

INTELIGÊNCIA ARTIFICIAL NA SAÚDE E A PROTEÇÃO DE DADOS: REFLEXOS NA CRISE COVID-19

João Carlos Hipólito Bernardes do Nascimento

Docente efetivo do Programa de Pós-Graduação *stricto sensu* em Gestão Pública, do Programa de Pós-Graduação *stricto sensu* em Administração Pública e do curso de Bacharelado em Ciências Contábeis da Universidade Federal do Piauí (UFPI), *campus* Ministro Petrônio Portella, Teresina/PI. Doutor em Ciências Contábeis pela Universidade Federal do Rio de Janeiro (UFRJ) – Rio de Janeiro/RJ. Mestre em Contabilidade na área de concentração Contabilidade Gerencial pela Fundação Instituto Capixaba de Pesquisas em Contabilidade, Economia e Finanças (FUCAPE) – Vitória/ES. Especialista em Gestão de Recursos Humanos pela Universidade de Pernambuco (UPE) – Recife/PE. MBA em Gestão de Negócios pela Escola de Engenharia e Agrimensura da Bahia (EEA) – Salvador/BA. Graduado em Ciências Contábeis pela Faculdade de Ciências Aplicadas e Sociais de Petrolina – Petrolina/PE e em Tecnologia em Processos Gerenciais pela Universidade Norte do Paraná.

Maria Leonildes Boavista Gomes Castelo Branco Marques

Docente efetiva do curso de Bacharelado em Direito da Universidade Federal do Piauí (UFPI), *campus* Ministro Petrônio Portella – Teresina/PI. Doutoranda em Ciências Criminais pela Pontifícia Universidade Católica do Rio Grande do Sul (PUCRS) – Porto Alegre/RS. Mestre em Direito pela Pontifícia Universidade Católica do Rio Grande do Sul (PUCRS) – Porto Alegre/RS. Especialista em Direito Público e em Direito Privado pela Universidade Federal do Piauí (UFPI), *campus* Ministro Petrônio Portella – Teresina/PI. Especialista em Contabilidade pela Faculdade Internacional Signorelli – Rio de Janeiro/RJ. Graduada em Direito pela Faculdade de Saúde, Ciências Humanas e Tecnológicas do Piauí (NOVAFPI) – Teresina/PI e em Ciências Contábeis pela Faculdade Santo Agostinho (FSA) – Teresina/PI.

Nayara Hanna Santiago Costa

Mestranda do Programa de Pós-Graduação *stricto sensu* em Gestão Pública pela Universidade Federal do Piauí, *campus* Ministro Petrônio Portella – Teresina/PI. Graduada em Direito pela Universidade Federal do Piauí (UFPI), *campus* Ministro Petrônio Portella – Teresina/PI.

Maria Isabel Boavista Gomes Castelo Branco

Pós-Graduada em Direito Público e em Direito Privado pela Universidade Federal do Piauí (UFPI), *campus* Ministro Petrônio Portella – Teresina/PI. Graduada em Direito pela Universidade Federal do Piauí (UFPI), *campus* Ministro Petrônio Portella – Teresina/PI.

Tâmara Beatriz Santos

Pós-Graduada em Direito Constitucional e Administrativo pela Escola Superior de Advocacia do Piauí (ESAPI/OAB-PI) – Teresina/PI. Graduada em Direito, pelo Instituto Camillo Filho – Teresina/PI.

Roger Vitório Oliveira Sousa

Pós-Graduando em Direito Constitucional e em Direito Público pela Faculdade Descomplica – vinculada ao Centro Universitário UniAmérica – Foz do Iguaçu/PR. Graduado em Direito pela Universidade Estadual do Piauí (UESPI), *campus* Poeta Torquato Neto – Teresina/PI.

Resumo: No presente trabalho investigou-se como está sendo feito o uso das tecnologias de informação e armazenamento de dados no auxílio ao combate à pandemia gerada pelo novo coronavírus, doença até então desconhecida, mas que gerou impacto mundial em razão da necessidade de distanciamento social e da ausência de medicamentos específicos ou cura comprovados. Em uma sociedade na qual a tecnologia e a comunicação se fazem bastante presentes, governos passam a fazer uso destes mecanismos e da inteligência artificial para frear o avanço da COVID-19. No entanto, salientou-se a necessidade de preocupação com a proteção dos dados de toda a população envolvida e com a forma como estes serão utilizados, não somente no cenário atual, mas também em um futuro próximo. Para tanto, foi realizada uma análise das legislações em um cenário nacional e internacional, bem como apresentaram-se as soluções adotadas no Brasil para enfrentar o problema apresentado, como a elaboração da Lei de Proteção de Dados e o uso de novas tecnologias.

Palavras-chave: proteção de dados; COVID-19; inteligência artificial; Lei de Proteção de Dados.

Sumário: **1** Introdução – **2** Inteligência artificial na saúde – **3** A crise COVID-19 – **4** Dispositivos legais de proteção de dados – **5** Possíveis soluções para a proteção de dados médicos no Brasil – **6** Conclusão – Referências

1 Introdução

A pandemia provocada pelo novo coronavírus reverberou nos mais diversos âmbitos da convivência humana. As atividades produtivas, a ciência, as relações interpessoais e o entretenimento sofreram os imperativos decorrentes de uma nova forma de agir para conter uma doença exclusivamente nova na face da Terra, na busca de soluções para frear seu avanço.

A ciência instantaneamente assistiu ao foco das atenções mundiais voltar-se para si, na esperança de soluções através de medidas preventivas, senão a longo prazo, como uma tão desejada vacina que possibilite reduzir drasticamente o impacto do vírus na sociedade, ao menos a curto prazo, freando novas contaminações e contribuindo na medida até então mais eficaz contra a propagação da doença: o distanciamento social. Neste propósito, as tecnologias decorrentes da quarta revolução industrial, como a inteligência artificial e a Big Data, antes já introduzidas gradualmente na área da saúde, diante do contexto da pandemia, aceleraram essa fusão, originando uma considerável variedade de tecnologias voltadas para o combate à COVID-19.

Novas tecnologias foram implementadas na área médica e o uso dos dados coletados a partir das ferramentas criadas, bem como a possibilidade da exposição daqueles, tornou-se motivo de preocupação. O direito à privacidade abrange todas as esferas em que a vida íntima dos cidadãos deve ser resguardada e os dados médicos constituem umas das mais restritas informações de um indivíduo. Vazamentos de dados dessa natureza podem ensejar resultados indesejáveis,

como: atos estigmatizantes a portadores de doenças marcadas pelo preconceito, vide portadores de HIV; atitudes restritivas de serviços de planos de saúde, visando aumento de preço dos serviços prestados a clientes portadores de doenças crônicas que demandam maiores cuidados médicos; assédio de organizações farmacêuticas quanto a produtos e medicamentos direcionados a problemas de saúde específicos de potenciais clientes, dentre outras consequências.

Portanto, é imprescindível garantir o direito à privacidade no tratamento de número significativo de dados médicos por empresas de tecnologia. O contraste entre a relevância da matéria e a carência de normas que disponham sobre os pormenores dessa questão é evidente, especialmente devido à realidade que o Brasil e as demais nações atualmente enfrentam.

Nesse contexto, o presente trabalho pretende analisar os impactos causados pela expansão da Inteligência Artificial na área da saúde, especialmente quanto à manipulação de dados pessoais nesse processo. Serão expostas as principais tecnologias usadas no combate à doença, suas relações com dados pessoais coletados e médicos, observando-se as legislações que se propõem a regular o tratamento de dados pessoais, nos níveis mundial, nacional, e em especial, a Lei Geral de Proteção dos Dados Pessoais (LGPD), além de explanar as possíveis soluções encontradas para garantir que não apenas o direito à saúde seja garantido nesse período de pandemia, mas também que o direito fundamental à privacidade seja resguardado. Nesse ponto, o presente estudo mostra-se relevante.

2 Inteligência artificial na saúde

Desde o início do século XXI, o mundo experimenta uma nova revolução industrial – a denominada Quarta Revolução Industrial, ou, Revolução Digital. Essa transformação tem como seus principais símbolos os sistemas e máquinas inteligentes e conectados. Entretanto, seu conceito abrange um alcance maior que apenas esses instrumentos. Nessa revolução, há a fusão das tecnologias e a interação dos domínios físicos, digitais e biológicos. Novas descobertas ocorrem concomitantemente em diversas áreas, e as inovações generalizadas são difundidas de forma vertiginosa, superando de forma exacerbada a velocidade de propagação das descobertas das revoluções anteriores.¹

Diante da nova revolução industrial, as mudanças refletem-se em todos os âmbitos relacionais. Desde as cadeias globais de valor às pequenas empresas, das seculares instituições de ensino superior às humildes escolas de ensino

¹ SCHWAB, Klaus. *A Quarta Revolução Industrial*. São Paulo: Edipro, 2016.

básico, do cenário de relações internacionais aos laços interpessoais do cotidiano: todas precisam adaptar-se à nova era, na qual a informação e o conhecimento configuram as mais valiosas ferramentas.

