Nota Técnica

O USO DE TECNOLOGIA DA INFORMAÇÃO PARA O ENFRENTAMENTO À PANDEMIA DA COVID-19

João Cláudio Basso Pompeu
Sivaldo Pereira da Silva
Daniel Pitangueira de Avelino
Igor Ferraz da Fonseca

Nº 38

Diest
Diretoria de Estudos e Políticas do Estado, das Instituições e da Democracia

Junho de 2020

ipea

Nota Técnica

O USO DE TECNOLOGIA DA INFORMAÇÃO PARA O ENFRENTAMENTO À PANDEMIA DA COVID-19

João Cláudio Basso Pompeu
Sivaldo Pereira da Silva
Daniel Pitangueira de Avelino
Igor Ferraz da Fonseca

Nº 38

Diest
Diretoria de Estudos e Políticas do Estado, das Instituições e da Democracia

ipea

Governo Federal

Ministério da Economia
Ministro Paulo Guedes

ipea **Instituto de Pesquisa Econômica Aplicada**

Fundação pública vinculada ao Ministério da Economia, o Ipea fornece suporte técnico e institucional às ações governamentais – possibilitando a formulação de inúmeras políticas públicas e programas de desenvolvimento brasileiros – e disponibiliza, para a sociedade, pesquisas e estudos realizados por seus técnicos.

Presidente
Carlos von Doellinger

Diretor de Desenvolvimento Institucional
Manoel Rodrigues Junior

Diretora de Estudos e Políticas do Estado, das Instituições e da Democracia
Flávia de Holanda Schmidt

Diretor de Estudos e Políticas Macroeconômicas
José Ronaldo de Castro Souza Júnior

Diretor de Estudos e Políticas Regionais, Urbanas e Ambientais
Nilo Luiz Saccaro Júnior

Diretor de Estudos e Políticas Setoriais de Inovação e Infraestrutura
André Tortato Rauen

Diretora de Estudos e Políticas Sociais
Lenita Maria Turchi

Diretor de Estudos e Relações Econômicas e Políticas Internacionais
Ivan Tiago Machado Oliveira

Assessora-chefe de Imprensa e Comunicação
Mylena Fiori

Ouvidoria: http://www.ipea.gov.br/ouvidoria
URL: http://www.ipea.gov.br

Nota Técnica

O USO DE TECNOLOGIA DA INFORMAÇÃO PARA O ENFRENTAMENTO À PANDEMIA DA COVID-19

João Cláudio Basso Pompeu
Sivaldo Pereira da Silva
Daniel Pitangueira de Avelino
Igor Ferraz da Fonseca

Nº 38

Diest
Diretoria de Estudos e Políticas do Estado, das Instituições e da Democracia

Junho de 2020

ipea

EQUIPE TÉCNICA

João Cláudio Basso Pompeu
Especialista em políticas públicas e gestão governamental na Diretoria de Estudos e Políticas do Estado, das Instituições e da Democracia (Diest) do Ipea. *E-mail*: <joao.pompeu@ipea.gov.br>.

Sivaldo Pereira da Silva
Professor da Faculdade de Comunicação (FAC) da Universidade de Brasília (UnB) e bolsista no Programa de Pesquisa para o Desenvolvimento Nacional (PNPD) na Diest/Ipea. *E-mail*: <sivaldop@gmail.com>.

Daniel Pitangueira de Avelino
Especialista em políticas públicas e gestão governamental na Diest/Ipea. *E-mail:* <daniel.avelino@ipea.gov.br>.

Igor Ferraz da Fonseca
Técnico de planejamento e pesquisa na Diest/Ipea. *E-mail*: <igor.fonseca@ipea.gov.br>.

SUMÁRIO

1 INTRODUÇÃO

Alguns países asiáticos têm obtido melhores resultados no controle da disseminação do novo coronavírus (Covid-19) do que os Estados Unidos e a maioria dos países europeus, o que surpreende pelo fato de estarem situados na região apontada como foco original da doença.

Três fatores têm sido apontados para esse sucesso: *i)* o fato de esses países terem passado pela epidemia da Sars, em 2003, o que os preparou para o controle de pandemias; *ii)* fatores culturais, tais como a maior obediência da população às recomendações governamentais; e iii) o uso intensivo de tecnologia da informação e comunicação – TICs (Castillo, 2020; Wang *et al.*, 2020; Ting *et al.*, 2020; Huang, Sun e Sui, 2020).[1]

Esta nota técnica aborda esse último fator. O uso de dados pessoais permanece como o ponto mais controverso a respeito da utilização de tecnologias da informação (TIs) para o combate à pandemia. Por um lado, há uma questão de interesse público representada pela necessidade de coleta de informações para o dimensionamento do problema e planejamento adequado das respostas governamentais. Por outro, há um fundamentado receio de que o compartilhamento de informações que não foram fornecidas com essa finalidade possa representar uma violação da intimidade e da privacidade dos indivíduos.

