III CONGRESSO INTERNACIONAL DE DIREITO E INTELIGÊNCIA ARTIFICIAL (III CIDIA)

OS DIREITOS HUMANOS NA ERA TECNOLÓGICA I

DEILTON RIBEIRO BRASIL

MARALUCE MARIA CUSTÓDIO

NATHALIA LIPOVETSKY E SILVA

O81
Os direitos humanos na era tecnológica I [Recurso eletrônico on-line] organização III Congresso Internacional de Direito e Inteligência Artificial (III CIDIA): Skema Business School – Belo Horizonte;

Coordenadores: Nathalia Lipovetsky e Silva, Deilton Ribeiro Brasil e Maraluce Maria Custódio – Belo Horizonte: Skema Business School, 2022.

Inclui bibliografia
ISBN: 978-65-5648-515-7
Modo de acesso: www.conpedi.org.br em publicações
Tema: A inteligência artificial e os desafios da inovação no poder judiciário.
1. Direitos humanos. 2. Inteligência artificial. 3. Tecnologia. I. III Congresso Internacional de Direito e Inteligência Artificial (1:2022 : Belo Horizonte, MG).

CDU: 34

III CONGRESSO INTERNACIONAL DE DIREITO E INTELIGÊNCIA ARTIFICIAL (III CIDIA)

OS DIREITOS HUMANOS NA ERA TECNOLÓGICA I

Apresentação

O Congresso Internacional de Direito e Inteligência Artificial (CIDIA) da SKEMA Business School Brasil, que ocorreu em formato híbrido do dia 08 ao dia 10 de junho de 2022, atingiu a maturidade em sua terceira edição. Os dezesseis livros científicos que ora são apresentados à comunidade científica nacional e internacional, que contêm os 206 relatórios de pesquisa aprovados, são fruto das discussões realizadas nos Grupos de Trabalho do evento. São cerca de 1.200 páginas de produção científica relacionadas ao que há de mais novo e relevante em termos de discussão acadêmica sobre a relação da inteligência artificial e da tecnologia com os temas acesso à justiça, Direitos Humanos, proteção de dados, relações de trabalho, Administração Pública, meio ambiente, formas de solução de conflitos, Direito Penal e responsabilidade civil, dentre outros temas.

Neste ano, de maneira inédita, professores, grupos de pesquisa e instituições de nível superior puderam propor novos grupos de trabalho. Foram recebidas as excelentes propostas do Professor Doutor Marco Antônio Sousa Alves, da Universidade Federal de Minas Gerais (SIGA-UFMG – Algoritmos, vigilância e desinformação), dos Professores Doutores Bruno Feigelson e Fernanda Telha Ferreira Maymone, da Universidade do Estado do Rio de Janeiro (Metalaw – A Web 3.0 e a transformação do Direito), e do Professor Doutor Valmir Cézar Pozzetti, ligado à Universidade Federal do Amazonas e Universidade do Estado do Amazonas (Biodireito e tutela da vida digna frente às novas tecnologias).

O CIDIA da SKEMA Business School Brasil é, pelo terceiro ano consecutivo, o maior congresso científico de Direito e Tecnologia do Brasil, tendo recebido trabalhos do Amazonas, Bahia, Ceará, Distrito Federal, Espírito Santo, Goiás, Maranhão, Minas Gerais, Mato Grosso do Sul, Mato Grosso, Pará, Pernambuco, Piauí, Paraná, Rio de Janeiro, Rio Grande do Norte, Rio Grande do Sul, Santa Catarina, Sergipe e São Paulo. Tamanho sucesso não seria possível sem os apoiadores institucionais do evento: o CONPEDI – Conselho Nacional de Pesquisa e Pós-graduação em Direito, o Instituto Brasileiro de Estudos de Responsabilidade Civil – IBERC e o Programa RECAJ-UFMG - Ensino, Pesquisa e Extensão em Acesso à Justiça e Solução de Conflitos da Faculdade de Direito da Universidade Federal de Minas Gerais. Destaca-se, mais uma vez, a presença maciça de pesquisadores do Estado do Amazonas, especialmente os orientandos do Professor Doutor Valmir César Pozzetti.

