dos principais casos da determinação da sensibilidade de um dado biométrico diz respeito ao tratamento de fotografias e vídeos contendo imagens de pessoas, em particular de seus rostos.

O GDPR somente trata imagens digitais de pessoas como uma categoria especial de dados (dados biométricos) quando "processada por meio de um meio técnico específico, permitindo a identificação ou autenticação exclusiva de uma pessoa". Conforme o mesmo *recital* 51, identificação única é entendida como a identidade do indivíduo. Assim, apenas dados biométricos utilizados para reconhecimento e ligados a um indivíduo já identificado é que se seriam enquadrados como dado pessoal sensível – ou categoria especial, para usar a linguagem do GDPR:

> The processing of photographs should not systematically be considered to be processing of special categories of personal data as they are covered by the definition of biometric data only when processed through a specific technical means allowing the unique identification or authentication of a natural person.

Antes mesmo da adoção desses parâmetros pelo GDPR, o A29WP já havia emitido duas opiniões sobre o tema em 2012.[35] Nesses documentos, define o reconhecimento facial como "o processamento automático de imagens digitais contendo o rosto de indivíduos para propósitos de identificação, autenticação/

[35] ARTICLE 29 DATA PROTECTION WORKING PARTY. *Opinion 02/2012 on facial recognition in online and mobile services.* 22/03/2012. Disponível em: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp192_en.pdf. Último acesso em: 14 jul. 2020; ARTICLE 29 DATA PROTECTION WORKING PARTY. *Opinion 3/2012 on developments in biometric technologies*. 27/04/2012. Disponível em: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp193_en.pdf. Último acesso em: 14 jul. 2020.

verificação e categorização destes indivíduos". As opiniões esclarecem como funciona esse processo de reconhecimento facial e quais as suas etapas[36] e finalidades.[37] Segundo essas classificações, é possível haver a identificação sem que haja necessariamente a autenticação/verificação.

As definições trazidas por tais documentos foram mais recentemente corroboradas por orientações e publicações oficiais de autoridades nacionais de proteção de dados por toda a Europa.

Seguindo essa linha interpretativa, a autoridade de proteção de dados francesa – *Commission Nationale Informatique & Libertés* ("CNIL") – elaborou documento sobre reconhecimento facial em 2019. Nele, a CNIL enquadra como dados biométricos o processo técnico que permite o reconhecimento facial da imagem de um rosto (em um vídeo ou fotografia) a partir de um *template*, isto é, de uma representação digital daquele rosto a partir de suas características distintivas, com o fim de autenticar ou identificar determinada pessoa.[38]

De forma similar e ainda mais restritiva, no Reino Unido,[39] as orientações oficiais hoje disponíveis no *site* da ICO indicam que o processamento de fotografias de indivíduos não é automaticamente considerado pela autoridade como dado biométrico, mesmo quando usada para propósitos de identificação. Para ser considerado dado biométrico, é necessário que seja conduzido processamento técnico específico, que geralmente envolve o uso da imagem para criação de *template* digital individual ou perfil, que por sua vez é utilizado para a correspondência automatizada com outras imagens ou identificação. Se os dados biométricos são utilizados para aprender algo sobre um indivíduo, autenticar a sua identidade, controlar seu acesso, tomar uma decisão sobre eles ou tratá-los de maneira diferenciada, haverá, então, enquadramento em categoria especial.[40]

---

[36] O reconhecimento facial tem, a princípio, seis etapas: (i) aquisição da imagem; (ii) detecção do rosto; (iii) normalização; (iv) extração de características; (v) registro; (vi) comparação → a comparação, última fase é a essencial para definir o propósito daquele reconhecimento facial e, em consequência, definir se ele é ou não um processamento de dados sensíveis.

[37] São finalidades do processo de reconhecimento facial: (i) identificação, a exemplo de fotografias carregadas em redes sociais nas quais pessoas podem ser marcadas ou se marcarem; (ii) autenticação/verificação - exemplo de reconhecimento facial utilizado para substituir usuário e senha para controle de acesso; (iii) categorização - rede social licencia o acesso à biblioteca de imagens para um terceiro que opera o serviço de reconhecimento com outros propósitos.

