# QUESTÕES TECNOLÓGICAS, ÉTICAS E NORMATIVAS DA PROTEÇÃO DE DADOS PESSOAIS NA ÁREA DA SAÚDE EM UM CONTEXTO DE *BIG DATA*

**Gabrielle Bezerra Sales Sarlet**

Doutora em Direito na Universidade de Augsburg (Alemanha). Pós-Doutora em Direito na Universidade de Hamburgo (Alemanha). Professora do curso de Graduação em Direito da Universidade Feevale (RS). Pós-Doutoranda em Direito na Pontifícia Universidade Católica do Rio Grande do Sul (PUCRS).

**Carlos Alberto Molinaro**

Doutor em Direito. Professor nos cursos de Mestrado e de Doutorado na Pontifícia Universidade Católica do Rio Grande do Sul (PUCRS).

**Resumo**: A tecnologia enceta radicais benefícios para a saúde, todavia, o contexto atual se ancora em inquietações quanto à segurança dos dados pessoais ante a inovação tecnológica. A indagação acerca da propriedade dos dados, da responsabilidade e da solidariedade, sobretudo quanto ao papel dos indivíduos, do Estado, das entidades profissionais e das empresas privadas no setor da saúde, compõe um campo fértil, demandando uma investigação em razão do necessário equacionamento dos danos e das oportunidades. Essa pesquisa teórica e bibliográfica e, tendo em vista os possíveis resultados, exploratória, objetiva analisar as especificidades dos dados da área da saúde e a repercussão do seu uso em função das formas contemporâneas de coleta, de armazenamento, de tratamento, de manipulação, sobretudo em um contexto de *big data*. Pretende-se, em razão da atual tendência à implantação de uma espécie de tecnocontrole por meio da algoritimização da sociedade atual empreendida pelos oligopólios mundiais, ante os riscos inerentes ao emprego da tecnologia de comunicação e de informação (TIC) e da fragilidade dos dispositivos que perfazem o sistema protetivo brasileiro, investigar, particularmente, alguns dos pontos lacunosos e controversos da Lei Geral de Proteção de Dados (LGPD) aplicáveis à área da saúde com o propósito de apresentar pautas e recomendações.

**Palavras-chave**: Saúde. *Big data*. Pesquisa médica. Dispositivos. Ética. Autodeterminação.



## 1 Noções básicas

*Big data* é um dos principais elementos do debate contemporâneo sobre as mudanças sociais induzidas tecnologicamente. A palavra descreve um

tratamento de grandes quantidades de dados que visa reconhecer padrões e obter novas percepções a partir deles. Isso requer abordagens vanguardistas em razão da abundância, da diversidade dos dados e da rapidez com que são coletados, analisados e revinculados ou reintroduzidos no sistema, ou seja, em um ambiente caracterizado pela volatilidade, pela incerteza, pela complexidade e pela ambiguidade.

A coleta sistemática e a análise dos dados tem sido um fator importante no desenvolvimento civilizacional, afirmando-se que o uso de computadores modernos, de tecnologias de armazenamento e de redes rápidas permite um radical incremento no volume gerenciável de dados, proporcionando igualmente uma variedade de melhorias qualitativas, como o uso de procedimentos computacionais mais complexos e, assim, o emprego de algoritmos em simulações computacionais, racionalizando, padronizando e melhorando a qualidade de muitos processos de trabalho. Evidencia-se nesse contexto, outrossim, uma hiperaceleração dos principais padrões de comportamentos humanos e, em consequência, o apelo por uma vida em *high performance*.

A propósito, o desenvolvimento em *big data*, destarte, revela uma evidente transformação de todas as fases do processamento de dados, que se caracteriza pelo aumento da automação, de *networking* etc. O volume e a velocidade da coleta de dados totalmente automatizada aumentaram exponencialmente em poucos anos, assim como a rápida disseminação e a rede de dispositivos que podem ser usados para a coleta de dados em todas as esferas do mundo humano. Consistindo, assim, em desdobramentos que, de tal sorte, estão constantemente colaborando e abrindo novas fontes de dados.

Isso se torna particularmente evidente no setor da saúde. De fato, mais e mais pesquisadores, empresas e médicos usam informações que surgiram a partir do processamento de enormes quantidades de dados. Além disso, a coleção individual de dados relevantes para a saúde está aumentando, por exemplo, por meio do uso dos aplicativos de telefones celulares e de sensores usados no corpo. Quando esses dados diversos são vinculados e analisados, fornecem *insights* profundos sobre o estado atual de saúde, a personalidade e o estilo de vida e, em alguns casos, até permitem previsões, consolidando-se como uma espécie de triunfo da saúde preditiva.

Uma vez que os dados são coletados, redes de dados e de sistemas de *software* em rede, por vezes, em tempo real, são acionadas para a sua troca e a sua conexão, geralmente, em projeções transnacionais. A coleta, o armazenamento e o processamento eficientes de dados exigem ambientes de computação de alto desempenho, implantados principalmente em *data centers* com muitos servidores em rede e, na maioria das vezes, oferecido por provedores comerciais.

O movimento de máquinas locais para a virtualidade desses *data centers* costuma ser denominado computação em nuvem.

A objetividade, a confiabilidade, a reprodutibilidade e a validade dos dados ou dos métodos de análise utilizados são, em rigor, essenciais para a avaliação de declarações, de conclusões ou de previsões baseadas em dados. Com a quantidade exponencial de dados, o significado da análise aumenta para os fatores individuais estudados e as possibilidades de levar em conta fatores adicionais, mesmo os fracos, e as suas interações. No entanto, a coleta e a verificação independentes das análises de dados permanecem de importância central. A partir de correlações estatísticas, não é fácil concluir sobre as causas (efeitos causais) ou mecanismos de ação. Estes últimos devem ser esclarecidos por meio de argumentos e de suposições adicionais ou pela obtenção de dados adicionais, por exemplo, de estudos de longo prazo ou experimentais.

O aprendizado de máquina é particularmente importante para o uso e para o desenvolvimento de aplicativos de *big data*. Aqui, os modelos estatísticos "aprendem" regras de cálculo com base em conjuntos de dados de treinamento, com os quais os dados podem ser classificados ou categorizados de certa maneira. Uma questão central é em que medida tais técnicas levam ao desenvolvimento de "agentes de máquinas" capazes de tomar decisões e autorizá-las, pois, por vezes, estão igualmente envolvidos, *e.g.*, na concepção das práticas terapêuticas ou mesmo nos processos decisórios das políticas de saúde.

Conveniente mencionar que os sistemas de autoaprendizagem podem usar dados de um grupo consideravelmente grande de pessoas para identificar fatores relevantes, como comportamentos relacionados à saúde, e localizar indivíduos e conteúdos neste sistema de coordenadas. Tais abordagens permitem recomendações e interações rápidas e individualizadas com "assistentes de máquina". Todavia, eles são necessariamente acompanhados pela divulgação de informações pessoais e, se necessário, induzem ao engano e à manipulação de decisões pessoais na medida em que podem adicionar vieses cognitivos nos processos deliberativos.

Os métodos baseados em dados grandes detectam diferenças sempre mais finas entre os indivíduos ao analisar relacionamentos, tornando possível ter maior consideração de características e de circunstâncias pessoais – por exemplo, em diagnósticos, prognósticos e terapias, ou em questões de seguro, em termos de classificação em grupos, pacientes com seguros privados, com cobertura assistencial etc. Não custa advertir que, ao formar tais grupos, melhor dizendo, estratificações por meio do emprego de algoritmos complexos de *big data*, importa considerar e minimizar as possíveis fontes de erro.

Os dados relacionados à saúde associados a uma pessoa específica são particularmente sensíveis na medida em que propiciam uma espécie de radiografia de uma área muito íntima.[1] Os dados pessoais, deve-se enfatizar, podem ser coletados e unidos a um número cada vez maior de fontes, sendo que, no decurso do processo de avaliação, tais dados podem adquirir igualmente uma relevância para a saúde que não dá inicialmente uma aparência correspondente, por exemplo, dados de transação ou dados de compra.

Os dados relevantes para a saúde são produzidos em vários contextos, por vezes sobrepostos, da prática médica e da investigação relacionada com a saúde, com agências governamentais e seguradoras, bem como a geração de dados ativa, intencional ou não, por cidadãos-pacientes-usuários. As tecnologias de *big data* possibilitam a descontextualização e a reorganização abrangentes dos dados coletados, analisados e revinculados ou reintroduzidos para diferentes finalidades.[2] Isso leva a uma delimitação da área relevante para a saúde, facilitando, por sua vez, a desanonimização dos dados ou a reidentificação de pessoas individuais.

Como todos os dados coletados de alguma forma podem ser interpretados em relação à saúde pessoal, é possível, em princípio, avaliar todos esses dados como relevantes para a saúde, engendrando um conjunto que tende a permanecer em ritmo de crescimento vertiginoso. Assim, consequentemente, muitas vezes já não é possível determinar se os dados são sensíveis ou relevantes para a saúde no momento da sua coleta, dependendo sobretudo do contexto em que são utilizados. E, por oportuno, deve-se destacar que esse contexto pode mudar ao longo do tempo, sobretudo em razão da volatilidade. Evidencia-se, de outra banda, que vários atores com diferentes funções e, ao menos, eivados de interesses parcialmente conflitantes em uma ampla gama de contextos estão envolvidos na coleta, no processamento, no tratamento e no uso de grandes quantidades de dados.

Assim, ante a complexidade e a relevância do tema, intenta-se empreender pesquisa teórica e, tendo em vista os possíveis resultados, exploratória, no que tange ao objetivo de analisar as especificidades dos dados da área da saúde e a repercussão do seu uso em função das formas contemporâneas de coleta, de armazenamento, de tratamento, de manipulação, sobretudo em um contexto de *big data*.

---

1 CATH, Corine *et al*. *Artificial Intelligence*: ethical, legal and technical opportunities and challenges. Phisophical Transactions of the Royal Society: Mathematical, Physical and Engineering Sciences. Londres: Royal Society, 2018. v. 376. Disponível em: https://doi.org/10.1098/rsta.2018.0080. Acesso em: 28 out. 2019.