No âmbito do mercado de trabalho, o ramo da medicina constitui um dos maiores beneficiários dessa revolução. Especialmente, considerando a inclusão da Inteligência Artificial na área médica e o uso da Big Data na composição de conhecimentos médicos. Para melhor observação das consequências desses eventos, uma delimitação adequada dos seus conceitos é necessária.

Inteligência artificial, de forma ampla, é o ramo da ciência da computação que desenvolve sistemas que simulam a capacidade humana diante da percepção de um problema, e, com isso, percorrem os seguintes passos: identificam os componentes do problema, resolvem o problema e propõem ou tomam decisões.² Quando utilizada na medicina, a Inteligência Artificial consiste no uso de máquinas que, através da análise de um grande volume de dados, e seguindo algoritmos definidos por especialistas na matéria, são aptas a propor soluções para problemas médicos.³

Depreende-se desses conceitos a utilização das tecnologias em aspectos antes inimagináveis em outras revoluções: abordagens antes consideradas próprias dos homens – como tomadas de decisões, atualmente podem ser delegadas a máquinas devidamente operacionalizadas para tal, capazes de atuar com um volume de dados em escala colossal em um curto período de tempo.

Outro conceito mencionado e relevante nessa discussão é o de algoritmo: “Um algoritmo pode ser definido como uma sequência finita de passos (instruções) para resolver um determinado problema”.⁴ De acordo com esse conceito para realizar a programação de um algoritmo em um computador são necessárias três etapas: entrada, processamento e saída de dados. Essa necessidade de alimentar os algoritmos com dados remete a outra estratégia digital: a Big Data.

A Big Data caracteriza-se como a análise e a interpretação de dados em grande volume e variedade armazenados remotamente. Essa estratégia utiliza dados armazenados em sistemas virtuais para diversos usos, dentre eles o *marketing*

² LOBO, Luiz Carlos. Inteligência artificial, o Futuro da Medicina e a Educação Médica. *Revista Brasileira de Educação Médica*, Brasília, v. 42, n. 3, p. 3-8, Setembro de 2018. Disponível em: http://www.scielo.br/scielo.php?script=sci_arttext&pid=S0100-55022018000300003&lng=en&nrm=iso. Acesso em: 09 jul. 2020.

³ LOBO, Luiz Carlos. Inteligência artificial e Medicina. *Revista Brasileira de Educação Médica*, Rio de Janeiro, v. 41, n. 2, p. 185-193, Junho de 2017. Disponível em: http://www.scielo.br/scielo.php?script=sci_arttext&pid=S0100-55022017000200185&lng=pt&nrm=iso. Acesso em: 10 jul. 2020.

⁴ FERRARI, Fabricio; CECHINEL, Cristian. *Introdução a Algoritmos e Programação*, p. 15. Universidade Federal do Pampa – Bagé, abril de 2008, versão 2.0. Disponível em: <https://www.ferrari.pro.br/home/documents/FFerrari-CCechinel-Introducao-a-algoritmos.pdf>. Acesso em: 10 jul. 2020.

e as análises de movimentações.⁵ No sistema de atenção à saúde, a Big Data vem sendo introduzida gradualmente, conforme se demonstra em hipóteses de utilização dessas informações:

Dados de prevalência, incidência e evolução de enfermidades permitiriam gerar dados estatísticos, antecipar surtos epidemiológicos e prescrever ações preventivas. Dados de pacientes, como idade, sexo, etnia, local de residência, antecedentes pessoais e familiares, sintomas e sinais apresentados, exames realizados ou obtidos por meios eletrônicos (*wearable devices*), diagnósticos feitos, tratamento e evolução coletados, permitiriam estabelecer uma base de dados e aprimorar condutas estabelecidas.⁶

Assim, diante dos conceitos abordados, percebe-se que a Inteligência Artificial na Medicina e o desenvolvimento de algoritmos específicos à área da saúde podem: prever a propagação de doenças, promover um ajustamento personalizado de tratamentos e um aumento da precisão dos diagnósticos, contribuir para a identificação de tendências diante de um grande volume de dados médicos, dentre outros benefícios.⁷

Se por um lado, os dados podem auxiliar no conhecimento de questões de saúde pública, por outro lado, a Inteligência Artificial pode – se não administrada de forma correta – provocar exposição de informações restritas a um dos aspectos mais intrínsecos aos cidadãos: os dados médicos. Dessa forma, é preciso cautela no tratamento de número significativo de dados médicos por empresas de tecnologia, pois deve-se priorizar a própria finalidade da utilização dessas informações, conforme os modelos legislativos de proteção de dados do Brasil e do mundo.⁸

⁵ FUNDAÇÃO INSTITUTO DE ADMINISTRAÇÃO. *Big Data: O que é, como aplicar, a importância e exemplos*. 11 de junho de 2018. Disponível em: <https://fia.com.br/blog/big-data/>. Acesso em: 07 jul. 2020.

⁶ LOBO, Luiz Carlos. Inteligência artificial e Medicina. *Revista Brasileira de Educação Médica*, Rio de Janeiro, v. 41, n. 2, p. 185-193, Junho de 2017, p. 190. Disponível em: http://www.scielo.br/scielo.php?script=sci_arttext&pid=S0100-55022017000200185&lng=pt&nrm=iso. Acesso em: 10 jul. 2020.

⁷ PRADO, Eduardo. O Dr Algoritmo da Inteligência Artificial. *Saúde Business*. 27 de junho de 2017. Disponível em: <https://saudebusiness.com/ti-e-inovacao/o-dr-algoritmo-da-inteligencia-artificial/>. Acesso em: 11 jul. 2020.

⁸ RODRIGUES, Paula Marques. A inteligência artificial médica e o uso de dados pessoais no atendimento aos pacientes. *Migalhas*. 23 de abril de 2020. Disponível em: <https://www.migalhas.com.br/depeso/325245/a-inteligencia-artificial-medica-e-o-uso-de-dados-pessoais-no-atendimento-aos-pacientes>. Acesso em: 08 jul. 2020.

3 A crise COVID-19

O presente tópico tem por escopo esmiuçar as tecnologias implementadas na área médica e o uso de dados coletados a partir das ferramentas criadas, bem como a possibilidade de exposição desses dados. Nesse contexto, também será analisado o uso de ferramentas de geolocalização em diálogo com a privacidade e a intimidade das pessoas no âmbito da crise COVID-19.

3.1 As novas tecnologias na área médica e os riscos de exposição dos dados médicos dos pacientes

De acordo com o Departamento de Evidência e Inteligência para Ação em Saúde (2020) da OPAS (Organização Pan-Americana da Saúde e Organização Mundial de Saúde), a quarentena e o isolamento social reúnem mais de 3 bilhões de pessoas no planeta e é nesse âmbito que as tecnologias de informação se inserem, pois são o meio principal utilizado por indivíduos, instituições de saúde e governos com o fito de trabalhar, gerar conhecimento, assim como se comunicar. Em tal cenário, entre as mais utilizadas estão aquelas que objetivam as teleconsultas, o monitoramento de sintomas e as informações genéricas sobre a COVID-19.⁹

Dessa maneira, existe um trabalho mundial para que as lacunas cognitivas que rondam a pandemia sejam supridas; ocorre que, para tanto, é indispensável que diversas medidas sejam tomadas, não somente aquelas ditas governamentais, como também aquelas oriundas de diversos setores sociais, com o objetivo principal de controlar a doença. Ademais, cumpre destacar que existe a necessidade de dados qualificados para esmiuçar os padrões que cercam a doença, além de gráficos matemáticos que amparam as decisões administrativas governamentais.¹⁰

Sobre isso, vale salientar que empresas como a *Apple* e o *Google* realizaram parceria com o objetivo de criar uma ferramenta capaz de rastrear a COVID-19 e compatível com os sistemas operacionais *Android* e *iOS*; nela os indivíduos usuários poderão optar pela participação, mas não há menção quanto à desistência.

⁹ OPAS. *Potencial das tecnologias da informação de uso frequente durante a pandemia*. 2020. Disponível em: https://iris.paho.org/bitstream/handle/10665.2/52023/Factsheet-TICs_por.pdf?sequence=7%20%20. Acesso em: 11 jul. 2020.

