# INTELIGÊNCIA ARTIFICIAL E *BIG DATA* NO DIAGNÓSTICO E TRATAMENTO DA COVID-19 NA AMÉRICA LATINA: NOVOS DESAFIOS À PROTEÇÃO DE DADOS PESSOAIS


**Miguel Kfouri Neto**

Pós-Doutor em Ciências Jurídico-Civis junto à Faculdade de Direito da Universidade de Lisboa. Doutor em Direito das Relações Sociais pela Pontifícia Universidade Católica de São Paulo. Mestre em Direito das Relações Sociais pela Universidade Estadual de Londrina. Bacharel em Direito pela Universidade Estadual de Maringá. Licenciado em Letras-Português pela Pontifícia Universidade Católica do Paraná. Professor-Doutor integrante do Corpo Docente Permanente do Programa de Doutorado e Mestrado em Direito Empresarial e Cidadania do Centro Universitário Curitiba (UNICURITIBA). Coordenador do grupo de pesquisas "Direito da Saúde e Empresas Médicas" (UNICURITIBA). Membro titular do Instituto Brasileiro de Estudos em Responsabilidade Civil (IBERC). Desembargador no Tribunal de Justiça do Estado do Paraná.

**Rodrigo da Guia Silva**

Doutorando e Mestre em Direito Civil pela Universidade do Estado do Rio de Janeiro (UERJ). Membro do Instituto Brasileiro de Direito Civil (IBDCivil), do Instituto Brasileiro de Estudos de Responsabilidade Civil (IBERC) e do Instituto Brasileiro de Direito Contratual (IBDCont). Pesquisador da Clínica de Responsabilidade Civil da UERJ. Advogado.

**Rafaella Nogaroli**

Especialista em Direito Aplicado pela Escola da Magistratura do Paraná (EMAP) e em Direito Processual Civil pelo Instituto de Direito Romeu Felipe Bacellar. Pós-graduanda em Direito Médico pelo Centro Universitário Curitiba (UNICURITIBA). Coordenadora do grupo de pesquisas em "Direito da Saúde e Empresas Médicas" (UNICURITIBA). Membro titular do Instituto Brasileiro de Estudos em Responsabilidade Civil (IBERC). Assessora de Desembargador no Tribunal de Justiça do Estado do Paraná.



**Resumo**: O presente estudo tem por escopo identificar e equacionar novos desafios à proteção de dados pessoais suscitados pelo advento da inteligência artificial e do *big data* no enfrentamento da pandemia da COVID-19 no contexto latino-americano, em geral, e brasileiro, em particular. A investigação ora propugnada visa a perquirir parâmetros para a efetiva tutela do paciente no contexto da pandemia da COVID-19, seja no que diz respeito à adequada alocação de responsabilidade civil por danos porventura causados a partir do emprego das referidas tecnologias, seja no que diz respeito à delimitação de diretrizes para a implementação da inteligência artificial em estrita conformidade com a política de proteção de dados pessoais (em especial, os dados sensíveis). Adota-se, para tanto, o método lógico-dedutivo, recorrendo-se a fontes bibliográficas brasileiras e estrangeiras. Ao final do percurso trilhado, o estudo formula alguns possíveis cânones hermenêuticos a auxiliar o intérprete-aplicador do direito na tarefa de assegurar a proteção dos direitos da pessoa humana face às novas tecnologias, sem inibir-lhes o contínuo desenvolvimento, cuja importância é diuturnamente corroborada

pela dificuldade de enfrentamento da pandemia da COVID-19 no Brasil e, com as devidas proporções, na América Latina.

**Palavras-chave**: Inteligência artificial; *big data*; dados pessoais; COVID-19.



## 1 Notas introdutórias: a revolução digital no setor da saúde e o implemento da inteligência artificial no combate à pandemia da COVID-19

As novas tecnologias têm alterado profundamente a relação médico-paciente. Do diagnóstico médico ao cuidado holístico do paciente, a inteligência artificial[1] está transformando mundialmente todo o setor da saúde.[2] Há diversos estudos que revelam o grande potencial dessa tecnologia no aprimoramento de diagnósticos e cuidados médicos.[3] A medicina, como muitos outros campos, está passando por uma confluência de dois desenvolvimentos recentes: a ascensão do b*ig data*[4] e o crescimento de sofisticados sistemas de inteligência artificial, que podem ser usados para encontrar padrões complexos nesses dados.[5]

1 Para uma análise do conceito e da evolução da inteligência artificial, com destaque para a centralidade assumida na matéria pelos algoritmos, v., por todos, FLASIŃSKI, Mariusz. *Introduction to Artificial Intelligence*. Cham: Springer, 2016, *passim*; TEGMARK, Max. *Life 3.0*: Ser-se Humano na Era da Inteligência Artificial. Trad. João Van Zeller. Alfragide: Dom Quixote, 2019, *passim*; LEE, Kai-Fu. *As Superpotências da Inteligência Artificial*: a China, Silicon Valley e a Nova Ordem Mundial. Trad. Maria Eduarda Cardoso. Lisboa: Relógio D'Água Editores, 2018, *passim*; e TURNER, Jacob. *Robot Rules*: Regulating Artificial Intelligence. Cham: Palgrave Macmillan, 2019, *passim*.

2 Ao propósito, no que diz respeito à transformação da área da saúde com a nova era de informação tecnológica e de inteligência artificial, v. GARCIA, Christine; UZBELGER, Georges. Artificial Intelligence to Help the Practitioner Choose the Right Treatment: Watson for Oncology. *In:* NORDLINGER, Bernard; VILLANI, Cédric; RUS, Daniela (Coord.). *Healthcare and Artificial Intelligence*. Cham: Springer, 2020, p. 81.

3 Nesse sentido, v. SHABAN-NEJAD, Arash; MICHALOWSKI, Martin. *Precision Health and Medicine*. A Digital Revolution in Healthcare. Cham: Springer, 2020, p. V; DANIEL, Christel; SALAMANCA, Elisa. Hospital Databases. AP-HP Clinical Data Warehouse. *In*: NORDLINGER, Bernard; VILLANI, Cédric; RUS, Daniela (Coord.). *Healthcare and Artificial Intelligence*. Cham: Springer, 2020, p. 65.

4 V., por todos, GOMES, Rodrigo Dias de Pinho. *Big Data*: desafios à tutela da pessoa humana na sociedade da informação. Rio de Janeiro: Lumen Juris, 2017, *passim*.

5 PRICE, William Nicholson. Artificial Intelligence in Health Care: Applications and Legal Issues. *University of Michigan Public Law Research Paper*, n. 599, 2017. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3078704. Acesso em: 20 jun. 2020.

O surgimento do *big data* é um fenômeno caracterizado, segundo Nicholson Price, pelos "três V's": volume (grandes quantidades de dados), variedade (heterogeneidade dos dados) e velocidade (acesso rápido aos dados).[6] Esses dados vêm de várias fontes: registros eletrônicos de saúde, literatura médica, ensaios clínicos, dados de solicitações de seguros, registros de farmácia e até mesmo os dados inseridos pelos pacientes em seus *smartphones* ou gravados em aplicativos de *fitness*. Diante dessa vasta quantidade de dados, os algoritmos de inteligência artificial ganham espaço para prover, por exemplo, diagnósticos e alternativas de tratamento de algumas doenças, por meio de referência cruzada dos dados da saúde de um paciente específico com toda a sua base de dados.[7]

Jacob Turner, no livro "Robot Rules: Regulating Artificial Inteligence" (2019), define inteligência artificial (IA) como "a capacidade de uma entidade não humana de fazer escolhas por um processo avaliativo".[8] De acordo com a Comissão da União Europeia, a inteligência artificial refere-se a "sistemas que revelam comportamento inteligente, analisando seu ambiente e realizando ações – com algum grau de autonomia – para atingir objetivos específicos. Os sistemas baseados em IA podem ser puramente baseados em *software*, agindo no mundo virtual (por exemplo, assistentes de voz, *software* de análise de imagem, mecanismos de busca, sistemas de reconhecimento de voz e expressão) ou podem ser incorporados em dispositivos de *hardware* (por exemplo, robôs avançados, carros autônomos, drones ou aplicações de Internet das coisas)".[9]

Para funcionamento da inteligência artificial são utilizados algoritmos, que representam um conjunto de instruções ou sequência de regras que, aplicando-se a um número de dados, permitem solucionar classes semelhantes de problemas. Na essência, os algoritmos são as diretrizes seguidas por uma máquina. Um algoritmo de inteligência artificial funciona com base no cálculo de uma probabilidade, sendo esta o resultado da multiplicação de um vetor de entrada com inúmeros parâmetros, cujos valores foram encontrados a partir do treinamento.[10]

---

6 PRICE, William Nicholson. Artificial Intelligence in Health Care, cit.

7 Em 2015, um grupo de cientistas no Mount Sinai Hospital (Nova Iorque – EUA) desenvolveu o *Deep Patient*, *software* inteligente que prevê futuras doenças dos pacientes, a partir de uma base de dados composta por cerca de setecentos mil prontuários eletrônicos. Para o desenvolvimento da análise acerca do Deep Patient, remete-se a MIOTTO, Riccardo; LI, L.; KIDD, Brian A.; DUDLEY, Joel T. Deep Patient: An Unsupervised Representation to Predict the Future of Patients from the Electronic Health Records. *Nature Scientific Reports*, v. 6, mai./2016.

8 TURNER, Jacob. Robot Rules, cit., p. 16.

9 Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions on Artificial Intelligence for Europe, Brussels, 25.4.2018 COM (2018) 237 final.

10 FLASIŃSKI, Mariusz. *Introduction to Artificial Intelligence*, cit., p. 16.

A proliferação do recurso de algoritmos de inteligência artificial (sobretudo os sistemas mais sofisticados dotados de *machine learning* e *deep learning*)[11] [12] na prática médica impulsionou o amplo fenômeno de mudança da *medicina convencional* para a *medicina dos 4 Ps* (preventiva, preditiva, personalizada e proativa).[13] Nesse novo cenário, os cuidados da saúde deixam de estar essencialmente limitados ao tratamento das patologias (tarefa jamais abandonada, por certo) e passam a ter como foco a adoção de medidas destinadas a prevenir doenças (*medicina preventiva*)[14] ou possibilitar a antecipação do seu diagnóstico (*medicina preditiva*). No que tange ao trato pessoal, o paciente é atendido de maneira tendencialmente mais individualizada (e menos padronizada, portanto), com base nos seus dados genéticos e de saúde (*medicina personalizada*).[15] Por fim, a relação médico-paciente deixa de ser algo pontual e passa a se desenvolver de maneira contínua

[11] A técnica de *machine learning* é "fortemente baseada na análise de volumes maciços de dados, originários de várias fontes e em grande velocidade, um conjunto de características que se convencionou chamar de *big data*. Em resumo, o papel do computador nesta técnica é encontrar padrões estatísticos, dentro de um universo de informações, capazes de apresentar soluções para problemas bem claros" (GOETTENAUER, Carlos Eduardo. Algoritmos, inteligência artificial, mercados. Desafios ao arcabouço jurídico. *In*: FRAZÃO, Ana; CARVALHO, Angelo Gamba Prata de Carvalho (Coord.). *Empresa, mercado e tecnologia*. Belo Horizonte: Fórum, 2019, p. 273). Sobre o conceito de *machine learning*, v., ainda, WISCHMEYER, Thomas; RADEMACHER, Timo (Coord.). *Regulating Artificial Intelligence*. Cham: Springer, 2020, p. 3.

[12] O *deep learning* "permite o processamento de grande quantidade de dados para encontrar relacionamentos e padrões que os humanos geralmente não conseguem detectar. A palavra 'profundo' refere-se ao número de camadas ocultas na rede neural, que fornecem grande parte do poder de aprendizado" (FLASIŃSKI, Mariusz. Introduction to Artificial Intelligence, cit., p. 157-174. Tradução livre do original). V., ainda, TAULLI, Ton. *Artificial Intelligence Basics*. Nova Iorque: Springer, 2019, p. 71.

[13] "O aumento da expectativa de vida das pessoas, juntamente com a crescente complexidade dos serviços médicos e da saúde aumentam drasticamente os custos de saúde em todo o mundo. Por isso, os avanços em aplicativos da computação, combinados com o uso de redes sofisticadas de sensores inteligentes, servem como uma importante solução a esse cenário. Enquanto o conceito de *smart health* (saúde inteligente) sustenta o conceito de medicina dos 4 Ps (preventiva, preditiva, personalizada e proativa), essa tecnologia também produz grandes quantidades de dados e informações. Todas essas abordagens tecnológicas, juntamente com o 'big data', estão mudando as ciências médicas em uma ciência intensiva apoiada em dados" (HOLZINGER, Andreas; RÖCKER, Carsten; ZIEFLE, Martina. From Smart Health to Smart Hospitals. *In: Smart Health*: Open Problems and Future Challenges. Cham: Springer, 2015, p. 1-20. Tradução livre do original).