2 SUSTEIN, Cass R. *Algorithm, Correting Biases*. Cambridge: Harvard, 2018. Preliminary Draft. p. 39.

Pretende-se, consequentemente, em razão da atual tendência à implantação de uma espécie de tecnocontrole por meio da algoritimização da sociedade atual, analisar em face dos riscos inerentes ao emprego da tecnologia de comunicação e de informação (TIC) e da fragilidade dos dispositivos que perfazem o sistema protetivo brasileiro, investigar alguns dos pontos lacunosos e controversos da Lei Geral de Proteção de Dados (LGPD) aplicáveis à área da saúde com o propósito de apresentar pautas e recomendações.

Cinco áreas selecionadas de aplicação de *big data*, em suma, serão examinadas no que toca às respectivas oportunidades e aos riscos: em primeiro lugar, a investigação biomédica, em segundo lugar, os cuidados de saúde, em terceiro lugar, a utilização de dados por seguradoras e por empregadores, em quarto lugar, a exploração comercial de dados relevantes para a saúde por parte de empresas de TI e internet globalmente ativas e, em quinto lugar, a sua coleta pelos próprios afetados.

Para fins procedimentais, interessa ainda apontar a investigação de natureza bibliográfica que deve ser empreendida, notadamente no âmbito do sistema normativo brasileiro e, mais apropriadamente, mediante a análise da doutrina, da jurisprudência e da legislação aplicável ao tema da proteção de dados para, em caráter de precariedade e de transitoriedade, ínsito à área que tangencia a tecnologia, apontar algumas recomendações e, em certa medida, algumas pautas de solução para o problema da vulnerabilização sem precedentes da pessoa humana na sociedade informacional, em especial no que se refere aos processos de saúde e de adoecimento em face do atual contexto de *big data*.

## 2 Dados e saúde

A solidariedade é, em rigor, baseada em expectativas de reciprocidade. A vontade de demonstrar solidariedade pode, por outro lado, diminuir se surgirem dúvidas quanto à capacidade de resgate de tais expectativas, por exemplo, se, a longo prazo, se suscite a impressão de que a necessidade de assistência e apoio dos outros é causada pela sua automutilância negligente ou uma falta de autoiniciativa e, assim, supera a estrutura da solidariedade.

A avaliação de dados abrangentes, diversificados e relevantes para a saúde possibilitados por *big data* permite a criação de perfis de risco mais precisos. Isto está relacionado à preocupação de que a assunção de uma vulnerabilidade comum aos riscos de doenças que não podem ser antecipadas seja a base da solidariedade no seguro de base estatutário, e no projeto de contrato em seguro de saúde privado poderia ser posta em causa. Dessa forma, os grupos de baixo

risco poderiam deixar cada vez mais a comunidade solidária, o que resultaria em consideráveis encargos suplementares para esta última.

Toma-se, nessa altura, por evidente atualidade, complexidade e alcance do tema, a tarefa de analisar alguns dos modos mais significativos em que se pode apontar riscos e, em contrapartida, alguns benefícios na utilização de dados pessoais em contexto de *big data*.

## 2.1 Na pesquisa biomédica

Na pesquisa biomédica, urge salientar, as aplicações mais intensivas em dados incluem técnicas modernas de imagem e de biologia molecular, como as utilizadas na neurociência e as chamadas disciplinas "ômicas" (genômica, proteômica, metabolômica e outras).[3] Os principais intervenientes no domínio científico são as instituições de pesquisa e o seu pessoal, mas igualmente os indivíduos e os pacientes, acometidos de enfermidades ou não. A pesquisa geralmente usa grandes quantidades de dados de acordo com padrões elevados e, em certa medida, facilmente controláveis de coleta de dados, de uso e de segurança. Não se deve olvidar que as organizações dedicadas à ciência aproveitam as novas possibilidades técnicas e as infraestruturas de *big data* e de rede para fins de intercâmbio de dados, de análise e de avaliação conjunta.

Em muitas enfermidades, as relações de determinação e de modulação da doença são muito complexas, em especial quando se toma por base a contemporânea interface saúde/doença.[4] *Big data*, de fato, abre oportunidades para integrar várias informações em análises abrangentes e de fontes-cruzadas. Além da considerável quantidade de dados incluídos, a qualidade de seu processamento interpretativo é, de modo inconteste, crucial para esse desempenho de integração.

A propósito, a fusão de dados coletados por diversas instituições em contextos frequentemente diferentes coloca desafios específicos para o uso de *big data* na pesquisa médica. Em muitos casos, faltam protocolos uniformes para a coleta, para a anotação e para a garantia de qualidade dos dados, bem como

[3] Cf. LEDERBERG, Joshua. 'Ome Sweet 'Omics – A genealogical treasury of words. *The Scientist – Exploring Life, Inspiring and Innovation*, abr. 2001. Disponível em: https://www.the-scientist.com/commentary/ome-sweet-omics—a-genealogical-treasury-of-words-54889. Acesso em: 11 ago. 2019. Ainda, PLAZA, N. C.; GARCÍA-GALBIS, M. R. Impact of the "Omics Sciences" in Medicine: New Era for Integrative Medicine. *J Clin Microbiol. Biochem Technol*, v. 3, n. 1, p. 9-13, 2017.

[4] RODRIGUES, José Carlos. *Higiene e ilusão*: o lixo como invento social. Rio de janeiro: NAU, 1995. p. 91; ALLAMEL-RAFFIN, Catherine; LEPLÈGE, Alain; MARTIRE JÚNIOR, Lybio. *História da Medicina*. Tradução de Aquiles Von Zuben. Aparecida/SP: Ideias &Letras, 2011. p. 76.

são escassas as regras de bom funcionamento para o intercâmbio de dados. Isso se deve, por um lado, às preocupações de proteção de dados e à falta de modelos de contato e de consentimento adequados para os pacientes e para os sujeitos no que toca ao uso secundário de dados. Por outro lado, há incertezas e ideias díspares quanto ao direito de dispor dos dados gerados, notadamente quanto à legitimidade e à legalidade do agente e quanto à medida que podem ser dispostos. Além dos novos modelos de consentimento, as soluções oferecem, acima de tudo, medidas técnicas para um intercâmbio de dados padronizado, o que garante a qualidade dos dados e os elevados padrões de proteção, mas igualmente medidas de apoio regulatórias e de suporte, bem como iniciativas de intercâmbio de dados abertos.

## 2.2 Nos cuidados de saúde

No que afeta os cuidados de saúde, o uso de *big data* inaugura oportunidades para tratamentos personalizados, incrementando a eficácia, a acurácia e a eficiência. O uso de grandes quantidades de dados possibilita uma melhor estratificação dos pacientes, de modo que, por exemplo, os efeitos colaterais são reduzidos e as tentativas terapêuticas fúteis podem ser evitadas. A coleta e a análise de dados relacionados à saúde abrem definitivamente novos potenciais no que se refere à medicina preditiva.

Ocorre que, de todo modo, o setor da saúde caracteriza-se por um grande número de atores com interesses por vezes divergentes em uma composição de um mosaico complexo. Inclui provedores, pagadores e beneficiários de serviços de saúde, mas inclui, igualmente, autoridades públicas, grupos de interesse e pesquisadores com vínculo direto com a prática clínica. De qualquer maneira, cumpre enaltecer que as oportunidades de abordagens intensivas em dados, a despeito de ganhos, devem ser combatidas quanto se trata de acarretarem riscos desproporcionais para os pacientes, como a perda de controle sobre seus próprios dados, o acesso cada vez maior a informações íntimas por prestadores de serviços ("paciente de vidro") e o uso indevido e facilitado de seus dados.[5]

Além disso, deve-se apontar que uma ênfase no exagerado tecnicismo e, portanto, no adensamento do uso de abordagens baseadas em *big data* poderá resultar em danos ainda de natureza intangível, em particular quando se coloca

[5] A transparência do vidro, assim parecem os pacientes relativamente à exposição de seus dados. Cf. CAREY, Corinne A.; STERN, Gillian. Protecting patient privacy: strategies for regulating electronic health records exchange. *New York Civil Liberties Union (NYCLU)*, Nova York, mar. 2012. Disponível em: https://bit.ly/305PT0F. Acesso em: 3 jul. 2019.

em xeque a atenção pessoal junto ao paciente. Dessa forma, impende lembrar que o seu uso indevido pode provocar erros de diagnóstico e de tratamento, afetando o *ethos*[6] do cuidado e da responsabilidade, elementar à área da saúde, particularmente quando se trata da afetação à individualidade e à singularidade da pessoa humana.

## 2.3 Seguradoras e empregadores

No que concerne ao binômio seguradoras/empregadores, o uso de *big data* abre amplas e novas opções de acesso e de avaliação, atualmente ainda infensas às disposições legais aplicáveis. Cada vez mais, grandes quantidades de dados e de opções de conexão permitem a criação de perfis mais refinados de indivíduos ou de grupos de pessoas. Assim, ao passo que se pode, em um primeiro momento, considerar uma atuação personalizada e, portanto, favorável à adequada capacitação e à colocação do trabalhador no mercado de trabalho, suscita, em outro giro, preocupações consistentes quanto ao seu uso discriminatório, nitidamente factíveis em cenários neoliberais, de *big data*, para visar a candidatos ou requerentes de baixo risco ou oferecer-lhes melhores termos.

Mesmo nos contratos já existentes, os empregadores e as companhias de seguro da saúde têm evidentemente um nítido interesse na saúde de seus contratantes. Monitorar o comportamento do paciente ou do empregado permite, em síntese, promover políticas de incentivos para os saudáveis ou de sanções para aqueles que insistem em estilos de vida considerados insalubres e, assim, podem emular afetações gravíssimas às esferas de liberdade inerentes ao desenvolvimento da pessoa humana.