¹⁰ ALMEIDA, Bethania de Araujo *et al.* Preservação da privacidade no enfrentamento da COVID-19: dados pessoais e a pandemia global. *Ciência & Saúde Coletiva*, [S.L.], v. 25, n. 1, p. 2487-2492, jun. 2020. Disponível em: https://www.scielo.br/scielo.php?script=sci_arttext&pid=S1413-81232020006702487&lng=en&nrm=iso. Acesso em: 9 jul. 2020.

Esse sistema equivale às soluções alcunhadas de *Contact Tracing*, que são regidas por trocas de identificação anônimas e utilizam conexão *Bluetooth*, podendo ser realizadas por aplicativo desenvolvido por autoridades de saúde nacional ou pelo sistema operacional e por meio desse instrumento, quando um indivíduo testar positivo para a doença, o aplicativo se encarregará de fazer o registro e transmitir os dados para as autoridades de saúde.¹¹

Sobre a discussão que existe entre dados e a intimidade das pessoas, é possível afirmar que:

Dados anonimizados ou agregados não são considerados dados pessoais por leis de proteção de dados porque protegem a identificação dos indivíduos. Contudo, mesmo sem fazer referência a qualquer indivíduo, podem prejudicar grupos em virtude de informações sobre locais, etnicidade, situações de saúde e condições socioeconômicas, por exemplo requerendo escrutinamento ético sobre os potenciais benefícios gerados por tais evidências.¹²

Assim, quando os dados são considerados anônimos ou agrupados perdem a característica de dados pessoais e deixam de ser regidos pelas leis que protegem dados, uma vez que estas visam à proteção da identificação de pessoas. Ocorre que é inevitável apontar que dessa forma existe a possibilidade de se prejudicar grupos, pois esses dados contêm informações de localidade, condições sociais, quadro de saúde e condições econômicas.

É por isso que os dados devem ser geridos de forma responsável, pois os indivíduos precisam compreender a coleta a fim de que se estabeleça uma relação de confiabilidade e segurança. Junto a isso, há a necessidade de ações conjuntas de gestores administrativos, universidades e empresas de tecnologia para que os acordos sejam expressos quanto à forma de recolhimento e os resultados almejados, devendo-se atentar às regras nacionais e internacionais, assim como protocolos e princípios rígidos.¹³

Vale ressaltar que as *pandemic-techs* – ferramentas tecnológicas surgidas no enfrentamento da pandemia – passaram a ser o diferencial no mundo, pois cada vez mais há a utilização de soluções de *Digital Health* – tecnologias digitais utilizadas na saúde – e por meio delas podem ser realizados tratamentos, atendimentos, bem como um controle epidêmico. Tais figuras também auxiliam nos estudos tanto de medicamentos terapêuticos como na produção de uma

¹¹ ALMEIDA, Bethania de Araujo *et al.* Preservação da privacidade no enfrentamento da COVID-19..., cit.

¹² ALMEIDA, Bethania de Araujo *et al.* Preservação da privacidade no enfrentamento da COVID-19..., cit.

¹³ ALMEIDA, Bethania de Araujo *et al.* Preservação da privacidade no enfrentamento da COVID-19..., cit.

vacina. Possibilitam ainda a modalidade de terapia digital, pois o elo entre uma equipe clínica e a tecnologia digital pode auxiliar de maneira grandiosa aqueles que sofreram o impacto da pandemia em sua saúde mental e como mecanismos relacionados é possível citar *Mindstrong*, *Meru Health*, *Talkspace* e *SilverCloud*. Salientando-se que o primeiro obteve 100 milhões de dólares em financiamento no mês de maio de 2020.¹⁴

No Reino Unido, a empresa *Babylon Health* lançou uma plataforma para o combate à doença, em que por meio dela, é possível aos usuários registrar sintomas, receber conselhos e um plano de tratamento para os contaminados, o que reduz o alcance de contaminação pela doença. Na Holanda, a *Spectator Healthcare Technology* criou a adaptação de uma teleconsulta para questões advindas do novo coronavírus. Ademais, a Universidade *College London* – em parceria com a *Health Analytics* – realiza previsões do vírus por meio das pesquisas do *Google*, pelas quais a ferramenta gera um catálogo por área geográfica, o que permite a localização das fontes de contágios.¹⁵

As tecnologias de informação são o meio principal utilizado pelos indivíduos e isso foi catalisado pela eclosão da pandemia. Além disso, diversos mecanismos estão sendo criados para qualificar a doença, mapear seu avanço e fomentar a realização de atividades que antes só poderiam ser realizadas presencialmente. Nesse contexto estão inseridas as ferramentas que auxiliam a medicina no enfrentamento da doença e na implementação de teleconsultas. Entretanto, o uso dessas ferramentas incorre no risco de exposição de dados pessoais – sobretudo de dados médicos. Por esse motivo, deve haver uma gestão integrada entre esses atores que busque o equilíbrio com a intimidade das pessoas.

3.2 Tecnologias para conter aglomerações e detectar localização de pessoas contaminadas: riscos à invasão de privacidade e intimidade

Aplicativos de geolocalização estão sendo cada vez mais desenvolvidos e utilizados para monitorar contágios e o contato entre pessoas. Além disso, o cumprimento das medidas de isolamento também pode ser averiguado por esses aplicativos. Estima-se que quando a população mundial começar a se adaptar a

¹⁴ HUMMEL, Guilherme. *Fatos e ações tecnológicas para mitigar o Covid-19*. 2020. Disponível em: <https://digital.hospitalar.com/pt-br/ti-inovao/fatos-e-aes-tecnologicas-para-mitigar-o-covid-19>. Acesso em: 11 jul. 2020.

¹⁵ HUMMEL, Guilherme. *Fatos e ações tecnológicas para mitigar o Covid-19...*, cit.

conviver com o vírus, eles serão utilizados para verificar a probabilidade de contágio, assim como uma forma de permitir que os indivíduos estejam em público.¹⁶

Além disso, a China utiliza um aplicativo que atribui cores aos usuários e, por esse meio, é possível impedir a circulação de uma pessoa de acordo com o risco de contaminação que ela represente. A Coreia do Sul foi mais específica, realizando testes em massa aliada ao uso de dados pessoais e assim tem sido possível alertar potenciais contaminados a realizar o teste e praticar o isolamento.¹⁷

O Brasil se apropriou dos dados de geolocalização de forma anônima para saber o percentual de pessoas que estão seguindo as recomendações de isolamento social. Entretanto, o presidente Jair Bolsonaro decidiu cessar a tratativa com operadoras de telefonia no âmbito do governo federal. Na visão dele, os riscos de violação do direito à privacidade precisariam ser melhor avaliados. O mesmo não ocorreu no âmbito dos entes federativos menores, como o estado de São Paulo e também a cidade do Rio de Janeiro.¹⁸

Schreiber aponta que Diego Aranha, um professor do departamento de Engenharia da *Aarhus University* da Dinamarca, afirma que as formas de controle oriundas da pandemia são de difícil reversão e merecem atenção especial. Entretanto, ele se posiciona no sentido de que os dados anônimos utilizados para medir o isolamento social não representam riscos, sustentando ainda que, de acordo com a exposição feita pelo advogado Ronaldo Lemos, não existe desrespeito à Lei Geral de Proteção de Dados, quando não há identificação do indivíduo. Além disso, seria possível o uso de dados pessoais individualizados em situações estritamente excepcionais, as quais envolvessem proteção à vida, tutelas de saúde e execução de políticas públicas previamente definidas em leis, além da obrigatoriedade de se respeitar os vetores de proporcionalidade e necessidade.¹⁹

Ademais, durante a última década houve uma tendência à extração de dados dos usuários da internet, para se obter informações e assim influenciar condutas específicas. Portanto, os dados representavam um ativo comercial de diversas empresas de tecnologia. Para Requião, o contexto atual ajuda a revelar que diferentes pesquisadores já analisavam a vigilância e o monitoramento de pessoas,

¹⁶ ALMEIDA, Bethania de Araujo *et al.* Preservação da privacidade no enfrentamento da COVID-19: dados pessoais e a pandemia global. *Ciência & Saúde Coletiva*, [S.L.], v. 25, n. 1, p. 2487-2492, jun. 2020. Disponível em: https://www.scielo.br/scielo.php?script=sci_arttext&pid=S1413-81232020006702487&lng=en&nrm=iso. Acesso em: 9 jul. 2020.

¹⁷ SCHREIBER, Mariana. *Coronavírus: uso de dados de geolocalização contra a pandemia põe em risco sua privacidade?* 2020. Disponível em: <https://www.bbc.com/portuguese/amp/brasil-52357879>. Acesso em: 11 jul. 2020.