Grandes nomes do Direito nacional e internacional estiveram presentes nos painéis temáticos do congresso. A abertura ficou a cargo do Prof. Dr. Felipe Calderón-Valencia (Univ. Medelín - Colômbia), com a palestra intitulada “Sistemas de Inteligência Artificial no Poder Judiciário - análise da experiência brasileira e colombiana”. Os Professores Valter Moura do Carmo e Rômulo Soares Valentini promoveram o debate. Um dos maiores civilistas do país, o Prof. Dr. Nelson Rosenvald, conduziu o segundo painel, sobre questões contemporâneas de Responsabilidade Civil e tecnologia. Tivemos as instigantes contribuições dos painelistas José Luiz de Moura Faleiros Júnior, Caitlin Mulholland e Manuel Ortiz Fernández (Espanha).

Momento marcante do congresso foi a participação do Ministro do Tribunal Superior do Trabalho – TST Maurício Godinho Delgado, escritor do mais prestigiado manual de Direito do Trabalho do país. Com a mediação da Profª. Drª. Adriana Goulart de Sena Orsini e participação do Prof. Dr. José Eduardo de Resende Chaves Júnior, parceiros habituais da SKEMA Brasil, foi debatido o tema “Desafios contemporâneos do gerenciamento algorítmico do trabalho”.

Encerrando a programação nacional dos painéis, o Prof. Dr. Caio Augusto Souza Lara, da SKEMA Brasil, dirigiu o de encerramento sobre inovação e Poder Judiciário. No primeiro momento, o juiz Rodrigo Martins Faria e a equipe da Unidade Avançada de Inovação do Tribunal de Justiça do Estado de Minas Gerais contaram sobre o processo de transformação em curso do Judiciário Estadual mineiro. Em seguida, o Prof. Dr. Fabrício Veiga Costa fez brilhante exposição sobre o projeto denominado “Processo Coletivo Eletrônico”, que teve a liderança do Desembargador Federal do Trabalho Vicente de Paula Maciel Júnior (TRT-3ª Região) e que foi o projeto vencedor do 18º Prêmio Innovare. O evento ainda teve um Grupo de Trabalho especial, o “Digital Sovereignty, how to depend less on Big tech?”, proposto pela Profª. Isabelle Bufflier (França) e o momento “Diálogo Brasil-França” com Prof. Frédéric Marty.

Os dezesseis Grupos de Trabalho contaram com a contribuição de 46 proeminentes professores ligados a renomadas instituições de ensino superior do país, os quais indicaram os caminhos para o aperfeiçoamento dos trabalhos dos autores. Cada livro desta coletânea foi organizado, preparado e assinado pelos professores que coordenaram cada grupo, os quais eram compostos por pesquisadores que submeteram os seus resumos expandidos pelo processo denominado double blind peer review (dupla avaliação cega por pares) dentro da plataforma PublicaDireito, que é mantida pelo CONPEDI.

Desta forma, a coletânea que ora torna-se pública é de inegável valor científico. Pretende-se, com ela, contribuir com a ciência jurídica e fomentar o aprofundamento da relação entre a graduação e a pós-graduação, seguindo as diretrizes oficiais da CAPES. Promoveu-se, ainda, a formação de novos pesquisadores na seara interdisciplinar entre o Direito e os vários campos da tecnologia, notadamente o da ciência da informação, haja vista o expressivo número de graduandos que participaram efetivamente, com o devido protagonismo, das atividades.

A SKEMA Business School é entidade francesa sem fins lucrativos, com estrutura multicampi em cinco países de continentes diferentes (França, EUA, China, Brasil e África do Sul) e com três importantes acreditações internacionais (AMBA, EQUIS e AACSB), que demonstram sua vocação para pesquisa de excelência no universo da economia do conhecimento. A SKEMA acredita, mais do que nunca, que um mundo digital necessita de uma abordagem transdisciplinar.

Agradecemos a participação de todos neste grandioso evento e convidamos a comunidade científica a conhecer nossos projetos no campo do Direito e da tecnologia. Foi lançada a nossa pós-graduação lato sensu em Direito e Tecnologia, com destacados professores e profissionais da área. No segundo semestre, teremos também o nosso primeiro processo seletivo para a graduação em Direito, que recebeu conceito 5 (nota máxima) na avaliação do Ministério da Educação - MEC. Nosso grupo de pesquisa, o Normative Experimentalism and Technology Law Lab – NEXT LAW LAB, também iniciará as suas atividades em breve.