[38] COMMISSION NATIONALE INFORMATIQUE & LIBERTÉS (CNIL). *Reconnaissance Faciale: pour un débat à la hauter des enjeux*. Novembro, 2019. (p. 3) Disponível em: https://www.cnil.fr/sites/default/files/atoms/files/reconnaissance_faciale.pdf. Último acesso em: 17 jul. 2020.

[39] INFORMATION COMISSIONER'S OFFICE. *Guide to the General Data Protection Rules*. Disponível em: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/special-category-data/what-is-special-category-data/#scd4. Último acesso em: 14 jul. 2020.

[40] Vale ainda citar como exemplos desse entendimento as autoridades belga e espanhola, que têm tratado fotografias como mera informação pessoal se for processada para fins de identificação. Apenas se a finalidade do processamento se relacionar com a informação sensível (por exemplo, triagem étnica, perfil

Como se depreende, o tema não é simples e possui sutilezas relevantes. A breve exposição do tratamento de reconhecimento facial em imagens na União Europeia e em alguns de seus Estados-membros é exemplo de que, na prática, há diversos usos e tratamentos possíveis, que podem ou não se enquadrar na disciplina de dados pessoais sensíveis. Na prática, os usos do processamento de fotografias e de reconhecimento facial são múltiplos e sujeitos a tratamento distinto.

Como adiantamos, porém, o tema ainda não foi detalhadamente tratado em regulamento ou em orientações interpretativas no Brasil. Não há nada que reconheça a importância dessas potenciais diferenças nos tipos de tratamento. Para evitar possíveis consequências indesejadas, é preciso haver adequada regulamentação e interpretação da lei pela ANPD, na forma dos incisos XIII e XX do Art. 55-J da lei.

V O consentimento para tratamento de dados pessoais sensíveis

Para além dos próprios elementos que integram a definição de dados pessoais sensíveis – ou categorias especiais, na dicção da legislação europeia – outro ponto de divergência relevante entre a LGPD e o GDPR diz respeito à qualificação do consentimento do titular que seria apto a autorizar o tratamento desses dados.

Trata-se de um conceito central para toda a estrutura normativa da lei, que destaca o consentimento como base legal privilegiada para o tratamento de dados – sensíveis ou não. Sua importância reflete a compreensão contemporânea do direito à proteção de dados pessoais e do direito à autodeterminação informativa[41]

de imigrantes, investigação de má conduta do aluno, etc.), a foto pode ser classificada como informação pessoal sensível (FACHINETTI, Aline Fuke. LGPD: fotos, inferências e a sensibilidade de dados pessoais – Uma análise sobre inferências e o seu impacto na sensibilidade dos dados pessoais. *Jota*, 03/09/2019. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/lgpd-fotos-inferencias-e-a-sensibilidade-de-dados-pessoais-03092019. Último acesso em: 17 jul. 2020).

41 A noção de um direito fundamental à autodeterminação informativa, essencial para tal transformação, tem como marco inicial a decisão do Tribunal Constitucional alemão de 1982, acerca da Lei do Recenseamento da População, Profissão, Moradia e Trabalho. Nas palavras de Laura Schertel Mendes: "A Corte afirmou que o moderno processamento de dados pessoais configura uma grave ameaça à personalidade do indivíduo, na medida em que possibilita o armazenamento ilimitado de dados, bem como permite a sua combinação de modo a formar um retrato completo da pessoa, sem a sua participação ou conhecimento. Nesse contexto, argumentou que a Constituição alemã protege o indivíduo contra o indevido tratamento de dados pessoais, por meio do direito fundamental ao livre desenvolvimento da personalidade, segundo o qual o indivíduo tem o poder para determinar o fluxo de suas informações na sociedade" (MENDES, Laura Schertel Ferreira. *Privacidade, proteção de dados e direito do consumidor*. São Paulo: Saraiva Educação, 2014).

como duas faces da mesma moeda, refletindo "a ideia de que o titular dos dados pessoais deve ser empoderado com o controle de suas informações pessoais e, sobretudo, na sua autonomia da vontade".[42]

Da mesma forma, conforme apontado anteriormente, o consentimento tem sido um ponto sensível no debate brasileiro acerca das ferramentas tecnológicas de monitoramento do contágio pelo COVID-19. Suas políticas de privacidade e termos de uso, no entanto, não demonstram ainda as preocupações e salvaguardas indicadas pela LGPD. Mais uma vez, a referência aos *standards* europeus não está totalmente alinhada com os requisitos previstos na legislação aprovada pelo Congresso Nacional em 2018.