Inegável, em outra perspectivação, que na medida em que esses programas conseguirem reduzir as concessões de licença de doença, isso abrirá novas oportunidades para todas as partes envolvidas. No entanto, como outrora salientado, os riscos[7] não devem ser ignorados. Os ajustamentos ou as advertências para o enquadramento de comportamentos nocivos, a título de exemplo, podem não ser, em um primeiro momento, do interesse dos respetivos fornecedores de dados e, por outro lado, consistem, de qualquer modo, em uma opção moral que efetivamente pode gerar distorções e, em última análise, violações aos direitos humanos e fundamentais.

[6] CORTINA, Adela; MARTÍNEZ, Emilio. Ética. Tradução de Silvana Cobucci Leite. São Paulo: Loyola, 2009. p. 35-36.

[7] MENDES, Laura Schertel. *Privacidade, proteção de dados e defesa do consumidor*: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014. p. 27-55.

No âmbito do seguro de saúde estatutário, as taxas de seguro baseadas em dados comportamentais prejudicam a ideia de solidariedade, que requer proteção contra a vulnerabilidade relacionada com a doença, em grande parte sem qualquer visão dos riscos comportamentais individuais.[8] O seguro de saúde privado, por outro lado, opera com prêmios equivalentes ao risco. Aqui, também, uma redistribuição de riscos em detrimento do segurado pode surgir se os prêmios forem no futuro regularmente recolhidos e avaliados por grandes dados; mesmo após o seguro ter sido retirado, seria ajustado. Isto prejudicaria completamente o princípio do seguro, segundo o qual os riscos são partilhados por um grupo maior e as tarifas não podem ser ajustadas individualmente. Poderia haver um grupo pautal cada vez menor, em que as reivindicações conduzem então a algumas contribuições mais elevadas rapidamente.[9] Além disso, os segurados privados que não estão dispostos ou, incapazes de participar de um modelo de seguro comportamental, poderiam ser privados de benefícios financeiros, o que deve acarretar desvantagens em longo prazo. Independentemente de se comportarem ou não em uma forma de promoção da saúde, seriam penalizados por não deixarem os seus dados em seguros e, em decorrência, seriam prejudicados em razão do seu direito à autodeterminação informativa.

Em princípio, torna-se imperioso relembrar, a liberdade de moldar a vida e o autodesenvolvimento tem precedência sobre uma obrigação estrita e permanente de evitar todos os riscos para a saúde. Embora isto não se aplique indefinidamente, a coleta orientada e contínua de dados sobre os estilos de vida individuais e a utilização de grandes perfis de risco alimentados por dados que abranjam todas as áreas da vida dificilmente poderiam ser consideradas uma expectativa razoável de corresponsabilidade pela própria saúde.

Se/e como às instituições de seguro de saúde estatutárias é permitido levar em consideração a responsabilidade da saúde e influenciar o comportamento de saúde de seus segurados é discutível.[10] Os sistemas de incentivo baseados em

---

[8] Cf. BUSSE, Reinhard; BLÜMEL, Miriam; KNIEPS, Franz; BÄRNIGHAUSEN, Till. Statutory health insurance in Germany: a health system shaped by 135 years of solidarity, self-governance, and competition. *Germany and health*, v. 390, issue 10097, p. 882-897, 26 ago. 2017.

[9] Cf. TRETTEL, Daniela Batalha; KOZAN, Juliana Ferreira; SCHEFFER, Mario César. Judicialização em planos de saúde coletivos: os efeitos da opção regulatória da Agência Nacional de Saúde Suplementar nos conflitos entre consumidores e operadoras. *Revista de Direito Sanitário*, v. 19, n. 1, p. 166-187, 2018. Disponível em: http://dx.doi.org/10.11606/issn.2316-9044.v19i1p166-187. Acesso em: 23 jan. 2019. Ainda, MOSSIALOS, Elias; WENZL, Martin; OSBORN, Robin; SARNAK, Dana (Ed.). 2015 International Profiles of Health Care Systems. *The Commonwealth Fund*, 2016. Disponível em: https://bit.ly/2P5nqHg. Acesso em: 13 ago. 2019.

[10] Cf. No Brasil, GIOVANELLA, Ligia *et al*. Sistema universal de saúde e cobertura universal: desvendando pressupostos e estratégias. *Ciênc. Saúde Coletiva*, Rio de Janeiro, v. 23, n. 6, jun. 2018. Disponível em: http://dx.doi.org/10.1590/1413-81232018236.05562018. Acesso em: 15 jun. 2018. Ainda, NORONHA, José Carvalho de; NORONHA, Gustavo Souto de; PEREIRA, Telma Ruth; COSTA, Ana Maria.

dados podem ter uma eficácia muito intensiva e de monitorização invasiva. No entanto, a divulgação diferenciada de fatores de risco por meio de análises de *big data* que, integrando dados de todas as áreas da vida, também pode mostrar no futuro que a maioria da população tem perfis de risco mistos que protegem e incluem fatores favoráveis, bem como fatores físicos, mentais, comportamentais e outros tipos negativos.

Em várias áreas da medicina, o uso de tecnologias de *big data* já levou ao desenvolvimento de novas práticas de apoio pró-social, como a formação de "grupos menores de pacientes", particularmente os de "riscos de doenças raras" ou da modalidade "compartilhe suas experiências" e "coloque seus dados e amostras biológicas (*biosamples*) em depósitos comunitários" para disponibilizá-los para pesquisa em "suas enfermidades".[11] Outros ganhos de solidariedade podem ser observados em fóruns *on-line*, em que os pacientes os alimentam de suas experiências e dados de doença da clínica e autoavaliação – trocá-los, discuti-los juntos tem sido útil para a gestão de doenças individuais.[12] Com o desenvolvimento crescente de ferramentas em rede e em linha para a autoajuda do paciente, tais práticas tendem a aumentar.

De todo modo, a responsabilidade como categoria moral pode ser diferenciada de acordo com o tipo de ação e de tomada de decisão, mas também de acordo com a concepção das estruturas institucionais. Os diferentes tipos de responsabilidade envolvidos são muitas vezes em uma relação matéria-de-fato: espera-se exatamente assumir a responsabilidade para o futuro, que se detém a conta em um caso real de danos.

A complexa interação entre indivíduos, instituições e tecnologia no uso do *big data* é de particular importância no campo da saúde. Logo, uma difusão opaca da responsabilidade, que ameaça a dimensão em que muitos atores e processos técnicos trabalham junto, deve ser evitada. Para que os provedores de dados individuais possam assumir a responsabilidade por seus dados mesmo em termos de *big data*, certas condições de estrutura são necessárias, podendo ser utilizadas de forma simples, tanto técnica quanto organizacionalmente. No setor de

Notas sobre o futuro do SUS: breve exame de caminhos e descaminhos trilhados em um horizonte de incertezas e desalentos. *Ciênc. Saúde Coletiva*, Rio de Janeiro, v. 23, n. 6, jun. 2018. Disponível em: http://dx.doi.org/10.1590/1413-81232018236.05732018. Acesso em: 21 set. 2019.

[11] Cf. em outro sentido, WANG, Y. *et al.* Big data analytics: Understanding its capabilities and potential benefits for healthcare organizations. *Technol. Forecast. Soc. Change*, 2016. Disponível em: http://dx.doi.org/10.1016/j.techfore.2015.12.019. Acesso em: 11 jul. 2019.

[12] Cf. WANG, Y.; KUNG, L.; WANG, Y. C. W.; CEGIELSKI, C. G. Integrated big data analytics-enabled transformation model: Application to health care. *Information and Management*, 2017. Disponível em: http://doi.org/10.1016/j.im.2017.04.001. Acesso em: 23 jan. 2019.

saúde, portanto sensível, também há maiores requisitos de *due diligence*,[13] para pesquisadores ou médicos.

Uma das maneiras pelas quais as empresas podem ser responsáveis por processos de *big data* é criar condições para monitorar e revogar os consentimentos e gerenciar a demanda de dados. Isso pode ser usado para excluir dados suficientemente agregados, dados derivados ou modelos que tenham sido mostrados para não inferência do indivíduo. O uso de tais abordagens para possibilitar contextualizações e recontextualizações específicas de dados, mantendo elevados padrões de anonimização e criando confiança institucional, é susceptível de se tornar uma das tarefas decisivas do futuro.

Outra maneira de assumir a responsabilidade pelos direitos do indivíduo enquanto ainda salvaguarda interesses comerciais legítimos seria usar sistemas de *proxy* nas interfaces programáticas em redes de dados. Essas interfaces podem usar as preferências dos controladores de dados para tratamento de dados como "agentes de dados". Isso substituiria o gerenciamento de dados individuais por meio de uma administração programática, o que daria aos indivíduos uma maneira tecnicamente baixa e confiável de assumir a responsabilidade de escolher em curto, médio e longo prazo suas próprias estratégias de manipulação de dados.

As empresas podem igualmente assumir, pautando-se na transparência, a responsabilidade, tornando seus procedimentos mais verificáveis, como no que concerne aos algoritmos utilizados, à exclusão de inocorrências sistemáticas, à conformidade com as regras de retenção de dados, de anonimização e/ou de apagamento de dados e o registro completo e à prova de adulteração da origem, do processamento, da utilização e da troca de dados. Assim, além da regulação estatal, existem outras formas de garantir ou de promover a assunção de responsabilidade por parte dos atores institucionais. As certificações, os selos de qualidade ou os compromissos fornecidos e revisados por interesses ou por associações profissionais podem, *e.g.*, aumentar a confiança nas respectivas organizações e processos.