[14] Ao propósito da denominada medicina preventiva, v. BALICER, Ran D.; COHEN-STAVI, Chandra. Advancing Healthcare Through Data-Driven Medicine and Artificial Intelligence. *In:* NORDLINGER, Bernard; VILLANI, Cédric; RUS, Daniela (Coord.). *Healthcare and Artificial Intelligence*. Cham: Springer, 2020, p. 9-15.

[15] A medicina personalizada ("*precision medicine*" ou "*personalized medicine*") é definida como "uma abordagem inovadora que leva em conta as diferenças individuais nos genes de cada pessoa, ambientes e estilos de vida das pessoas, ao diagnosticar doenças e tomar decisões sobre diferentes opções de tratamento em tempo hábil. Ao contrário das abordagens e tratamentos mais tradicionais, 'one-size-fits-all', a medicina de precisão (personalizada) pretende projetar intervenções e tratamentos personalizados, considerando as diferenças entre os pacientes e suas doenças. A medicina de precisão pode facilitar o desenvolvimento e a descoberta de novos medicamentos, fornecendo melhor compreensão da interação entre genômica, resposta aos medicamentos e possíveis opções de tratamento da doença ou da condição de um paciente específico" (SHABAN-NEJAD, Arash; MICHALOWSKI, Martin. Precision Health and Medicine, cit., p. V. Tradução livre do original).

(*medicina proativa*),[16] o que é sobremaneira facilitado pelo implemento de algoritmos de inteligência artificial, pois o paciente tende a procurar ajuda médica não mais apenas quando adoece, tendo em vista que suas informações vitais são constantemente capturadas por aparelhos e monitores *vestíveis* ("*wearable devices*").[17]

A transformação do atendimento médico nesse modelo mais proativo, preventivo, preciso e centrado na individualidade de cada paciente tornou-se possível, nos últimos anos, a partir da combinação de grande volume de dados de saúde e *softwares* de inteligência artificial.[18] A Era Digital da assistência médica permitiu que os dados físicos dos pacientes fossem transferidos de pastas de papel para registros eletrônicos de saúde. Com isso, após décadas de digitalização de registros médicos (com o crescente armazenamento em nuvem), o setor de saúde criou um conjunto enorme (e continuamente crescente) de dados.

Vários tipos de bancos de dados de saúde foram estabelecidos desde o início da revolução digital (o que se conjuga à consequente multiplicação do poder de análise computacional), valendo destacar: prontuários médicos eletrônicos, dados administrativos digitais, dados coletados de equipamentos médicos conectados à internet ("Internet das Coisas" na medicina), dados de pesquisas clínicas e farmacêuticas, dados genômicos etc.[19] Afirma-se que os prontuários médicos eletrônicos representam a maior fonte de dados da saúde, pois neles está contida a soma da generalidade das informações a respeito do paciente, no objetivo de organizar todas as etapas da intervenção médica, desde a anamnese e procedimentos médicos relativos à terapia, até a evolução do tratamento.[20] A ilustrar o cenário contemporâneo, pode-se destacar que, em 2017, 80% dos prontuários médicos e 100% dos registros hospitalares de pacientes nos Estados Unidos foram digitalizados, facilitando a troca de informações como resultado desses arquivos digitalizados, que são denominados "registros eletrônicos de saúde" ("*electronic health records*" – EHRs, na abreviação em inglês).[21]

---

16 Para uma análise dos benefícios da denominada medicina proativa ("*proactive medicine*"), v. BALICER, Ran D.; COHEN-STAVI, Chandra. Advancing Healthcare Through Data-Driven Medicine and Artificial Intelligence, cit., p. 9-15.

17 NORDLINGER, Bernard; VILLANI, Cédric; RUS, Daniela (Coord.). *Healthcare and Artificial Intelligence*. Cham: Springer, 2020, *passim*.

18 NORDLINGER, Bernard; VILLANI, Cédric; RUS, Daniela (Coord.). *Healthcare and Artificial Intelligence*, cit., p. 10.

19 DEGOS, Laurent. International Vision of Big Data. *In*: NORDLINGER, Bernard; VILLANI, Cédric; RUS, Daniela (Coord.). *Healthcare and Artificial Intelligence*. Cham: Springer, 2020, p. 242; GRALL, Matthieu. CNIL (Commission Nationale de l'Informatique et des Libertés) and Analysis of Big Data Projects in the Health Sector. *In:* NORDLINGER, Bernard; VILLANI, Cédric; RUS, Daniela (Coord.). *Healthcare and Artificial Intelligence*. Cham: Springer, 2020, p. 236.

20 DEGOS, Laurent. International Vision of Big Data, cit., p. 242.

21 Assim relata DEGOS, Laurent. International Vision of Big Data, cit., p. 245.

No que importa mais diretamente ao presente estudo, pode-se notar que essa *digitalização* do setor da saúde foi um fator determinante para se tornar possível a implementação da inteligência artificial na eficiência dos diagnósticos médicos, sobretudo na detecção precoce de doenças.[22] Em emblemático exemplo do desenvolvimento da inteligência artificial aplicada à seara de diagnósticos médicos, pesquisadores da Universidade de Oxford (Inglaterra) desenvolveram, no Hospital John Radcliffe, o chamado *EchoGo Core*, um aparelho inteligente, que, por meio de *machine learning*, propõe o diagnóstico precoce de doenças cardíacas.[23] Esse *software* de ecocardiografia costuma ser apontado como o mais preciso do mundo e, para isso ser possível, programaram-se os algoritmos com bancos de dados contendo milhões de imagens de ecocardiografia, estando estas vinculadas às informações sobre questões particulares de cada pessoa examinada e o seu quadro clínico ao longo do tempo. O *software* atingiu a precisão diagnóstica de doenças cardíacas coronarianas em taxa de aproximadamente 90%, o que representa um melhor resultado do que o acerto médio de 80% alcançado por médicos.[24]

Atualmente, a IBM é uma das empresas, em escala global, que mais cria soluções tecnológicas para a área de saúde. Desde outubro de 2015, a multinacional possui uma unidade focada exclusivamente em inteligência artificial para a saúde – a "Watson Health".[25] Dentre os produtos inteligentes já disponíveis no mercado, destaca-se o "Watson for Oncology", "uma solução alimentada por informações obtidas de diretrizes relevantes, melhores práticas, periódicos médicos

[22] Há diversas empresas no mundo (como Cerner, Aldoc e Arterys) que utilizam a plataforma de serviços de computação em nuvem *Amazon Web Services (AWS)* para armazenar e processar grande volume de dados de saúde em alta velocidade, possibilitando, assim, a criação de novas ferramentas digitais inteligentes. Ao propósito, v. LANDI, Heather. Cerner taps Amazon Web Services to ramp up healthcare AI capabilities, predictive technology. *FierceHealthCare*, 3.12.2019. Disponível em: https://www.fiercehealthcare.com/tech/cerner-taps-amazon-web-services-to-ramp-up-healthcare-ai-capabilities-predictive-technology. Acesso em: 2 jul. 2020.

[23] GILLESPIE, Stuart. The Oxford spinout company using AI to diagnose heart disease. *University of Oxford*, 15/10/2018. Disponível em: https://www.research.ox.ac.uk/Article/2018-10-15-the-oxford-spinout-company-usingai-to-diagnose-heart-disease. Acesso em: 2 jul. 2020. Para maiores informações: https://ultromics.com/echogo/. Acesso em: 2 jul. 2020.

[24] Assim relata GILLESPIE, Stuart. The Oxford spinout company using AI to diagnose heart disease, cit. Os desenvolvedores desse dispositivo inteligente fundaram a empresa Ultromics e, recentemente, ganharam aprovação da *Food and Drug Administration* (FDA) para comercializar o EchoGo, que utiliza inteligência artificial para automatizar a análise e a quantificação de exames cardíacos baseados em ultrassom e, além disso, possui a capacidade de detecção precoce de doenças cardiovasculares. Ao propósito, v. PENNIC, Fred. *FDA Clears AI-Powered Echo Go Core for Early Detection of Cardiovascular Disease*. Hit Consultant, 15/11/2019. Disponível em: https://hitconsultant.net/2019/11/15/fda-clears-ai-powered-echogo-core-for-early-detection-of-cardiovascular-disease/#.XkBLijJKiUk. Acesso em: 24 abr. 2020.

[25] Remeta-se, por oportuno, ao portal em língua portuguesa disponibilizado pela própria empresa: IBM Watson Health – Cognitive Healthcare Solutions. Disponível em: https://www.ibm.com/watson/br-pt/health/. Acesso em: 2 jul. 2020.

e livros didáticos".[26] Essa tecnologia cognitiva avalia as informações do prontuário de um paciente, juntamente com as evidências médicas (artigos científicos e estudos clínicos), exibindo, assim, possíveis opções de tratamento para pacientes oncológicos, classificadas por nível de confiança. Ao final, caberá ao médico analisar as conclusões trazidas pela inteligência artificial e decidir qual a melhor opção de tratamento para aquele paciente específico. Desde 2017, o "Watson for Oncology" é utilizado em hospitais da América Latina, como Brasil[27] e México.[28]

A inteligência artificial para diagnóstico e tratamento de doenças tem demonstrado enorme potencial no contexto da pandemia da COVID-19 (doença causada pelo novo coronavírus, variante SARS-CoV-2). Na ausência de medicamentos ou vacinas terapêuticas específicas para o novo coronavírus, faz-se essencial detectar a doença em um estágio inicial e, dentro de parâmetros razoáveis, isolar do convívio com a população saudável as pessoas infectadas.[29]

A pandemia tem causado grande alarme em todo o globo, desde que os primeiros casos começaram a surgir, no final de 2019, em Wuhan (China). Apesar de a maioria dos infectados pelo novo coronavírus não desenvolver sintomas graves, há um considerável número de indivíduos dentro dos grupos de risco (como idosos e pacientes cardíacos, asmáticos, diabéticos e hipertensos) que podem apresentar síndromes respiratórias graves e letais. Nesse cenário, a maior preocupação apontada pela comunidade médica diz respeito à velocidade de propagação do vírus.[30]

Como se sabe, o diagnóstico da infecção por COVID-19 é realizado em duas etapas: diagnóstico clínico e diagnóstico confirmatório por exame laboratorial. O diagnóstico clínico depende da investigação clínico-epidemiológica e do exame físico. Caso a situação do paciente seja considerada, a partir do diagnóstico clínico, um *caso suspeito de COVID-19*, passa a ser indicada a realização do exame

[26] IBM Watson for Oncology. Disponível em: https://www.ibm.com/products/clinical-decision-support-oncology. Acesso em: 02 jul. 2020.

[27] *Hospital Mãe de Deus será o primeiro da América Latina a utilizar a tecnologia Watson da IBM*. 8 jun. 2017. Disponível em: https://setorsaude.com.br/hospital-mae-de-deus-sera-o-primeiro-a-utilizar-a-tecnologia-watson-da-ibm/. Acesso em: 12 jul. 2020.

[28] Grupo Ángeles Servicios de Salud Implements IBM Watson for Oncology to Help Oncologists Identify Evidence-Based Cancer Treatment Options. 30 jun. 2017. Disponível em: https://valoragregado.com/2017/06/30/grupo-angeles-servicios-de-salud-implements-ibm-watson-for-oncology-to-help-oncologists-identify-evidence-based-cancer-treatment-options/. Acesso em: 12 jul. 2020.

[29] Trata-se de matéria extremamente delicada, por envolver um sensível dilema entre liberdade e solidariedade no contexto do combate à Covid-19. Imperiosa, ao propósito, a remissão ao artigo de Thamis Dalsenter: https://www.migalhas.com.br/coluna/migalhas-de-vulnerabilidade/321211/direito-a-saude-entre-a-liberdade-e-a-solidariedade-os-desafios-juridicos-do-combate-ao-novo-coronavirus-covid-19. Acesso em: 12 jul. 2020.