¹⁸ SCHREIBER, Mariana. *Coronavírus: uso de dados de geolocalização contra a pandemia põe em risco sua privacidade?...*, cit.

¹⁹ SCHREIBER, Mariana. *Coronavírus: uso de dados de geolocalização contra a pandemia põe em risco sua privacidade?...*, cit.

em especial por meio de aparelhos celulares e na simples expressão “aceito os termos de uso e privacidade”. Ele também levanta o ponto de que há um esforço comum pela saúde e por esse motivo, a preocupação que cerca a violação de privacidade deverá ser posta em segundo plano, promovendo uma mais fácil aceitação da vigilância e do monitoramento de pessoas, razão pela qual medidas extremas podem se tornar razoáveis.²⁰

Segundo a Organização para a Cooperação e Desenvolvimento Econômico (OCDE) em sua publicação de abril do presente ano, a quantidade de dados pessoais que os aplicativos reúnem e divulgam é ampla e de cognição difícil ao acesso dos usuários, uma vez que possibilitam execução em segundo plano. Com isso, poderá existir uma troca de informações entre aplicativos. Como mecanismo de controle, o reconhecimento facial também se mostra eficaz, pois reduz o contato físico e facilita o rastreamento dos indivíduos que contraíram a doença. Cabe então destacar o conceito de privacidade desde sua concepção ou *privacy-by-design*, que denota um grau máximo de privacidade e concorre para que os sistemas acoplem mecanismos de proteção a dados pessoais. De acordo com a OCDE, também é necessário que os governos considerem qual fundamento legal autoriza o uso das tecnologias, se as tecnologias e a coleta dos dados são proporcionais e principalmente, se o público entende o que está sendo feito, se há prestação de contas e prazo determinado para que os dados deixem de ser armazenados.²¹

Existe um aspecto ético que rodeia o processamento de dados, além de possíveis desconfiças que visam o equilíbrio entre os direitos individuais e coletivos, buscando proteger a intimidade das pessoas, bem como auxiliar as autoridades no enfrentamento da pandemia.²² Destarte, os dados coletados pelos aplicativos são utilizados de forma comercial e a pandemia fez com que o tema entrasse em foco, visto que dados de geolocalização passaram a ser utilizados para mensurar os índices de isolamento e de visita a hospitais e por este motivo a implementação desse tipo de vigilância e monitoramento obriga-se a estar em acordo com as regulamentações exigidas, devendo preservar a intimidade e a

²⁰ REQUIÃO, Maurício. *Covid-19 e proteção de dados pessoais: o antes, o agora e o depois*. 2020. Disponível em: <https://www.conjur.com.br/2020-abr-05/direito-civil-atual-covid-19-protecao-dados-pessoais-antes-agora-depois>. Acesso em: 11 jul. 2020.

²¹ OCED. *Rastreamento e monitoramento da COVID: proteção da privacidade e dos dados pessoais na utilização de aplicativos e biometria*. 2020. Disponível em: <http://www.oecd.org/coronavirus/policy-responses/rastreamento-e-monitoramento-da-covid-protecao-da-privacidade-e-dos-dados-pessoais-na-utilizacao-de-aplicativos-e-biometria-78260de1/>. Acesso em: 11 jul. 2020.

²² ALMEIDA, Bethania de Araujo *et al.* Preservação da privacidade no enfrentamento da COVID-19: dados pessoais e a pandemia global. *Ciência & Saúde Coletiva*, [S.L.], v. 25, n. 1, p. 2487-2492, jun. 2020. Disponível em: https://www.scielo.br/scielo.php?script=sci_arttext&pid=S1413-81232020006702487&lng=en&nrm=iso. Acesso em: 9 jul. 2020.

privacidade das pessoas, salvo quando houver proteção à vida e implementação de políticas públicas de saúde.

4 Dispositivos legais de proteção de dados

Nesse trecho do debate, é flagrante a necessidade de se identificar o objeto regulado pela LGPD, revelar seu vínculo com o direito da privacidade e analisar a atuação dos Estados Soberanos na contenção do vírus, frisando a carência de uma lei que tutele a privacidade, que evite abusos por parte dos países e garanta que as esferas privadas se mantenham incólumes. Posteriormente, serão estudadas as experiências do direito comparado e de como o Brasil tem lidado com a proteção dos dados pessoais.

4.1 Legislação brasileira: o que a Lei Geral de Proteção de Dados vem regular?

A Lei Geral de Proteção de Dados Pessoais extrai sua validade da própria carta política e se revela verdadeiro reflexo do direito à privacidade, vindo justamente para adaptar o ordenamento jurídico à nova ordem social imposta pelo avanço tecnológico cada vez mais vigoroso. Essa correlação é vista de forma plena ao se contemplar que ela mesma enumera - como fundamento da disciplina da proteção de dados pessoais - o respeito à privacidade em seu artigo segundo. Ademais, o próprio artigo inaugural da legislação já indica esse vínculo, ao aduzir que a lei lida com o tratamento de dados pessoais “inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural”.²³

Antes de continuar o curso da discussão, todavia, cumpre entender qual seria a significação real do direito à privacidade, já que tal conceito vai delinear o alcance da interpretação realizada na norma e os objetivos que ela apresenta. Para Mendes e Branco,²⁴ “O direito à privacidade, em sentido mais estrito, conduz à pretensão do indivíduo de não ser foco da observação por terceiros, de não ter

²³ BRASIL. *Lei nº 13.709, de 14 de agosto de 2018*. Brasília, DF: Presidência da República, 2020. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/Lei/L13979.htm. Acesso em: 10 jul. 2020.

²⁴ BRANCO, Paulo Gustavo Gonet; MENDES, Gilmar Ferreira. *Curso de Direito Constitucional*. 12. ed. São Paulo: Saraiva, 2017. p. 247.

os seus assuntos, informações pessoais e características particulares expostas a terceiros ou ao público em geral”.

Do conceito ofertado pelo doutrinador, é possível inferir que a privacidade nada mais é, em verdade, que uma salvaguarda aos dados do indivíduo e à intimidade dele. Assim, como ensina Sarlet:²⁵

[...] de um ponto de vista material o direito à privacidade cobre os aspectos da vida pessoal que, de acordo com as pautas sociais vigentes, costuma ser tido como reservado e indisponível ao legítimo interesse do Estado e de terceiros, especialmente tudo que tiver de ficar oculto para assegurar ao indivíduo uma vida com um mínimo de qualidade.

Vê-se, pois, que o escopo da lei está diretamente inserido na concepção do doutrinador. E isso até por ser ínsito à privacidade o controle sobre a divulgação das informações pessoais pertinentes ao indivíduo.

Embora de relevância incontestável, a privacidade, assim como ocorre com os demais direitos fundamentais, é um direito relativo, o que permite, portanto, sua limitação, podendo ser tal limitação inclusive promovida pelo próprio indivíduo, como se dá nos casos em que alguém consente com a exposição de forma expressa ou tácita, de informações que lhes são pertinentes.²⁶ É o caso de alguém que, de dentro de sua esfera de liberdade, escolhe divulgar determinada informação sobre si. Nesse diapasão, o tratamento dos dados pessoais poderá, por exemplo, ser realizado mediante o consentimento do titular. Não obstante, a própria LGPD acaba por atribuir finalismo a tal consentimento, ao conceituá-lo, em seu artigo quinto, como “manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada”. Assim, autorizações irrestritas, incondicionadas e vagas não preenchem o requisito legal e afastam a legitimidade de eventual tratamento de dados feito com fundamento nelas. Na verdade, esse finalismo ainda é expressamente previsto no oitavo artigo da lei, que em seu parágrafo quarto guarda: “O consentimento deverá referir-se a finalidades determinadas, e as autorizações genéricas para o tratamento de dados pessoais serão nulas”.²⁷

Por óbvio, a própria lei traz hipóteses que revelam ser desnecessário o consentimento do titular: casos de cumprimento de obrigação legal ou regulatória pelo

²⁵ MARINONI, Luiz Guilherme; MITIDIERO, Daniel; SARLET, Ingo Wolfgang. *Curso de direito constitucional*. 6. ed. São Paulo: Saraiva, 2017. p. 431.

²⁶ FERNANDES, Bernardo Gonçalves. *Curso de Direito Constitucional*. 9. ed. Salvador: JusPodivm, 2017.