A próxima seção revisa brevemente algumas experiências do uso de TI para o controle da pandemia em países asiáticos e no Brasil. Pelo fato do surgimento da pandemia ser muito recente e haver poucos estudos acadêmicos sobre ela, esta seção se baseia principalmente em artigos da imprensa coletados na internet. Os limites para acesso e compartilhamento de dados pessoais são centrais nestas discussões e serão tratados na seção 3, sob a perspectiva da legislação brasileira. Na seção 4, os modelos de uso de tecnologias de acesso à informação são cotejados com a legislação brasileira. Ao fim, algumas considerações e recomendações são apresentadas.

2 EXPERIÊNCIAS INTERNACIONAIS NO USO DE TECNOLOGIA DA INFORMAÇÃO NO CONTROLE DA PANDEMIA DA COVID-19

É cada vez mais intensivo o uso de TIs que utilizam amplos conjuntos de dados (*Big Data*). Essas tecnologias, utilizadas tanto por governos quanto por grandes corporações econômicas, são vistas, por um lado, em uma perspectiva "apologética", como uma nova revolução na comunicação, que trará benefícios para a economia e contribuirá para o maior bem-estar dos cidadãos (Macfee e Brynolfsson, 2017; Mayer-Schonberger e Cukier, 2014). Por outro lado, em uma perspectiva "distópica", como uma ameaça à autonomia, um potencial gerador de desemprego, aumento de preconceitos e de desigualdade (O'Neil, 2016; Pasquale, 2015). As duas perspectivas, no entanto, reconhecem o potencial risco à privacidade individual representada pelas novas tecnologias.[2]

No enfrentamento à pandemia, vários países têm utilizado tecnologias que acessam informações pessoais sobre os cidadãos. Eles desenvolveram aplicativos com o "mesmo princípio: o cruzamento dos dados permite monitorar o trânsito das pessoas e, consequentemente, a transmissão do vírus" (Castro, 2020). As matérias jornalísticas a que tivemos acesso para a elaboração desta nota técnica não deixam claro que tipo de dados, além da localização geográfica são acessados pelos aplicativos, mas afirmam que é muito provável que os dados pessoais dos usuários sejam acessados. O uso destas tecnologias foi incentivado pelos governos destes países, e muitas vezes era obrigatório.

A Coreia do Sul tem sido reconhecida pelo uso de aplicativos de celular para o combate à pandemia. Dentre os principais aplicativos, destacam-se o *Corona100m* e o *Coronamap*.[3, 4] O *primeiro* é extremamente popular. Dez dias após o seu lançamento, mais de 1 milhão de pessoas haviam feito o seu *download*. Usando informações do governo, o *Corona100m* identifica se existem indivíduos potencialmente contaminados pela Covid-19 num raio de 100 metros do usuário. Já o *Coronamap* identifica regiões com casos confirmados de coronavírus. Este é atualmente o segundo aplicativo com mais *downloads* na Coreia do Sul. Ambos os aplicativos foram desenvolvidos por empresas privadas.

1. Para mais informações, ver: <https://bityli.com/JzQKH>.

2. "Meanwhile the danger to us as individuals shifts from privacy to probability: algorithms will predict the likelihood that one will get a heart attack (and pay more for health insurance), default on a mortgage (and be denied a loan), or commit a crime (and perhaps get arrested in advance). It leads to an ethical consideration of the role of the free will versus the dictatorship of data. Should individual volition trump big data, even if statistics argue otherwise? Just as the printing press prepared the ground for laws guaranteeing free speech (...) the age of big data will require new rules to safeguard the sanctity of the individual" (Mayer-Schonberger e Cukier, 2014, p. 17).

3. Para mais dados, ver: <https://bityli.com/CQlaE>.

4. Para mais informações, ver: <https://bityli.com/cSPmh>.

Outro país que tem sido destaque positivo no controle da pandemia é Singapura. Neste país, um dos destaques foi o aplicativo *TraceTogether*, desenvolvido pelo governo, que identifica todos os contatos físicos mantidos pelo usuário nos últimos quatorze dias com outras pessoas. Os cidadãos são fortemente encorajados a utilizar este aplicativo. Uma pesquisa do governo demonstra que 70% da população aprovava o uso destas tecnologias (Huang, Sun e Sui, 2020). Uma vez identificado que determinado cidadão está infectado, o Ministério da Saúde do país solicita a sua permissão para ter acesso a todas as pessoas com quem ele manteve contato em período recente. Tais pessoas são aconselhadas a procurar as autoridades médicas.[5]

Se, no caso de Singapura, o governo teve preocupações com a privacidade dos usuários – a partir da requisição de permissão dos usuários do *TraceTogether* – este não parece ser o caso da China. Neste país, foi amplamente utilizado o aplicativo *Alipay Health Code*, uma plataforma de pagamentos criada na China em 2004.[6] Este aplicativo fornece um código QR que dá três cores aos usuários de seus celulares (Kupferschmidt e Cohen, 2020).[7] A cor verde indica que o usuário pode transitar livremente. A amarela significa que o usuário deve fazer quarentena por uma semana. A cor vermelha implica que o usuário deve fazer quarentena por duas semanas. O que não está claro é como a empresa classifica os usuários.[8] A hipótese mais provável é que ela usa algoritmos para prever a possibilidade de o usuário estar infectado. Na prática, mesmo não tendo havido uma determinação explícita do governo, as matérias informam que esse aplicativo foi usado como um "passaporte", tendo sido exigido pela polícia para que os cidadãos pudessem transitar pelas cidades.[9] Isto gera questões relevantes sobre a privacidade do usuário e sobre sua liberdade enquanto cidadão.[10] Como diz Castro (2020): "No caso chinês cabe dizer, ainda, que a plataforma embora garanta a proteção dos dados individuais, não oferece instrumentos de monitoramento e controle sociais da sua utilização – ou seja, não está publicizado em código aberto. Além disso também cabe referir o fato sociológico e político importante de que houve uma tendência geral de que os chineses aderissem às novas funções do aplicativo, justamente para obter o referido código QR, percebido como um atestado de pureza para a vida social."