V.1 Consentimento qualificado como base legal

A razão de ser da categoria de dados sensíveis é a necessidade de proteção adicional ao tratamento desse tipo de dado em razão da sua potencialidade lesiva. Em linha com esse entendimento, uma das diferenças da disciplina legal para dados sensíveis é que a principal base legal para seu tratamento, qual seja, o consentimento, apresenta exigências adicionais à modalidade exigida de forma mais ampla para o tratamento de dados pessoais sem a mesma sensibilidade. Exige-se, neste caso, a obtenção do chamado "consentimento qualificado".

Assim, o Art. 5º, inciso XII, da LGPD define consentimento como a "manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada". Contudo, mais adiante, no Art. 11, a lei exige, para tratamento de dados pessoais sensíveis, que o consentimento do titular seja dado "de forma específica e destacada, para finalidades específicas".

Em outras palavras, enquanto para os demais dados pessoais a LGPD requer que o consentimento seja livre, inequívoco e informado, para os dados sensíveis deve-se garantir que este seja também *específico* e *destacado*, bem como obtido para *finalidades específicas*. Novamente a lei não esclarece os contornos dessas cinco características: livre, inequívoco, informado, específico e destacado. Não há – como no caso dos *recitals* 42 e 43 do GDPR – uma contextualização mais detalhada.

Tais qualificadoras, no entanto, são resultado de algumas décadas de construção normativa, doutrinária e jurisprudencial em torno do direito à proteção de

[42] BIONI, Bruno Ricardo. *Proteção de Dados Pessoais* – A Função e os Limites do Consentimento. Rio de Janeiro: Forense. Edição do Kindle. 2019 (p. 133).

dados pessoais, que remontam – apenas no que tange à tradição europeia – à Diretriz Europeia de Proteção de Dados Pessoais de 1995. Com base nas fontes internacionais é possível arriscar alguns parâmetros para seu entendimento:

> (i) Livre: O titular dos dados não pode ser forçado a consentir. É ainda, recomendável que seja oferecida a oportunidade de o titular dos dados consentir ou não para cada tipo de uso. O oferecimento do serviço não pode ser condicionado ao consentimento, exceto se o dado for essencial para o próprio fornecimento.
>
> (ii) Informado: O titular deve conhecer o contexto de tratamento dos dados que fornece – a identidade do controlador, as atividades de tratamento que serão conduzidas, o objetivo dessas atividades e a possibilidade de o titular retirar seu consentimento a qualquer tempo.
>
> (iii) Inequívoco: Não deve haver dúvida sobre o fato de o titular ter consentido.
>
> (iv) Específico/finalidades específicas: O titular deve consentir de maneira específica para cada modalidade de tratamento de dados sensíveis e sua respectiva finalidade.
>
> (v) Destacado: O consentimento para tratamento de dados sensíveis deve ser claramente distinguível de outras expressões de vontade do titular, como o consentimento para termos e condições de uso gerais.

Não obstante, tendo em vista que a Autoridade competente para tal interpretação no Brasil ainda não foi instalada, não é possível estabelecer com segurança qual será a interpretação válida no contexto brasileiro. A ANPD deverá determinar de forma clara esses requisitos, trazendo maior segurança jurídica para titulares de dados e controladores, bem como trabalhar as formas preferenciais ou exemplos de bons modelos de obtenção do consentimento nos termos da lei, a exemplo do que fazem outras autoridades de proteção de dados ao redor do mundo. Vejamos abaixo o exemplo da já mencionada autoridade britânica:

Orientações da ICO sobre a forma adequada de obtenção do consentimento com base na GDPR e na lei britânica

Checklists

Asking for consent

☐ We have checked that consent is the most appropriate lawful basis for processing.

☐ We have made the request for consent prominent and separate from our terms and conditions.

☐ We ask people to positively opt in.

☐ We don't use pre-ticked boxes or any other type of default consent.

☐ We use clear, plain language that is easy to understand.

☐ We specify why we want the data and what we're going to do with it.