²⁷ BRASIL, 2018, cit.

controlador, exercício regular de direitos em processo judicial, administrativo ou arbitral ou, até mesmo, de proteção da vida ou da incolumidade física do sujeito ou de terceiro. Não só isso, e em observância à própria lógica, afasta-se também essa exigência quando os dados forem tornados manifestamente públicos pelo próprio titular.²⁸

É possível questionar se seriam válidas essas limitações, haja vista no Brasil prevalecer o direito à liberdade, o que, por sua vez, afastaria a intervenção estatal indevida nas matérias privadas. Ocorre que, embora inicialmente vistos como limitadores da atuação estatal, os direitos fundamentais – incluído nestes o direito a privacidade, que é pedra de toque da LGPD – passaram a sofrer uma releitura, segundo a qual também seriam aplicáveis às relações estabelecidas apenas entre particulares. Aqui entra lição de Manoel Jorge e Silva Neto, que é cirúrgico na temática sobre o cabimento da oposição de direitos fundamentais a particulares:²⁹

O surgimento da proteção aos direitos fundamentais confundiu-se com a limitação do arbítrio e interferência estatais no âmbito da liberdade dos indivíduos, fazendo eclodir a tutela aos direitos civis e políticos dos cidadãos. Transcorridos, no entanto, mais de dois séculos desde a ocorrência da racionalização do poder, nota-se que o Estado não é o único protagonista de transgressões aos direitos dos indivíduos. Com efeito, a opção generalizada pelo modo capitalista de produção atribuiu aos agentes econômicos considerável parcela de poder, ao ponto de se defender a necessidade de criação de plexo de normas tendente a lhes adscreverem limites dada a rivalização dos grupos econômicos com o poder estatal. *Surgiu, assim, no século passado na Alemanha, a teoria da eficácia direta dos direitos fundamentais. O que significa? Simplesmente a aplicabilidade dos direitos fundamentais às relações entre particulares. Se, no contexto de tais relações, observa-se grande desigualdade entre os indivíduos, impõe-se o reconhecimento de aplicação dos direitos fundamentais para evitar o predomínio do arbítrio, como costuma acontecer nas relações entre o produtor/prestador de serviço e o consumidor e nas relações de trabalho.*

Na toada desta comparação, que apenas reforça a necessidade da existência de um marco normativo apto a disciplinar os pormenores dessa questão delicada, cumpre trazer a lume que o diploma normativo em debate, a LGPD, ainda não está

²⁸ BRASIL, 2018, cit.

²⁹ SILVA NETO, Manoel Jorge e. *Curso de direito constitucional*: atualizado até a EC 52/2006. 2 ed. Rio de Janeiro: Lumen Juris, 2006. p. 520-521, grifo nosso.

em vigor. Foi promovida, inclusive, a dilatação de sua *vacatio legis*, postergando-se, por meio da Medida Provisória 959/20, para o dia primeiro de agosto de 2021 a vigência das disposições contidas na Seção I (“Das Sanções Administrativas”) do Capítulo VIII (“Da Fiscalização”) e para 03 de maio de 2021 quanto aos demais dispositivos excetuando-se apenas as regras referentes à organização da administração pública, as quais entraram em vigor em 28 de dezembro de 2018 e que disciplinam a criação de um órgão de fiscalização e de promoção da proteção dos dados pessoais: a Autoridade Nacional de Proteção de Dados (ANPD). Desta forma, vê-se que há uma lacuna quanto à regulamentação da proteção dos dados pessoais dos indivíduos e a ausência de uma tutela específica a essa matéria.³⁰

O contraste entre a relevância da matéria e a carência de uma norma que disponha sobre os pormenores dessa questão é evidente, especialmente em vista da realidade que o país e demais nações atualmente enfrentam: enquanto a emergência de saúde pública de importância internacional decorrente do surto de 2019 causado pelo coronavírus continua a assolar o Brasil e o mundo, os governos de diversos Estados Soberanos têm colocado cada vez mais em debate a utilização de rastreamento em tempo real de *smartphones* para se avaliar as taxas de isolamento social. Em terras brasis, o Tribunal de Justiça de São Paulo já atestou a legalidade da criação de um sistema de monitoramento inteligente, o qual almejaria identificar índices de isolamento social e contribuiria para definir estratégias de prevenção e combate à pandemia no estado, afastando a alegação de eventuais violações à intimidade e à vida privada dos cidadãos.³¹ Não só isso, nos Estados Unidos da América, por exemplo, tem-se utilizado o rastreamento de contatos (*contact tracing*) para investigar e identificar agentes que supostamente praticaram crimes nas manifestações ocorridas por lá.³² Acerca do uso de dados pessoais pelo Estado no intuito do combate à disseminação do vírus, Dias e Damiani são incisivos:³³

³⁰ À época em que foi escrito o estudo, vigia a Medida Provisória 959/20, a qual prorrogava a *vacatio legis* da Lei nº 13.709/18, LGPD. Ocorre que, quando de sua conversão em lei, a disposição que prorrogava a *vacatio legis* não foi mantida, o que ensejou o retorno da redação do art. 65, II, dada pela Lei nº 13.853/19, e fez com que, a partir de 18 de setembro de 2020, a Lei Geral, quase que integralmente, já estivesse em vigor.

³¹ BRASIL. Procuradoria-Geral do Estado de São Paulo. *TJSP reconhece legalidade do Sistema de Monitoramento Inteligente (SIMI)*. 2020. Disponível em: <http://www.pge.sp.gov.br/visualizanoticia.aspx?id=4175>. Acesso em: 08 jul. 2020.

³² ALECRIM, Emerson. Polícia dos EUA diz usar rastreamento de contato contra manifestantes. *Tecnoblog*, 02 jun. 2020. Disponível em: <https://tecnoblog.net/343157/rastreamento-contato-policia-estados-unidos-manifestantes/>. Acesso em: 08 jul. 2020.

³³ DAMIANI, André; DIAS, Marina. A perigosa transformação do telefone celular em espião estatal. *Revista Consultor Jurídico*, 30 mai. 2020. Disponível em: <https://www.conjur.com.br/2020-mai-30/damiani-dias-transformacao-celular-espiao-estatal>. Acesso em: 09 jul. 2020.

Para a legislação, ‘dado pessoal’ é a informação que permite identificar, direta ou indiretamente, uma pessoa natural. Posto isso, *toda e qualquer ação caracterizada pelo tratamento de dados de pessoas deverá observar os princípios da boa-fé, da transparência, da prevenção, da segurança e da prestação de contas*. À luz desses mandamentos gerais, quando a Administração Pública declaradamente rastreia celulares, por exemplo, deve fazê-lo na persecução do interesse público, com o objetivo de cumprir suas atribuições legais, e desde que forneça aos titulares dos dados coletados informações claras e atualizadas sobre suas ações. Nesse contexto, é condição para o tratamento de dados pela administração que se preste exaustivo esclarecimento à população sobre o real alcance das políticas invasoras da privacidade.

E é em virtude disso que, no presente contexto - especialmente se levado em consideração o estado de calamidade pública reconhecido pelo Decreto Legislativo nº 6, de 20 de março de 2020 – identificam-se dois problemas principais no tocante ao uso de dados pessoais para controle e monitoramento da pandemia e para vigilância dos acometidos por ela: um primeiro referente à coleta destes dados, visto que, mesmo sendo realizada a sua “anonimização”, procedimento descrito no artigo quinto da LGPD como “utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo”, continua a persistir, em certos casos, a chance de identificação do usuário de quem esses dados foram extraídos; por outro lado, a posterior manutenção desses sistemas de controle e vigilância e a destinação dos dados coletados e seu uso futuro também levantam questionamentos, inclusive podendo mitigar ou suprimir, de certa forma, a democracia.³⁴

4.2 Dispositivos internacionais: quais as resoluções em nível mundial para a proteção de dados?

Explorada a legislação vindoura, resta analisar o direito comparado e a experiência brasileira da tutela de dados até o momento. A legislação brasileira foi francamente inspirada na disposição regulatória da União Europeia, a General

³⁴ REQUIÃO, Maurício. Covid-19 e proteção de dados pessoais: o antes, o agora e o depois. *Revista Consultor Jurídico*, 5 abr. 2020. Disponível em: <https://www.conjur.com.br/2020-abr-05/direito-civil-atual-covid-19-protexao-dados-pessoais-antes-agora-depois>. Acesso em: 10 jul. 2020.

Data Protection Regulation (GDPR). O Brasil, todavia, não foi o único país a ter uma legislação adequada às disposições da GDPR.