Outra questão diz respeito às possíveis intervenções das organizações na comunicação pessoal entre os utilizadores, por exemplo, a forma de aconselhamento saudável ou de ofertas de ajuda. A rejeição de interferência óbvia na esfera privada ou íntima fala contra isso. No entanto, se a confiabilidade funcional de tais algoritmos for bem documentada cientificamente, seria preciso também ter em conta uma perspectiva ética de que o seu uso poderia, se necessário, prevenir

[13] Cf. RICE, Kelley H. *Physician practice mergers*: the importance of due diligence and mutual trust for all involved. American College of Medical Practice Executives. Disponível em: https://bit.ly/2YMO7Vy. Acesso em: 1º dez. 2018.

o sofrimento grave ou mesmo a morte, por exemplo, no caso de ofertas de ajuda para pessoas em risco de suicídio em redes sociais. O Estado, de qualquer sorte, pode assumir a responsabilidade nacionalmente, podendo atuar igualmente como ator internacional. Todavia, tendo em vista o referido problema de bom emprego jurídico, deve-se aplicar um princípio regulamentar da subsidiariedade que dê preferência aos autocompromissos e às certificações sobre os regulamentos jurídicos pormenorizados, desde que sejam de forma eficaz.

Tendo em conta os três níveis de possível atribuição de responsabilidade na área de aplicações de *big data* relacionadas com a saúde (indivíduos, organizações, governo), os indivíduos permanecem obrigados a assumir a responsabilidade pelo uso de seus dados. Entretanto, as organizações de coleta de dados, de transformação e de passagem são responsáveis pela garantia de condições-quadro para o *design* responsável pela liberdade informativa dos prestadores de dados. Às organizações menos dispostas ou capazes de fornecer meios técnicos para facilitar o controle do indivíduo sobre seus dados, a partir de uma perspectiva ética responsável, insta que o Estado garanta que os dados sejam monitorizados e, se for caso, a regulação e a sanção. O objetivo de dar ao indivíduo a oportunidade de lidar com seus dados de maneira soberana só pode ser alcançado, então, se a respectiva responsabilidade for assumida por todos.

## 2.4 Corporações, empresas de TI e internet

Corporações, empresas de TI e a internet atuam, em regra, como prestadores de serviços. Nesse sentido, com base no seu acesso às enormes quantidades de dados e à infraestrutura de dados adequada, fornecem motores de busca, plataformas de informação interativa e ofertas, tais como as que propiciam as compras *on-line*, bem como uma ampla gama de dispositivos multifuncionais. Para as empresas voltadas para as áreas da saúde, é, consequentemente, possível a associação de dados relevantes para a saúde, evidenciando-se, em certa medida, um grande potencial de abuso.

As empresas, em regra, oferecem *software*, *hardware*, desenvolvimento de tecnologia e serviços *on-line* para aplicativos de *big data*, fornecendo inclusive plataformas orientadas para dados com sistemas dedicados, algoritmos, dispositivos, infraestrutura para a coleta, a avaliação, o gerenciamento, o armazenamento e a análise de dados para acelerar e para aprimorar processos e, portanto, garantir o uso eficiente de cada e de todas as informações pertinentes. De outra banda, torna-se inegável que o incremento das empresas digitais no setor da saúde

ofereça oportunidades de pesquisa de relevo no campo da medicina, em especial no que afeta à dimensão preditiva. Consistem, dessa forma, em melhores possibilidades de análise e de conversão em ativos financeiros. Em razão da falta de neutralidade da ciência e da atual formação de oligopólios mundiais na área da tecnologia, inclusive no que se refere à saúde, trata-se de uma problemática que requer urgência em seu trato.

Por outro lado, qualquer espécie de restrição em absoluto ao acesso aos dados da área da saúde, em especial os afeitos à medicina e à pesquisa, torna-se, por vezes, obstáculo ao progresso em medicamentos e à inovação terapêutica, devendo-se na medida do possível, portanto, condicionar o uso ao consentimento e, assim, à autodeterminação informativa e existencial do usuário/paciente ou, em casos específicos em que seja constatada a total e irrevogável incapacidade ou a capacidade relativa em termos civis, da sua família ou do responsável, sempre pautando-se no melhor interesse do titular dos dados.

## 2.5 Dispositivos portáteis e sensores para uso privado

Muitos dispositivos portáteis com sensores e com aplicativos estão atualmente disponíveis no mercado para a coleta de dados relevantes para a saúde, prometendo facilitar o acesso da pessoa em causa às suas próprias informações e, dessa forma, obter por meio do mapeamento genético o autoconhecimento e, portanto, promover o bem-estar pessoal. Oportunizam igualmente a investigação na medida em que forem utilizadas como uma importante extensão quantitativa e qualitativa da base de dados.

Conveniente assinalar que a autorregulação excessiva com a ajuda de tais ofertas pode contribuir para a medicalização dos processos de vida "natural", gerando as multidões de pessoas viciadas em medicalização, isto é, os enfermos saudáveis. Além disso, é duvidoso se a automedida é uma expressão da soberania pessoal ou se consiste em uma forma da determinação exógena autoinduzida. Igualmente crítica é a possibilidade de que a discriminação se torne inevitável, sobretudo contra pessoas incapazes ou que não queiram participar. A orientação prévia de muitas ofertas para os interesses econômicos dos fabricantes, o escamoteamento acerca do uso, do armazenamento, do tratamento e da manipulação dos dados obtidos, bem como o lado oculto na facilidade de uso, na transparência e na proteção de dados provocam críticas igualmente sustentáveis.

Em resumo, os pontos fortes, as fraquezas, as oportunidades e os riscos de utilização de *big data* em áreas relacionadas à saúde podem ser identificados em contextos de aplicativos: os pontos fortes incluem a crescente base de dados, o

desenvolvimento associado de instrumentos digitais e o alto grau de *networking* entre os atores. Em contrapartida, incluem as flutuações na qualidade dos dados, a falta de transparência dos fluxos de dados, a perda de controle e a maior coordenação, requisitos regulamentares e de qualificação.

Incontestavelmente, as oportunidades oferecidas pela manipulação dos grandes dados são, acima de tudo, melhores possibilidades de estratificação no diagnóstico, na terapia e, de modo particular, na prevenção e no aumento associado à acurácia na eficiência e na eficácia no que concerne ao comportamento de promoção e de proteção da saúde. Não se deve descurar dos riscos em termos de dessolidarização, de difusão de responsabilidade, de monopolização, de abuso de dados e, como outrora salientado, de automutilação informativa. Entende-se que a avaliação concreta das aplicações de *big data* com relação à saúde depende, em grande parte, dos intervenientes envolvidos com os seus respectivos interesses e de posse de suas próprias avaliações de risco, bem como do respectivo contexto de aplicação.

## 3 Requisitos legais para a regulamentação em contexto de *big data*

*Big data* representa um desafio significativo para o sistema jurídico. Particularmente, consiste em um desafio para a devida adequação aos requisitos constitucionais, à Lei Geral de Proteção de Dados (LGPD),[14] às disposições específicas de proteção de dados do setor da saúde e do direito dos dispositivos médicos,[15] bem como no que toca aos mecanismos de incentivo subjacentes e aos mecanismos de controle autorregulatórios e híbridos.[16] De qualquer forma, impende ressaltar que os elementos essenciais da Lei de Proteção de Dados são constituídos por direitos fundamentais e, em razão dos aspectos transnacionais do contexto de sua aplicação, por direitos humanos.

Assim, os dispositivos constitucionais estruturantes são o direito à privacidade e o direito à informação, em especial, na medida em que suportam o "direito de autodeterminação informativa", revelado em pronunciamento jurisdicional pelo

[14] BRASIL. *Lei nº 13.853, de 8.7.2019*. Disponível em: https://bit.ly/2YLG07A. Acesso em: 12 ago. 2019.

[15] Cf. CONSELHO NACIONAL DE SAÚDE (MS). *Legislação*. Disponível em: https://bit.ly/2TtexFR. Acesso em: 12 ago. 2019. Cf. ainda, AGÊNCIA NACIONAL DE SAÚDE SUPLEMENTAR. *Legislação*. Disponível em: https://bit.ly/2YJbbV8. Acesso em: 13 ago. 2019.

[16] FRAZÃO, Ana. Fundamentos da proteção dos dados pessoais – Noções introdutórias para a compreensão da importância da Lei Geral de Proteção de Dados. *In*: FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato (Coord.). *Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro*. 2. tir. São Paulo: Thomson Reuters Brasil, 2019. p. 33.

Tribunal Constitucional Federal da Alemanha, no julgamento censitário como uma expressão específica do direito geral de personalidade.[17] Por oportuno, deve-se asseverar que esse atributo se estende para a proteção da privacidade e da liberdade de conduta ao abrigo da Constituição Federal de 1988. Estas liberdades de desenvolvimento, destarte, podem entrar em conflito com algumas situações que afetam o interesse público, como a promoção do progresso científico ou a garantia de cuidados de saúde.

Não custa afirmar, pois, que a Lei de Proteção de Dados (LGPD) baseia-se nos requisitos constitucionais e que sua entrada em vigor vai impulsionar expressivas mudanças na sociedade brasileira. Contudo, não se deve negligenciar quanto à afirmação da relevância e do pioneirismo do Regulamento Geral sobre a Proteção de Dados (RGPD, pelo acrônimo em português, GDPR, sobretudo em sua incidência ultramarina).[18] De qualquer forma, tudo leva ao exame de um fenômeno *big data* insuficientemente ajustado, pois não se tem em conta os progressos claros que estes novos requisitos significam, por exemplo, no que se refere ao estabelecimento de normas transfronteiriças cuja efetividade seja factível e à maior integração do conceito de privacidade por *concepção*.[19]

A atual Lei de Proteção de Dados, em seu âmbito de aplicabilidade, está ligada à relação pessoal e identitária transcrita em dados, colocando especial ênfase nas finalidades específicas associadas. Para os grandes dados, destaque-se,

[17] Cf. BVerfG, Urteil v. 15. Dezember 1983, Az. 1 BvR 209, 269, 362, 420, 440, 484/83.

[18] Cf. texto em português em: https://bit.ly/2uCGPmb (*link* permanente).