☐ We give separate distinct ('granular') options to consent separately to different purposes and types of processing.

☐ We name our organisation and any third party controllers who will be relying on the consent.

☐ We tell individuals they can withdraw their consent.

☐ We ensure that individuals can refuse to consent without detriment.

☐ We avoid making consent a precondition of a service.

☐ If we offer online services directly to children, we only seek consent if we have age-verification measures (and parental-consent measures for younger children) in place.

Nesse sentido, o GDPR parece adotar disciplina ligeiramente distinta acerca do consentimento exigido para o tratamento de dados pessoais sensíveis. Segundo o Art. 4 (11) do regulamento, o consentimento é ali entendido como:

> (...) any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.[43]

[43] Embora a doutrina e a jurisprudência construídas na União Europeia, com destaque para as orientações mencionadas da autoridade britânica (ICO), façam uma diferenciação clara entre os termos "explícito" e "inequívoco", a tradução oficial para o português, na contramão dessa construção interpretativa, traduz o termo "unambiguous" como "explícito, demonstrando a miscelânea que é feita no uso dos termos.

Mais adiante, admite o tratamento de categorias especiais de dados pessoais (dados sensíveis) quando "o titular dos dados tiver dado o seu consentimento *explícito* para o tratamento desses dados pessoais para uma ou mais finalidades específicas".

Desse modo, o caráter explícito do consentimento – que não aparece em nenhum momento na LGPD – ocupa um espaço central na disciplina do tratamento de dados sensíveis no arcabouço normativo europeu. Como o próprio texto indica, os adjetivos *explícito* e *inequívoco* parecem não ser sucedâneos e referem-se a requisitos distintos para atestar a validade do consentimento. De fato, a própria ICO ao detalhar os elementos necessários para caracterizar um consentimento válido sob o GDPR estabelece a diferenciação entre esses dois termos e oferece um exemplo hipotético para demonstrar que é possível obter o consentimento inequívoco do titular dos dados sem que ele seja explícito.[44] De forma resumida, segundo a ICO, inequívoco é aquele sobre o qual não pesa dúvida; expresso seria aquele declarado em palavras.

A doutrina reforça esse entendimento. Segundo Korkmaz[45] e Bioni,[46] a diferença entre os termos específico e expresso é meramente semântica e "a consequência normativa [de ambos] deve ser a mesma, na medida em que o propósito da qualificação é reservar uma autorização singular por parte da pessoa à qual os dados se referem".[47]

Contudo, os autores entendem que o mesmo não se aplica à qualificação do consentimento como inequívoco. Isso porque o termo inequívoco deve ser entendido como o consentimento não ambíguo, mas evidente, que precisa se dar forma clara, não presumida. Ou seja, deve-se verificar um comportamento concludente por parte da pessoa à qual os dados se referem, uma "ação afirmativa que não deixe dúvidas sobre a intenção do cidadão".[48] A imprescindibilidade do trabalho

[44] Ver explicação de consentimento explícito em https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/consent/what-is-valid-consent/. Último acesso em: 14 jul. 2020.

[45] KORKMAZ, Maria Regina Detoni Cavalcanti Rigolon. *Dados Sensíveis na Lei Geral de Proteção de Dados Pessoais*: mecanismos de tutela para o livre desenvolvimento da personalidade. Tese de mestrado da Faculdade de Direito da Universidade Federal de Juiz de Fora. Juiz de Fora, 2019. Disponível em: https://repositorio.ufjf.br/jspui/bitstream/ufjf/11438/1/mariareginadetonicavalcanti rigolonkorkmaz.pdf. Último acesso em: 16 jul. 2020.

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

[47] KORKMAZ, Maria Regina Detoni Cavalcanti Rigolon. *Dados Sensíveis na Lei Geral de Proteção de Dados Pessoais*: mecanismos de tutela para o livre desenvolvimento da personalidade. Tese de mestrado da Faculdade de Direito da Universidade Federal de Juiz de Fora. Juiz de Fora, 2019. (p.74) Disponível em: https://repositorio.ufjf.br/jspui/bitstream/ufjf/11438/1/mariareginadetonicavalcanti rigolonkorkmaz.pdf. Último acesso em: 16 jul. 2020.