Externamos os nossos agradecimentos a todas as pesquisadoras e a todos os pesquisadores pela inestimável contribuição e desejamos a todos uma ótima e proveitosa leitura!

Belo Horizonte-MG, 20 de junho de 2022.

Profª. Drª. Geneviève Daniele Lucienne Dutrait Poulingue

Reitora – SKEMA Business School - Campus Belo Horizonte

Prof. Dr. Edgar Gastón Jacobs Flores Filho

Coordenador dos Projetos de Direito da SKEMA Business School

INTERESSE PÚBLICO E TRATAMENTO DE DADOS NO CONTEXTO DA PANDEMIA DO COVID-19

PUBLIC INTEREST AND DATA PROCESSING IN REGARDS TO COVID-19 PANDEMIC

João Araújo Monteiro Neto [1]
Maria Neuzyanne Nogueira Gurgel [2]
Ana Carolina Teles Maciel [3]

Resumo

A inovação tecnológica permite um trâmite veloz de atividades corriqueiras, entregando conforto e produtividade à sociedade. Contudo, em determinadas ações causa-se a exposição exacerbada dos dados pessoais em vias, que podem não ter o tratamento necessário. Paralelamente, com o surgimento da pandemia do Covid-19, Governos baseando-se no interesse público, utilizaram medidas de monitoramento populacional, como medida de reter a disseminação do vírus. Dessa forma, o presente trabalho busca avaliar as iniciativas adotadas sob a perspectiva dos direitos à privacidade e à proteção de dados das pessoas naturais, avaliando os limites, os pontos críticos e a aplicabilidade dessas tecnologias e tratamentos.

Palavras-chave: Privacidade, Proteção, Dados pessoais, Pandemia, Covid-19, Interesse público

Abstract/Resumen/Résumé

Technological innovation allows for a fast-moving process of everydays activities, delivering comfort and productivity to society. However, sometimes there is exposition of personal data on, which tends not to observe the rules of processing and good-faith. In the context, fighting against the Covid-19 Pandemic, Governments, based on technological monitoring, was in order to enable the fight against the crisis and against the spread of the virus. Therefore,this paper seeks to evaluate these measures under the perspective of the rights to privacy and protection of natural persons, thus, evaluating the limits, critical points, and the applicability of technologies and data processing.

Keywords/Palabras-claves/Mots-clés: Data protection, Pandemic, Public interest

---

[1] Professor do Curso de Direito da Universidade de Fortaleza.

[2] Graduanda de Direito na Faculdade Evolução Alto Oeste Potiguar.

[3] Advogada especializada em Direito Processual Civil e em Direito Digital, Tecnologia e Proteção de Dados.

INTRODUÇÃO

No Brasil, com a promulgação da Constituição Federal, em 1988, há o estabelecimento dos direitos e garantias fundamentais, os quais têm como objetivo garantir a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade.

Menciona-se que além de estabelecer a privacidade como direito fundamental, após a aprovação da Emenda Constitucional de 115/22, a Constituição Federal brasileira também considera a proteção de dados também como direito fundamental. Assim sendo, não há questionamentos em relação à importância desses dois institutos para a sociedade brasileira e, também, mundial, já que essas mudanças e inclusões sofreram forte influência internacional.

Estabelecido a importância desses institutos, há que se analisar o equilíbrio entre a proteção e prioridade em relação à privacidade e tratamento de dados de pessoais naturais e o interesse do Poder Público (e parcerias público-privadas) em meios a crises estatais - e mundiais - que motivam monitoramento e fiscalização da população de forma assertiva.

Em 2020, o mundo se deparou com uma crise sanitária sem precedentes: a pandemia do COVID-19. Por isso, os Governos ao redor do mundo, em conjunto com a Organização Mundial da Saúde (OMS) entraram em uma corrida para conter a disseminação do vírus e mitigar os danos em cada território.