[19] *Privacy by design*. No Brasil, alguns denominam "privacidade desde o projeto", preferimos a expressão "privacidade por concepção", isto é, desde a concepção. Na verdade, o conceito foi desenvolvido pela Dra. Ann Cavoukian, então Comissária de Informações e Privacidade de Ontário, Canadá, em meados dos anos 90, quando documentou os 7 Princípios Fundamentais, ou em inglês, "7 Foundational Principles – FOU". O termo *privacy by design* começou a ser reconhecido por profissionais de proteção de dados e órgãos reguladores na América do Norte e na Europa. Em outubro de 2010, foi adotado por unanimidade como um padrão de privacidade internacional na Conferência Internacional de Comissários de Proteção e Privacidade de Dados em Jerusalém. Ele está incluído na Lei de Declaração de Direitos de Privacidade Comercial dos EUA. Ele foi incluído no RGPD da UE e aceito pelos comissários de proteção de dados em todo o mundo como um conceito que garantirá a proteção adequada da privacidade em um mundo de sistemas de TI em constante evolução com capacidade de coletar e processar grande quantidade de dados. Cf. OKOYE, John Nwachukwu. *Privacy by design*. Norwegian University of Science and Technology. Department of Information Security and Communication Technology. July 2017. Disponível em: https://bit.ly/33utFaA. Acesso em: 5 set. 2019. No RGPD encontramos a atribuição no "Considerando 78" e no art. 25 – Proteção de dados desde a concepção e por defeito (*Data protection by design and by default*). O RGPD com esses dispositivos pretende que as empresas ou organizações sejam incentivadas a aplicar medidas técnicas e organizativas, nas fases iniciais da concepção das operações de tratamento, de modo a garantir os princípios da privacidade e proteção de dados desde o início ("proteção de dados desde a concepção"). Por "defeito", as empresas ou organizações devem garantir que os dados pessoais sejam tratados com a mais elevada proteção da privacidade (por exemplo, apenas os dados necessários devem ser tratados, período de conservação curto, acessibilidade limitada) para que, *por defeito, os dados pessoais não sejam disponibilizados a um número indefinido de pessoas* (proteção de dados por defeito). Na LGPD encontramos a atribuição no art. 46 e no seu §2º.

é crucial compreender que as aplicações futuras não sejam previsíveis quando os dados são coletados e que a relação pessoal ou a relação com a saúde só podem ser produzidas retrospectivamente. Os dados armazenados para outros fins são, por sua vez, frequentemente avaliados para novos propósitos ou, de qualquer forma, os dados são coletados para fins não especificados.

Outrossim, o princípio da economia ou da minimização de dados está em contradição com o uso de grandes dados. Isso facilmente levaria a crer em uma grande exclusão das possibilidades de *big data* no que toca ao atual sistema protetivo. No entanto, não é demasiado apontar, que, em função da quantidade de dados armazenados, o risco para a efetividade do direito à autodeterminação informativa também aumenta de modo a emergir a necessidade de mecanismos de proteção alternativos. A exigência de consentimento, base e fruto dos avanços civilizatórios, conforme estabelecido de modo proeminente, mas não exclusivo, na Lei Geral de Proteção de Dados, segundo a qual a utilização de dados só é permitida se o titular dos dados demonstrar anuência livre, irrefutável e esclarecida e, em outro giro, exsurge em razão da importância e do alcance do uso intencional de dados, mas, também, pode assumir um papel meramente formal,[20] como se deduz da percepção da realidade contemporânea.

## 3.1 Incompatibilidades da regulamentação atual com *big data* – Pontos controversos do atual sistema protetivo aplicado aos dados pessoais da área da saúde

*Big data*, em suma, reforça significativamente um problema nuclear, ou seja, aponta que os usos futuros são muitas vezes desconhecidos ou alterados em relação àqueles do momento da coleta. Importa enfatizar, nesse sentido, que a atual Lei de Proteção de Dados oferece apenas algumas possibilidades, além do consentimento, para influenciar o destino dos dados. Entretanto, dispõe que qualquer outro uso além do que fora esclarecido requer novo consentimento, asseverando ainda que, uma vez que os dados tenham sido coletados com o consentimento, ele não pode mais ser acompanhado pela pessoa em causa. A dinâmica dos grandes dados, no entanto, não se encaixa neste feixe de regras, implicando a necessidade de buscar novas formas de proteção em que esta funcionalidade seja igualmente útil.

[20] BLASIMME, Alessandro; FADDA, Marta; SCHNEIDER. Manuel; VAYENA, Effy. Data sharing for precision medicine: policy lessons and future. *Health Affairs*, v. 37, n. 5, p. 702-709, 2018. Disponível em: https://www.healthaffairs.org/doi/pdf/10.1377/hlthaff.2017.1558. Acesso em: 27 jun. 2019.

*Big data*, resta mencionar, intensifica as possibilidades de reidentificação, ligando uma ampla gama de dados, aumentando assim a complexidade e, assim, as dúvidas sobre a eficácia da exigência de anonimização ou de pseudoanonimização. A questão acerca do modo e da medida do risco de uma reidentificação de dados anonimizados torna-se suficiente para a aceitação de uma referência pessoal dos dados, exacerbando o problema em torno do já controverso conceito de referência pessoal na Lei de Proteção de Dados.

As referências à informação, à retificação, à supressão e ao bloqueio servem como medida de transparência, mas, por vezes, não proporcionam uma proteção efetiva. Especialmente no contexto de *big data*, *e.g.*, o controlador de dados dificilmente conhecerá todos os potenciais reclamantes. Assim, a compreensibilidade do processo de processamento de dados, entendida pelos direitos de informação, incluindo a capacidade de obter informações apropriadas, é obstaculizada em razão de algoritmos complexos e de autoaprendizagem, evidenciando que, no que toca ao direito de retificação e ao apagamento a regulamentação, é vazia, pois a pessoa em causa não pode exercer estes direitos sem um acordo global.[21]

De fato, as soluções normativas assentadas na Lei de Proteção de Dados de saúde permanecem em grande parte relacionadas a uma perspectiva problemática do "período pré-*big data*". O efeito compensatório, à guisa de sugestão, poderia ser o disposto em uma lei dos dispositivos médicos, que regulasse a livre circulação de aparelhos médicos, assegurando simultaneamente a segurança, a adequação e o desempenho dos dispositivos para a proteção de pacientes, de usuários e de terceiros. Ao contrário dos medicamentos, importa evidenciar, os dispositivos médicos não necessitam de aprovação governamental, mas necessitam de certificação após a avaliação de risco específica do produto, sobretudo quanto à minimização de riscos e quanto à análise de risco-benefício em um procedimento adequado para o risco do produto no que concerne à avaliação da conformidade. O *software* pode ser classificado como um dispositivo médico se tiver um propósito médico. Assim, depende, em grande medida, das informações fornecidas pelo fabricante. Daí, a distinção entre aplicações médicas e simples estilo de vida ou aplicativos de *fitness* é muitas vezes difícil de se evidenciar na prática cotidiana.

De outro modo, as exigências da lei do seguro de saúde igualmente provam ser relevantes para *big data*. A classificação dos pedidos na remuneração dos seguros de saúde estatutários e privados, de modo exemplar, cria, como outrora salientado, incentivos financeiros para os desenvolvedores de tais ofertas e,

[21] MOURA, José; SERRÃO, Carlos. Security and privacy issues of big data. *In*: MOURA, José; SERRÃO, Carlos. *Handbook of Research on Trends and Future Directions in Big Data and Web Intelligence*. Pensilvânia: IGI Global, 2015 Disponível em: https://arxiv.org/ftp/arxiv/papers/1601/1601.06206.pdf. Acesso em: 27 set. 2019.

assim, cria um contador-modelo para os "números com dados". Contudo, é necessário fornecer provas de eficácia. A discriminação, por óbvio, também deve ser alvo de atenção, incluindo situações em que esses dados são tidos em conta na concessão das contribuições.[22]

## 3.2 Implicações tecnonormativas

Tendo em vista a recente reorganização abrangente da Lei de Proteção de Dados no âmbito europeu e ultramarino e pela LGPD em âmbito nacional, resta saber se/e como os novos padrões e os mecanismos provarão a si mesmos. Deve-se notar, oportunamente, que alguns dos princípios básicos do atual sistema jurídico de proteção de dados são difíceis de conciliar com o conceito de *big data*.

Essa tensão pode ser levada em conta no âmbito do escopo concedido pelo direito constitucional com regulamentações flexíveis, que igualmente incluem o uso de autoridades fiscais mais complexas, tanto públicas como privadas. Em particular, seria necessário examinar se a falta de concretude dos pedidos de grandes dados relevantes para a saúde seria compensada por salvaguardas técnico-organizacionais, bem como substantivas e processuais adicionais.

Assim, no decurso da continuação do desenvolvimento da legislação em matéria de proteção de dados, nomeadamente um modelo mais diferenciado de "modelos de consentimento", que conferissem espaço às especificidades de uma área reguladora e às preferências das pessoas em causa, ou poderia ser utilizado um inquérito mais aprofundado. E, ainda, a utilização de dados com base em normas de autorização legal. O direito privado, interessante reforçar, é também de grande importância para o desenvolvimento da proteção de dados, nomeadamente o direito do consumidor, o direito de responsabilidade, o direito da personalidade e as regras para a atribuição de dados e o poder de determinar a sua utilização ("propriedade" dos dados).[23]

---

[22] Cf. BISOTO JUNIOR, Geraldo; SILVA, Pedro Luís de Barros; DAIN, Sulamis (Org.). *Regulação do setor saúde nas Américas*: as relações entre o público e o privado numa abordagem sistêmica. Brasília: Organização Pan-Americana da Saúde, 2006 Cf. ainda, EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS. *Relatório da FRA* – Inequalities and multiple discrimination in access to and quality of healthcare. Disponível em: https://fra.europa.eu/sites/default/files/inequalities-discrimination-healthcare_en.pdf. Acesso em: 1º ago. 2019.

[23] Cf. ROBERTS, Jessica L. Progressive Genetic Ownership. University of Houston Law Center. *Notre Dame L. Rev.*, v. 93, n. 1105, 2018. Disponível em: https://bit.ly/31Jk7qB. Acesso em: 18 dez. 2018. Ainda, CONTRERAS, J. L. The false promise of (health) data ownership. *University of Utah College of Law Research Paper*, n. 304, 2018. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3328258. Acesso em: 4 jul. 2019.