[48] BIONI, Bruno. *Proteção de dados pessoais*: a função e os limites do consentimento. Rio de Janeiro: Forense, 2019, p. 199.

da ANPD quanto a esse assunto evidencia-se na possibilidade de confusão de alguns termos e no impacto que isso pode gerar na atuação dos agentes públicos e privados.

Na mesma direção, no caso brasileiro será preciso afastar eventuais confusões entre o texto adotado em 2014 pelo Marco Civil da Internet ("MCI") e o adotado pela Lei Geral de Proteção de Dados em 2018. Embora não traga uma definição de consentimento, o MCI menciona a necessidade de "consentimento expresso" do titular para a coleta e o tratamento de dados nos casos que especifica.[49] Ainda que a LGPD pareça se sobrepor neste âmbito ao MCI, por se tratar de lei especial e posterior – à qual o próprio Marco Civil faz referência e indica deferência no inciso III do Art. 3º apenas regulamentação ou orientação interpretativa da ANPD poderá dar segurança ao ponto.

Embora pareça trivial, a questão atinge frontalmente o debate sobre as ferramentas utilizadas ao longo da pandemia no país. Muitas das aplicações e plataformas de monitoramento utilizam como base legal para obtenção dos dados pessoais o consentimento.

As duas questões endereçadas acima, do caso particular dos dados biométricos e do consentimento como base legal para o tratamento de dados sensíveis, são apenas dois desafios com os quais se depara quem se dispõe a debater a proteção de dados pessoais no país neste momento de indefinição normativa e institucional. Esses exemplos demonstram a urgência da efetiva implementação da ANPD, ator central na interpretação e aplicação da LGPD, bem como da constituição de uma regulamentação adequada do tema.

VI Conclusão

Por todo o mundo, medidas de enfrentamento à pandemia do COVID-19 têm se utilizado de diversas tecnologias digitais com finalidades de monitoramento e controle de propagação da doença, como o *contact tracing*. Se inequivocamente

[49] Art. 7º O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos: (...)
VII - não fornecimento a terceiros de seus dados pessoais, inclusive registros de conexão, e de acesso a aplicações de internet, *salvo mediante consentimento livre, expresso e informado* ou nas hipóteses previstas em lei;
(...)
X - *consentimento expresso* sobre coleta, uso, armazenamento e tratamento de dados pessoais, que deverá ocorrer de forma destacada das demais cláusulas contratuais; (...).
Art. 16. Na provisão de aplicações de internet, onerosa ou gratuita, é vedada a guarda: (...)
II - de dados pessoais que sejam *excessivos em relação à finalidade para a qual foi dado consentimento pelo seu titular* (...). (grifos nossos).

úteis à saúde pública, o emprego de tais ferramentas têm sido bastante questionado no Brasil e no mundo, visto o extenso tratamento de dados pessoais sensíveis e os consequentes riscos à privacidade e à proteção de dados dos cidadãos.

Embora tal questionamento seja válido e importante, o presente artigo argumenta que o debate no Brasil sobre o tema está estruturalmente atrás do debate europeu, uma vez que o país sequer possui um arcabouço jurídico-institucional plenamente constituído.

Não se nega já existir importante lastro teórico sobre o assunto, bem como princípios que lhe são inequivocamente aplicáveis. Contudo, a falta de regulamentação da lei e a ausência de Autoridade efetivamente instaurada responsável pela interpretação e pela orientação de aplicação da norma limitam a caracterização detalhada da proteção de dados pessoais sensíveis no país e prejudicam a orientação efetiva para legitimar condutas e processos dos setores público e privado.

Não se olvida a óbvia aplicabilidade dos princípios que regem a proteção de dados pessoais, especialmente após o recente reconhecimento do direito autônomo à proteção de dados pessoais pelo Supremo Tribunal Federal. No entanto, os exemplos relativos ao tratamento de dados biométricos – especialmente quanto ao uso de imagens digitais de pessoais e à definição do consentimento exigido para o tratamento de dados pessoais sensíveis – demonstram a relevante margem interpretativa dos dispositivos da LGPD, como a ausência do conceito de dados biométricos e quando eles são dados sensíveis ou as exatas características do consentimento qualificado, e os problemas práticos que essa incerteza gera.