Nesse contexto, a tecnologia foi uma das soluções para auxiliar na gestão da pandemia. Cita-se, por exemplo, a parceria entre a *Apple* e o *Google*, a qual tinha como objetivo rastrear a localização das pessoas usando a tecnologia *Bluetooth* para compartilhar com as autoridades públicas. A iniciativa teve a seguinte justificativa, conforme posicionamento das empresas (APPLE, 2020)[1]:

> [...] Nesse espírito de colaboração, Google e Apple estão anunciando um trabalho conjunto, utilizando a tecnologia Bluetooth para ajudar governos e agências de saúde a frear o avanço do vírus, tendo a privacidade e segurança do usuário como pontos centrais. [...] Como a COVID-19 pode ser transmitida às pessoas pela proximidade, autoridades de saúde pública perceberam que o rastreamento de contato é uma ferramenta valiosa para conter a propagação. Diversas autoridades de saúde pública, universidades e ONGs de destaque ao redor do mundo têm feito um trabalho importante no desenvolvimento de tecnologias optativas de rastreamento de contato. Em apoio a essa causa, Apple e Google lançarão uma solução completa que inclui interfaces de programação de aplicações (APIs) e tecnologia de sistema operacional para auxiliar no rastreamento de contato.

Nesse contexto, também é válido ressaltar a aprovação da Medida Provisória n° 954/20, a qual determinava o compartilhamento de dados pelas empresas de telecomunicação,

[1] https://www.apple.com/br/newsroom/2020/04/apple-and-google-partner-on-covid-19-contact-tracing-technology/

prestadoras de Serviço Telefônico Fixo Comutado (STFC) e de Serviço Móvel Pessoal (SMP), com o Instituto Brasileiro de Geografia e Estatística (IBGE) com a finalidade de monitorar e conter avanço do COVID-19 no Brasil. Ainda que, a princípio, o seu objetivo parece ser nobre e dentro das regras normativas, tal medida foi alvo de duras críticas, as quais resultaram em 05 ADI's (Ação Direta de Inconstitucionalidade).

Com isso em mente, é importante analisar outras estratégias utilizadas ao redor do mundo no contexto do COVID-19 para apontar maneiras lúcidas e legítimas que asseguram tanto à proteção do indivíduo em si, como também a sociedade civil em geral, priorizando, assim, a observância aos princípios fundamentais básicos, os seus limites básicos e a supremacia do interesse público em determinadas situações.

OBJETIVO

O presente trabalho avalia de forma comparativa se certas iniciativas utilizadas para fins de monitoramento no cenário pandêmico possuem o condão de ferir direitos e garantias fundamentais dos cidadãos ou se as tais se apoiam em questões contundentes da primazia do interesse público.

METODOLOGIA

A metodologia e preparação para desenvolver o presente trabalho tem como base a análise das iniciativas e tecnologias de monitoramento e/ou rastreamento utilizadas no contexto da COVID-19 ao redor do mundo e seus possíveis impactos sociais.

Concomitantemente, analisou-se também o teor geral dos princípios de proteção de dados já pré-determinados e pacificados anteriormente a determinadas legislações focadas na regulamentação do tema, para que se pudesse verificar com clareza a legitimidade dos propósitos, bem como os limites da utilização de determinadas iniciativas, ainda que baseadas, primeiramente, no interesse público geral.

Isto posto, diante de uma análise contextual entre o surgimento de novas iniciativas com finalidade de controlar a transmissão do COVID-19 e os limites morais, legais e éticos, foi possível, portanto, fomentar discussões e conclusões sobre o tema, conforme se demonstra no decorrer dos próximos tópicos.

DISCUSSÕES

Assim que a Pandemia do COVID-19 se estabeleceu na realidade global, a Organização Mundial da Saúde (OMS) trabalhou incessantemente em busca do controle e contenção do vírus em todo o contexto mundial.

As orientações se disseminaram por todos os países e, a partir de alguns parâmetros, muitos deles iniciaram movimentos de prevenção, com o intuito de obter resultados efetivos sobre a forma em que o vírus se movia.

O Brasil, assim que possível, se incluiu nessa lista. Já em abril de 2020, o Governo de São Paulo anunciou a celebração de parceria isenta de ônus ao Estado com operadoras de telefonia, tais como Vivo, Claro e TIM, para medir o distanciamento social e enviar alertas aos celulares dos cidadãos sobre áreas com possível alto risco de contágio.