A Alemanha também possui disposição adequada aos preceitos da GDPR e já trazia regulamentação da matéria desde 2001. Sua nova lei, a Lei Federal de Proteção de Dados de 2017 (*Bundesdatenschutzgesetz – BDSG*), dispõe sobre os direitos e deveres de órgãos públicos e privados para as atividades de coleta e processamento de dados, algo próximo ao que a norma brasileira fará quando em vigor. Na Austrália, por outro lado, o diploma que trata sobre a matéria é a Lei de Privacidade de 1988, a qual incide indistintamente nos âmbitos público e privado.³⁵

Já na América Latina, é possível citar, por exemplo, o caso do Chile, país que possui regulamentação do século passado, a qual limita o uso dos dados ao propósito informado no ato da coleta. Excepciona-se, contudo, dessa regra o caso de registros públicos, algo próximo do que, conforme anteriormente exposto, a LGPD tratou de dispor no parágrafo quarto de seu sétimo artigo.

Há ainda o caso dos Estados Unidos da América, país que, em virtude de sua organização tipicamente federativa e delimitação fragmentada de competências legislativas, apresenta normas que são referência mundial, como na Lei de Privacidade de Comunicação Eletrônica (ECPA, em inglês), exemplificadamente. Trata-se de norma que veda a interceptação de comunicações telefônicas ou eletrônicas e garante a segurança do diálogo tanto durante a transmissão quanto após. Algo próximo do que já propõe a Carta Política pátria, que encarta o sigilo de dados como direito fundamental. Existem por lá, ademais, a Lei de Privacidade, a qual impõe diretrizes para a coleta, o armazenamento, o uso e a disseminação de dados por agências federais e a Lei de Proteção da Privacidade de Crianças, que define parâmetros e regras a serem seguidas pelos responsáveis por *websites* e serviços digitais, buscando a promoção e a tutela da privacidade dos infantes.³⁶

A experiência brasileira tem mostrado que, ao menos por enquanto, a tutela judicial se fará imprescindível, especialmente no curso do vácuo legislativo que se sucede. Recentemente, a título de ilustração, o STF enfrentou caso em que se discutia a constitucionalidade de Medida Provisória que determinava que as empresas de telecomunicações compartilhassem os dados em seu poder (nomes, números telefone e endereços de seus consumidores, pessoas físicas ou

³⁵ GONZÁLEZ, Mariana. Conheça o cenário das leis de proteção de dados ao redor do mundo. *IDBlog*, 14 fev. 2020. Disponível em: <https://blog.idwall.co/protacao-de-dados-cenario-mundial-das-leis/>. Acesso em: 11 jul. 2020.

³⁶ VALENTE, Jonas. Legislação de proteção de dados já é realidade em outros países. *Agência Brasil*, 07 maio 2018. Disponível em: <https://agenciabrasil.ebc.com.br/politica/noticia/2018-05/legislacao-de-protacao-de-dados-ja-e-realidade-em-outros-paises>. Acesso em: 11 jul. 2020.

jurídicas) de seus usuários com a Fundação Instituto Brasileiro de Geografia e Estatística – IBGE, para fins de suporte à produção estatística oficial, em virtude da situação de emergência de saúde pública de importância internacional decorrente do coronavírus. Neste julgamento, em entendimento de cognição sumária e referendando a cautelar concedida, o tribunal acabou por reconhecer a existência, no ordenamento pátrio, do direito à autodeterminação informativa.³⁷ Aliás, um dos fundamentos para a sustação cautelar da eficácia da Medida Provisória, além da ausência de garantias de tratamento adequado e seguro dos dados compartilhados, foi justamente o fato de a LGPD ainda não ter entrado em vigor.³⁸

Embora o panorama demande uma presença legislativa específica, que disponha sobre os pormenores da questão sensível a que se refere o manejo e a aquisição de dados pessoais de particulares, ao menos por enquanto essa lacuna poderá ser preenchida pelas normas aplicáveis aos casos em geral, a se valer do princípio hermenêutico da integração para preencher inoportunos buracos no ordenamento pátrio: eventuais danos causados pelas práticas ilícitas de outros particulares ou do próprio Estado serão compensados com indenização, na forma do que dispõe o Código de Reale (ou Código Civil), ao aduzir, em seu artigo 927, que “aquele que, por ato ilícito, causar dano a outrem, fica obrigado a repará-lo”³⁹ ou na forma do que ordena a própria Carta de Outubro, a Constituição da República Federativa do Brasil, no tocante aos danos causados pelo Estado, atuando nessa qualidade (nos dizeres do art. 37, §6º, CRFB, “as pessoas jurídicas de direito público e as de direito privado prestadoras de serviços públicos responderão pelos danos que seus agentes, nessa qualidade, causarem a terceiros, assegurado o direito de regresso contra o responsável nos casos de dolo ou culpa”⁴⁰).

Para além, o Marco Civil da Internet, Lei nº 12.965/14, também traz diretrizes que poderão ser úteis ao preenchimento de eventuais lacunas. Em certos pontos, verifica-se a ressonância entre as matérias tratadas na LGPD e as tratadas na

³⁷ COELHO, Marcus Vinicius Furtado. O direito à proteção de dados e a tutela da autodeterminação informativa. *Revista Consultor Jurídico*, 28 jun. 2020. Disponível em: <https://www.conjur.com.br/2020-jun-28/constituicao-direito-protacao-dados-tutela-autodeterminacao-informativa>. Acesso em: 09 jul. 2020.

³⁸ BRASIL. Supremo Tribunal Federal (Plenário). *Medida Cautelar Referendada na Ação de Inconstitucionalidade 6387/DF*. Medida Cautelar de Urgência. Requerente: Conselho Federal da Ordem dos Advogados do Brasil – CFOAB. Relatora: Min. Rosa Weber, 17 de abril de 2020. Disponível em: <https://jurisprudencia.stf.jus.br/pages/search/despacho1095308/false>. Acesso em: 09 jul. 2020.

³⁹ BRASIL. *Lei nº 10.406, de 10 de janeiro de 2002*. Brasília, DF: Presidência da República, 2020. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/2002/110406.htm. Acesso em: 10 jul. 2020.

⁴⁰ BRASIL. *Constituição da República Federativa do Brasil de 1988*. Brasília, DF: Presidência da República, 2020. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 09 jul. 2020.

Lei nº 12.965/14, como visto por Carvalho, ao identificar conteúdo símile, visto a privacidade ser princípio informativo de ambos os diplomas:⁴¹

Percebe-se, destarte, a importância conferida pelo legislador à auto-determinação informativa e ao consentimento nas relações dadas no âmbito da internet, estabelecendo fundamentação legal à necessidade de transparência, conscientização, ética e mesmo boa-fé das empresas que utilizam os dados pessoais e a privacidade dos usuários em seus modelos de negócio.

Embora não tenha a profundidade técnica e a riqueza de detalhes apresentadas pela LGPD, o Marco Civil da Internet, enquanto antecessor espiritual, pode também ajudar na tortuosa navegação em busca de tentativas de solução de eventuais conflitos ocasionados por abusos cometidos na captação de dados ou na divulgação de informações sensíveis.

5 Possíveis soluções para a proteção de dados médicos no Brasil

No decorrer deste trabalho foram expostos os riscos e desafios do uso da inteligência artificial na área da saúde, em especial, no período da Crise COVID-19. Então, quais as principais medidas que devem ser implementadas no Brasil para que se preserve a privacidade dos dados no uso da área da saúde?

Em primeiro lugar, a LGPD é um importante passo para a regulação do manuseio dos dados pessoais e em relação à área da saúde, essa norma possui dispositivos que prescrevem a profissionais de saúde, serviços de saúde ou autoridades sanitárias autoridade para tratar dados pessoais, ainda que sem o consentimento do titular, em virtude da sua saúde (art. 11, II, alínea “f”).⁴² Tal dispositivo, entretanto, é uma justa exceção da regra geral que predomina no instrumento legal: a de que os dados pessoais devem ser disponibilizados conforme o interesse e a necessidade do seu titular.

⁴¹ CARVALHO, Victor Miguel Barros de. *O Direito fundamental à privacidade ante a monetização de dados pessoais na internet*: apontamentos legais para uma perspectiva regulatória. 145 f. Dissertação (Mestrado em Direito) – Programa de Pós-Graduação em Direito da Universidade Federal do Rio Grande do Norte, Natal, 2018, p. 54. Disponível em: https://repositorio.ufrn.br/jspui/bitstream/123456789/26851/1/Direitofundamentalprivacidade_Carvalho_2018.pdf. Acesso em: 10 jul. 2020.

⁴² BRASIL. *Lei nº 13.709, de 14 de agosto de 2018*. Brasília, DF: Presidência da República, 2020. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/Lei/L13979.htm. Acesso em: 10 jul. 2020.