Dilemas em torno da privacidade e da liberdade também surgem no modelo adotado por Hong Kong. Em tal caso, o governo utilizou o aplicativo *Stayhomesafe.*[11] Trata-se de uma pulseira eletrônica de uso obrigatório para as pessoas que ingressaram no país e para aquelas colocadas em quarentena. O governo monitorava o uso da pulseira durante todo o período. O cidadão estava sujeito a uma pena de seis meses de prisão e multa caso saísse de sua residência sem permissão (Huan, Sun e Sui, 2020).

O governo de Taiwan, país territorialmente próximo à China, no qual há milhares de cidadãos que residem ou trabalham naquele país, fez amplo uso da TI, monitorando os passageiros que chegaram ou partiram da região de Wuhan (onde a pandemia começou) e identificando qualquer cidadão que manifestasse sintomas da doença (Wang *et al.*, 2020).

Em relação às experiências mencionadas no continente asiático, o uso de TICs e aplicativos específicos para a Covid-19 ainda é embrionário no Brasil. Não obstante, existem algumas iniciativas em curso. Uma delas é o portal e aplicativo do Meudigisus, criado pelo Ministério da Saúde (MS), que fornece dados sobre a saúde do usuário.[12] Embora seja anterior a pandemia da Covid-19, o Meudigisus pode ser um aliado no combate ao coronavírus. Mais especificamente, o MS criou o aplicativo Coronavírus – SUS[13] que fornece informações sobre a doença, informa a localização de unidades de saúde e fornece outros serviços.

Os aplicativos geridos pelo MS ainda são recentes e não são centrais nas estratégias dos governos brasileiros para o controle da pandemia. Embora não seja um aplicativo, a principal TIC utilizada pelos governos na definição de políticas e estratégias para o enfrentamento da pandemia tem sido a mensuração do índice de isolamento social. Divulgado diariamente, esse índice é calculado por meio de aplicativos de interface de programação (APIs) de empresas parceiras e permite estimar o número de pessoas que está em isolamento em determinado dia e território. Segundo informações disponíveis, os índices de isolamento não permitem a divulgação de dados pessoais.[14]

5. Disponível em: <https://www.gov.sg/article/help-speed-up-contact-tracing-with-tracetogether>.
6. Disponível em: <https://intl.alipay.com/?locale=pt_BR>.
7. Disponível em: <https://www.nytimes.com/2020/03/01/business/china-coronavirus-surveillance.html>.
8. Disponível em: <https://www.theguardian.com/world/2020/apr/01/chinas-coronavirus-health-code-apps-raise-concerns-over-privacy>.
9. Disponível em: <https://hbr.org/2020/04/how-digital-contact-tracing-slowed-covid-19-in-east-asia>.
10. Disponível em: <https://www.japantimes.co.jp/news/2020/03/24/asia-pacific/china-green-light-alipay-app/#.XrXXV2hKjIU>.
11. Disponível em: <https://www.coronavirus.gov.hk/eng/stay-home-safe.html>.
12. Disponível em: <https://meudigisus.saude.gov.br/>.
13. Disponível em: <https://www.gov.br/pt-br/apps/coronavirus-sus>.
14. Disponível em: <http://www.cofen.gov.br/mapa-mostra-indices-de-isolamento-social-no-brasil_78808.html>.

3 QUADRO NORMATIVO DA PROTEÇÃO DE DADOS NO BRASIL

Embora o debate jurídico sobre privacidade tenha se configurado mais claramente desde o fim do século XIX (Warren e Brandeis, 1890), a discussão sobre leis de proteção de dados pessoais no contexto do uso massivo de dados começa a se formar, de fato, nas últimas décadas do século XX.

Mendes (2014), com base na análise geracional de Viktor Mayer-Schönberger (1997), explica esse processo de produção normativa em "gerações" de leis de proteção de dados. A primeira geração surgiu na década de 1970, no contexto de centralização de grandes bancos de dados nacionais. Nesse período, ganharam destaque as iniciativas governamentais, no âmbito do Estado de Bem-Estar Social, de coleta e armazenamento de dados populacionais, confrontadas por reações dos cidadãos contra os riscos da centralização de informações pessoais. As normas desse período enfatizavam uma perspectiva funcional, disciplinando procedimentos e orientações técnicas para a formação de bases de dados.