[30] SHAW, Rajib; KIMB, Yong-kyun; HUAA, Jinling. Governance, technology and citizen behavior in pandemic: Lessons from COVID-19 in East Asia. *Progress in Disaster Science*, v. 6, abr. 2020, p. 1-11.

laboratorial. Em que pesem os benefícios proporcionados pelo exame laboratorial, fatores como os altos custos e a própria carência de material têm levado autoridades públicas e instituições hospitalares a restringir os testes aos pacientes sintomáticos – e, preferencialmente, àqueles com sintomas graves.[31]

É justamente nesse contexto – da impossibilidade de realização de exames laboratoriais para testar toda a população e do rápido contágio da doença – que aflora a renovada importância da inteligência artificial (IA) na análise diagnóstica.[32]

Na China, por exemplo, um *software* com algoritmos de IA, já utilizado em milhares de pacientes (e concedido gratuitamente para utilização de centenas de instituições médicas ao redor do mundo), é capaz de diagnosticar a COVID-19, em poucos segundos, a partir da análise da tomografia de tórax.[33] O *software* inteligente realiza, com taxa de precisão de aproximadamente 90%, a análise de uma imagem tomográfica em 15 segundos; com isso, consegue, quase instantaneamente, distinguir entre pacientes infectados com o novo coronavírus e aqueles com pneumonia comum ou outra doença. Trata-se de uma grande vantagem no enfrentamento da pandemia, em especial por se levar em consideração que os radiologistas geralmente precisam de cerca de 15 minutos para ler essas imagens de pacientes com suspeita de COVID-19.[34]

Na América Latina, noticia-se que o Equador foi o primeiro país a ter um sistema auxiliar com IA para diagnóstico da COVID-19. O *software* tecnológico, baseado em algoritmo fornecido pela empresa chinesa Huawei, contém milhares de imagens radiológicas armazenadas de pacientes ao redor do mundo com suspeita, confirmação e negativa de COVID-19, o que permite comparar os resultados obtidos em hospitais equatorianos e, desse modo, proporciona um diagnóstico

[31] MINISTÉRIO DA SAÚDE. *Diretrizes para diagnóstico e tratamento da Covid-19*. Disponível em: https://portalarquivos.saude.gov.br/images/pdf/2020/May/08/Diretriz-Covid19-v4-07-05.20h05m.pdf. Acesso em: 28 ago. 2020. Colhe-se, ainda, da imprensa: CAMBRICOLI, Fabiana. Com alta demanda hospitalar, hospital Albert Einstein começa a limitar exames no novo coronavírus. *Estadão*, 16/3/2020. Disponível em: https://saude.estadao.com.br/noticias/geral,com-alta-demanda-einstein-comeca-a-limitar-exames,70003235787. Acesso em: 12 jul. 2020.

[32] Um relevante ponto para a análise holística da matéria – incabível nesta sede – diz respeito ao papel do consentimento livre e esclarecido do paciente para a utilização da inteligência artificial em apoio à decisão médica. Para um desenvolvimento da análise da relevância do consentimento do paciente, em especial no contexto da cirurgia robótica e da telecirurgia, v. KFOURI NETO, Miguel; NOGAROLI, Rafaella. Responsabilidade civil pelo inadimplemento do dever de informação na cirurgia robótica e telecirurgia: uma abordagem de direito comparado (Estados unidos, União Europeia e Brasil). *In*: ROSENVALD, Nelson; MENEZES, Joyceane Bezerra de; DADALTO, Luciana. *Responsabilidade civil e medicina*. Indaiatuba: Foco, 2020, *passim*.

[33] *Ping An Launches COVID-19 Smart Image-Reading System to Help Control the Epidemic*. Disponível em: https://www.prnewswire.com/news-releases/ping-an-launches-covid-19-smart-image-reading-system-to-help-control-the-epidemic-301013282.html. Acesso em: 12 jul. 2020.

[34] *Ping An Launches COVID-19 Smart Image-Reading System to Help Control the Epidemic*, cit.

mais preciso e célere.[35] No Brasil, o Hospital de Clínicas da Faculdade de Medicina da Universidade de São Paulo (USP), em parceria com o Ministério da Ciência, Tecnologia, Inovação e Comunicações (MCTIC) e diversas empresas, criou a plataforma RadVid-19, que também utiliza o algoritmo da Huawei e tem o objetivo de coletar exames de raio-x e de tomografia computadorizada de casos confirmados ou suspeitos de COVID-19, tornando-se, assim, um grande repositório de casos no país.[36]

A breve enunciação desses exemplos da incorporação da inteligência artificial à prática médica no contexto da pandemia da COVID-19 serve para ilustrar alguns dos diversos benefícios que a referida tecnologia pode propiciar ao setor da saúde. Tais potenciais benefícios são acompanhados, contudo, por importantes questionamentos ético-jurídicos a serem enfrentados pela comunidade acadêmica, com particular destaque para a proteção e a forma de tratamento de dados pessoais sensíveis. Para isso, o presente estudo se propõe a investigar parâmetros para a efetiva tutela do paciente no contexto da pandemia da COVID-19, seja no que diz respeito à adequada alocação de responsabilidade civil por danos porventura causados a partir do emprego das referidas tecnologias, seja no que diz respeito à delimitação de diretrizes para a implementação da inteligência artificial em estrita conformidade com a política de proteção de dados pessoais (em especial, os dados sensíveis). Eis, em síntese essencial, o propósito norteador do presente estudo, a que se dedicam os itens subsequentes.

## 2 Benefícios e riscos dos algoritmos de inteligência artificial para auxiliar o diagnóstico e a escolha de tratamento médico

Os programas de inteligência artificial na área da saúde fornecem importante suporte à decisão clínica, como previamente exposto, tendo em vista a sua capacidade de processar e analisar rapidamente – e, tendencialmente, de maneira eficiente – grande quantidade de dados. A combinação da inteligência artificial com a expertise e o conhecimento médicos tem, portanto, o potencial de reduzir consideravelmente as taxas de erro. Não se trata de pugnar por uma substituição dos profissionais da saúde por sistema de IA, mas tão somente de reconhecer

[35] Equador, pioneira na América Latina no uso de inteligência artificial para detectar COVID-19. Disponível em: https://www.trt.net.tr/portuguese/america-latina/2020/04/01/equador-pioneira-na-america-latina-no-uso-de-inteligencia-artificial-para-detectar-covid-19-1389457. Acesso em: 12 jul. 2020.

[36] RadVid-19. Disponível em: https://radvid19.com.br/. Acesso em: 12 jul. 2020.

os potenciais benefícios dessa nova tecnologia no que tange, sobretudo, ao auxílio dos profissionais na tomada de decisão. Entre outros possíveis benefícios, destaca-se que o fornecimento de um diagnóstico rápido por um *software* com inteligência artificial pode ser, muitas vezes, fator crucial para o imediato início do tratamento e a subsequente recuperação do paciente, especialmente em doenças de evolução rápida ou em situações de urgência e emergência.

Pense-se, por exemplo, no salto qualitativo que se poderia ter experimentado no enfrentamento à pandemia da COVID-19 caso já se dispusesse, desde o início do surto da doença, de *softwares* avançados em matéria de diagnóstico em nível macro. Na China, como anteriormente exposto, desenvolveu-se, cerca de dois meses após o primeiro caso de contágio pelo novo coronavírus, um *software* com IA, utilizado em milhares de pacientes. O *software* inteligente realizou, com taxa de precisão de aproximadamente 90%, a análise de uma imagem tomográfica em quinze segundos; com isso, conseguiu, quase instantaneamente, distinguir entre pacientes infectados com o novo coronavírus e aqueles com pneumonia comum ou outra doença. Tratou-se de uma grande vantagem no enfrentamento da pandemia, em diversos países, sobretudo diante da falta de medicamentos ou vacinas terapêuticas específicas para o novo coronavírus. A inteligência artificial foi muito importante para diagnosticar a doença, o mais rápido possível, ainda em um estágio inicial – inclusive para isolar o infectado do convívio com o restante da população saudável. Além disso, destaque-se que os radiologistas geralmente precisavam de cerca de quinze minutos para ler essas imagens de pacientes com suspeita de COVID-19 , tempo este expressivamente superior aos quinze segundos utilizados pelo *software* inteligente.[37]

Como se sabe, os dados são o *combustível* da IA; afinal de contas, é justamente a partir do *input* dos dados que funcionam os algoritmos regentes dos *softwares* em comento, tal como no caso dos sistemas capazes de diagnosticar pacientes com COVID-19 . No referido exemplo da experiência chinesa, para se programar o algoritmo, foram inseridos dados de milhares de pacientes contaminados e suas respectivas tomografias de tórax. Assim, o sistema inteligente foi capaz de ler a imagem da tomografia, e distinguir, em quinze segundos, entre pacientes infectados com o novo coronavírus e aqueles com outras doenças pulmonares. Por isso, é preciso compreender que a qualidade dos dados para programação dos algoritmos é fundamental para o bom desempenho dos sistemas inteligentes, pois essa espécie de algoritmo – pautada em juízo de probabilidade – elabora conclusões a partir do conhecimento armazenado em suas bases e dos dados de cada paciente que lhe são fornecidos.

[37] Ping An Launches COVID-19 Smart Image-Reading System to Help Control the Epidemic, cit.

Há de se destacar, ainda, o enorme potencial do já referido *Watson for Oncology*, que utiliza um banco de dados em nuvem, por meio do qual é capaz de fazer referência cruzada e analisar dados de 20 milhões de trabalhos científicos de oncologia de institutos de pesquisa em todo o mundo.[38] Em janeiro de 2015, uma mulher de 60 anos foi internada em um hospital afiliado ao Instituto de Ciências Médicas da Universidade de Tóquio, no Japão. Os médicos inicialmente a diagnosticaram com leucemia mieloide aguda, um tipo de câncer no sangue.[39] No entanto, após uma rodada bem-sucedida de sessões de quimioterapia, os médicos observaram que sua recuperação da terapia pós-remissão era extraordinariamente lenta, levando-os a acreditar que estavam diante de um tipo diferente de leucemia.

Diante disso, a equipe de pesquisas do hospital socorreu-se do dispositivo inteligente de diagnóstico da IBM. Surpreendendo a comunidade médica, o *Watson for Oncology* realizou o diagnóstico da paciente em apenas dez minutos, ao passo que seres humanos levariam em média duas semanas. Por meio do rápido diagnóstico do *Watson*, descobriu-se que a paciente japonesa tinha uma rara leucemia secundária causada por síndromes mielodisplásicas, um grupo de doenças nas quais a medula óssea produz pouquíssimas células sanguíneas saudáveis.[40] De imediato, iniciou-se o tratamento adequado a esse tipo de leucemia que acometia a paciente.

O desfecho positivo do diagnóstico apoiado na IA não impede, contudo, que se enunciem riscos: por mais notável que o *Watson* seja na análise de números e no processamento de dados, ele possui o expressivo grau de imprecisão de 10%, ou seja, há considerável possibilidade de alguma falha nessa conclusão diagnóstica, o que pode conduzir à produção de danos ao paciente após o tratamento inapropriado. Justamente por conta disso, em 2017, o *Watson for Oncology* foi muito criticado por profissionais da saúde, sob a alegação de que não atenderia às expectativas ou até mesmo ofereceria diagnósticos imprecisos aos usuários médicos.[41]

[38] DAVID, Eric. Watson correctly diagnoses woman after doctors were stumped. *Silicon Angle*, 05/08/2016. Disponível em: https://siliconangle.com/2016/08/05/watson-correctly-diagnoses-woman-after-doctors-were-stumped/. Acesso em: 20jul. 2020.

[39] NG, Alfred. IBM's Watson gives proper diagnosis for Japanese leukemia patient after doctors were stumped for months. New York Daily News, 07/08/2016. Disponível em: https://www.nydailynews.com/news/world/ibm-watson-proper-diagnosis-doctors-stumped-article-1.2741857. Acesso em: 2 jul. 2020.

[40] DAVID, Eric. Watson correctly diagnoses woman after doctors were stumped, cit.

[41] IBM's Watson supercomputer recommended 'unsafe and incorrect' cancer treatments, internal documents show. Disponível em: https://www.statnews.com/2018/07/25/ibm-watson-recommended-unsafe-incorrect-treatments/. Acesso em: 2 jul. 2020.