Entendemos que apenas com o efetivo funcionamento da ANPD teremos a necessária regulamentação da lei e o efetivo estabelecimento dos parâmetros de interpretação e de aplicação ainda ausentes relativos à proteção de dados sensíveis no Brasil, incluindo os dados de saúde tratados no contexto da pandemia causada pela disseminação do novo coronavírus (COVID-19).

COVID-19: the need for an appropriate regulatory framework to sensitive data protection in Brazil

Abstract: This article offers an analysis on the challenges of the implementation of an appropriate legal and regulatory framework for sensitive data protection in Brazil. Although such challenges already existed, the current crisis scenario has highlighted them, due to the dissemination of technological tools to restrain and control the COVID-19 pandemic, which involve the processing of personal data. To do so, the article analyses two central topics of the Brazilian data protection law (Lei Geral de Proteção de Dados) on sensitive personal data: the category of biometric data and consent as the main legal basis for the processing of sensitive personal data. In this analysis we will evince the differences between the Brazilian and European regimes, as well as the challenges that result from the legislator's choices.

Keywords: LGPD; sensitive personal data; biometric data; consent; pandemic; Covid-19; contact-tracing.

Referências

A29DPWP – ARTICLE 29 DATA PROTECTION WORKING PARTY. *Working document on biometrics*. 01/08/2003 Disponível em: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2003/wp80_en.pdf. Último acesso em: 14 jul. 2020.

A29DPWP – ARTICLE 29 DATA PROTECTION WORKING PARTY. *Opinion 4/2007 on the concept of personal data*. 20/06/2007. Disponível em: https://www.clinicalstudydatarequest.com/Documents/Privacy-European-guidance.pdf. Último acesso em: 14 jul. 2020.

A29DPWP – ARTICLE 29 DATA PROTECTION WORKING PARTY. *Opinion 02/2012 on facial recognition in online and mobile services*. 22/03/2012. Disponível em: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp192_en.pdf. Último acesso em: 14 jul. 2020.

A29DPWP – ARTICLE 29 DATA PROTECTION WORKING PARTY. *Opinion 3/2012 on developments in biometric technologies*. 27/04/2012. Disponível em: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp193_en.pdf. Último acesso em: 14 jul. 2020.

BIONI, Bruno Ricardo. *Proteção de Dados Pessoais* – A Função e os Limites do Consentimento. Rio de Janeiro: Forense. Edição do Kindle. 2019.

BRASIL. *Lei nº 12.965, de 23 de abril de 2014*. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília, DF, abril de 2014.

BRASIL. *Lei nº 13.709 de 14 de agosto de 2018*. Lei Geral de Proteção de Dados Pessoais (LGPD). (Redação dada pela Lei nº 13.853, de 2019). Brasília, DF, abril de 2018.

BRASIL. *Medida Provisória nº 954, de 17 de abril de 2020*. Dispõe sobre o compartilhamento de dados por empresas de telecomunicações prestadoras de Serviço Telefônico Fixo Comutado e de Serviço Móvel Pessoal com a Fundação Instituto Brasileiro de Geografia e Estatística, para fins de suporte à produção estatística oficial durante a situação de emergência de saúde pública de importância internacional decorrente do coronavírus (covid-19), de que trata a Lei nº 13.979, de 6 de fevereiro de 2020. Brasília, DF, abril de 2018.

BRASIL. *Medida Provisória nº 959, de 29 de abril de 2020*. Estabelece a operacionalização do pagamento do Benefício Emergencial de Preservação do Emprego e da Renda e do benefício emergencial mensal de que trata a Medida Provisória nº 936, de 1º de abril de 2020, e prorroga a vacatio legis da Lei nº 13.709, de 14 de agosto de 2018, que estabelece a Lei Geral de Proteção de Dados Pessoais - LGPD. Brasília, DF, abril de 2018.

BRASIL. Ministério da Saúde. Coronavírus SUS. Disponível em: https://www.gov.br/pt-br/apps/coronavirus-sus. Último acesso em: 14 jul. 2020.

CHAVES, Luis Fernando Prado; VIDIGAL, Paulo. *Privacy implications of Coronavirus tracking mobile apps*. Disponível em: https://www.lexology.com/library/detail.aspx?g=498613c4-9587-4117-9ff2-de99d614ee99. Último acesso em: 14 jul. 2020.

