

O USO DE TECNOLOGIA DA INFORMAÇÃO PARA O ENFRENTAMENTO DA PANDEMIA DA COVID-19^{1,2}

João Cláudio Basso Pompeu³

Sivaldo Pereira da Silva⁴

Daniel Pitangueira de Avelino⁵

Igor Ferraz da Fonseca⁶

1 INTRODUÇÃO

Alguns países asiáticos têm obtido melhores resultados no controle da disseminação do novo coronavírus (Covid-19), o que surpreende pelo fato de estarem situados na região considerada foco original da doença. Três fatores têm sido apontados para este sucesso: i) o fato desses países terem passado pela epidemia da síndrome respiratória aguda grave (*severe acute respiratory syndrome* – 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 (Castillo, 2020; Wang, Ng e Brook, 2020; Ting *et al.*, 2020; Huang, Sun e Sui, 2020). Este artigo aborda este último fator.

O uso de dados pessoais permanece como o ponto mais controverso a respeito da utilização de tecnologias da informação para o combate à pandemia. Por um lado, há uma questão de interesse público representada pela necessidade de coleta de informações para dimensionamento do problema e planejamento das respostas governamentais. Por outro, há o receio de que o compartilhamento de informações possa representar uma violação da privacidade dos indivíduos.

A seção 2 revisa brevemente algumas experiências com o uso de tecnologia da informação para o controle da pandemia em países asiáticos e no Brasil. Os limites legais para acesso e compartilhamento de dados pessoais no Brasil serão tratados na seção 3. Na seção 4, os modelos de uso de tecnologias de acesso à informação são cotejados com a legislação brasileira. Ao final, algumas considerações e recomendações são apresentadas.

2 EXPERIÊNCIAS INTERNACIONAIS NO USO DE TECNOLOGIA DA INFORMAÇÃO NO CONTROLE DA PANDEMIA

É cada vez mais intensivo o uso de tecnologias de informação que utilizam amplos conjuntos de dados (*big data*). Essas tecnologias 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 (McAfee e Brynjolfsson, 2017; Mayer-Schönberger e Cukier, 2014), e, por

1. DOI: <http://dx.doi.org/10.38116/bapi25art5>

2. Uma versão deste artigo foi publicada como *Nota Técnica* nº 38 pelo Ipea em junho de 2020. Disponível em: <https://www.ipea.gov.br/portal/index.php?option=com_content&view=article&id=35931>.

3. 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>.

4. Pesquisador do Programa de Pesquisa para o Desenvolvimento Nacional (PNPD) na Diest/Ipea; e professor na Faculdade de Comunicação da Universidade de Brasília (FAC/UnB). E-mail: <sivaldop@gmail.com>.

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

6. Técnico de planejamento e pesquisa na Diest/Ipea. E-mail: <igor.fonseca@ipea.gov.br>.

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 representado pelas novas tecnologias.

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, conseqüentemente, a transmissão do vírus” (Castro, 2020). 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, como o Corona 100m e o Coronamap (Santirso, 2020; Baleun e Minji, 2020). O Corona 100 m verifica se existem indivíduos potencialmente contaminados pela Covid-19 em um raio de 100 m do usuário. Já o Coronamap identifica regiões com casos confirmados de coronavírus.

Em Singapura, o aplicativo TraceTogether identifica todos os contatos físicos mantidos pelo usuário nos últimos catorze dias com outras pessoas. 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.

Na China, foi amplamente utilizado o aplicativo Alipay Health Code, que atribui três cores aos usuários dos celulares (Kupferschmidt e Cohen, 2020; Mozur, Zhong e Krolik, 2020): a cor verde indica que o usuário pode transitar livremente; a cor amarela, que o usuário deve fazer quarentena por uma semana; e a cor vermelha, que o usuário deve fazer quarentena por duas semanas. 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 (Huang, Sun e Sui, 2020).

Em Hong Kong, o governo utilizou o aplicativo Stay Home Safe,⁷ que acompanhava uma pulseira eletrônica de uso obrigatório para as pessoas que acessaram o país durante a 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 (Huang, Sun e Sui, 2020).