Emblemática, a esse respeito, a pesquisa conduzida por uma equipe de quinze pesquisadores no *Manipal Hospitals*, na Índia, ao longo de três anos, com mil pacientes diagnosticados com câncer, no intuito de avaliar a precisão dos resultados do *Watson for Oncology*.[42] Ao final, os pesquisadores identificaram 90% de acerto dos diagnósticos pelo sistema de inteligência artificial. Nos casos em que ocorreu discordância entre o *software* e os médicos, estes últimos alteraram, em 63% dos casos, os seus próprios diagnósticos para seguir aquele dado pelo *Watson*.[43] Aqui está um ponto central para a presente reflexão: a inteligência artificial conduziu à alteração da decisão final dos oncologistas em diversos casos. De qualquer modo, a referida pesquisa revelou que em 37% dos casos o profissional não mudou seu diagnóstico em discordância com o resultado obtido pela inteligência artificial. Justifica-se, então, a enunciação de alguns questionamentos: na hipótese de superveniência de um resultado danoso que, em tese, poderia ser evitado caso se houvesse seguido o diagnóstico proposto pela inteligência artificial, deveria o médico ser responsabilizado? Se, ao revés, o médico segue o diagnóstico equivocado proposto pela inteligência artificial, pode o profissional ser isento de responsabilidade pelos danos porventura sofridos pelo paciente?[44]

De igual modo, deve-se ter em mente que os algoritmos criados para diagnóstico da COVID-19 possuem expressivo grau de imprecisão, o que pode acarretar resultados particularmente gravosos. Isso porque o diagnóstico falso negativo é muito mais grave do que em outras doenças, pois o paciente pode contaminar a sua família e pessoas próximas, além de se transformar em um involuntário e inconsciente vetor de multiplicação das taxas de infecção e contágio. Por outro lado, um resultado falso positivo implicará no fato de o paciente ficar em quarentena por quatorze dias, o que pode afetar sua atividade laboral e as suas relações pessoais e familiares.

Por isso, parece de bom tom reforçar que, ao menos no atual estado da sociedade, os *softwares* de diagnóstico devem servir como importante apoio à tomada de decisão do médico, sem o condão, contudo, de substituí-lo. Com efeito, a decisão final segue sob o controle (e sob a responsabilidade) do profissional

[42] BICUDO, Lucas. Inteligência Artificial descobre 1.000 casos de câncer com precisão de 90%. *StartSe*, 29/05/2017. Disponível em: https://www.startse.com/noticia/nova-economia/tecnologia-inovacao/inteligencia-artificial-descobre-1-000-casos-de-cancer-com-precisao-de-90. Acesso em: 2 jul. 2020.

[43] BICUDO, Lucas. Inteligência Artificial descobre 1.000 casos de câncer com precisão de 90%, cit.

[44] Para um desenvolvimento da análise acerca da utilização da inteligência artificial na análise diagnóstica da COVID-19 e suas repercussões sobre a responsabilidade médica, v. SILVA, Rodrigo da Guia; NOGAROLI, Rafaella. Inteligência artificial na análise diagnóstica da COVID-19: possíveis repercussões sobre a responsabilidade civil do médico. *In*: ROSENVALD, Nelson; MONTEIRO FILHO, Carlos Edison do Rêgo; DENSA, Roberta (Coord.). *Coronavírus e responsabilidade civil*: impactos contratuais e extracontratuais. Indaiatuba: Foco, 2020, p. 293-300.

da saúde. Dessa conclusão não se há de extrair, porém, uma banalização da responsabilização pessoal do médico. Seguindo a tônica do momento atual, deve-se socorrer da prudência também para a valoração da conduta do médico em eventual demanda indenizatória. Pode-se, assim, construir bases sólidas para a rejeição de demandas frívolas, evitando-se a difusão de uma postura de medicina defensiva que pouco (ou nada) contribuiria para o combate da pandemia em seu estágio atual.

Para além da análise da responsabilidade civil médica no caso de erro de diagnóstico, deve ser destacada a existência destes riscos de danos ao paciente, em decorrência de resultados imprecisos ou imprevistos que são próprios da inteligência artificial.

Vale mencionar, ainda, que os resultados desastrosos dos famosos acidentes com carros autônomos[45] serve de alerta para a possibilidade de a IA causar danos imprevisíveis,[46] sobretudo pela capacidade de autoaprendizagem da IA e pela possibilidade de ela evoluir de forma a gerar algum resultado indesejado (e, quiçá, jamais previsto). A aptidão dos algoritmos a produzir resultados que não poderiam ser efetivamente previstos pelos seus programadores – e tampouco pelos usuários diretos – é amplamente discutida na doutrina,[47] sobretudo por suas implicações ético-jurídicas na área da saúde.[48] Nos processos decisórios dos sistemas inteligentes há o chamado "problema da caixa preta" ("*black box problem*", em inglês),[49] isto é, os algoritmos executam determinadas ações para chegar a um resultado específico, mas nem sempre são capazes de realmente explicar ao homem como essa decisão foi tomada.[50]

---

[45] Em 2017, um modelo do carro autônomo Tesla S, dirigindo no piloto automático na China, chocou-se contra um caminhão, matando seu passageiro (Tesla Model 3: Autopilot engaged during fatal crash. Disponível em: https://www.bbc.com/news/technology-48308852. Acesso em: 2 jul. 2020). Em 2018, um carro autônomo da Uber atropelou um pedestre no estado do Arizona, nos Estados Unidos (Self-driving Uber kills Arizona woman in first fatal crash involving pedestrian. Disponível em: https://www.theguardian.com/technology/2018/mar/19/uber-self-driving-car-kills-woman-arizona-tempe. Acesso em: 2 jul. 2020).

[46] Sobre as condutas imprevisíveis decorrentes do aprendizado de máquina, v., por todos, MATTHIAS, Andreas. The responsibility gap: ascribing responsibility for the actions of learning automata. *Ethics and Information Technology*, v. 6, issue 3, set. 2004, p. 175-183; e MITTELSTADT, Brent Daniel; ALLO, Patrick; TADDEO, Mariarosaria; WACHTER, Sandra; FLORIDI, Luciano. The ethics of algorithms: mapping the debate. *Big Data & Society*, v. 3, issue 2, dez. 2016. p. 3 e ss

[47] MITTELSTADT, Brent Daniel; ALLO, Patrick; TADDEO, Mariarosaria; WACHTER, Sandra; FLORIDI, Luciano. The ethics of algorithms, cit., p. 5-7.

[48] Trust problem with AI needs to be addressed, says US-based Indian scientist. Disponível em: https://www.outlookindia.com/newsscroll/trust-problem-with-ai-needs-to-be-addressed-says-usbased-indian-scientist/1684755. Acesso em: 2 jul. 2020.

[49] Sobre o tema, imperiosa a remissão à já clássica lição de PASQUALE, Frank. *The black box society*: the secret algorithms that control money and information. Cambridge: Harvard University Press, 2015, *passim*.

[50] Por isso, ao implantar sistemas algorítmicos, mostra-se essencial "conhecer suas limitações e o que é efetivamente levado em conta para a tomada de decisões. Entender os limites dos algoritmos ajudará o agente a melhor julgar suas decisões e propostas, evitando, assim, visões simplistas e reducionistas,

Há dois casos emblemáticos que ilustram a problemática sobre as condutas imprevisíveis decorrentes da autoaprendizagem da IA e a falta de confiabilidade nos resultados trazidos pelos algoritmos. Durante experimento realizado em 2002, por cientistas do Magna Science Center, na Inglaterra, ocorreu um evento imprevisto: dois robôs inteligentes foram colocados em uma arena para simular um cenário de "predadores" e "presas", a fim de constatar se os robôs seriam capazes de se beneficiar da experiência adquirida com o *machine learning* para desenvolverem novas técnicas de caça e autodefesa. Sucedeu, contudo, que o Gaak, um dos robôs, adotou uma conduta imprevisível, encontrou uma saída através do muro da arena e foi para a rua, onde acabou atingido por um carro.[51]

Destaque-se, ainda, a situação na qual Sameer Singh, professor assistente no Departamento de Ciência da Computação da Universidade da Califórnia (UCI), nos Estados Unidos, relata que um aluno criou um algoritmo para categorizar fotos de huskies e lobos.[52] Inicialmente, parecia que o algoritmo era capaz de classificar quase perfeitamente os dois animais. No entanto, após inúmeras análises cruzadas posteriores, Singh descobriu que o algoritmo estava identificando lobos com base apenas na neve no fundo da imagem, e não próprias características do animal. Agora, imagine-se, por exemplo, um algoritmo mal programado, ou com algum grau de falibilidade, na já mencionada tecnologia cognitiva que foi utilizada em alguns países para diagnosticar pacientes infectados pelo novo coronavírus. Caso fossem introduzidos dados errados de pacientes contaminados ou o algoritmo fosse mal programado, os danos, obviamente, poderiam alcançar patamares imensuráveis.

Não por acaso, Nicholson Price explica que um dos maiores receios para o setor de saúde em tempos de inteligência artificial decorre justamente dos eventos imprevisíveis resultantes do aprendizado de máquina e da chamada *black box medicine* ("medicina de caixa-preta"), diante da obscuridade no modo de processamento das informações pelos algoritmos.[53] O autor também aponta sua

sob pena de tornar as pessoas, em certa medida, reféns de decisões tomadas na 'caixa-preta' dos algoritmos" (TEFFÉ, Chiara Spadaccini de; MEDON, Filipe. Responsabilidade civil e regulação de novas tecnologias: questões acerca da utilização de inteligência artificial na tomada de decisões empresariais. *Revista Estudos Institucionais*, v. 6, n. 1, jan./abr. 2020, p. 325).

[51] CERKA, Paulius; GRIGIEN, Jurgita; SIRBIKYT, Gintar. Liability for damages caused by artificial intelligence. *Computer Law & Security Review*, v. 31, n. 3, jun. 2015, p. 376-389.

[52] Husky or Wolf? Using a Black Box Learning Model to Avoid Adoption Errors. Disponível em: http://innovation.uci.edu/2017/08/husky-or-wolf-using-a-black-box-learning-model-to-avoid-adoption-errors/. Acesso em: 26 mar. 2020.

[53] Por outro lado, Price indica vantagens associadas à *black box medicine*: "a 'medicina caixa preta' tem o poder de auxiliar na resolução de problemas médicos complexos, a partir do poder do *big data*. Usando algoritmos de aprendizado de máquina para analisar grandes quantidades de dados médicos individuais – *medical big data* – os pesquisadores podem descobrir conexões entre atributos particulares do paciente com sintomas, doenças ou tratamentos específicos. A promessa da 'medicina caixa-preta', então, é que

preocupação no que se refere à privacidade, pois uma quantidade imensa de informações sensíveis é coletada por tais sistemas e, ainda, podem ser compartilhadas com outras entidades, o que aumenta o potencial de vazamentos de dados e de danos mediatos e imediatos aos seus titulares.[54]

Sobre o tema, Frank Pasquale relata evento ocorrido em 2008, nos Estados Unidos, em que os dados de prescrição médica estavam sendo utilizados no mercado de seguros individuais, pois as farmácias repassavam a relação de compras de remédios às seguradoras.[55] Com a coleta de milhões de informações de pedidos, as empresas readequavam suas políticas, a fim de excluir da cobertura algumas doenças e impor cobranças mais altas do prêmio a determinadas pessoas. Aproximadamente uma década após referido episódio, na era do *big data*, o risco à privacidade inevitavelmente demonstra-se acentuado. Isso porque, segundo Pasquale, "as empresas nem precisam consultar os registros médicos para atribuir-nos condições médicas e agir de acordo. Faça algumas pesquisas online sobre uma doença, preencha um formulário e você poderá acabar associado a essa doença em bancos de dados comerciais".[56]

Observa-se que, apesar dos potenciais benefícios da digitalização de dados, a sua utilização pode vir a configurar violação aos deveres de sigilo, transparência e informação, com desrespeito à autonomia do paciente e ao seu direito de consentir de modo amplo ao tratamento dos seus dados pessoais.[57] Na área médica, o risco de exposições é considerado mais profundo, tendo em vista que os dados de saúde são considerados como um recorrente alvo de crimes virtuais.[58] O grande desafio é manter "todos os avanços da digitalização da saúde sem comprometer o seu lado ético e humano, reforçando os códigos de conduta para proteger a

---

as decisões médicas podem se tornar personalizadas, prevendo doenças e adaptando diagnósticos e tratamentos para cada paciente individualmente considerado (...). O *black-box algorithm* pode orientar as decisões de tratamento, prevendo que um medicamento pode funcionar melhor que outro para um paciente específico, ou ter menos efeitos colaterais, ou que o paciente provavelmente responderá melhor a uma dose específica em um horário específico. Tais algoritmos podem eliminar a necessidade de os médicos experimentarem medicamentos diferentes, economizando tempo e dinheiro significativos" (FORD, Roger Allan; PRICE, W. Nicholson. Privacy and Accountability in Black-Box Medicine, *Michigan Telecommunications & Technology Law Review*, v. 23, 2016, p. 5. Tradução livre do original).

54 PRICE, William Nicholson. Artificial Intelligence in Health Care, cit., p. 6.

55 PASQUALE, Frank. The black box society, cit., p. 26-30.

56 PASQUALE, Frank. The black box society, cit., p. 28. A questão guarda relação com problemática geral da discriminação algorítmica. Ao propósito, v. JUNQUEIRA, Thiago. *Tratamento de dados pessoais e discriminação algorítmica nos seguros*. São Paulo: Thomson Reuters Brasil, 2020, *passim*.