Todas as abordagens para os grandes dados têm de enfrentar o problema da urgência em oferecer resposta a um fenômeno global por meio do emprego de legislação territorialmente limitada. Os respectivos direitos de proteção de dados variam muito do ponto de vista internacional, o que coloca desafios específicos tanto para as partes interessadas como para os reguladores. De fato, a despeito de uma vasta gama de esforços de harmonização, existem ainda muitos obstáculos práticos à ação transfronteiriça efetiva. Tendo em vista a dinâmica e a volatilidade específicas da área reguladora, os mecanismos fiscais não públicos e cooperativos também ganham importância, por exemplo, no que compete às certificações com selos de proteção de dados ou de segurança de dados ou regras de ação, e aos códigos para ciência e para os negócios.

## 4 Sobre os demais limites para o uso de grandes dados e a sua repercussão na área da saúde

Os *big data* afetam ambos os padrões de orientação ética, que abordam o papel, a função e a posição do indivíduo que disponibiliza os dados e a orientação social. Dada a plurivocidade terminológica, deve ser feita uma distinção entre a ação como condição fundamental da liberdade e a autodeterminação como um "tornar-se prático da liberdade" dependendo de circunstâncias mais ou menos visivelmente experimentadas.

### 4.1 Autodeterminação da ação em graus variados

O conceito de autodeterminação refere-se à capacidade de uma pessoa de moldar sua vida de acordo com suas próprias ideias, bem como ao exercício real dessa habilidade e uma forma de vida apresentada como ideal. Deve ser feita uma distinção entre estas formas de autodeterminação pessoal e a proteção jurídica do seu exercício. As formas e os graus de autodeterminação são de considerável importância prática. Em certos contextos, pode-se delegar o direito ao autocontrole ou, em alguns casos, restrições à autodeterminação podem ser parcialmente compensadas pelos representantes.

No contexto dos grandes dados, foram desenvolvidos novos modelos de consentimento nos últimos anos, especialmente para os biobancos, que, no que diz respeito à autodeterminação dos prestadores de dados, atingem um equilíbrio entre uma finalidade pouco realista e uma única e excessivamente ampla finalidade que deve garantir a liberdade. Aqui, modelos dinâmicos, nos quais os elementos

individuais podem ser aceitos várias vezes, são complementados com opções adicionais, como opções de delegação. Os participantes também podem decidir qual a forma de consentimento que geralmente preferem.

No que se refere à autodeterminação, o contexto social deve ser levado em conta. Neste contexto, ser livre e ser capaz de agir de forma independente significa, ao menos, a possibilidade realista de preservar e moldar a própria identidade e de responder às próprias ações perante si e os outros.[24] Isso requer padrões confiáveis e justos de ação enquanto bases do Estado de Direito.

Privacidade é, classicamente, o direito de ser deixado sozinho ou, em outra dicção, uma esfera de vida em que o controle público e a necessidade de justificação indesejada são desnecessários. Intimamente associado com a privacidade é o conceito de intimidade. Identifica as áreas de vida que são reservadas exclusivamente para aqueles diretamente afetados e que os fazem, se em tudo, somente acessíveis aos outros selecionados em uma maneira autodeterminada. O que é ou deve ser considerado privado e íntimo é culturalmente variante. Isso posto, a preservação da privacidade pode ser normativamente justificada pelo seu significado antropológico e social. A privacidade abre espaços de intimidade e de confidencialidade, em que as pessoas cultivam relacionamentos e podem ser imparciais e imperturbadas – protegidas externamente, mas abertamente voltadas para o seu interior.

No que diz respeito ao *big data*, possíveis perigos de privacidade surgem das múltiplas e novas oportunidades de coleta, de análise e de nova vinculação de dados e de informações, bem como a difícil anonimização e a pseudoanonimização associadas.[25] Os detalhes mais íntimos podem ser divulgados digitalmente e esse é um risco flagrante.

Embora na sociedade digital um controle completo de seus próprios traços de dados possa ter se tornado impossível, a expectativa de que os usuários de dados tratarão os dados disponibilizados a eles de modo confidencial e confiável está crescendo, mesmo no contexto das descontextualizações. De toda sorte, as condições de *big data* afetam não só os indivíduos, mas, também, os grupos. A análise de grandes quantidades de dados muitas vezes torna possível combinações características entre muitas pessoas. Assim, os afetados são geralmente

[24] Cf. KOOLE, Sander L.; SCHLINKERT, Caroline; MALDEI, Tobias; BAUMANN, Nicola. Becoming who you are: An integrative review of self-determination theory and personality systems interactions theory. *Journal of Personality*, v. 87, p. 15-36, 2019. Disponível em: https://doi.org/10.1111/jopy.12380. Acesso em: 15 mar. 2019.

[25] Cf. KIM, J. W.; JANG, B.; YOO, H. Privacy preserving aggregation of personal health data streams. *PLoS ONE*, v. 13, n. 11, e0207639, 2018. Disponível em: https://doi.org/10.1371/journal.pone.0207639. Acesso em: 15 jun. 2018.

agrupados por sistemas de algoritmos potencialmente estigmatizantes, discriminatórios ou excludentes,[26] tornando-se, todavia, imperceptível para o indivíduo.

O conceito de soberania, de autodeterminação pessoal, assume uma importância central no contexto dos grandes dados. Origina-se, culturalmente, principalmente da esfera religioso-política, e recebe diferentes sensos concretos em inúmeras áreas da vida. De acordo com uma compreensão da soberania, que, em qualquer caso, em princípio, exclui o poder dos seres humanos sobre outras pessoas, os dados pessoais para colecionadores e para os usuários estão apenas em empréstimo, nunca livre e de propriedade arbitrariamente disponível. Inversamente, isso não significa que o provedor de dados é automaticamente o proprietário de dados de um indivíduo ou pode realizar sua reivindicação à soberania em todas as circunstâncias, mas, em princípio, dá origem às possibilidades de controle de longo alcance do provedor de dados.

O conceito de soberania, deve-se enfatizar, está intimamente ligado ao poder. A soberania é realizada no modo do exercício do poder e é revertida pelo exercício do poder soberano dos outros. No contexto de grandes dados, formas específicas de poder estão se tornando eticamente significativas: em primeiro lugar, aquelas que podem manipular as preferências e as crenças dos outros; e, em segundo lugar, aquelas que até mesmo podem permitir uma formação sutil, uma mudança e, portanto, um possível domínio de seus personagens.

Certamente o uso de algoritmos de *big data* abre novas possibilidades para que os prestadores de serviços de internet influenciem o pensamento, o sentimento e as ações dos usuários. O espectro varia de um estímulo aberto, que se destina a sutilmente excitar o comportamento de promoção da saúde, à ação secreta e, sobretudo, às intervenções manipulativas exógeno-amigáveis. Essas últimas são, ao menos, particularmente necessitadas de justificação e de limites.

Outro ponto de referência normativo pertinente surge da obrigação moral de caridade, segundo a qual, em muitas situações, as próprias ações, além da mera prevenção de danos, também beneficiam outras, em especial as que necessitam de assistência, direta e indiretamente. Dois aspectos da caridade são de particular interesse para o tema de *big data* e saúde: por um lado, o aumento do conhecimento e da informação e, por outro lado, o valor acrescentado terapêutico,

[26] Cf. KLEINBERG, Jon; LUDWIG, Jens; MULLAINATHAN, Sendhil; SUNSTEIN, Cass R. Discrimination in the Age of Algorithms. *Journal of Legal Analysis*, v. 10, laz001, 2018. Disponível em: https://doi.org/10.1093/jla/laz001. Acesso em: 27 fev. 2019. Ver ainda, e especialmente, LAAT, Paul B. Algorithmic decision-making based on machine learning from big data: can transparency restore accountability? *Philosophy & Technology*, v. 31, issue 4, p. 525-541, dez. 2018. Disponível em: https://doi.org/10.1007/s13347-017-0293-z. Acesso em: 27 set. 2019.

que é o resultado de novas oportunidades para a coleta digital de informação e de processamento de grandes quantidades de dados no setor da saúde para diferentes partes interessadas. Conhecimento e informação são de grande importância para a autoconstituição do indivíduo e para a sua capacidade de viver uma vida autônoma. Além disso, a revisão crítica, a salvaguarda e a expansão dos recursos do conhecimento têm uma importante função social.

Urge, pois, proteger a comunicação comprometida com a veracidade. Os requisitos metodológicos e científicos-teóricos diferenciados, cumpre mencionar, se desenvolveram para fixá-los, especialmente no campo das ciências. Portanto, é importante garantir que os novos processos de coleta, de análise e de vinculação de dados digitais não levem à redução dos padrões epistemológicos ou à perda de confiabilidade das declarações derivadas deles. É evidentemente necessário esclarecer quais os grupos de pessoas que devem se beneficiar principalmente das medidas baseadas no conhecimento produzido e alcançadas por meio do uso de grandes dados, como de qual maneira as barreiras existentes podem ser removidas por meio de um desenho mais eficiente do processo de utilização de dados e de como uma distribuição justa dos efeitos positivos resultantes do aumento esperado do conhecimento pode ser alcançada.

## 4.2 Justiça e dados de saúde

A coleta e a difusão de grandes quantidades de dados relacionados com a saúde abordam questões fundamentais afeitas à noção de justiça. Como um princípio normativo das relações sociais, a justiça exige a evasão arbitrária de privilégios de indivíduos ou de determinados grupos. Em vez disso, o que é adequado para cada indivíduo deve ser determinado de modo racional e relacional. Isso pressupõe que critérios uniformes sejam utilizados e que as diferenças no tratamento dos indivíduos sejam justificadas de modo consensual.