O governo de Taiwan fez amplo uso da tecnologia da informação, monitorando os passageiros que chegavam ou partiam da região de Wuhan e identificando qualquer cidadão que manifestasse sintomas da doença (Wang, Ng e Brook, 2020).

O uso de tecnologias da informação e aplicativos específicos para a Covid-19 ainda é embrionário no Brasil. O Ministério da Saúde criou o aplicativo Coronavírus-SUS,⁸ que informa sobre a doença, sobre a localização de unidades de saúde, e fornece outros serviços.

Embora não seja um aplicativo, a principal tecnologia da informação utilizada pelos governos na definição de políticas e estratégias para o enfrentamento da pandemia tem sido a mensuração do Índice de Isolamento Social, que permite estimar o número de pessoas que está em isolamento em determinado dia e território.

7. Disponível em: <<https://www.coronavirus.gov.hk/eng/stay-home-safe.html>>.

8. Disponível em: <<https://www.gov.br/pt-br/apps/coronavirus-sus>>.

3 QUADRO NORMATIVO DA PROTEÇÃO DE DADOS NO BRASIL

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) explica esse processo de produção normativa falando em “gerações” de leis de proteção de dados. A primeira geração surgiu na década de 1970, em um cenário de centralização de grandes bancos de dados nacionais. Nesse período, ganharam destaque as iniciativas 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 nasce da insuficiência das normas anteriores para alcançar um conjunto de bancos de dados públicos e privados cada vez mais fragmentados. Ela 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 tentou tornar mais factível o exercício dessas garantias, diminuindo custos e riscos para os indivíduos. Procurou, ao mesmo tempo, fortalecer o controle dos indivíduos sobre os próprios dados e reconhecer a existência de dados sensíveis que deveriam ser protegidos independentemente do consentimento individual.

Em 2014, foi sancionada a Lei nº 12.965, que “estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil” (Brasil, 2014) e que 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 (inciso III) (Brasil, 2014). A lei garante a inviolabilidade e o sigilo, 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” (Brasil, 2014). Além disso, o texto inclui também uma autorização genérica para a violação “nas hipóteses previstas em lei” (*op. cit.*).

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” (Brasil, 2014, art. 10, § 2º). Entretanto, 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” (Brasil, 2014, art. 10, § 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 art. 2º, ela lista os fundamentos da proteção de dados pessoais e inclui, entre eles, o respeito à privacidade e a autodeterminação informativa, elemento da terceira

geração de normas. 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.

4 ADEQUAÇÃO DAS EXPERIÊNCIAS COM TECNOLOGIA DA INFORMAÇÃO À LEGISLAÇÃO BRASILEIRA

O possível uso da tecnologia da informação no enfrentamento da pandemia suscita o debate sobre o acesso a dados pessoais por órgãos governamentais. No caso brasileiro, a edição da Medida Provisória nº 954, de 2020, previa, entre outras ações, a obrigatoriedade de compartilhamento de dados pessoais 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 [Instituto Brasileiro de Geografia e Estatística] para a produção estatística oficial”. O ato normativo foi objeto de questionamentos judiciais, e teve sua eficácia suspensa por decisão do Supremo Tribunal Federal. Esse caso evidencia o papel decisivo assumido pelo Poder Judiciário na solução dessas controvérsias.

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 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.

Há duas maneiras de usar a tecnologia da informação para o combate à pandemia: por meio de uma estratégia “centralizada”, na qual o governo acessa os dados pessoais dos cidadãos sem o seu consentimento; e por meio de 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.

Analisando as experiências internacionais, pode-se inferir que a utilização de tecnologias semelhantes seria complexa no Brasil. A maioria dos aplicativos relatados na seção 2 tende a conflitar com a LGPD, pois acessam 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 forem indispensáveis para a proteção da vida do titular ou de terceiro (art. 11, inciso II, alínea e). 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. Essa é uma discussão a ser enfrentada pelo sistema judiciário em casos concretos.