57 SCHULMAN, Gabriel. Tecnologias de telemedicina, responsabilidade civil e dados sensíveis. O *princípio ativo* da proteção de dados pessoais do paciente e os efeitos colaterais do coronavírus. *In*: MONTEIRO FILHO, Carlos Edson do Rego; ROSENVALD, Nelson; DENSA, Roberta. *Coronavírus e Responsabilidade Civil*. Indaiatuba: Foco, 2020, p. 344-357.

58 Why cyber-criminals are attacking healthcare – and how to stop them. Disponível em: https://www.forbes.com/sites/kateoflahertyuk/2018/10/05/why-cyber-criminals-are-attacking-healthcare-and-how-to-stop-them/#5efc83f57f69. Acesso em: 2 jul. 2020.

informação clínica e os dados pessoais",[59] garantindo, ao final, a adequada tutela da privacidade do paciente.[60]

Entre os anos de 2018 e 2020, 562 episódios de invasões de dados em organizações da saúde foram reportados ao *U.S. Department of Health and Human Services Office for Civil Rights*.[61] Nos Estados Unidos, apenas em 2015, ocorreram 51 incidentes com *hackers* em instituições de saúde, envolvendo, na maioria das vezes, acesso ilícito aos dados sensíveis e prontuários eletrônicos de pacientes.[62] A empresa prestadora de serviços de saúde chamada *American Medical Tech* anunciou, em junho de 2020, a conclusão de investigação sobre episódio ocorrido em dezembro de 2019, no qual foi vítima de um ataque cibernético. Estima-se que a violação de dados afetou cerca de 50 mil pacientes e uma grande quantidade de dados pessoais pode ter ficado disponível ao *hacker* durante o incidente, incluindo-se: nomes de pacientes, números de seguro social, dados de prontuários médicos, informações de diagnóstico, apólice de seguro de saúde, informações de histórico médico, números de carteira de motorista etc.[63]

Diversas empresas e entidades hospitalares de países da Europa, como Espanha, Inglaterra e Portugal, também têm sido alvos de ataques cibernéticos nos últimos anos.[64] No Reino Unido, 16 hospitais do Serviço Público de Saúde foram afetados e alguns pacientes em situação de emergência precisaram ser transferidos. Além disso, informações sobre pacientes, agenda de consultas, linhas internas de telefone e e-mails ficaram temporariamente inacessíveis.[65] Noticia-se que o Brasil é líder em execução de ciberataques na América Latina e 11º no mundo,[66] tendo sido registrada a ocorrência de aproximadamente 15 bilhões de

[59] RIBEIRO, José Medeiros. *Saúde Digital*: um sistema de saúde para o século XXI. Lisboa: Fundação Francisco Manuel dos Santos, 2019, p. 27.

[60] DONEDA, Danilo. *Da Privacidade à Proteção de Dados Pessoais*: elementos da formação da Lei Geral de Proteção de Dados Pessoais. 2. ed. São Paulo: Revista dos Tribunais, 2019, p. 128-129.

[61] U.S. Department of Health and Human Services Office for Civil Rights Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Information. Disponível em: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf. Acesso em: 2 jul. 2020.

[62] Breaches of Unsecured Protected Health Information. Number of individuals affected by protected health information breaches: 2010 – 2015. Disponível em: https://dashboard.healthit.gov/quickstats/pages/breaches-protected-health-information.php. Acesso em: 2 jul. 2020.

[63] AMT healthcare data breach impacts nearly 50,000 patients. Disponível em: https://portswigger.net/daily-swig/amt-healthcare-data-breach-impacts-nearly-50-000-patients. Acesso em: 2 jul. 2020.

[64] *Empresas e hospitais sofrem ataque cibernético em massa*. Disponível em: https://link.estadao.com.br/noticias/empresas,empresas-e-hospitais-sofrem-ataque-cibernetico-em-massa-na-europa,70001776946. Acesso em: 2 jul. 2020.

[65] *Ciberataque paralisa 16 hospitais do Reino Unido*. Disponível em: https://brasil.elpais.com/brasil/2017/05/12/internacional/1494602389_458942.html. Acesso em: 2 jul. 2020.

[66] *Brasil é líder em execução de ciberataques na América Latina, aponta pesquisa*. 26 set. 2019. Disponível em: https://ipnews.com.br/brasil-e-lider-em-execucao-de-ciberataques-na-america-latina-aponta-pesquisa/. Acesso em: 12 jul. 2020

ataques cibernéticos apenas nos três primeiros meses de 2020.[67] Em um desses episódios, os computadores do Hospital das Clínicas de Barretos, em São Paulo, sofreram ataques cibernéticos, paralisando temporariamente alguns atendimentos.[68] A Interpol (Organização Internacional de Polícia Criminal) e diversas empresas de segurança digital têm alertado entidades hospitalares e organizações de saúde para tomarem cuidado redobrado, vez que elas se tornaram alguns dos principais alvos de *hackers* durante a pandemia da COVID-19 .[69] Em julho de 2020, ocorreu tentativa de ciberataque no Hospital Sírio-Libanês, em São Paulo, mas os próprios sistemas de segurança identificaram a tentativa de invasão e desconectaram o servidor da *internet* antes mesmo que o crime pudesse ser concretizado. Na ocasião, alguns pacientes ficaram sem acesso a exames, como ressonância magnética e tomografia, serviços estes que foram normalizados somente após cinco dias.[70] Poucos dias depois, a Secretaria de Saúde de Arapongas, no Paraná, abriu um procedimento administrativo para apurar o vazamento e divulgação na *internet* de uma lista com dados pessoais de pacientes infectados pela COVID-19.[71] Alguns meses antes desses episódios, a Microsoft enviou um alerta a hospitais e organizações de saúde vulneráveis a ataques de *hackers*, na América Latina e outras localidades, especialmente porque os criminosos sabem que os hospitais encontram-se sob pressão em tempos de pandemia e, diante disso, não têm tempo para instalarem atualizações ou se atentarem para detalhes nas configurações de rede.[72]

Os referidos incidentes de invasões de dados podem decorrer dos mais variados fatores, tais como a falta de segurança na transmissão das informações, inexistência de chaves de acesso e permissividades diversas dos sistemas e aplicativos que fragilizam a guarda e troca de informações. Todo o problemático cenário apresentado acerca dos diversos riscos na utilização de algoritmos de

---

[67] *Brasil sofreu 15 bilhões de ataques cibernéticos em 3 meses, diz estudo*. 6 ago. 2019. Disponível em: https://exame.abril.com.br/tecnologia/brasil-sofreu-15-bilhoes-de-ataques-ciberneticos-em-3-meses-diz-estudo/. Acesso em: 2 jul. 2020.

[68] *Os crimes dos hackers que interrompem até quimioterapia em sequestros virtuais de hospitais*. Disponível em: https://www.bbc.com/portuguese/brasil-40870377. Acesso em: 2 jul. 2020.

[69] *Após tentativa de ciberataque no Sírio-Libanês, setor da saúde teme invasões*. Disponível em: https://www1.folha.uol.com.br/cotidiano/2020/07/apos-tentativa-de-ciberataque-no-sirio-libanes-setor-da-saude-teme-invasoes.shtml. Acesso em: 12 jul. 2020.

[70] *Após tentativa de ciberataque no Sírio-Libanês, setor da saúde teme invasões*, cit.

[71] *Prefeitura vai apurar vazamento de lista de pessoas com Covid-19*. Disponível em: https://www.bonde.com.br/bondenews/parana/prefeitura-vai-apurar-vazamento-de-lista-de-pessoas-com-covid-19-520472.html. Acesso em: 15 jul. 2020.

[72] *Microsoft envia alerta 'inédito' para hospitais vulneráveis a ataques de hackers*. Disponível em: https://g1.globo.com/economia/tecnologia/blog/altieres-rohr/post/2020/04/03/microsoft-envia-alerta-inedito-para-hospitais-vulneraveis-a-ataques-de-hackers.ghtml. Acesso em: 12 jul. 2020.

inteligência artificial e tratamento de dados sensíveis traz a necessidade de serem discutidas importantes questões ético-jurídicos, às quais se dedica o capítulo subsequente.

## 3 Aspectos ético-jurídicos no tratamento de dados pessoais sensíveis do paciente por algoritmos de inteligência artificial no contexto da pandemia do novo coronavírus

Na área médica, quando se trata de processamento de dados pessoais sensíveis, dentre os principais riscos estão, conforme exposto anteriormente, o tratamento irregular de dados (especialmente em relação à privacidade), as decisões automatizadas no processamento dos dados[73] e a falta de informações ou consentimento sobre como os dados foram coletados, tratados e compartilhados.[74] Desse modo, é sobremaneira essencial a investigação das legislações que protegem os dados pessoais.

Observa-se, nos últimos anos, uma profunda mudança na compreensão, em diversos ordenamentos jurídicos, sobre a proteção de dados pessoais, ora entendidos como aspecto inerente à privacidade da pessoa humana.[75] Nesse contexto, enuncia-se o reconhecimento do direito à autodeterminação informativa, em ressignificação da acepção com que tradicionalmente era compreendido o direito à privacidade.[76] Especificamente na seara médica, a integral promoção da autodeterminação informativa pressupõe transparência e esclarecimento sobre quais dados do paciente serão tratados, qual a destinação dada a eles (princípio da finalidade) e com quem serão compartilhados.[77]

---

[73] Mencione-se, a esse respeito, a controvérsia sobre a existência ou não do direito do titular de dados pessoais à revisão, por pessoa humana, das decisões tomadas unicamente com base em tratamento automatizado. Tal controvérsia remonta à circunstância de a Medida Provisória nº 869/2018 e a subsequente Lei nº 13.853/2019 terem alterado o art. 20 da Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018) para suprimir a previsão, constante da redação originária do referido dispositivo legal, segundo a qual "(O) titular dos dados tem direito a solicitar revisão, *por pessoa natural*, de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses" (grifou-se).

[74] GRALL, Matthieu. CNIL (Commission Nationale de l'Informatique et des Libertés) and Analysis of Big Data Projects in the Health Sector, cit., p. 235.

[75] DONEDA, Danilo. Da Privacidade à Proteção de Dados Pessoais, cit., p. 29.

[76] Para o desenvolvimento da análise acerca da ressignificação da privacidade, hoje associada à autodeterminação informativa, faz-se imperiosa à clássica lição de RODOTÀ, Stefano. *A vida na sociedade da vigilância*: a privacidade hoje. Org. Maria Celina Bodin de Moraes. Trad. Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008, p. 15 e ss. Ao propósito, v., ainda, SOUZA, Eduardo Nunes de; SILVA, Rodrigo da Guia. Tutela da pessoa humana na lei geral de proteção de dados pessoais: entre a atribuição de direitos e a enunciação de remédios. *Pensar*, vol. 24, n. 3, jul.-set./2019, p. 9 e ss.

[77] SCHAEFER, Fernanda; GONDIM, Glenda Gonçalves. Telemedicina e lei geral de proteção de dados. *In*: ROSENVALD, Nelson; MENEZES, Joyceane Berreza de; DADALTO, Luciana (Coord.). *Responsabilidade Civil e Medicina*. Indaiatuba: Foco, 2020, p. 194-195.

No que diz respeito especificamente à experiência comunitária da América Latina, parece possível afirmar que não há mecanismos institucionais destinados à uniformização das normas e diretrizes de proteção de dados pessoais, diversamente do que sucede na experiência comunitária da União Europeia por força do Regulamento Geral de Proteção de Dados (RGPD).[78] Diversos Estados latino-americanos, no entanto, contam com legislação específica em vigor sobre proteção de dados pessoais. A Argentina, ilustrativamente, a partir do advento da Lei nº 25.326/2000,[79] afigura-se, até o momento, um dos países com experiência normativa mais rica em matéria de proteção de dados pessoais; o referido diploma legal argentino é pioneiro ao receber o juízo positivo de adequação pela União Europeia de sua normativa aos padrões europeus.[80] Por tais circunstâncias, afigura-se de todo recomendável um breve paralelo da legislação brasileira com a argentina no âmbito do esforço de compreensão do panorama latino-americano na matéria.