A segunda geração de leis de proteção de dados nasce da insuficiência das normas anteriores para alcançar um conjunto de bancos de dados públicos e privados cada vez mais fragmentados. É caracterizada por normas de hierarquia superior, inseridas em textos constitucionais e enfatiza uma perspectiva de direitos, associada à privacidade e às liberdades individuais. A estratégia regulatória é marcada pela ampliação de poderes das autoridades administrativas responsáveis pela proteção de dados.

A terceira geração toma forma a partir da decisão de 1983 do Tribunal Constitucional alemão que declarou a inconstitucionalidade parcial da Lei do Censo daquele país. A corte defendeu o direito à "autodeterminação informativa", prevendo a participação dos indivíduos no controle sobre o processamento de seus dados.

Por fim, a quarta geração de leis de proteção de dados tentou tornar mais factível o exercício dessas garantias, diminuindo custos e riscos para os indivíduos. Por um lado, procurou fortalecer o controle dos indivíduos sobre os próprios dados, mas, por outro, reconheceu a existência de dados sensíveis (como etnia, religião, sexualidade) que deveriam ser protegidos independentemente do consentimento individual. Também surgiram normas setoriais, complementando as leis nacionais de caráter mais geral.

No caso brasileiro, esse percurso geracional também pode ser observado. O Código Penal (Decreto-Lei nº 2.848/1940), como exemplo de norma de primeira geração, previa a violação de correspondência e de comunicação telegráfica, radioelétrica ou telefônica como modalidades de crimes contra a liberdade individual. A Constituição Federal de 1988 (CF/1988) confirmou a inviolabilidade da vida privada como um direito fundamental e, no seu art. 5º, XII, expressamente menciona a inviolabilidade do sigilo "de dados",[15] refletindo a elevação hierárquica típica das normas de segunda geração.

A definição dos "dados" alcançados por essa proteção não está expressa na Constituição e, nesse sentido, a legislação infraconstitucional vem traçando tais contornos de modo mais flexível. O Código de Defesa do Consumidor (Lei nº 8.078/1990), por exemplo, previu a garantia de acesso do consumidor às suas próprias informações, bem como a possibilidade de correção dos dados, mas não previu limites ao quê e quanto poderia ser compartilhado. A possibilidade de interceptação de comunicações telefônicas, por ordem judicial, foi disciplinada pela Lei nº 9.296, de 24 de julho de 1996, que previu sua aplicação também "à interceptação do fluxo de comunicações em sistemas de informática e telemática" (art. 1º).

Em 2014, foi sancionada a Lei nº 12.965, que "estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil" e veio a ser conhecida como o Marco Civil da Internet. Entre os princípios listados no seu art. 3º estão incluídas a proteção da privacidade (inciso II) e a proteção dos dados pessoais (III). Em relação ao fluxo de comunicações e comunicações privadas armazenadas, a lei garante a inviolabilidade e o sigilo, salvo por ordem judicial (art. 7º, II e III), em um paralelismo em relação ao regramento referente ao sigilo das comunicações telefônicas.

Em relação ao fornecimento de dados pessoais (inciso VII), no entanto, o Marco Civil da Internet traz uma disciplina um pouco diferente. Nessa situação, desaparece a exigência de ordem judicial para violação do sigilo, que é substituída pela possibilidade de compartilhamento "mediante consentimento livre, expresso e informado". Além disso, inclui também uma autorização genérica para a violação "nas hipóteses previstas em lei".

15. XII – é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal.

Mais adiante, o Marco Civil da Internet disciplina os procedimentos para armazenamento e guarda de dados pessoais. Inicialmente, repete a regra de que "o conteúdo das comunicações privadas somente poderá ser disponibilizado mediante ordem judicial" (art. 10, § 2º). No entanto, admite "o acesso aos dados cadastrais que informem qualificação pessoal, filiação e endereço, na forma da lei, pelas autoridades administrativas que detenham competência legal para a sua requisição" (§ 3º).

Esse cenário se altera com a Lei nº 13.709, de 2018, conhecida como Lei Geral de Proteção de Dados Pessoais (LGPD). Em seu segundo artigo, lista os fundamentos da proteção de dados pessoais e inclui, entre eles, o respeito à privacidade e a autodeterminação informativa, elemento típico da terceira geração de normas de proteção de dados. Avança, ainda, em controvérsias próprias da quarta geração, como a possibilidade de tratamento de dados pessoais sensíveis (art. 11) com ou sem consentimento do titular.

É importante lembrar, ainda, que a criação da Autoridade Nacional de Proteção de Dados, prevista nos arts. 55 a 59 da LGPD, foi vetada pelo presidente da República, por questões formais. O órgão autárquico teria, entre outras funções, zelar pela proteção dos dados pessoais, fiscalizar e aplicar sanções em caso de descumprimento à legislação.

A Medida Provisória (MP) nº 869, de 27 de dezembro de 2018 (posteriormente convertida na Lei nº 13.853, de 8 de julho de 2019), criou a Autoridade Nacional de Proteção de Dados (ANPD), órgão federal que tem como finalidade editar normas e fiscalizar procedimentos que envolvem a proteção de dados pessoais.[16] O órgão, ainda sem existência jurídica na prática,[17], nascerá vinculado ao Poder Executivo federal (sem clara independência), embora a própria lei estipule que essa característica é transitória uma vez que a ANPD poderá se tornar uma autarquia (com maior autonomia) após dois anos de sua criação, a critério do governo federal.