No que se refere às aplicações de *big data* no setor da saúde, quatro áreas principais são particularmente relevantes para a justiça: em primeiro lugar, o acesso às coleções de dados para pesquisa, em segundo lugar, o registo eletrônico de estruturas monopolistas, em terceiro lugar, a inclusão de aplicativos de saúde e vários dispositivos para automensuração privada na precificação do seguro de saúde e, em quarto lugar, aspectos da equidade da capacidade de lidar com o seguro de saúde de modo responsável.

## 4.3 Soberania de dados como liberdade informativa

A soberania de dados, entendida como uma forma de liberdade informativa responsável, adequada às oportunidades e aos riscos de *big data*, deve ser o objetivo ético e jurídico central nessa temática. O conceito de "*design* de liberdade informativa", reafirme-se, desenvolve ainda mais o conceito de autodeterminação informativa e existencial. Esse não atribui um direito de propriedade e de exclusão, mas o poder de determinar para si o conteúdo com o qual uma pessoa se relaciona com seu ambiente.

*Design* de liberdade informativa, nesse sentido, significa o desenvolvimento de personalidade interativa, preservando a privacidade em um mundo em rede e, desse modo, é caracterizado pela possibilidade de efetivamente entrar em um "córrego" com base em preferências pessoais e em dados pessoais relevantes. Essa garantia de liberdade é derivada de atitude responsável, se for, ao mesmo tempo, orientada para as exigências sociais da solidariedade e da justiça.

Com a soberania dos dados no sentido representado aqui, trata-se de aplicar os requisitos normativos básicos designados, incluindo a autodeterminação informativa ancorada em direitos humanos e fundamentais, em posturas éticas e nas disposições morais e, portanto, igualmente no que toca à tecnologia e, naturalmente, à proteção de dados, nas condições de *big data*, vez que a proteção de dados serve, incontestavelmente, à proteção da pessoa, em sua integralidade, exigindo uma garantia complexa. Ao mesmo tempo, o conceito de soberania de dados enfatiza a intenção de vincular o soberano, ou seja, o manuseio auto-confiante e responsável do indivíduo com seus próprios dados pessoais. Em função disso, duas esferas que são cada vez mais aproximadas e já parcialmente sobrepostas podem ser distinguidas: primeiro, a esfera da proteção de dados previamente já comparativamente desobstruída e estrita, normas de qualidade e segurança, utilização de dados na investigação médica e na prática clínica; em segundo lugar, a esfera das ofertas de mercado cada vez mais importantes, mas muito heterogêneas e livres.

Inolvidável esclarecer que desenvolvimentos de *big data* não podem ser interrompidos, podendo ser moldados. Como as formas e as salvaguardas da proteção tradicional dos dados à direita, não é suficiente desenvolver um modelo de *design* e regulamentar alterado que seja mais reflexivo acerca da complexidade e da dinâmica de desenvolvimento de *big data*. Isso deve refletir a soberania dos dados como um projeto de liberdade informativa multidimensionalmente e com vista aos diferentes atos de grupos e de contextos de ação, atribuindo as possibilidades e as atribuições de responsabilidade anteriormente delineadas.

## 4.4 Dados de saúde e consentimento

O consentimento livre, informado, esclarecido e consciente é ética, moral e legalmente exigido na relação médico-paciente, de modo especial quando estão envolvidos dados sensíveis. Em outro giro, o médico tem a responsabilidade/o dever moral de preservar o sigilo e a confidencialidade, identificando os melhores tratamentos para cada paciente com base nas evidências médicas disponíveis. E, assim, tem o dever de dialogar com os pacientes a respeito dos benefícios esperados e dos riscos potenciais, facilitando o processo cognitivo e deliberativo, cabendo aos médicos informar e bem esclarecer as perguntas e/ou interrogações dos pacientes relativamente ao tratamento, aos benefícios e aos riscos propostos não só a partir de sua experiência profissional, mas também informando sobre a literatura médica disponível.

Essa permuta de informações, conceituações e de opiniões formata o alicerce da relação médico-paciente, promovendo melhores e mais ajustadas decisões informadas, notadamente nas situações médicas mais complexas.[27] Nesse estado da arte, portanto, independentemente do alcance do emprego de *big data*, deve-se sublinhar que, no que toca à complexidade do processo de anuência e a exigência quanto ao respeito, à proteção do protagonismo do usuário/paciente na condução da sua vida, as informações devem ser previamente apresentadas em linguagem clara, precisa, apropriada e suficiente, mormente observando o esclarecimento quanto à pertinência, à finalidade, à adequação, ao tempo da coleta, às modalidades de armazenamento, ao tratamento e à transmissão dos dados obtidos no sentido de possibilitar a renúncia, a alteração, o uso, a cessão, e a disponibilidade ou a recusa daquele que consente.

Diga-se nessa altura, em razão da notoriedade, que, no que toca à LGPD, houve um enaltecimento desse instituto, mas foram incluídas outras modalidades de justificação de tratamento de dados pessoais que igualmente não são aplicáveis de modo eficaz na sua dicção atual ao contexto de *big data*.

## 5 Pontos conclusivos e recomendações

A proteção de dados, em síntese, confere um novo e atual sentido à proteção da pessoa humana e da dignidade, da autonomia e das esferas de liberdade que lhes são inerentes. Com efeito, ante a realidade tecnológica atual, ela deve

[27] Cf. PATERICK, Timothy J. *et al*. Medical Informed Consent: General Considerations for Physicians. *Mayo Clin Proc.*, v. 83, n. 3, p. 313-319, mar. 2008. Disponível em: https://mayocl.in/31FSmPK. Acesso em: 2 ago. 2019.

estar preparada para recombinações e para recontextualizações constantes. Entende-se, de fato, que a mera aplicação dos atuais instrumentos normativos em vigor, incluindo-se aqui os instituídos pela LGPD, não é suficientemente apropriada para o enfrentamento e a implantação de meios de resolução factíveis em face dos conflitos e das prováveis violações de direitos humanos e fundamentais resultantes do irrestrito manejo dos dados pessoais em contexto de *big data*, especialmente quando se trata de dados referentes à saúde humana. Entende-se igualmente que a saúde e tampouco a ciência e a tecnologia podem ser arroladas como áreas neutras, infensas ao poder.

A propósito, um modelo de *design* e de regulamentação voltado para a soberania de dados concentra-se sobretudo no provedor de dados como um propósito decisivo para proteção e para o respeito. O objetivo do projeto de liberdade informacional responsável no setor da saúde é seguramente explorar os grandes potenciais de dados específicos para a pesquisa médica, para a aplicação clínica e para o comportamento de saúde individual, e para minimizar os riscos associados.

O ponto primordial, deve-se grifar, é possibilitar que os sujeitos na qualidade de usuários e de pacientes, bem como as organizações a eles associados, tratem seus dados de maneira soberana, por meio da regulação e do desenho institucional que seja tão sensível ao contexto quanto apropriado às nuances da constante mutação da tecnologia. Soluções mais simples de taxa fixa devem ser abandonadas, devendo-se optar por modelos de combinação mais complexos, mas igualmente mais flexíveis e mais adequados ao problema, ou seja, institucionalmente diversificados.

Recomenda-se um conceito de *design* e de regulação orientado para o objetivo central da soberania de dados e, dessa forma, entende-se pela urgência do amplo debate sobre a ressignificação da ideia de consentimento no intuito de adequá-la aos parâmetros que compreendam o paradigma volátil, incerto, complexo e ambíguo típico dos dias atuais. Tal empreendimento exige um esforço global da sociedade como um todo, que, incorporando elementos jurídicos e extralegais, deve compreender os desenvolvimentos técnicos mais sofisticados em uma constelação de limites equânimes, éticos e justos, portanto, a fim de que sua disponibilidade se estenda a todos, ademais de qualquer elemento de desnível, tornando-se aplicável para todos os atores sociais. Essencial advertir que, a despeito dos riscos, tangíveis e intangíveis, convém uma análise que supere a heurística do medo, reconhecendo igualmente as possibilidades de benefícios e de oportunidades que podem advir e repercutir na qualidade de vida das pessoas em geral.

Logo, recomenda-se urgência na necessidade de forjar um projeto específico com abordagem regulamentar que contenha metas concretas para a ação em

quatro áreas temáticas, que objetivam, em primeiro lugar, *desbloquear o potencial dos grandes dados* e, em segundo lugar, *preservar a liberdade e a privacidade individuais*; em terceiro plano, incentivar *a justiça e a solidariedade* e, finalmente, *promover a responsabilidade e a confiança*.

**Technological, ethical and normal issues of personal data protection in the health area in a big data context**

**Abstract**: Technology brings radical health benefits, but the current context is anchored in concerns about the security of personal data in the face of technological innovation. The question about data ownership, responsibility and solidarity, especially regarding the role of individuals, the State, professional entities and private companies in the health sector, is a fertile field, demanding an investigation due to the necessary equation of the data. damage and opportunities. This theoretical and bibliographical research and, in view of the possible exploratory results, aims to analyze the specificities of health data and the repercussion of its use due to contemporary forms of collection. , storage, handling, manipulation, especially in a Big Data context. Due to the current trend towards the implementation of a kind of techno-control through the algorithmization of the current society undertaken by the world oligopolies, in view of the risks inherent in the use of communication and information technology (ICT) and the fragility of devices. which make up the Brazilian protective system, investigate, in particular, some of the shortcomings and controversies of the General Data Protection Law (LGPD) applicable to the health area with the purpose of presenting guidelines and recommendations.

**Keywords**: Health. Big data. Medical research. Devices. Ethics. Self-determination.



## Referências

AGÊNCIA NACIONAL DE SAÚDE SUPLEMENTAR. *Legislação*. Disponível em: https://bit.ly/2YJbbV8. Acesso em: 13 ago. 2019.

BENNETT, Colin J. *Regulating privacy*: data protection and public policy in Europe and the United States. Nova York: Cornell University Press, 1992.

BISOTO JUNIOR, Geraldo; SILVA, Pedro Luís de Barros; DAIN, Sulamis (Org.). *Regulação do setor saúde nas Américas*: as relações entre o público e o privado numa abordagem sistêmica. Brasília: Organização Pan-Americana da Saúde, 2006.