No Brasil, por sua vez, sem prejuízo dos percalços enfrentados para a plena vigência da Lei Geral de Proteção de Dados Pessoais (LGPD – Lei nº 13.709/2018), suscitam-se prementes reflexões quanto aos seus dispositivos que tratam de conceitos e princípios gerais no tratamento de dados, os quais encontram amparo também em outras fontes normativas e podem ser utilizados em interpretação extensiva. Não por acaso, já se reconhece que o direito fundamental à proteção de dados pessoais é "um princípio atualmente implícito no ordenamento brasileiro, mas a proteção que se pode dele deduzir irradia seus efeitos sobre todo o arcabouço normativo complementar, garantindo racionalidade ao sistema jurídico e propiciando proteção mesmo antes do fim do prazo de *vacatio legis* da LGPD".[81]

---

[78] Apesar da inexistência de mecanismos comunitários voltados especificamente à regulação da proteção de dados pessoais, nota-se um fenômeno comum no contexto latino-americano, qual seja, a introdução da ação de *habeas data* nos ordenamentos jurídicos, sobretudo na década de 1990. Vale registrar, ao propósito, o caráter pioneiro da atuação do poder constituinte originário brasileiro no estabelecimento do *habeas data* na Constituição Federal de 1988 (art. 5º, LXXII), o que veio a simbolizar um expressivo ponto de ruptura com o regime ditatorial, por assegurar ao cidadão a prerrogativa de conhecer e retificar as informações pessoais em bancos de dados de caráter público. O instituto do *habeas data* foi incorporado – nem sempre com o mesmo *nomen juris* –, por exemplo, nos ordenamentos jurídicos da Colômbia (1991), Paraguai (1993), Peru (1993), Argentina (1994), Equador (1996), Venezuela (1999) e México (2002). Para uma análise da superação dos impasses e indefinições que circundavam a proteção dos dados pessoais no Brasil antes do advento da Lei Geral de Proteção de Dados Pessoais (LGPD – Lei nº 13.709/2018), especialmente em razão da função eminentemente instrumental e simbólica atribuída pela práxis ao *habeas data*, remete-se a DONEDA, Danilo. *Da Privacidade à Proteção de Dados Pessoais*, cit., p. 276-288.

[79] Disponível em: https://www.oas.org/juridico/PDFs/arg_ley25326.pdf. Acesso em: 31 ago. 2020.

[80] DONEDA, Danilo. *Da Privacidade à Proteção de Dados Pessoais*, cit., p. 279.

[81] FALEIROS JUNIOR, José Luiz de Moura; NOGAROLI, Rafaella; CAVET, Caroline Amadori. Telemedicina e proteção de dados: reflexões sobre a pandemia da Covid-19 e os impactos jurídicos da tecnologia aplicada à saúde. *Revista dos Tribunais*, São Paulo, v. 1016, jun. 2020. Ainda no que tange ao reconhecimento

Deve-se ter em mente que os dados pessoais relativos à saúde, fonte primária de *abastecimento* das tecnologias envolvidas no setor médico, tendem a ser, por natureza, *dados pessoais sensíveis*. No plano doméstico brasileiro, a LGPD expressamente incluiu os dados relativos à saúde (conquanto sem defini-los) no conceito de "dado pessoal sensível", por ela definido como "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" (art. 5º, II). Em sentido similar, a supramencionada lei argentina não contém definição explícita de dados relativos à saúde, embora eles estejam expressamente incluídos no conceito de dados pessoais sensíveis (art. 2º).[82] Por outro lado, ao se observar o âmbito da União Europeia, o art. 35 do RGPD fornece extensa e valiosa definição do conceito de *dados pessoais relativos à saúde*:

> (...) todos os dados relativos ao estado de saúde de um titular de dados que revelem informações sobre a sua saúde física ou mental no passado, no presente ou no futuro. O que precede inclui informações sobre a pessoa singular recolhidas durante a inscrição para a prestação de serviços de saúde, ou durante essa prestação (...) as informações obtidas a partir de análises ou exames de uma parte do corpo ou de uma substância corporal, incluindo a partir de dados genéticos e amostras biológicas; e quaisquer informações sobre, por

de um direito fundamental à proteção de dados, afirma-se: "apesar de não existir no Brasil previsão constitucional sobre o direito à proteção de dados enquanto uma categoria de Direitos Fundamentais, é certo que o seu reconhecimento pode se dar por diversos dispositivos constitucionais: a partir da proteção da intimidade (artigo 5º, X), do direito à informação (artigo 5º, XIV), do direito ao sigilo das comunicações e dados (artigo 5º, XII), ou da garantia individual ao conhecimento e correção de informações sobre si pelo habeas data (artigo 5º, LXXII) (...) a privacidade é o *locus* constitucional adequado da proteção de dados, isto reflete no reconhecimento de que 'os dados são elemento constituinte da identidade da pessoa e que devem ser protegidos na medida em que compõem parte fundamental da sua personalidade, que deve ter seu desenvolvimento privilegiado, por meio do reconhecimento de sua dignidade' (...). O reconhecimento do direito à proteção de dados pessoais enquanto um Direito Fundamental os dota de eficácia direta e imediata, típica desta categoria de direito, decorrendo daí que os mesmos sejam respeitados não apenas na relação constituída entre Estado e sujeito, mas necessariamente nas relações travadas entre particulares" (MULHOLLAND, Caitlin; FRAJHOF, Isabella Z. Inteligência Artificial e a Lei Geral de Proteção de Dados Pessoais: breves anotações sobre o direito à explicação perante a tomada de decisões por meio de *machine learning*. *In:* FRAZÃO, Ana; MULHOLLAND, Caitlin (Coord.). *Inteligência artificial e direito*. São Paulo: Revista dos Tribunais, 2019, p. 270).

[82] Artigo 2º: "Datos sensibles: Datos personales que revelan origen racial y étnico, opiniones políticas, convicciones religiosas, filosóficas o morales, afiliación sindical e información referente a la salud o a la vida sexual". Em tradução livre: "Dados sensíveis: Dados pessoais que revelam origem racial e étnica, opiniões políticas, convicções religiosas, filosóficas ou morais, filiação sindical e informação referente à saúde ou à vida sexual".

> exemplo, uma doença, deficiência, um risco de doença, historial clínico, tratamento clínico ou estado fisiológico ou biomédico do titular de dados, independentemente da sua fonte, por exemplo, um médico ou outro profissional de saúde, um hospital, um dispositivo médico ou um teste de diagnóstico *in vitro*.[83]

Em consonância com a própria centralidade dos dados pessoais para a tutela contemporânea da privacidade, no Brasil, a LGPD estabelece, como regra geral, a necessidade de consentimento do titular para que ocorra o tratamento de dados pessoais (art. 7º, I). Para os fins da lei, considera-se como consentimento a "manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada" (art. 5º, XII). Faleiros e Dresch explicam a função essencial do consentimento do titular de dados pessoais:

> O consentimento se torna a estrutura basilar do tratamento dos dados pessoais. Para traçar um comparativo, o RGPD europeu cita 72 vezes a palavra 'consentimento'. No art. 4º sobre as definições, define consentimento como 'uma manifestação de vontade, livre, específica, informada e explícita, pela qual o titular dos dados aceita, mediante declaração ou ato positivo inequívoco, que os dados pessoais que lhe dizem respeito sejam objeto de tratamento (...).' Não foi diferente o tratamento conferido ao tema pelo legislador brasileiro, que, no art. 7º da Lei nº 13.709/2018, atribuiu ao consentimento do titular a natureza de requisito essencial para o tratamento dos dados pessoais: não sendo o consentimento livre, informado e inequívoco (art. 5º, XII), a medida se torna ilegal.[84]

[83] Regulamento Geral sobre a Proteção de Dados (Regulamento UE 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE). Disponível em https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32016R0679. Acesso em: 03 jun. 2020.

[84] DRESCH, Rafael de Freitas Valle; FALEIROS JÚNIOR, José Luiz de Moura. Reflexões sobre a Responsabilidade Civil na Lei Geral de Proteção de Dados (Lei nº 13.709/2018). *In:* ROSENVALD, Nelson; DRESCH, Rafael de Freitas Valle; WESENDONCK, Tula (Coord.). *Responsabilidade Civil*: Novos Riscos. Indaiatuba: Foco, 2019, p. 74.

No que se refere ao tratamento de dados pessoais *sensíveis*, as leis argentina[85] e brasileira[86] são categóricas no sentido de que somente será permitido quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas.[87] A finalidade no tratamento dos dados pessoais consiste em princípio disposto no art. 6º, inc. I, da LGPD.[88] No mesmo sentido, há disposições contidas no art. 4º, §3º, e art. 6º, da lei argentina.[89] Na hipótese de mudanças da finalidade para o tratamento de dados pessoais não compatíveis com o consentimento original, a LGPD prevê que "o controlador deverá informar previamente o titular sobre as mudanças de finalidade, podendo o titular revogar o consentimento, caso discorde das alterações" (art. 9º, §2º, da LGPD).

Na LGPD, apesar da regra geral de necessidade do consentimento para o tratamento de dados pessoais (art. 7º, I), em especial para os reputados sensíveis

[85] Art. 5º da Lei nº 25.326/2000: "1. El tratamiento de datos personales es ilícito cuando el titular no hubiere prestado su consentimiento libre, expreso e informado, el que deberá constar por escrito, o por otro médio que permita se le equipare, de acuerdo a las circunstancias. El referido consentimiento prestado con otras declaraciones, deberá figurar en forma expresa y destacada, previa notificación al requerido de datos, de la información descrita en el artículo 6° de la presente ley". Em tradução livre: "1. O tratamento de dados pessoais é ilícito quando o titular não tenha dado o seu consentimento livre, expresso e informado, que deve ser feito por escrito, ou por outro meio que permita equivalente, de acordo com as circunstâncias. O referido consentimento prestado com outras declarações deverá constar de forma expressa e destacada, após notificação ao requerido dos dados solicitados, da informação descrita no artigo 6º desta lei".

[86] Art. 11, inc. I, da LGPD: "O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses: I - quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas".

[87] As disposições das leis brasileira e argentina, no que diz respeito à necessidade de consentimento específico do titular de dados para cada finalidade determinada no tratamento destes dados, seguem lógica similar à indicada nos artigos 32 e 33 do RGPD. A esse respeito, Aurelia Tamò-Larrieux explica a necessidade de o consentimento do titular de dados ser sempre específico a uma determinada finalidade: "O princípio de limitação de finalidade afirma essencialmente que os dados pessoais devem ser coletados para fins específicos, legais e legítimos, e não devem ser processados de maneira incompatível com essas finalidades. O objetivo subjacente a esse princípio [finalidade] é (...) não permitir um 'cheque em branco' para usos adicionais ilimitados dos dados. O princípio da limitação de propósito exige uma avaliação do propósito originalmente declarado para a coleta de dados e se ele é consistente com a maneira pela qual o processamento de dados está sendo realizado" (TAMÒ-LARRIEUX, Aurelia. *Designing for Privacy and its Legal Framework*. Data Protection by Design and Default for the Internet of Things. Cham: Springer, 2018, p. 90).

[88] *In verbis*: "Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios: (...) finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades".

[89] Arts. 4º, §3º, e 6º, "a", da Lei nº 25.326/2000: "Los datos objeto de tratamiento no pueden ser utilizados para finalidades distintas o incompatibles con aquellas que motivaron su obtención"; "Cuando se recaben datos personales se deberá informar previamente a sus titulares en forma expresa y clara: a) La finalidad para la que serán tratados y quiénes pueden ser sus destinatarios o clase de destinatarios". Em tradução livre: "Os dados objeto de tratamento não podem ser utilizados para finalidades diferentes ou incompatíveis com aquelas que motivaram a sua obtenção"; "Quando os dados pessoais são coletados, deverá ser informado previamente a seus titulares, de forma expressa e clara: a) A finalidade para a qual serão tratados e quem podem ser seus destinatários ou classe de destinatários".

(art. 11, I), estabelece-se a desnecessidade do consentimento para tratamento dos dados pessoais sensíveis em certas finalidades excepcionais, entre as quais se incluem a "proteção da vida ou da incolumidade física do titular ou de terceiro" (art. 11, II, "e") e a "tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária" (art. 11, II, "f"). A partir de semelhante ordem de inspiração, o diploma em comento estabelece a possibilidade de conservação dos dados pessoais após o seu tratamento diante de algumas excepcionais finalidades, valendo destacar o "estudo por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais" (art. 16, II).

A lei argentina, por sua vez, no art. 5º, §2º, "d", prevê a desnecessidade de o titular dos dados consentir quando o tratamento derivar de uma relação contratual firmada com ele, sendo o tratamento necessário para o cumprimento da obrigação contratual.[90] Ademais, o art. 8º é específico sobre a autorização aos estabelecimentos de saúde públicos ou privados e os profissionais para tratamento de dados relativos à saúde dos pacientes em tratamento médico, respeitado o dever de sigilo profissional.[91]

Parece possível, então, afirmar que, segundo os ditames das leis argentina e brasileira sobre proteção de dados pessoais, o médico de um paciente com suspeita de COVID-19 não precisaria obter o consentimento para a inserção dos dados de saúde do paciente – como exames de raio-x e tomografia computadorizada – na plataforma já referida *RadVid-19*, em auxílio na realização do diagnóstico por algoritmos de inteligência artificial.