4 ADEQUAÇÃO DAS EXPERIÊNCIAS DE TECNOLOGIA DA INFORMAÇÃO À LEGISLAÇÃO BRASILEIRA

O possível uso da TI no enfrentamento à pandemia suscita o debate sobre o acesso a dados pessoais por órgãos governamentais. No caso brasileiro, a situação ganhou visibilidade com a edição da MP nº 954, de 2020, que previa, entre outras ações, a obrigatoriedade de compartilhamento de dados pessoais (como nome, número de telefone e endereço) em poder das operadoras de serviços telefônicos, mediante requisição do poder público. Os dados seriam fornecidos apenas durante o período de emergência de saúde pública decorrente do coronavírus e seriam utilizados "exclusivamente pela Fundação IBGE para a produção estatística oficial". Visto com desconfiança, o ato normativo foi objeto de vários questionamentos judiciais, até que teve sua eficácia suspensa por decisão do Supremo Tribunal Federal (STF), para prevenir "danos irreparáveis à intimidade e ao sigilo da vida privada de mais de uma centena de milhão de usuários dos serviços de telefonia fixa e móvel".[18]

Casos como o da MP nº 954/2020 evidenciam o papel decisivo assumido pelo Poder Judiciário na solução dessas controvérsias. Mais do que protagonismo judicial, esse deslocamento da arena decisória é um indício de que as ações adotadas pelo Poder Executivo não estão sendo suficientes para provocar a coesão de esforços que se espera em um momento de emergência de saúde pública.

O quadro normativo brasileiro é um dos fatores que estimulam esse dissenso. Há, de um lado, uma afirmação constitucional ampla do direito à proteção de dados e, de outro, uma legislação infraconstitucional que trouxe poucas garantias aos titulares de dados pessoais, nos momentos de compartilhamento dessas informações. A LGPD inaugurou uma nova perspectiva, trazendo conceitos e debates próprios de terceira e quarta geração, mais voltados à ampliação da participação dos cidadãos no controle do tratamento dos seus dados. Essas medidas de garantia, no entanto, ainda não foram implementadas de maneira adequada, o que estimula ainda mais a desconfiança e as resistências ao uso de TI no combate à pandemia.

16. A Lei nº 13.853/2020 também modificou o prazo para início de vigência da LGPD para 24 meses após sua publicação (ou seja, agosto de 2020). No entanto, essa regra foi modificada pela MP nº 959, em apreciação no Congresso Nacional, que adiou o início da vigência para 3 de maio de 2021. Por sua vez, o Projeto de Lei (PL) nº 1.179/2020 (autoria do senador Antonio Anastasia PSD/MG), aguardando sanção presidencial, estabelece o início da vigência da lei (exceto as punições) em 1º de janeiro de 2021. É importante ressaltar que as disposições sobre a criação da ANPD já estão em vigor.

17. De forma mais restrita, o Decreto nº 10.046, de 9 de outubro de 2019, criou o Comitê Central de Governança de Dados (CCGD) no âmbito do poder público federal, com competência para deliberar sobre "as regras e os parâmetros para o compartilhamento restrito, incluídos os padrões relativos à preservação do sigilo e da segurança" (art. 21, II), entre outras. Na ausência da ANPD, é o CCGD, sob a coordenação da Secretaria de Governo Digital do Ministério da Economia, que vem adotando as medidas para a implementação da LGPD no âmbito do governo federal (a exemplo do Guia de Boas Práticas adotado por resolução de abril de 2020).

18. Na Ação Direta de Inconstitucionalidade (ADI) nº 6.387. Disponível em: <http://www.stf.jus.br/arquivo/cms/noticiaNoticiaStf/anexo/ADI-6387MC.pdf>.

As experiências apresentadas na seção 2 desta nota técnica mostram que há duas maneiras de se utilizar a TI para o combate à pandemia: uma estratégia "centralizada", na qual o governo acessa os dados pessoais dos cidadãos sem o seu consentimento (modelo chinês); e uma abordagem "descentralizada", na qual os cidadãos permitem o acesso a seus celulares pelas autoridades de maneira que elas possam identificar a localização dos indivíduos, assim como os contatos por eles mantidos em períodos recentes (modelo de Singapura). Os países europeus, em geral, estão adotando o segundo modelo.[19]

Analisando as experiências internacionais, pode-se inferir que a utilização de tecnologias semelhantes seria complexa no Brasil. Os aplicativos relatados na seção 2 desta nota técnica, com exceção do aplicativo de Singapura, tendem a conflitar com a LGPD. Tais aplicativos, na maioria dos casos, acessam os dados pessoais sem o consentimento dos usuários, o que contraria o disposto no inciso I do art. 7º. No entanto, a lei prevê que dados pessoais sensíveis podem ser tratados sem o consentimento do cidadão se envolverem proteção à vida do titular ou de terceiro (alínea 'e' do inciso II do art. 11). Uma interpretação abrangente da lei pode alegar que a informação sobre o deslocamento do usuário pela cidade é importante para a proteção da sua vida ou de terceiro. Dessa forma, o governo poderia, em tese, acessar os dados pessoais sem o consentimento do cidadão e teria uma estimativa do número de cidadãos que não estão cumprindo normas de isolamento social. Essa é uma discussão a ser enfrentada pelo sistema Judiciário em casos concretos.