A lei regula também sobre a proibição de uso compartilhado entre controladores de dados pessoais sensíveis relativos à saúde visando vantagem econômica, listando como exceção a prestação de serviços de saúde e de assistência farmacêutica – em benefício dos interesses dos titulares de dados e para permitir a portabilidade dos dados e as transações financeiras e administrativas resultantes do uso e da prestação dos serviços de saúde (art. 11, §4º).⁴³ Em relação aos planos de saúde, a legislação proibiu as operadoras desses planos de tratar dados pessoais para seleção de riscos na contratação e exclusão de beneficiários (art. 11, §5º).⁴⁴

Dessa forma, ainda que se detenha certa margem de liberdade diante de situações como na tutela da saúde do titular para tratar dados pessoais sem o consentimento dos sujeitos, permanecem hipóteses específicas para adaptação dos serviços de saúde ao novo regulamento jurídico. É esperado, dos agentes atuantes nesse setor, a adoção de novos padrões de segurança e privacidade, voltados não somente à infraestrutura virtual, mas também aos profissionais, técnicos, auxiliares, gestores e operadores, que deverão qualificar seus processos de segurança da informação e *compliance* digital para que a proteção de dados seja garantida.⁴⁵

Quanto à Administração Pública, espera-se que a materialização da ANPD contribua para a fiscalização da conformidade das organizações à LGPD, fomentando o conhecimento adequado de práticas de segurança e respeito à proteção de dados. Observar a conduta de países que se destacaram na preservação da privacidade de dados pessoais também pode trazer grandes vantagens ao sistema brasileiro. A doutrina estabelece um bom exemplo a ser seguido:

A conformidade com as leis gerais de proteção de dados, portanto, requer tecnologia, infraestrutura e pessoal especializado para que os dados sejam tratados de forma lícita, justa e responsável em relação aos titulares dos mesmos, além de prever o princípio da responsabilização através de acompanhamento das atividades de processamento pelas autoridades designadas, que poderão aplicar sanções quando houver descumprimento da lei. Inclusive, alguns países possuem centros de dados criados por meio de parcerias entre governo,

⁴³ BRASIL. 2018, cit.

⁴⁴ BRASIL, 2018, cit.

⁴⁵ REBELO, Tertius. Por que os profissionais e empresas de saúde precisam se adequar à Lei Geral de Proteção de Dados? *JUS*. Junho de 2019. Disponível em: <https://jus.com.br/artigos/74825/por-que-os-profissionais-e-empresas-de-saude-precisam-se-adequar-a-lei-geral-de-protecao-de-dados>. Acesso em: 10 jul. 2020.

universidades e institutos de pesquisa para processar e prover acesso a dados anonimizados de forma segura e controlada para pesquisas de interesse público.⁴⁶

Também se torna categórico implementar as novas tecnologias com total transparência, em consulta com as principais partes interessadas, com sólido resguardo da privacidade desde a concepção dos sistemas.

Portanto, sustentar uma política de segurança de dados é imprescindível no nível de evolução crescente da inteligência artificial na área da saúde e tal garantia deve ser efetivada através de ações conjuntas entre todos os agentes da sociedade - desde os cidadãos, que devem estar atentos aos seus direitos estabelecidos na legislação que entrará em vigor, passando pelas organizações, que devem adaptar suas estruturas e seu pessoal para lidar com os cuidados inerentes à nova forma de lidar com os dados pessoais médicos. Por fim, em plano mais estratégico, as ações de órgãos públicos, como a ainda não materializada ANPD, devem informar e conscientizar sobre as novas diretrizes no tratamento de dados médicos, fiscalizar o cumprimento da lei, e, em último caso, aplicar as sanções previstas na legislação, em caso de desobediência aos ditames legais. Estabelecidas tais condutas, será possível garantir a todos, aliado ao progresso científico da inteligência artificial, o respeito à privacidade dos seus dados médicos.

6 Conclusão

Em tempos de pandemia, a necessidade de responder efetivamente aos desafios colocados pelo surgimento de um novo agente etiológico e a peculiaridade da doença fizeram com que a utilização de dados pessoais de diferentes fontes venha a ser requerida para explorar questões científicas, partindo de características relativas à população, de dados laboratoriais e hospitalares, dentre outros.

Conforme exposto, é necessário que tudo isso tenha embasamento ético e legal, uma vez que não restam dúvidas quanto ao esforço mundial que vem sendo desenvolvido para que as lacunas do conhecimento sobre a pandemia sejam preenchidas rapidamente pela ciência e serviços de saúde, a fim de que medidas ágeis, oportunas e eficientes possam ser adotadas pelas autoridades sanitárias

⁴⁶ ALMEIDA, Bethania de Araujo *et al.* Preservação da privacidade no enfrentamento da COVID-19: dados pessoais e a pandemia global. *Ciência & Saúde Coletiva*, [S.L.], v. 25, n. 1, p. 2487-2492, jun. 2020. Disponível em: https://www.scielo.br/scielo.php?script=sci_arttext&pid=S1413-81232020006702487&lng=en&nrm=iso. Acesso em: 9 jul. 2020.

para melhorar a capacidade de diagnóstico, manejo clínico e reabilitação dos casos de COVID-19, bem como as estratégias de prevenção.

Todas essas ações necessitam de que os governos tenham capacidade em articular medidas de diferentes segmentos da sociedade dispostos a maximizar os esforços no controle da doença. Para tanto, as tecnologias digitais fornecem ferramentas poderosas aos governos no combate à propagação da pandemia COVID-19, mas geram impactos na privacidade e na proteção de dados, que, conforme discutido, precisam ser reconhecidos.

Torna-se imprescindível, portanto, que as ações do Estado, das organizações privadas e dos próprios indivíduos titulares dos dados sejam direcionadas de forma conjunta à proteção dos dados pessoais. Diante da criação de legislações específicas a esse setor, como a LGPD, as pessoas estarão aptas a exigirem seus direitos e a cobrar pelo sigilo das informações que possam dispor a prestar no momento em que recorram às novas tecnologias. As organizações privadas devem submeter-se aos ditames legais, adaptando seus capitais humanos e materiais a fim de que se tornem compatíveis com as exigências das legislações cabíveis. E o Estado, por oportuno, especialmente através de órgãos específicos – no Brasil, especialmente a ainda não materializada Autoridade Nacional de Proteção de Dados – deve estar atento para fiscalizar o cumprimento da legislação, além de prestar informações e conhecimento à sociedade.

Dessa forma, ao unir esforços de todos os sujeitos da sociedade, será viável que o progresso da medicina, fomentado pela Inteligência Artificial, não invada a esfera privada dos indivíduos. Instauradas essas atuações, notadamente será possível garantir, no lapso decorrente da pandemia, que não só o direito à saúde seja efetivado, como também que o direito à privacidade seja a todos assegurado.

Artificial intelligence in health and data protection: reflections in the COVID-19 crisis

Abstract: The purpose of this work is to analyze how information and data storage technologies are being used to help combat the pandemic generated by the new coronavirus, an unknown disease until now, but which has generated a worldwide impact due to the need for social isolation and the absence of proven medication or cure. In a society where technology and communication are very present, governments begin to use these mechanisms to slow the progress of COVID-19, however, it is necessary to emphasize the need to be concerned with protecting the data of the entire population involved mainly how these will be used, not only in the current scenario, but also in the near future. To this end, an analysis of the legislation is done in a national and international scenario, as well as presenting the solutions adopted in Brazil to face the problem presented.

Keywords: data protection; COVID-19; artificial intelligence; Protection Law Data.