Ainda, observa-se que, segundo disposições da LGPD, tampouco seria necessário o consentimento do paciente para a manutenção dos seus dados na tecnologia cognitiva de diagnóstico da COVID-19, para a finalidade de estudo por órgão de pesquisa (art. 16, II), desde que devidamente anonimizados, ou para outra finalidade excepcional prevista no art. 16 da LGPD. De igual modo, a lei

[90] Art. 5º, § 2º, "d", da Lei nº 25.326/2000: "No será necesario el consentimiento cuando: (...) d) Deriven de una relación contractual, científica o profesional del titular de los datos, y resulten necesarios para su desarrollo o cumplimiento". Em tradução livre: "O consentimento não será necessário quando: (...) d) Derivem de uma relação contratual, científica ou profissional do titular dos dados, e sejam necessários ao seu desenvolvimento ou cumprimento".

[91] Art. 8º da Lei nº 25.326/2000: "Los establecimientos sanitarios públicos o privados y los profesionales vinculados a las ciencias de la salud pueden recolectar y tratar los datos personales relativos a la salud física o mental de los pacientes que acudan a los mismos o que estén o hubieren estado bajo tratamiento de aquéllos, respetando los principios del secreto profesional". Em tradução livre: "Os estabelecimentos de saúde públicos ou privados e os profissionais vinculados às ciências da saúde podem coletar e tratar dados pessoais referentes à saúde física ou mental dos pacientes que os procuram ou que estão ou tenham estado em tratamento, respeitando os princípios do sigilo profissional".

argentina prevê, no art. 11, §3º, "d" e "e", a desnecessidade do consentimento para a cessão dos dados de saúde para fins de pesquisa, desde que anonimizados.[92]

Frise-se, todavia, que há de se ter em mente que as referidas exceções à necessidade de consentimento na disciplina das leis brasileira e argentina precisam ser interpretadas restritivamente e com cautela, em deferência à tutela prioritária conferida pela tábua axiológica constitucional à dignidade da pessoa humana e à sua privacidade. Cumpre destacar, ademais, que, nada obstante a excepcional dispensa do consentimento, a LGPD estabelece expressamente a necessidade de as atividades de tratamento de dados pessoais observarem a boa-fé e o princípio da transparência (art. 6º, *caput* e inciso VI).[93] Levando-se tais considerações para o campo da saúde, parece impor-se o reconhecimento de um dever do médico de repassar ao paciente informações sobre o tratamento dos seus dados, tanto no que se refere à finalidade (*e.g.*, inserção no *Watson for Oncology*) quanto à conservação dos seus dados de saúde (anonimizados) na tecnologia cognitiva após o término do tratamento originário. Trata-se, vale esclarecer, de padrão de conduta imposto ao profissional inclusive (*rectius*: sobretudo) nas hipóteses excepcionais de desnecessidade de consentimento.

Diante da importância de toda a matéria, assume destacado relevo a preocupação com a integridade ou conformidade (*compliance*) em matéria de proteção de dados pessoais no campo da saúde.[94] Precisamente nesse sentido, a LGPD enuncia normas gerais acerca das boas práticas e da governança (arts. 50 e 51). Fala-se, com isso, em *compliance digital*, com o que se pretende aludir a diretrizes sólidas para a implementação das políticas de proteção de dados pessoais, manifestando-se "em uma série de deveres relacionados ao proceder ético dos

[92] Art. 11, §3º, "d" e "e", da Lei nº 25.326/2000: "El consentimiento no es exigido cuando: (...) d) Se trate de datos personales relativos a la salud, y sea necesario por razones de salud pública, de emergencia o para la realización de estudios epidemiológicos, en tanto se preserve la identidad de los titulares de los datos mediante mecanismos de disociación adecuados; e) Se hubiera aplicado un procedimiento de disociación de la información, de modo que los titulares de los datos sean inidentificables". Em tradução livre: "O consentimento não é exigido quando: (...) d) Se tratar de dados pessoais referentes à saúde, e seja necessário, por razões de saúde pública, de emergência ou para realização de estudos epidemiológicos, desde que se preserve a identidade dos titulares dos dados por meio de mecanismos de desassociação adequados; e) Se tenha aplicado um procedimento de desassociação da informação, de modo que os titulares dos dados não são identificáveis".

[93] *In verbis*: "Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios: (...) transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial".

[94] Para uma análise da origem e de alguns dos principais efeitos jurídicos do *compliance* no direito brasileiro, seja consentido remeter a OLIVA, Milena Donato; SILVA, Rodrigo da Guia. Notas sobre o *compliance* no direito brasileiro. *Quaestio Iuris*, vol. 11, n. 4, 2018, *passim*.

agentes de tratamento de dados".[95] A título ilustrativo, vale mencionar que a IBM, desenvolvedora da plataforma de computação cognitiva *Watson for Oncology*, disponibiliza um documento sobre "Princípios de Privacidade e Segurança de Dados: Serviços em Nuvem IBM", no qual a empresa indica medidas de segurança e privacidade dos dados nos serviços em nuvem, políticas e procedimentos projetados para gerenciar riscos associados à aplicação de mudanças em seus serviços em nuvem.[96]

A governança de dados também está prevista nas "Orientações Éticas para uma IA de Confiança", da Comissão Europeia, sendo considerada um requisito diretamente ligado ao princípio de prevenção de danos e ao direito fundamental à privacidade. Isso porque, ao longo de todo o ciclo de vida de um sistema com algoritmos de inteligência artificial – tal como o *Watson for Oncology* –, devem ser adotados protocolos de segurança dos dados, com indicação de informações como o modo de tratamento dos dados do usuário, as pessoas que terão acesso a eles e as circunstâncias específicas em que esse acesso poderá ocorrer.[97]

## 4 Conclusão

A Era Digital e as novas tecnologias, neste século, transformaram completamente as possibilidades de um melhor e mais preciso diagnóstico, como se buscou destacar neste artigo. O processo de digitalização das informações permitiu que os dados físicos dos pacientes fossem transferidos de pastas de papel para registros eletrônicos de saúde. Com isso, após décadas de digitalização de registros médicos (com o crescente armazenamento em nuvem), o setor de saúde criou um conjunto enorme (e continuamente crescente) de dados. Essa *digitalização* na área da saúde foi um determinante passo inicial para se tornar possível a implementação da inteligência artificial na racionalização dos fluxos de trabalho em hospitais, na eficiência dos diagnósticos médicos e, sobretudo, na detecção precoce de doenças.

A revolução digital alavancada pela disseminação da inteligência artificial e pelo fenômeno de *big data* tem provocado profundas transformações das mais diversas ordens no campo da saúde. Não por acaso, no cenário atual foram

[95] MARTINS, Guilherme Magalhães; FALEIROS JÚNIOR, José Luiz de Moura. Compliance digital e responsabilidade civil na Lei Geral de Proteção de Dados. *In*: MARTINS, Guilherme Magalhães; ROSENVALD, Nelson. *Responsabilidade civil e novas tecnologias*. Indaiatuba: Foco, 2020, p. 264.

[96] Princípios de Privacidade e Segurança de Dados: Serviços em Nuvem IBM. Disponível em: https://www-03.ibm.com/software/sla/sladb.nsf/pdf/KUP12494/$file/KUP12494BRPT.pdf. Acesso em: 23 jun. 2020.

[97] COMISSÃO EUROPEIA. *Orientações éticas para uma IA de confiança*, de 11 de agosto de 2019.

justamente os dados digitalizados dos milhares de pacientes diagnosticados com COVID-19 que tornaram possível a criação de um algoritmo capaz de identificar a doença a partir da análise da tomografia de tórax de novos pacientes. O sistema de inteligência artificial na análise diagnóstica da COVID-19 fornece, como visto, importante suporte à decisão clínica, tendo em vista a sua capacidade de processar e analisar eficiente e rapidamente grande quantidade de dados. Assim, abre-se possibilidade para diagnósticos rápidos de uma doença, com crescimento exponencial de infectados, e que tem evolução extremamente rápida.

A celebração das benesses da inteligência artificial no apoio ao diagnóstico da COVID-19 não deve, contudo, ofuscar a atenção quanto aos riscos subjacentes à incorporação dessa tecnologia à prática médica. Por mais notável que a inteligência artificial seja na análise de números e no processamento de dados, não se pode ignorar a sua natural falibilidade, já que há expressivo grau de imprecisão algorítmica, ao que se soma a possibilidade de resultados imprevisíveis em decorrência do potencial de autoaprendizagem dos algoritmos inteligentes.

Eis, em síntese essencial, o propósito fundamental que se espera ter alcançado com o presente estudo, no qual se buscou não apenas identificar os possíveis riscos associados à revolução digital no setor da saúde, mas igualmente formular algumas possíveis diretrizes hermenêuticas a auxiliar o intérprete-aplicador do direito na árdua tarefa de assegurar a proteção dos direitos da pessoa humana face às novas tecnologias, sem inibir-lhes o contínuo desenvolvimento. Espera-se que as investigações críticas ora desenvolvidas possam, ao final, contribuir para a premente renovação das discussões acerca dos impactos jurídicos da incorporação das novas tecnologias (em especial, a inteligência artificial e o tratamento de *big data*) à medicina e aos cuidados com a saúde, temática cuja importância é diuturnamente corroborada pela dificuldade de enfrentamento da pandemia da COVID-19 no contexto da América Latina.

**Artificial intelligence and big data in the diagnosis and treatment of Covid-19 in Latin America: new challenges to the protection of personal data**

**Abstract**: The present study aims to identify and address new challenges to the protection of personal data raised by the advent of artificial intelligence and big data against the Covid-19 pandemic in Latin America, in general, and in Brazil, in particular. The investigation now proposed aims to examine parameters for the effective protection of the patient in the context of the Covid-19 pandemic, whether with regard to the appropriate allocation of civil liability for damages possibly caused by the use of these technologies, or with regard to the delineation of guidelines for the implementation of artificial intelligence in strict accordance with the personal data protection policy (in particular, sensitive data). For this purpose, the study adopts the logical-deductive method, using Brazilian and foreign bibliographic sources. At the end of the trail, the study formulates some possible hermeneutical canons to assist the interpreter of the law in the task of ensuring the protection of the rights of the human person in the

face of new technologies, without inhibiting their continuous development, whose importance is daily corroborated by the difficulty of fighting the Covid-19 pandemic in Brazil and, with due proportions, in Latin America.

**Keywords**: Artificial intelligence; big data; personal data; Covid-19.



## Referências

BALICER, Ran D.; COHEN-STAVI, Chandra. Advancing Healthcare Through Data-Driven Medicine and Artificial Intelligence. *In*: NORDLINGER, Bernard; VILLANI, Cédric; RUS, Daniela (Coord.). *Healthcare and Artificial Intelligence*. Cham: Springer, 2020, p. 9-15.

BARROSO, Luís Roberto; MARTEL, Letícia de Campos Velho. A morte como ela é: dignidade e autonomia individual no final da vida. *In:* GOZZO, Débora; LIGIERA, Wilson Ricardo (Org.). *Bioética e Direitos Fundamentais*. São Paulo: Saraiva, 2012.

BODDINGTON, Paula. *Towards a Code of Ethics for Artificial Intelligence*. Cham: Springer, 2017.

CAMBRICOLI, Fabiana. Com alta demanda hospitalar, hospital Albert Einstein começa a limitar exames no novo coronavírus. *Estadão*, 16/3/2020. Disponível em: https://saude.estadao.com.br/noticias/geral,com-alta-demanda-einstein-comeca-a-limitar-exames,70003235787. Acesso em: 12 jul. 2020.

CERKA, Paulius; GRIGIEN, Jurgita; SIRBIKYT, Gintar. Liability for damages caused by artificial intelligence. *Computer Law & Security Review*, v. 31, n. 3, jun. 2015, p. 376-389.

DALLARI, Dalmo de Abreu. O habeas data no sistema jurídico brasileiro. *Revista da Faculdade de Direito*, Universidade de São Paulo, São Paulo, n. 97, p. 239-253.

DANIEL, Christel; SALAMANCA, Elisa. Hospital Databases. AP-HP Clinical Data Warehouse. *In:* NORDLINGER, Bernard; VILLANI, Cédric; RUS, Daniela (Coord.). *Healthcare and Artificial Intelligence*. Cham: Springer, 2020, p. 57-67.