À época, o então Governador do Estado (Portal do Governo, 2020)[2] argumentou que: *[...] Com 100% dos usuários de telefonia celular em São Paulo, nós podemos identificar os locais onde as pessoas estarão e onde houver concentração para analisar o percentual de isolamento e também ações de orientação e advertência, se necessário*.

Na prática, o Estado de São Paulo recebia informações sobre o percentual de isolamento e aglomeração vinculados no perímetro de cada antena de telefonia móvel. Com isso em mente, os responsáveis argumentaram que a privacidade dos indivíduos, em si, não era diretamente ameaçada, já que a trajetória individual não era monitorada. Portanto, os dados seriam anonimizados e apenas apresentados de forma agregada.

É possível identificar, nesse contexto, que, certos grupos e cidadãos paulistas contestaram o monitoramento com argumento de que haveria invasão da privacidade do indivíduo.

Quanto a isso, importante ressaltar que, conforme já mencionado, tanto o direito à privacidade quanto o direito à proteção de dados pessoais, hoje, são considerados direitos fundamentais de acordo com a legislação brasileira (Constituição Federal, 1988)[3].

A partir disso, destaca-se que, enquanto o direito à privacidade traz a ideia do direito do indivíduo ser deixado só na segurança da sua intimidade, conforme célebre artigo *The Right To Privacy*, escrito por Louis Brandeis e Samuel D. Warren, em 1890, o princípio da proteção de dados pessoais não se pauta, necessariamente, em restringir o fluxo dessas informações em uma economia movida por elas, mas sim regulamentar princípios, bases legais e medidas de segurança para a realização do processamento.

---

[2] https://www.saopaulo.sp.gov.br/noticias-coronavirus/governo-de-sp-apresenta-sistema-de-monitoramento-inteligente-contra-coronavirus/

[3] http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm

Neste ponto, inclusive, menciona-se, por oportuno, que os fundamentos da Lei de Proteção de Dados brasileira (Lei Geral de Proteção de Dados, 2018)[4] são, entre outros, o desenvolvimento econômico e tecnológico e a inovação, bem como a livre iniciativa, a livre concorrência e a defesa do consumidor.

Esclarecidos esses pontos, no contexto da iniciativa supracitada do Governo de São Paulo, há questões relacionadas tanto à privacidade quanto à proteção de dados, uma vez que havia monitoramento de forma genérica dos indivíduos e tratamento de dados que, ainda que se tornassem anonimizados posteriormente, poderiam, *a priori*, identificar as pessoas. Dito isso, há requisitos que o tratamento deve preencher para se tornar aceitável e legal. Isto é, ele deve ser razoável, transparente, necessário, limitado a sua finalidade, bem como também dispor de uma base legal legítima prevista na legislação específica. Quanto a este último ponto, percebe-se que a proteção da vida ou da incolumidade física do titular ou de terceiro se apresenta como hipótese cabível para justificar tal tratamento.

Além disso, a transparência foi observada quando se considera que os dados do isolamento em todas as regiões de São Paulo eram divulgados em boletins diários (de forma geral e não específica), assim como a questão da limitação do tratamento para a finalidade previamente informada.

Por outro lado, nesse ínterim, é importante destacar que não há qualquer direito individual absoluto, uma vez que é especialmente prudente analisar a realidade contextual de um monitoramento a esse nível. Em caso de força maior, como um acontecimento de uma Pandemia sem precedentes, o interesse público pode ser considerado um aspecto latente que justifica medidas excepcionais, inclusive, previstas por lei.