Summary: **1** Introduction – **2** Artificial intelligence in health – **3** The COVID-19 crisis – **4** Legal data protection devices – **5** Possible solutions for protecting medical data in Brazil – **6** Conclusion – References

Referências

- ALECRIM, Emerson. Polícia dos EUA diz usar rastreamento de contato contra manifestantes. *Tecnoblog*, 02 jun. 2020. Disponível em: <https://tecnoblog.net/343157/rastreamento-contato-policia-estados-unidos-manifestantes/>. Acesso em: 08 jul. 2020.
- ALMEIDA, Bethania de Araujo *et al.* Preservação da privacidade no enfrentamento da COVID-19: dados pessoais e a pandemia global. *Ciência & Saúde Coletiva*, [S.L.], v. 25, n. 1, p. 2487-2492, jun. 2020. Disponível em: https://www.scielo.br/scielo.php?script=sci_arttext&pid=S1413-81232020006702487&lng=en&nrm=iso. Acesso em: 9 jul. 2020.
- BRANCO, Paulo Gustavo Gonet; MENDES, Gilmar Ferreira. *Curso de Direito Constitucional*. 12. ed. São Paulo: Saraiva, 2017.
- BRASIL. *Constituição da República Federativa do Brasil de 1988*. Brasília, DF: Presidência da República, 2020. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 09 jul. 2020.
- BRASIL. *Lei nº 10.406, de 10 de janeiro de 2002*. Brasília, DF: Presidência da República, 2020. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/2002/110406.htm. Acesso em: 10 jul. 2020.
- BRASIL. *Lei nº 13.709, de 14 de agosto de 2018*. Brasília, DF: Presidência da República, 2020. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/Lei/L13979.htm. Acesso em: 10 jul. 2020.
- BRASIL. Supremo Tribunal Federal (Plenário). *Medida Cautelar Referendada na Ação de Inconstitucionalidade 6387/DF*. Medida Cautelar de Urgência. Requerente: Conselho Federal da Ordem dos Advogados do Brasil – CFOAB. Relatora: Min. Rosa Weber, 17 de abril de 2020. Disponível em: <https://jurisprudencia.stf.jus.br/pages/search/despacho1095308/false>. Acesso em: 09 jul. 2020.
- CARVALHO, Victor Miguel Barros de. *O Direito fundamental à privacidade ante a monetização de dados pessoais na internet*: apontamentos legais para uma perspectiva regulatória. 145 f. Dissertação (Mestrado em Direito) – Programa de Pós-Graduação em Direito da Universidade Federal do Rio Grande do Norte, Natal, 2018. Disponível em: https://repositorio.ufrn.br/jspui/bitstream/123456789/26851/1/Direitofundamentalprivacidade_Carvalho_2018.pdf. Acesso em: 10 jul. 2020.
- COELHO, Marcus Vinicius Furtado. O direito à proteção de dados e a tutela da autodeterminação informativa. *Revista Consultor Jurídico*, 28 jun. 2020. Disponível em: <https://www.conjur.com.br/2020-jun-28/constituicao-direito-protECAo-dados-tutela-autodeterminacao-informativa>. Acesso em: 09 jul. 2020.
- DAMIANI, André; DIAS, Marina. A perigosa transformação do telefone celular em espião estatal. *Revista Consultor Jurídico*, 30 maio 2020. Disponível em: <https://www.conjur.com.br/2020-mai-30/damiani-dias-transformacao-celular-espiao-estatal>. Acesso em: 09 jul. 2020.
- FERNANDES, Bernardo Gonçalves. *Curso de Direito Constitucional*. 9. ed. Salvador: JusPodivm, 2017.
- FERRARI, Fabricio; CECHINEL, Cristian. *Introdução a Algoritmos e Programação*. Universidade Federal do Pampa – Bagé, abril de 2008, versão 2.0. Disponível em: <https://www.ferrari.pro.br/home/documents/Ferrari-CCechinel-Introducao-a-algoritmos.pdf>. Acesso em: 10 jul. 2020.
- FUNDAÇÃO INSTITUTO DE ADMINISTRAÇÃO. *Big Data*: O que é, como aplicar, a importância e exemplos. 11 de jun. de 2018. Disponível em: <https://fia.com.br/blog/big-data/>. Acesso em 07 jul. 2020.
- GONZÁLEZ, Mariana. Conheça o cenário das leis de proteção de dados ao redor do mundo. *IDBlog*, 14 fev. 2020. Disponível em: <https://blog.idwall.co/protECAo-de-dados-cenario-mundial-das-leis/>. Acesso em: 11 jul. 2020.

HUMMEL, Guilherme. *Fatos e ações tecnológicas para mitigar o Covid-19*. 2020. Disponível em: <https://digital.hospitalar.com/pt-br/ti-inovao/fatos-e-aes-tecnologicas-para-mitigar-o-covid-19>. Acesso em: 11 jul. 2020.

LOBO, Luiz Carlos. Inteligência artificial, o Futuro da Medicina e a Educação Médica. *Revista Brasileira de Educação Médica*, Brasília, v. 42, n. 3, p. 3-8, Setembro de 2018. Disponível em: http://www.scielo.br/scielo.php?script=sci_arttext&pid=S0100-55022018000300003&lng=en&nrm=iso. Acesso em: 09 jul. 2020.

LOBO, Luiz Carlos. Inteligência artificial e Medicina. *Revista Brasileira de Educação Médica*, Rio de Janeiro, v. 41, n. 2, p. 185-193, jun. de 2017. Disponível em: http://www.scielo.br/scielo.php?script=sci_arttext&pid=S0100-55022017000200185&lng=pt&nrm=iso. Acesso em: 10 jul. 2020.

MARINONI, Luiz Guilherme; MITIDIERO, Daniel; SARLET, Ingo Wolfgang. *Curso de direito constitucional*. 6. ed. São Paulo: Saraiva, 2017.

OCED. *Rastreamento e monitoramento da COVID: proteção da privacidade e dos dados pessoais na utilização de aplicativos e biometria*. 2020. Disponível em: <http://www.oecd.org/coronavirus/policy-responses/rastreamento-e-monitoramento-da-covid-protexcao-da-privacidade-e-dos-dados-pessoais-na-utilizacao-de-aplicativos-e-biometria-78260de1/>. Acesso em: 11 jul. 2020.

OPAS. *Potencial das tecnologias da informação de uso frequente durante a pandemia*. 2020. Disponível em: https://iris.paho.org/bitstream/handle/10665.2/52023/Factsheet-TICs_por.pdf?sequence=7%20%20. Acesso em: 11 jul. 2020.

PRADO, Eduardo. O Dr Algoritmo da Inteligência Artificial. *Saúde Business*. 27 de junho de 2017. Disponível em: <https://saudebusiness.com/ti-e-inovacao/o-dr-algoritmo-da-inteligencia-artificial/>. Acesso em: 11 jul. 2020.

REQUIÃO, Maurício. *Covid-19 e proteção de dados pessoais: o antes, o agora e o depois*. 2020. Disponível em: <https://www.conjur.com.br/2020-abr-05/direito-civil-actual-covid-19-protexcao-dados-pessoais-antes-agora-depois>. Acesso em: 11 jul. 2020.

REBELO, Tertius. Por que os profissionais e empresas de saúde precisam se adequar à Lei Geral de Proteção de Dados? *JUS*. Junho de 2019. Disponível em: <https://jus.com.br/artigos/74825/por-que-os-profissionais-e-empresas-de-saude-precisam-se-adequar-a-lei-geral-de-protexcao-de-dados>. Acesso em: 10 jul. 2020.

RODRIGUES, Paula Marques. A inteligência artificial médica e o uso de dados pessoais no atendimento aos pacientes. *Migalhas*. 23 de abril de 2020. Disponível em: <https://www.migalhas.com.br/depeso/325245/a-inteligencia-artificial-medica-e-o-uso-de-dados-pessoais-no-atendimento-aos-pacientes>. Acesso em: 08 jul. 2020.

SÃO PAULO. Procuradoria-Geral do Estado. *TJSP reconhece legalidade do Sistema de Monitoramento Inteligente (SIM)*. 2020. Disponível em: <http://www.pge.sp.gov.br/visualizanoticia.aspx?id=4175>. Acesso em: 08 jul. 2020.

SCHREIBER, Mariana. *Coronavírus: uso de dados de geolocalização contra a pandemia põe em risco sua privacidade?*. 2020. Disponível em: <https://www.bbc.com/portuguese/amp/brasil-52357879>. Acesso em: 11 jul. 2020.

SCHWAB, Klaus. *A Quarta Revolução Industrial*. São Paulo: Edipro, 2016.

SILVA NETO, Manoel Jorge e. *Curso de direito constitucional: atualizado até a EC 52/2006*. 2. ed. Rio de Janeiro: Lumen Juris, 2006.

VALENTE, Jonas. Legislação de proteção de dados já é realidade em outros países. *Agência Brasil*, 07 maio 2018. Disponível em: <https://agenciabrasil.ebc.com.br/politica/noticia/2018-05/legislacao-de-protecao-de-dados-ja-e-realidade-em-outros-paises>. Acesso em: 11 jul. 2020.

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

NASCIMENTO, João Carlos Hipólito Bernardes do; MARQUES, Maria Leonildes Boavista Gomes Castelo Branco; COSTA, Nayara Hanna Santiago; BRANCO, Maria Isabel Boavista Gomes Castelo; SANTOS, Tâmara Beatriz; SOUSA, Roger Vítório Oliveira. Inteligência artificial na saúde e a proteção de dados: reflexos na crise COVID-19. *Direitos Fundamentais & Justiça*, Belo Horizonte, ano 14, p. 207-230, nov. 2020. Número especial.

Recebido em: 15.07.2020
Pareceres: 08.09.2020, 26.08.2020
Aprovado em: 12.09.2020