DEGOS, Laurent. International Vision of Big Data. *In:* NORDLINGER, Bernard; VILLANI, Cédric; RUS, Daniela (Coord.). *Healthcare and Artificial Intelligence*. Cham: Springer, 2020, p. 241-254

DONEDA, Danilo. *Da Privacidade à Proteção de Dados Pessoais*: elementos da formação da Lei Geral de Proteção de Dados Pessoais**.** 2. ed. São Paulo: Revista dos Tribunais, 2019.

DRESCH, Rafael de Freitas Valle; FALEIROS JÚNIOR, José Luiz de Moura. Reflexões sobre a Responsabilidade Civil na Lei Geral de Proteção de Dados (Lei nº 13.709/2018). *In:* ROSENVALD, Nelson; DRESCH, Rafael de Freitas Valle; WESENDONCK, Tula (Coord.). *Responsabilidade Civil*: Novos Riscos. Indaiatuba: Foco, 2019, p. 65-89.

FALEIROS JUNIOR, José Luiz de Moura; NOGAROLI, Rafaella; CAVET, Caroline Amadori. Telemedicina e proteção de dados: reflexões sobre a pandemia da Covid-19 e os impactos jurídicos da tecnologia aplicada à saúde. *Revista dos Tribunais*, São Paulo, v. 1016, jun. 2020.

FLASIŃSKI, Mariusz. *Introduction to Artificial Intelligence*. Cham: Springer, 2016.

FORD, Roger Allan; PRICE, W. Nicholson. Privacy and Accountability in Black-Box Medicine, *Michigan Telecommunications & Technology Law Review*, v. 23, 2016, p. 1-43.

GARCIA, Christine; UZBELGER, Georges. Artificial Intelligence to Help the Practitioner Choose the Right Treatment: Watson for Oncology. *In:* NORDLINGER, Bernard; VILLANI, Cédric; RUS, Daniela (Coord.). *Healthcare and Artificial Intelligence*. Cham: Springer, 2020, p. 81-84.

GOETTENAUER, Carlos Eduardo. Algoritmos, inteligência artificial, mercados. Desafios ao arcabouço jurídico. *In:* FRAZÃO, Ana; CARVALHO, Angelo Gamba Prata de Carvalho. *Empresa, mercado e tecnologia*. Belo Horizonte: Fórum, 2019, p. 269-286.

GOMES, Rodrigo Dias de Pinho. *Big Data*: desafios à tutela da pessoa humana na sociedade da informação. Rio de Janeiro: Lumen Juris, 2017.

GRALL, Matthieu. CNIL (Commission Nationale de l'Informatique et des Libertés) and Analysis of Big Data Projects in the Health Sector. *In:* NORDLINGER, Bernard; VILLANI, Cédric; RUS, Daniela (Coord.). *Healthcare and Artificial Intelligence*. Cham: Springer, 2020, p. 235-240.

HOLZINGER, Andreas; RÖCKER, Carsten; ZIEFLE, Martina. From Smart Health to Smart Hospitals. *In: Smart Health*: Open Problems and Future Challenges. Cham: Springer, 2015, p. 1-20

KFOURI NETO, Miguel. *Responsabilidade civil do médico*. 10. ed. São Paulo: Revista dos Tribunais, 2019.

KFOURI NETO, Miguel; NOGAROLI, Rafaella. Responsabilidade civil pelo inadimplemento do dever de informação na cirurgia robótica e telecirurgia: uma abordagem de direito comparado (estados unidos, união europeia e brasil). *In*: ROSENVALD, Nelson; MENEZES, Joyceane Berreza de; DADALTO, Luciana. (Coord.). *Responsabilidade Civil e Medicina*. Indaiatuba: Foco, 2020, p. 159-186.

LEE, Kai-Fu. *As Superpotências da Inteligência Artificial*: a China, Silicon Valley e a Nova Ordem Mundial. Trad. Maria Eduarda Cardoso. Lisboa: Relógio D'Água Editores, 2018.

MARTINS, Guilherme Magalhães; FALEIROS JÚNIOR, José Luiz de Moura. *Compliance* digital e responsabilidade civil na Lei Geral de Proteção de Dados. *In:* MARTINS, Guilherme Magalhães; ROSENVALD, Nelson (Coord.). *Responsabilidade civil e novas tecnologias*. Indaiatuba: Foco, 2020, p. 263-297.

MATTHIAS, Andreas. The responsibility gap: ascribing responsibility for the actions of learning automata. *Ethics and Information Technology*, v. 6, issue 3, set. 2004, p. 175-183.

MITTELSTADT, Brent Daniel; ALLO, Patrick; TADDEO, Mariarosaria; WACHTER, Sandra; FLORIDI, Luciano. The ethics of algorithms: mapping the debate. *Big Data & Society*, jul. 2016. p. 1-21.

MINISTÉRIO DA SAÚDE. *Diretrizes para diagnóstico e tratamento da Covid-19*. Disponível em: https://portalarquivos.saude.gov.br/images/pdf/2020/May/08/Diretriz-Covid19-v4-07-05.20h05m.pdf. Acesso em: 28 ago. 2020.

MULHOLLAND, Caitlin; FRAJHOF, Isabella Z. Inteligência Artificial e a Lei Geral de Proteção de Dados Pessoais: breves anotações sobre o direito à explicação perante a tomada de decisões por meio de machine learning. *In:* MULHOLLAND, Caitlin; FRAZÃO, Ana. *Inteligência artificial e direito*. São Paulo: Revista dos Tribunais, 2019, p. 265-290.

NORDLINGER, Bernard; VILLANI, Cédric; RUS, Daniela (Coord.). *Healthcare and Artificial Intelligence*. Cham: Springer, 2020.

OLIVA, Milena Donato; SILVA, Rodrigo da Guia. Notas sobre o *compliance* no direito brasileiro. *Quaestio Iuris*, vol. 11, n. 4, 2018, p. 2708-2729.

PASQUALE, Frank. *The black box society*: the secret algorithms that control money and information. Cambridge: Harvard University Press, 2015.

PASQUALE, Frank. Toward a Fourth Law of Robotics: Preserving Attribution, Responsibility, and Explainability in an Algorithmic Society. *University of Maryland Francis King Carey School of Law Legal Studies Research Paper*, n. 2017-21. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3002546. Acesso em: 02 jun. 2020.

PEREIRA, André Gonçalo Dias. *O consentimento informado na relação médico-paciente*. Estudo de Direito Civil. Coimbra: Coimbra Editora, 2004.

PRICE, William Nicholson. Artificial Intelligence in Health Care: Applications and Legal Issues. *University of Michigan Public Law Research Paper*, n. 599, 2017. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3078704. Acesso em: 20 jun. 2020.

RIBEIRO, José Medeiros. *Saúde Digital*: um sistema de saúde para o século XXI. Lisboa: Fundação Francisco Manuel dos Santos, 2019.

RODOTÀ, Stefano. *A vida na sociedade da vigilância*: a privacidade hoje. Org. Maria Celina Bodin de Moraes. Trad. Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008.

RODOTÀ, Stefano. Por que é necessária uma Carta de Direitos da Internet? *Civilistica.com*, Rio de Janeiro, ano 4, n. 2, 2015. Disponível em: http://civilistica.com/por-que-e-necessaria-uma-carta-de-direitos-da-internet/. Acesso em: 02 jun. 2020.

RUS, Daniela. Artificial Intelligence: A Vector for Positive Change in Medicine. *In:* NORDLINGER, Bernard; VILLANI, Cédric; RUS, Daniela (Coord.). *Healthcare and Artificial Intelligence*. Cham: Springer, 2020, p. 17-22.

ROSENVALD, Nelson; BRAGA NETTO, Felipe Peixoto. Responsabilidade civil na área médica. *In:* BRAGA NETTO, Felipe Peixoto; CÉSAR SILVA, Michael. *Direito privado e contemporaneidade*. Indaiatuba: Foco, 2020, p. 25-68.

SCHAEFER, Fernanda; GONDIM, Glenda Gonçalves. Telemedicina e lei geral de proteção de dados. *In*: ROSENVALD, Nelson; MENEZES, Joyceane Berreza de; DADALTO, Luciana (Coord.). *Responsabilidade Civil e Medicina*. Indaiatuba: Foco, 2020, p. 187-202.

SCHULMAN, Gabriel. Tecnologias de telemedicina, responsabilidade civil e dados sensíveis. o *princípio ativo* da proteção de dados pessoais do paciente e os efeitos colaterais do coronavírus. *In*: MONTEIRO FILHO, Carlos Edson do Rego; ROSENVALD, Nelson; DENSA, Roberta. *Coronavírus e Responsabilidade Civil*. Indaiatuba: Foco, 2020, p. 344-357.

SHABAN-NEJAD, Arash; MICHALOWSKI, Martin. *Precision Health and Medicine*. A Digital Revolution in Healthcare. Cham: Springer, 2020.

SILVA, Rodrigo da Guia; NOGAROLI, Rafaella. Inteligência artificial na análise diagnóstica da COVID-19: possíveis repercussões sobre a responsabilidade civil do médico. *In*: ROSENVALD, Nelson; MONTEIRO FILHO, Carlos Edison do Rêgo; DENSA, Roberta (Coord.). *Coronavírus e responsabilidade civil*: impactos contratuais e extracontratuais. Indaiatuba: Foco, 2020, p. 293-300.

SILVA, Rodrigo da Guia; TEPEDINO, Gustavo. Dever de informar e ônus de se informar: a boa-fé objetiva como via de mão dupla. *In: Migalhas*, 09/06/2020. Disponível em: https://www.migalhas.com.br/depeso/328590/dever-de-informar-e-onus-de-se-informar-a-boa-fe-objetiva-como-via-de-mao. Acesso em: 02 jul. 2020.

SHAW, Rajib; KIMB, Yong-kyun; HUAA, Jinling. Governance, technology and citizen behavior in pandemic: Lessons from COVID-19 in East Asia. *Progress in Disaster Science*, v. 6, abr. 2020, p. 1-11.

SOARES, Flaviana Rampazzo. Veículos autônomos e responsabilidade por acidentes: trajetos possíveis e desejáveis no direito civil brasileiro. *In:* ROSENVALD, Nelson; DRESH, Rafael de Freitas Valle; WESENDONCK, Tula (Coord.). *Responsabilidade civil*: novos riscos. Indaiatuba: Foco, 2019, p. 149-176.

SOUZA, Eduardo Nunes de; SILVA, Rodrigo da Guia. Tutela da pessoa humana na lei geral de proteção de dados pessoais: entre a atribuição de direitos e a enunciação de remédios. *Pensar*, vol. 24, n. 3, jul.-set./2019.

TAMÒ-LARRIEUX, Aurelia. *Designing for Privacy and its Legal Framework*. Data Protection by Design and Default for the Internet of Things. Cham: Springer, 2018.

TAULLI, Ton. *Artificial Intelligence Basics*. Nova Iorque: Springer, 2019.

TEFFÉ, Chiara Spadaccini de; MEDON, Filipe. Responsabilidade civil e regulação de novas tecnologias: questões acerca da utilização de inteligência artificial na tomada de decisões empresariais. *Revista Estudos Institucionais*, v. 6, n. 1, jan./abr. 2020, p. 301-333.

TEGMARK, Max. *Life 3.0*: Ser-se Humano na Era da Inteligência Artificial. Trad. João Van Zeller. Alfragide: Dom Quixote, 2019.

TURNER, Jacob. *Robot Rules*: Regulating Artificial Intelligence. Cham: Palgrave Macmillan, 2019.

VOIGT, Paul; BUSSCHE, Axel von dem. The EU General Data Protection Regulation (*GDPR*). A Practical Guide. Cham: Springer, 2017.

WISCHMEYER, Thomas. Artificial Intelligence and Transparency: Opening the Black Box. *In*: WISCHMEYER, Thomas; RADEMACHER, Timo (Coord.). *Regulating Artificial Intelligence*. Cham: Springer, 2020, p. 75-101.

WISCHMEYER, Thomas; RADEMACHER, Timo (Coord.). *Regulating Artificial Intelligence*. Cham: Springer, 2020.

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

KFOURI NETO, Miguel; SILVA, Rodrigo da Guia; NOGAROLI, Rafaella. Inteligência artificial e *big data* no diagnóstico e tratamento da COVID-19 na América Latina: novos desafios à proteção de dados pessoais. *Direitos Fundamentais & Justiça,* Belo Horizonte, ano 14, p. 149-178, nov. 2020. Número especial.

Recebido em: 15.07.2020
Pareceres: 17.08.2020 e 21.08.2020
Aprovado em: 14.09.2020