CIDRI NETO, Oscar Carlos. *O Tratamento de dados pessoais e sensíveis frente ao contact tracing durante o COVID-19*. Grupo de Estudos de Direito Autoral e Industrial da Universidade Federal do Paraná. Junho, 2020. Disponível em: https://www.gedai.com.br/o-tratamento-de-dados-pessoais-e-sensiveis-frente-ao-contact-tracing-durante-o-covid-19/. Último acesso em: 14 jul. 2020.

COMMISSION NATIONALE INFORMATIQUE & LIBERTÉS (CNIL). *Reconnaissance Faciale: pour un débat à la hauter des enjeux*. Novembro, 2019. Disponível em: https://www.cnil.fr/sites/default/files/atoms/files/reconnaissance_faciale.pdf. Último acesso em: 14 jul. 2020.

EUROPEAN DATA PROTECTION BOARD (EDPB). *Diretrizes 03/2020 sobre o tratamento de dados relativos à saúde para efeitos de investigação científica no contexto do surto de COVID-19*. 2020. Disponível em: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202003_healthdatascientificresearchcovid19_pt.pdf. Último acesso em: 14 jul. 2020.

EUROPEAN DATA PROTECTION BOARD (EDPB). *Diretrizes 4/2020 sobre a utilização de dados de localização e meios de rastreio de contactos no contexto do surto de COVID-19*. Adotadas em 21 de abril de 2020. Disponível em: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_20200420_contact_tracing_covid_with_annex_pt.pdf. Último acesso em: 14 jul. 2020.

GLOBAL PRIVACY ASSEMBLY (GPA). *COVID-19 Resources Library*. Disponível em: https://globalprivacyassembly.org/covid19/covid19-resources/. Último acesso em: 14 jul. 2020.

GROSSMAN, Luís Osvaldo. Casa Civil nega obstrução, mas argumenta que COVID-19 atrasou Autoridade de Dados. *Convergência Digital*, São Paulo, 13/07/2020. Governo/Legislação. Disponível em: https://www.convergenciadigital.com.br/cgi/cgilua.exe/sys/start.htm?UserActiveTemplate=site&infoid=54207&sid=9. Último acesso em: 14 jul. 2020.

GRÜVEN, Kübra. *Facial Recognition Technology:* Lawfulness of Processing under the GDPR in Employment, Digital Signage and Retail Context. Tese de mestrado, Tilburg University, 2019. Disponivel em: http://arno.uvt.nl/show.cgi?fid=147258. Último acesso em: 14 jul. 2020.

INFORMATION COMISSIONER'S OFFICE (ICO). *Guide to the General Data Protection Rules.* Disponível em: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/special-category-data/what-is-special-category-data/#scd4. Último acesso em: 14 jul. 2020.

JASSERAND, Catherine. *Legal nature of biometric data: from 'generic' personal data to sensitive data*. University of Groningen Faculty of Law Research Paper Series n. 24/2018. Junho de 2016

KORKMAZ, Maria Regina Detoni Cavalcanti Rigolon. *Dados Sensíveis na Lei Geral de Proteção de Dados Pessoais*: mecanismos de tutela para o livre desenvolvimento da personalidade. Tese de mestrado da Faculdade de Direito da Universidade Federal de Juiz de Fora. Juiz de Fora, 2019. Disponível em: https://repositorio.ufjf.br/jspui/bitstream/ufjf/11438/1/mariareginadetonicavalcantirigolonkorkmaz.pdf. Último acesso em: 14 jul. 2020.

MEDEIROS, Henrique. Covid-19: 173 milhões de pessoas baixaram apps de rastreamento de contatos. *Mobile Time*, 14/07/20. Disponível em: https://www.mobiletime.com.br/noticias/14/07/2020/covid-19-173-milhoes-de-pessoas-baixaram-apps-de-rastreio-de-contato/. Último acesso em: 16 jul. 2020.

MENDES, Laura Schertel. *Privacidade, proteção de dados e defesa do consumidor:* linhas gerais de um novo direito fundamental. São Paulo: Saraiva Educação, 2014. (Série IDP: linha de pesquisa acadêmica).