Algumas das preocupações em relação ao tema envolvem as garantias de que o acesso aos dados se limite ao menor número de informações possíveis e de que não haja possibilidade de vazamentos. A anonimização da coleta deve ser uma premissa. A adoção de aplicativos auxiliares no combate à pandemia precisa respeitar os direitos expressos na legislação. Isto posto, as experiências descentralizadas seriam modelos mais adequados à nossa realidade do que as experiências centralizadas. Para isso, é preciso lançar mão de tecnologias com privacidade *by design*, por exemplo, o *bluetooth*, em que os aparelhos conversam entre si, não sendo necessário um agente para centralizar os dados, mantendo a maior parte das informações fragmentada nos celulares e não em uma base de dados única.

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 aos dados.

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

5 CONSIDERAÇÕES FINAIS E RECOMENDAÇÕES

Levando em conta os princípios estabelecidos na legislação brasileira e observando estudos científicos, relatórios de organizações especializadas e recomendações de organismos multilaterais (por exemplo, Abeler *et al.*, 2020; Bell *et al.*, 2020; Ienca e Vayena, 2020; Castillo, 2020; Yasaka, Lehrich e Sahyouni, 2020; EENA, 2020; OECD, 2020; EDPB, 2020),⁹ são apresentadas algumas recomendações que envolvem o devido uso de dados para aplicações no combate à Covid-19:

- elaboração de uma estratégia – construída de forma dialogada – para coleta dos dados estatísticos necessários para subsidiar as políticas públicas;
- atuação junto aos ministérios para elaboração de normas setoriais sobre uso e proteção de dados pessoais no contexto da emergência de saúde pública;
- utilização e refinamento de ferramentas e bases de dados já existentes, atualmente disponíveis de forma fragmentada na administração pública federal, para suprimimento das lacunas enquanto a política nacional de proteção de dados não for definida;
- incentivo, por parte dos governos, à organização de *hackathons*,¹⁰ visando criar soluções com os dados abertos, preservando os princípios da LGPD;
- agilidade e qualidade na publicação de dados abertos, por todos os entes federativos;
- presença de um ente regulador forte e independente, responsável pela coordenação das ações e proposição de uma política nacional de proteção de dados, construída com a participação dos setores envolvidos.

9. Outro exemplo de fonte consultada está disponível em: <<https://www.accessnow.org/releases-recommendations-on-privacy-data-protection-covid-19/>>.

10. *Hackathons* 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 mesmo criar novos *softwares* e *hardwares*.

REFERÊNCIAS

- ABELER, Johannes *et al.* Covid-19 contact tracing and data protection can go together. **JMIR mHealth and uHealth**, v. 8, n. 4, p. 1-5, 2020.
- BALEUN, Song; MINJI, Kim. Mobile apps, websites offer real-time data on Covid-19 outbreak. **Korea.net**, 10 Mar, 2020. Disponível em: <<http://www.korea.net/NewsFocus/Society/view?articleId=183129>>.
- BELL, James *et al.* TraceSecure: towards privacy preserving contact tracing. **ArXiv**, 8 Apr. 2020.
- BRASIL. Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil. **Diário Oficial da União**, p. 1, 24 abr. 2014. Seção 1. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em: 22 maio 2020.
- CASTILLO, Aída Ponce del. **Covid-19 contact-tracing apps**: how to prevent privacy from becoming the next victim. Brussels: ETUI, 2020. (ETUI Policy Brief, n. 5).
- CASTRO, Fábio Fonseca de. Impactos da Covid-19 sobre os processos comunicacionais: primeiras observações sobre dinâmicas, impasses e riscos. **Papers do NAEA**, v. 29, n. 1, 2020. Disponível em: <<https://periodicos.ufpa.br/index.php/pnaea/article/view/8799/6270>>.
- COMO TAIWAN, Singapura e Hong Kong conseguiram controlar o coronavírus sem medidas drásticas. **G1**, 14 mar. 2020. Disponível em: <<https://glo.bo/3mvDAF0>>.
- EDPB – EUROPEAN DATA PROTECTION BOARD. **Statement on the processing of personal data in the context of the Covid-19 outbreak**. Brussels: EDPB, 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**. Brussels: EENA, 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. **Harvard Business Review**, 15 Apr. 2020. Disponível em: <<https://hbr.org/2020/04/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, n. 4, p. 463-464, 2020.
- KUPFERSCHMIDT, Kai; COHEN, Jon. Can China's Covid-19 strategy work elsewhere? **Science**, v. 367, n. 6482, p. 1061-1062, 2020.
- MAYER-SCHÖNBERGER, Viktor. Generational development of data protection in Europe. In: AGRE, Philip E.; ROTENBERG, Marc (Ed.). **Technology and privacy: the new landscape**. Cambridge: MIT Press, 1997, p. 219-236.
- MAYER-SCHÖNBERGER, Viktor; CUKIER, Kenneth. **Big data**. Boston: Mariner Books, 2014.
- MCAFEE, Andrew; BRYNJOLFSSON, Andrew. **Machine, platform, crowd**. New York: Norton, 2017.
- 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).