Uma preocupação a ser endereçada é a garantia de que o acesso aos dados se limite ao menor número de informações possíveis e que não haja possibilidade de vazamentos. Esse tipo de precaução não é seguida pelas experiências internacionais de tipo centralizadas, mas seriam obrigatórias caso fossem implementadas no Brasil. No uso de dados pessoais para aplicações, a anonimização da coleta de dados deve ser uma premissa, não sendo necessária a vinculação de dados pessoais como o número do celular, o endereço do usuário, entre outros. A adoção de aplicativos auxiliares no combate à pandemia precisa respeitar os direitos expressos na legislação sobre o tema. Assim sendo, as experiências "descentralizadas" seriam modelos mais adequados à nossa realidade do que as "centralizadas".

Nesse sentido, atendendo ao princípio da prevenção e segurança dos dados, conforme a lei brasileira exige, o processamento também precisa ser, sempre que possível, descentralizado. Para isso, é preciso lançar mão de tecnologias com privacidade *by design*, como por exemplo, o *bluetooth*, em que os aparelhos conversam entre si, sem precisar de um agente centralizando os dados e mantendo a maior parte das informações fragmentada nos celulares e não em uma base de dados única.[20]

Quando excepcionalmente houver a necessidade de processamento centralizado, isso deve ocorrer de modo criptografado, sendo importante haver justificativa quando algum nível de centralidade é adotado. Quem gerencia o sistema determina o que o algoritmo deve fazer com os dados, mas o gerente não deve ter acesso a eles.

Para responder ao princípio da finalidade e segurança, o acesso aos dados deve ficar restrito somente aos agentes que precisam usar as informações para combater a pandemia e devem ser guardados de forma segura para evitar vazamentos ou falhas similares. A coleta deve ser feita sempre que possível por amostragem (evitando o universo dos dados), pois isso diminui o custo de coleta e processamento, aumenta a velocidade de tratamento e também serve como um instrumento adicional de segurança. A coleta de dados sem o consentimento do cidadão, quando autorizada pelo Poder Judiciário, deve se limitar às informações absolutamente necessárias ao enfrentamento da pandemia.

5 CONSIDERAÇÕES E RECOMENDAÇÕES

Levando em conta os princípios estabelecidos na legislação brasileira e observando estudos científicos, relatórios de organizações especializadas e organismos multilaterais (Abeler *et al.*, 2020; Bell *et al.*, 2020; Ienca e Vayena, 2020; Castillo *et al.*, 2020; Yasaka,2020; Accessnow, 2020; EENA, 2020; OECD, 2020; CEPD, 2020) que vêm alimentando o debate sobre o tema, são apresentadas algumas recomendações que envolvem o devido uso de dados para aplicações no combate à Covid-19:

19. Disponível em: <https://reut.rs/2BJ9FaE>.

20. Por exemplo, no aplicativo TraceTogether a função de *bluetooth* do aparelho detecta se duas pessoas tiveram aproximação o suficiente para um risco de infecção. O aplicativo criptografa dados, gera um ID temporário e quando um outro telefone se aproxima, isso é gravado e armazenado localmente, isto é, nos próprios aparelhos. Quando um usuário do aplicativo é diagnosticado com Covid-19, o médico pede para que ele compartilhe seus dados com o sistema. Se o usuário consentir, o computador-central recebe toda a informação dos IDs temporários do infectado. Este computador não está habilitado para identificar esta informação (que está criptografada), ele apenas notificará todos os donos dos celulares afetados que procurem fazer o teste ou se mantenham isolados no período exigido, pois houve proximidade com um infectado (sem a necessidade de identificação do usuário infectado) (Abeler *et al.*, 2020).

1) Elaboração de uma estratégia – construída de forma dialogada com os órgãos reguladores, as operadoras de telecomunicações, organizações civis, academia e Parlamento – para coleta dos dados estatísticos necessários para subsidiar as políticas públicas.

2) Atuação junto aos ministérios, em especial ao Ministério da Saúde, para elaboração de normas setoriais sobre uso e proteção de dados pessoais no contexto da emergência de saúde pública.

3) Utilização e refinamento de ferramentas e bases de dados já existentes, atualmente disponíveis de forma fragmentada na administração pública federal, para suprimento das lacunas enquanto a Política Nacional de Proteção de Dados não for definida.

4) Os governos devem incentivar *hackatons*[21] para criar soluções com os dados abertos, preservando os princípios da LGPD.

5) A publicação de dados abertos precisa ser ágil e com qualidade, por todos os entes federativos (isso amplia o alcance e volume de atores pensando em soluções sobre o problema).

6) A presença de um ente regulador forte e independente seria de suma importância em cenários como esse, pois somente uma entidade instituída nestes termos seria capaz de incentivar, fiscalizar e estipular parâmetros para o uso correto de dados, visando às soluções efetivas.