Mas, ainda em casos de crises sanitárias como esse, revela-se muito importante o cuidado e a segurança no gerenciamento de dados dos indivíduos pelo poder público, conforme sustentado acima e como também orientam Marcello Ienca and Effy Vayena (*Nature Medicine*, 2020)[5] (tradução livre):

> As práticas cuidadosas de gerenciamento de dados devem governar tanto a coleta de dados quanto o processamento de dados. No contexto do tratamento dos dados pessoais das pessoas envolvidas, o princípio de proporcionalidade deve ser aplicado, o que significa que a coleta de dados deve (i) ser proporcional à gravidade do ameaça à saúde pública, (ii) ser limitado ao que é necessário para atingir um determinado objetivo de saúde pública, e (iii) ser justificado cientificamente. Obter acesso aos dados de dispositivos pessoais para rastreamento de localização, por exemplo, pode ser justificado se ocorrer dentro de limites específicos. Isto é, precisa ter um propósito - *por exemplo, alertar e isolar pessoas que podem ter sido expostas ao vírus* - e não haver nenhuma alternativa menos invasiva - *por exemplo, não há possibilidade de*

[4] http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm
[5] https://pubmed.ncbi.nlm.nih.gov/32284619/

> *usar dados de posicionamento móvel anônimos* - assim, esse tratamento será adequado para esse fim. [...] Além disso, no contexto do tratamento de dados, os controles de qualidade e segurança dos dados envolvidos também são necessários.

Adicionalmente, a clareza entre a observância do interesse público e as boas práticas do gerenciamento de dados são pontos ainda mais cruciais quando estão envolvidos monitoramento específico de dados de saúde.

A Lei Geral de Proteção de Dados brasileira, inspirada em tantas outras legislações deste nicho mundo afora, estabelece que dado de saúde é um dado pessoal sensível (Art. 5º, inciso II, LGPD)[6]. Isto quer dizer que tratar estes dados requer ainda mais segurança e cuidado, bem como observância a um grupo mais restrito de bases legais. Afinal, eventuais incidentes de segurança que envolvem tais dados apresentam maiores riscos de discriminação aos titulares.

Várias foram as iniciativas que envolviam, também, monitoramento de dados de saúde para verificar a expansão do vírus. O que ocorreu em Taiwan, por exemplo, demonstra uma capacidade de tratar e monitorar esses dados em prol do interesse público sem que houvesse a perda da confiança da população.

Nesse caso, as autoridades procederam com a integração dos bancos de dados de seguros-saúde com os dados de histórico de viagens e alfandegários para aprimorar a identificação dos casos positivos no país. (WANG; CHUN; BROOK, 2020)[7].

Também foram utilizadas tecnologias como leitura de *QR Code* e produção de relatórios online para ajudar na contenção do vírus. A transparência na comunicação pública sobre como e o porquê esses dados estavam sendo utilizados para o "bem comum" foi uma prioridade do Governo de Taiwan e este é um exemplo a ser seguido. Além disso, neste contexto se torna mais que necessário a realização de Relatórios de Impacto à Proteção de Dados Pessoais para ornamentar e mapear os riscos de tais tratamentos antes mesmo de desenhar a nova tecnologia ou adotar iniciativa preexistente como soluções para gerir esse tipo de crise sanitária.

Ocorre que, infelizmente, em outros lugares do mundo, foi constatado que houve desvio da finalidade para monitorar os cidadãos em prol de conter o COVID-19. Há informações, inclusive, de que a China, um dos países mais afetados pelo vírus, foi acusada de compartilhar dados dos sensores responsáveis por identificar a presença de alguém, bem como

---

[6] [...] Dado pessoal sensível: 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.

[7] https://jamanetwork.com/journals/jama/fullarticle/2762689

dados disponíveis dos aplicativos utilizados para monitorar a geolocalização com a polícia. (MOZUR; ZHONG, 2020).

Tais situações, portanto, não são compatíveis com um justo tratamento dos dados das pessoas naturais para combater crises sanitárias. Pelo contrário, as finalidades nunca devem ser extrapoladas para possibilitar o uso dos dados em segmentos completamente diferenciados.

Com isso em mente, verifica-se que, nem sempre, pode-se dizer que há uma linha tênue entre assegurar a privacidade e proteção de dados do indivíduo e conter a expansão do COVID-19 para a sociedade em geral, já que esses dois elementos podem coexistir e perseguir os mesmos princípios. No entanto, isso só pode ser bem compreendido a todos, quando há transparência pelo Poder Público, observância às estritas finalidades, medidas de segurança robustas, análises prévias de riscos e, o mais importante, proposições educativas para conscientizar toda a população ao que ela está sendo, temporariamente, submetida.