MENDES, Laura Schertel. Decisão histórica do STF reconhece direito fundamental à proteção de dados pessoais. *Jota*, 10/05/2020. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/decisao-historica-do-stf-reconhece-direito-fundamental-a-protecao-de-dados-pessoais-10052020. Último acesso em: 06 jul. 2020.

MULHOLLAND, Caitlin Sampaio. Dados Pessoais Sensíveis e a Tutela de Direitos Fundamentais: uma análise à luz da Lei Geral de Proteção de Dados (Lei nº 13.709/18). *R. Dir. Gar. Fund.*, Vitória, v. 19, n. 3, p. 159-180, set./dezembro, 2018. Disponível em: file:///D:/Users/Beatriz%20Bellintani/AppData/Local/Temp/1603-4931-1-PB-1.pdf. Último acesso em: 16 jul. 2020.

NEGRI, Sérgio Marcos Carvalho de Ávila; KORKMAZ, Maria Regina Detoni Cavalcanti Rigolon. A normatividade dos dados sensíveis na Lei Geral de Proteção de dados: ampliação conceitual e proteção da pessoa humana. *Rev. de Direito, Governança e Novas Tecnologias*, v. 5 n. 1, p. 63-85. Goiânia, Jan/Jun. 2019 (p. 74). Disponível em: https://indexlaw.org/index.php/revistadgnt/article/view/5479/pdf

NORTON ROSE FULBRIGHT. *Contact tracing apps: a new world for data privacy*. Junho, 2020. Disponível em: https://www.nortonrosefulbright.com/en-sg/knowledge/publications/d7a9a296/contact-tracing-apps-a-new-world-for-data-privacy#Singapore

NORTON ROSE FULBRIGHT. *Contact tracing apps in Singapore: a new world for data privacy*. 11/06/2020. Disponível em: https://www.nortonrosefulbright.com/-/media/files/nrf/nrfweb/contact-tracing/singapore-contact-tracing.pdf?la=en-sg&revision=. Último acesso em: 14 ago. 2020.

ORGANIZAÇÃO PARA A COOPERAÇÃO E DESENVOLVIMENTO (OCDE). *Tracking and tracing COVID*: Protecting privacy and data while using apps and biometrics in Policy Responses to Coronavirus (COVID-19). Paris, 2020. Disponível em: http://www.oecd.org/coronavirus/policy-responses/tracking-and-tracing-covid-protecting-privacy-and-data-while-using-apps-and-biometrics-8f394636/#section-d1e181. Último acesso em: 14 jul. 2020.

ORGANIZAÇÃO PARA A COOPERAÇÃO E DESENVOLVIMENTO (OCDE). *Leveraging biometric data adds both benefits and challenges*. Paris, 2020. Disponível em: http://www.oecd.org/coronavirus/policy-responses/tracking-and-tracing-covid-protecting-privacy-and-data-while-using-apps-and-biometrics-8f394636/#section-d1e194. Último acesso em: 14 jul. 2020.

TSANG, Amanda. *Here are the contact tracing apps being deployed around the world*. IAAP – The International Association of Privacy Professionals. 28/04/2020. Disponível em: https://iapp.org/news/a/here-are-the-contact-tracing-apps-being-employed-around-the-world. Último acesso em: 14 jul. 2020.

UNIÃO EUROPEIA. *Recital 51 on the GDPR*. Disponível em: https://www.privacy-regulation.eu/en/recital-51-GDPR.htm. Último acesso em: 14 jul. 2020.

VARKIANI, Marianne. *Future of Privacy Forum. Comparing Privacy Laws*: GDPR *v.* CCPA. Data Guidance, 18/12/2019. Disponível em: https://fpf.org/2019/12/18/comparing-privacy-laws-gdpr-v-ccpa/. Último acesso em: 14 jul. 2020.

Informação bibliográfica deste texto, conforme a NBR 6023:2018 da Associação Brasileira de Normas Técnicas (ABNT):

CORRÊA, Ivo; PAULA, Felipe de; BELLINTANI, Beatriz. COVID-19: a necessidade de disciplina adequada à proteção de dados sensíveis no Brasil. *Direitos Fundamentais & Justiça,* Belo Horizonte, ano 14, p. 179-206, nov. 2020. Número especial.

Recebido em: 30.07.2020
Pareceres: 13.08.2020, 31.08.2020
Aprovado em: 12.09.2020