7) Na ausência da ANPD, é necessário que haja a definição de um órgão equivalente para a coordenação das ações e proposição urgentes de uma Política Nacional de Proteção de Dados, construída com a participação dos diversos setores envolvidos (organizações civis, academia, empresas e governos).

REFERÊNCIAS

ABELER, Johannes et al. Covid-19 Contact Tracing and Data Protection Can Go Together. **JMIR Mhealth Uhealth**, v. 8, n. 4, p. 1-5, 2020.

ACCESSNOW. **Recommendations on privacy and data protection in the fight against Covid-19**. Nova York, 2020. Disponível em <https://www.accessnow.org/releases-recommendations-on-privacy-data-protection-covid-19/>.

BELL, James *et al.* **TraceSecure**: Towards Privacy Preserving Contact Tracing. ArXiv e-prints, 2020.

CASTILLO, Aída Ponce del. Covid-19 contact-tracing apps: how to prevent privacy from becoming the next victim. **ETUI Policy Brief: European Economic, Employment and Social Policy**, n. 5, 2020.

CASTRO, Fábio Fonseca de. **Impactos da Covid-19 sobre os processos comunicacionais**: primeiras observações sobre dinâmicas, impasses e riscos. 2020. Disponível em: <https://periodicos.ufpa.br/index.php/pnaea/article/view/8799/6270>.

CEPD – COMITÉ EUROPEU PARA A PROTEÇÃO DE DADOS. **Statement on the processing of personal data in the context of the COVID-19 outbreak**. Bruxelas: União Europeia, 2020. Disponível em: <https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_statement_2020_processingpersonaldataandcovid-19_en.pdf>.

EENA – EUROPEAN EMERGENCY NUMBER ASSOCIATION. COVID-19 Apps. Bruxelas: União Europeia, 2020. Disponível em: <https://eena.org/document/covid-19-apps/>.

HUANG, Yasheng; SUN, Meicen; SUI, Yuze. How digital contact tracing slowed Covid-19 in East-Asia. 2020. Disponível em: <https://hbr.org/2020/how-digital-contact-tracing-slowed-covid-19-in-east-asia>.

IENCA, Marcello; VAYENA, Effy. On the responsible use of digital data to tackle the COVID-19 pandemic. **Nature Medicine**, v. 26, p. 458-464, 2020.

KUPFERSCHMIDT, Kai; COHEN, Jon. Can China's Covid-19 strategy work elsewhere? **Science**, v. 367, n. 6482, p. 1061-1062, 2020.

McAFEE, Andrew; BRINJOLFSSON, Andrew. **Machine, platform, crowd**. Norton, Nova Iorque, 2017.

MAYER-SCHÖNBERGER, Viktor. Generational Development of Data Protection in Europe. *In*: AGRE, P.; ROTENBERG, M. (Eds.). **Technology and privacy**: the new landscape. Cambridge: MIT Press, 1997. p. 219-236.

MAYER-SCHÖNBERGER, Viktor; CUKIER, Kenneth. **Big Data**. Marinner Books, Boston, 2014.

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

21. *Hackatons* são maratonas de programação (realizadas, de forma ininterrupta, por horas, dias ou semanas) em que *hackers*, desenvolvedores e programadores exploram dados abertos e códigos, além de discutir, propor soluções inovadoras e inclusive criar novos *softwares* e *hardwares*.

OECD. Tracking and tracing COVID: Protecting privacy and data while using apps and biometrics. Paris: OECD, 2020. Disponível em: < http://www.oecd.org/coronavirus/policy-responses/tracking-and-tracingcovidprotecting-privacy--and-data-while-using-apps-and-biometrics-8f394636>.

O'NEIL, Cathy. **Wheapons of math destruction**. Nova Iorque: Broadway Books, 2016. 13.

OLIVER, Nuria *et al.* **Mobile phone data and COVID-19**: Missing an opportunity? arXiv, Cornell University, 2020. Disponível em: <https://arxiv.org/ftp/arxiv/papers/2003/2003.12347.pdf >. Acesso em: 28 maio 2020.

PASQUALE, Frank. **The black box society**. Cambridge: Harvard University Press, 2015.

TING, D. S. W. *et al.* Digital technology and Covid-19. **Nature Medicine**, v. 26, p. 459-461, 2020.

WANG, C. Jason; NG, Chun Y.; BROOK, Robert H. Response to Covid-19 in Taiwan: Big Data Analytics, New Technology, and Proactive Testing. **JAMA**, v. 323, n. 14, p. 1341-1342, 2020.

WARREN, Samuel Dennis; BRANDEIS, Louis Dembitz. The right to privacy. **Harvard Law Review**, v. IV, n. 5, Dec. 15 1890. Disponível em: <https://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html>. Acesso em: 14 maio 2020.

YASAKA, Tyler M. *et al.* Peer-to-Peer Contact Tracing: Development of a Privacy-Preserving Smartphone App. **JMIR Mhealth Uhealth**, v. 8, n. 4, p.1-8, 2020.

NORMAS CONSULTADAS

BRASIL. Decreto-Lei nº 2.848, de 7 de dezembro de 1940. **Código Penal**. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm>. Acesso em: 22 maio 2020.

_____. **Constituição da República Federativa do Brasil de 1988**. Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm>. Acesso em: 22 maio 2020.