MOZUR, Paul; ZHONG, Raymond; KROLIK, Aaron. In coronavirus fight, China gives citizens a color code, with red flags. **The New York Times**, 1 Mar. 2020. Disponível em: <<https://www.nytimes.com/2020/03/01/business/china-coronavirus-surveillance.html>>.

OECD – ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT. **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-tracing-covid-protecting-privacy-and-data-while-using-apps-and-biometrics-8f394636>>.

OLIVER, Nuria *et al.* Mobile phone data and Covid-19: missing an opportunity? **ArXiv**, 26 Mar. 2020. Disponível em: <<https://arxiv.org/ftp/arxiv/papers/2003/2003.12347.pdf>>. Acesso em: 28 maio 2020.

O'NEIL, Cathy. **Weapons of math destruction**. New York: Broadway Books, 2016.

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

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

TING, Daniel Shu Wei *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, 15 Dec. 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.; LEHRICH, Brandon M.; SAHYOUNI, Ronald. Peer-to-peer contact tracing: development of a privacy-preserving smartphone app. **JMIR mHealth and 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. **Diário Oficial da União**, Brasília, 31 dez. 1940. 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. **Diário Oficial da União**, Brasília, 5 out. 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. **Diário Oficial da União**, Brasília, 12 set. 1990. 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. **Diário Oficial da União**, Brasília, 25 jul. 1996. Disponível em: <http://www.planalto.gov.br/ccivil_03/LEIS/L9296.htm>. Acesso em: 22 maio 2020.

_____. Lei nº 13.709, de 14 de agosto de 2018. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). **Diário Oficial da União**, Brasília, 15 ago. 2018. 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. **Diário Oficial da União**, Brasília, 15 ago. 2018. 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. 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). **Diário Oficial da União**, Brasília, 5 set. 2019. 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. 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. **Diário Oficial da União**, Brasília, 10 out. 2019. 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. Aperfeiçoa a legislação penal e processual penal. **Diário Oficial da União**, Brasília, 24 dez. 2019. 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. Institui normas de caráter transitório e emergencial para a regulação de relações jurídicas de direito privado em virtude da pandemia da Covid-19; e altera a Lei nº 13.709, de 14 de agosto de 2018. Brasília: Senado Federal, 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. 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. **Diário Oficial da União**, Brasília, 17 abr. 2020. Disponível em: <http://www.planalto.gov.br/CCIVIL_03/_Ato2019-2022/2020/Mpv/mpv954.htm>. Acesso em: 22 maio 2020.

_____. 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. **Diário Oficial da União**, Brasília, p. 18, 27 abr. 2020. Seção 1. 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 de 2020. Relatora Ministra Rosa Weber. Brasília: STF, 2020. 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**. Paris: ONU, 1948. Disponível em: <<https://www.ohchr.org/EN/UDHR/Pages/Language.aspx?LangID=por>>. Acesso em: 22 maio 2020.