CONSIDERAÇÕES FINAIS

É certo dizer que com a comunicação da OMS, em 30 de janeiro de 2020, que indicava o COVID-19 como uma emergência pública de saúde internacional, a vida como se conhecia realmente mudou.

As iniciativas para conter o vírus se tornaram pilares basilares da maioria dos Governos e, nesse sentido, não há como separar os questionamentos sobre invasão à privacidade das medidas de monitoramento que foram implementadas.

Assim sendo, parece prudente analisar o monitoramento da localização do indivíduo, bem como os seus dados pessoais de saúde sob o prisma dos limites de atuação e atribuição do Poder Público. Percebe-se que há finalidades legítimas para essas iniciativas, afinal, rememora-se que o direito individual não é absoluto e não há sobreposição deste ao interesse público em emergências sanitárias como essa.

Por outro lado, esse tipo de justificativa não pode ser considerada uma carta branca para uma coleta e tratamento desregrado e que desrespeita princípios básicos da privacidade e proteção aos dados. Na realidade, nesse contexto de incertezas sociais, torna-se mais que necessário que o responsável pela coleta e tratamento - tanto na esfera pública quanto na privada - entenda que tais tratamentos só podem ser realizados se respeitados os direitos fundamentais das pessoas naturais, tais como, transparência, minimização dos dados e observância restrita à finalidade.

Isto posto, conclui-se que, após a análise dos casos reais apresentados neste trabalho, os limites do tratamento e monitoramento de dados no contexto do COVID-19 se encontram exatamente no que determina os direitos fundamentais de uma sociedade, bem como legislações específicas de cada país. Para além disso, antes de qualquer análise em termos legais, a cultura da sociedade também deve ser considerada e a empatia e reciprocidade no momento de coletar e tratar dados, especialmente os de saúde, devem, também, ser observadas.

REFERÊNCIAS

BIONI, Bruno; ZANATTA, Rafael; MONTEIRO, Renato; RIELLI, Mariana. **Privacidade e pandemia: recomendações para o uso legítimo de dados no combate à COVID-19.** Conciliando o combate à COVID-19 com o uso legítimo de dados pessoais e o respeito aos direitos fundamentais. São Paulo: Data Privacy Brasil, 2020. Acesso em 10 abr. 2022.

BRASIL. **Constituição Federal da República Federativa do Brasil de 1988**. In: Palácio do Planalto. 1988. Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm>. Acesso em 05 mai. 2022.

BRASIL. **Lei Geral de Proteção de Dados**. In: Palácio do Planalto. 2018. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>. Acesso em 05 mai. 2022.

BROOK, Robert. CHUNG, Ng. WANG, MD. **Response to COVID-19 in Taiwan: Big Data Analytics, New Technology, and Proactive Testing**. 2020. Disponível em: <https://doi.org/10.1001/jama.2020.3151>. Acesso em 05 mai. 2022.

GRIMLEY, Naomi; CORNISH, Jack; STYLIANOU Nassos. **Número real de mortes por covid no mundo pode ter chegado a 15 milhões, diz OMS**. BBBC News, 2022. Disponível em: <https://www.bbc.com/portuguese/internacional-61332581>. Acesso em 10 abr. 2022.

MOZUR, P. ZHONG, R. KROLIK, A. **In Coronavirus Fight, China Gives Citizens a Color Code, With Red Flags**. 2020. Disponível em: <https://www.nytimes.com/2020/03/01/business/china-coronavirus-surveillance.html>. Acesso em 05 mai. 2022.

SÃO PAULO. **Governo de SP apresenta Sistema de Monitoramento Inteligente contra coronavírus.** In: Portal do Governo. 2020. Disponível em: <https://www.saopaulo.sp.gov.br/noticias-coronavirus/governo-de-sp-apresenta-sistema-de-monitoramento-inteligente-contra-coronavirus/>. Acesso em 10 abr. 2022.

SOPRANA, Paula. Folha de São Paulo. **Google e Apple lançam tecnologia que notifica contato com contaminado por coronavírus**. 2020. Disponível em: <https://www1.folha.uol.com.br/tec/2020/04/google-e-apple-lancam-tecnologia-que-notifica-se-pessoa-teve-contato-com-alguem-que-tem-covid-19.shtml>. Acesso em 15 abr. 2022.