_____. Lei nº 8.078, de 11 de setembro de 1990. Dispõe sobre a proteção do consumidor e dá outras providências. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/l8078.htm>. Acesso em: 22 maio 2020.

_____. Lei nº 9.296, de 24 de julho de 1996. Regulamenta o inciso XII, parte final, do art. 5º da Constituição Federal. Disponível em: <http://www.planalto.gov.br/ccivil_03/LEIS/L9296.htm>. Acesso em: 22 maio 2020.

_____. Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil. Disponível em: < http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm >. Acesso em: 22 maio 2020.

_____. Lei nº 13.709, de 14 de agosto de 2018 (a). Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015- 2018/2018/lei/L13709.htm>. Acesso em: 22 maio 2020.

_____. Presidência da República. Mensagem nº 451, de 14 de agosto de 2018 (b). Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/Msg/VEP/VEP-451.htm>. Acesso em: 22 maio 2020.

_____. Lei nº 13.869, de 5 de setembro de 2019 (a). Dispõe sobre os crimes de abuso de autoridade; altera a Lei nº 7.960, de 21 de dezembro de 1989, a Lei nº 9.296, de 24 de julho de 1996, a Lei nº 8.069, de 13 de julho de 1990, e a Lei nº 8.906, de 4 de julho de 1994; e revoga a Lei nº 4.898, de 9 de dezembro de 1965, e dispositivos do Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal). Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/L13869.htm>. Acesso em: 22 maio 2020.

_____. Decreto nº 10.046, de 9 de outubro de 2019 (b). Dispõe sobre a governança no compartilhamento de dados no âmbito da administração pública federal e institui o Cadastro Base do Cidadão e o Comitê Central de Governança de Dados. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2019/Decreto/D10046.htm>. Acesso em: 22 maio 2020.

_____. Lei nº 13.964, de 24 de dezembro de 2019 (c). Aperfeiçoa a legislação penal e processual penal. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/L13964.htm>. Acesso em: 22 maio 2020.

_____. Senado Federal. Projeto de Lei nº 1.179, de 2020 (a). Autoria Senador Antonio Anastasia (PSD/MG). Leitura da matéria na sessão do Senado Federal nº1, em 30 mar. 2020. Disponível em: <https://www25.senado.leg.br/web/atividade/materias/-/materia/141962>. Acesso em: 22 maio 2020.

_____. Medida Provisória nº 954, de 17 de abril de 2020 (b). 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. Disponível em: <http://www.planalto.gov.br/CCIVIL_03/_Ato2019-2022/2020/Mpv/mpv954.htm>. Acesso em: 22 maio 2020.

_____. Ministério da Economia. Comitê Central de Governança de Dados. Resolução nº 4, de 14 de abril de 2020. Disponibiliza o Guia de Boas Práticas para Implementação da Lei Geral de Proteção de Dados na Administração Pública Federal. Disponível em:<http://www.in.gov.br/web/dou/-/resolucao-n-4-de-14-de-abril-de-2020-253999748 >. Acesso em: 22 maio 2020.

_____. Supremo Tribunal Federal. Ação Direta de Inconstitucionalidade nº 6.387. Protocolada em 20 de abril 2020 (d). Relatora ministra Rosa Weber. Disponível em: <http://portal.stf.jus.br/processos/detalhe.asp?incidente=5895165>. Acesso em: 22 maio 2020.

ONU – ORGANIZAÇÃO DAS NAÇÕES UNIDAS. Declaração Universal dos Direitos Humanos. Tradução oficial para o português. Paris: ONU, 1948. Disponível em: <https://www.ohchr.org/EN/UDHR/Pages/Language.aspx?LangID=por>. Acesso em: 22 maio 2020.

Ipea – Instituto de Pesquisa Econômica Aplicada

EDITORIAL

Coordenação
Reginaldo da Silva Domingos

Assistente de Coordenação
Rafael Augusto Ferreira Cardoso

Supervisão
Camilla de Miranda Mariath Gomes
Everson da Silva Moura

Editoração
Aeromilson Trajano de Mesquita
Cristiano Ferreira de Araújo
Danilo Leite de Macedo Tavares
Herllyson da Silva Souza
Jeovah Herculano Szervinsk Junior
Leonardo Hideki Higa

Capa
Danielle de Oliveira Ayres
Flaviane Dias de Sant'ana

The manuscripts in languages other than Portuguese published herein have not been proofread.

Livraria Ipea
SBS – Quadra 1 – Bloco J – Ed. BNDES, Térreo
70076-900 – Brasília – DF
Tel.: (61) 2026-5336
Correio eletrônico: livraria@ipea.gov.br

Composto em linux libertine 10/13 (texto)
Ubuntu bold (títulos, gráficos e tabelas)
Brasília-DF

Missão do Ipea
Aprimorar as políticas públicas essenciais ao desenvolvimento brasileiro por meio da produção e disseminação de conhecimentos e da assessoria ao Estado nas suas decisões estratégicas.

ipea Instituto de Pesquisa Econômica Aplicada

MINISTÉRIO DA ECONOMIA

PÁTRIA AMADA BRASIL GOVERNO FEDERAL