BLASIMME, Alessandro; FADDA, Marta; SCHNEIDER. Manuel; VAYENA, Effy. Data sharing for precision medicine: policy lessons and future. *Health Affairs*, v. 37, n. 5, p. 702-709, 2018. Disponível em: https://www.healthaffairs.org/doi/pdf/10.1377/hlthaff.2017.1558. Acesso em: 27 jun. 2019.

BRASIL. *Lei nº 13.853, de 8.7.2019*. Disponível em: https://bit.ly/2YLG07A. Acesso em: 12 ago. 2019.

BRASIL. *LGPD*. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm. Acesso em: 18 fev. 2018.

BUNDESDATENSCHUTZGESETZ (BDSG). Disponível em: https://bit.ly/30yYXvh. Acesso em: 17 out. 2019.

BUSSE, Reinhard; BLÜMEL, Miriam; KNIEPS, Franz; BÄRNIGHAUSEN, Till. Statutory health insurance in Germany: a health system shaped by 135 years of solidarity, self-governance, and competition. *Germany and health*, v. 390, issue 10097, p. 882-897, 26 ago. 2017.

BVERFG. Urteil v. 15. Dezember 1983, Az. 1 BvR 209, 269, 362, 420, 440, 484/83.

BVERFGE 65, 1 – Volkszählung. Disponível em: http://www.servat.unibe.ch/dfr/bv065001.html. Acesso em: 13 out. 2019.

CAREY, Corinne A.; STERN, Gillian. Protecting patient privacy: strategies for regulating electronic health records exchange. *New York Civil Liberties Union (NYCLU)*, Nova York, mar. 2012. Disponível em: https://bit.ly/305PT0F. Acesso em: 3 jul. 2019.

COMUNICAÇÃO DA COMISSÃO AO PARLAMENTO EUROPEU E AO CONSELHO. *Proteção, novas oportunidades* – Orientações da Comissão relativas à aplicação direta do Regulamento Geral sobre a Proteção de Dados a partir de 25 de maio de 2018/FMT. Comissão Europeia, Bruxelas, 24.1.2018 – COM. 2018. Disponível em: https://bit.ly/2LVxh0e. Acesso em: 17 ago. 2019.

CONSELHO NACIONAL DE SAÚDE (MS). *Legislação*. Disponível em: https://bit.ly/2TtexFR. Acesso em: 12 ago. 2019.

CONTRERAS, J. L. The false promise of (health) data ownership. *University of Utah College of Law Research Paper*, n. 304, 2018. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3328258. Acesso em: 4 jul. 2019.

COUNCIL OF EUROPE. *Convenção 108+*. Disponível em: https://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f1. Acesso em: 17 ago. 2019.

COUNCIL OF EUROPE. *Human Rights Intergovernmental Cooperation*. Disponível em: https://www.coe.int/en/web/human-rights-intergovernmental-cooperation/. Acesso em: 17 ago. 2019.

COUNCIL OF EUROPE. *Modernization of Convention 108*. Disponível em: https://www.coe.int/en/web/dataprotection/convention108/modernised. Acesso em: 17 ago. 2019.

DRZ – BUSINESS SOLUTION. Disponível em: https://www.drz.global/ . Acesso em: 15 fev. 2019.

EUR-LEX. *ECJ C-131/12 Google Espanha vs. AEPD*. Disponível em: https://bit.ly/2OKMoHs. Acesso em: 13 set. 2019.

EUR-LEX. *RGPD*. Disponível em: https://bit.ly/2JQGtkb.

EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS. *Relatório da FRA* – Inequalities and multiple discrimination in access to and quality of healthcare. Disponível em: https://fra.europa.eu/sites/default/files/inequalities-discrimination-healthcare_en.pdf. Acesso em: 1º ago. 2019.

FRIEDEWALD, Michael; LAMLA, Jörn; ROßNAGEL, Alexander. *Informationelle Selbstbestimmung im digitalen Wandel*. Berlin: Springer-Verlag, 2017.

GIOVANELLA, Ligia *et al*. Sistema universal de saúde e cobertura universal: desvendando pressupostos e estratégias. *Ciênc. Saúde Coletiva*, Rio de Janeiro, v. 23, n. 6, jun. 2018. Disponível em: http://dx.doi.org/10.1590/1413-81232018236.05562018. Acesso em: 15 jun. 2018.

HESSE. *Hessische Datenschutzgesetz (Lei de Proteção de Dados Hessiana) de 1970*. Disponível em: http://starweb.hessen.de/cache/GVBL/1970/00041.pdf#page=1. Acesso em: 6 ago. 2019.

HULL, G. Successful failure: what Foucault can teach us about privacy self-management in a world of Facebook and big data. *Ethics Inf Technol*, v. 17, n. 2, p. 89-101, 2015.

KIM, J. W.; JANG, B.; YOO, H. Privacy preserving aggregation of personal health data streams. *PLoS ONE*, v. 13, n. 11, e0207639, 2018. Disponível em: https://doi.org/10.1371/journal.pone.0207639. Acesso em: 15 jun. 2018.

KLEINBERG, Jon; LUDWIG, Jens; MULLAINATHAN, Sendhil; SUNSTEIN, Cass R. Discrimination in the Age of Algorithms. *Journal of Legal Analysis*, v. 10, laz001, 2018. Disponível em: https://doi.org/10.1093/jla/laz001. Acesso em: 27 fev. 2019.

KOOLE, Sander L.; SCHLINKERT, Caroline; MALDEI, Tobias; BAUMANN, Nicola. Becoming who you are: An integrative review of self-determination theory and personality systems interactions theory. *Journal of Personality*, v. 87, p. 15-36, 2019. Disponível em: https://doi.org/10.1111/jopy.12380. Acesso em: 15 mar. 2019.

KOOPS, Bert-Jaap. The Trouble with European Data Protection Law. *International Data Privacy Law*, 29 ago. 2014. Disponível em: https://ssrn.com/abstract=2505692. Acesso em: 12 jan. 2018.

LAAT, Paul B. Algorithmic decision-making based on machine learning from big data: can transparency restore accountability? *Philosophy & Technology*, v. 31, issue 4, p. 525-541, dez. 2018. Disponível em: https://doi.org/10.1007/s13347-017-0293-z. Acesso em: 27 set. 2019.

LEDERBERG, Joshua. 'Ome Sweet 'Omics – A genealogical treasury of words. *The Scientist – Exploring Life, Inspiring and Innovation*, abr. 2001. Disponível em: https://www.the-scientist.com/commentary/ome-sweet-omics--a-genealogical-treasury-of-words-54889. Acesso em: 11 ago. 2019.

LUHMANN, N.; FRIEDEWALD, Michael; LAMLA, Jörn; ROßNAGEL, Alexander. *Informationelle Selbstbestimmung im digitalen Wandel*. Berlin: Springer-Verlag, 2017.

MAYER-SCHÖNBERGER, Viktor. Generational development of data protection in Europe. *In*: AGRE, Philip E.; ROTENBERG, Marc. *Technology and privacy*: the new landscape. Cambridge: MIT Press, 1998.

MCCARTY-SNEAD, Steven S.; HILBY, Anne Titus. Research Guide to European Data Protection Law. *Legal Research Series*, paper 1, 2013. Disponível em: http://scholarship.law.berkeley.edu/leg_res/1. Acesso em: 19 ago. 2018.

MOEREL, Lokke; PRINS, Corien. *Privacy for the homo digitalis*: proposal for a new regulatory framework for data protection in the light of big data and the internet of things. 2016. Disponível em: http://dx.doi.org/10.2139/ssrn.2784123. Acesso em: 19 ago. 2018.

MOSSIALOS, Elias; WENZL, Martin; OSBORN, Robin; SARNAK, Dana (Ed.). 2015 International Profiles of Health Care Systems. *The Commonwealth Fund*, 2016. Disponível em: https://bit.ly/2P5nqHg. Acesso em: 13 ago. 2019.

MOURA, José; SERRÃO, Carlos. Security and privacy issues of big data. *In*: MOURA, José; SERRÃO, Carlos. *Handbook of Research on Trends and Future Directions in Big Data and Web Intelligence*. Pensilvânia: IGI Global, 2015 Disponível em: https://arxiv.org/ftp/arxiv/papers/1601/1601.06206.pdf. Acesso em: 27 set. 2019.

NORONHA, José Carvalho de; NORONHA, Gustavo Souto de; PEREIRA, Telma Ruth; COSTA, Ana Maria. Notas sobre o futuro do SUS: breve exame de caminhos e descaminhos trilhados em um horizonte de incertezas e desalentos. *Ciênc. Saúde Coletiva*, Rio de Janeiro, v. 23, n. 6, jun. 2018. Disponível em: http://dx.doi.org/10.1590/1413-81232018236.05732018. Acesso em: 21 set. 2019.

OECD. *OECD Privacy Guidelines*. Disponível em: https://www.oecd.org/internet/ieconomy/privacy-guidelines.htm. Acesso em: 11 maio 2019.

OKOYE, John Nwachukwu. *Privacy by design*. Norwegian University of Science and Technology. Department of Information Security and Communication Technology. July 2017. Disponível em: https://bit.ly/33utFaA. Acesso em: 5 set. 2019.

ÖMAN, Sören. *Implementing Data Protection in Law*. Stockholm Institute for Scandianvian Law, 1957-2010. Disponível em: http://www.scandinavianlaw.se/pdf/47-18.pdf. Acesso em: 2 set. 2019.

PARLAMENTO EUROPEU E CONSELHO. *Diretiva (UE) 2015/1535 do Parlamento Europeu e do Conselho, de 9 de setembro de 2015, relativa a um procedimento de informação no domínio das regulamentações técnicas e das regras relativas aos serviços da sociedade da informação*. Disponível em: https://bit.ly/2EhG1b0. Acesso em: 10 set. 2018.

PATERICK, Timothy J. *et al*. Medical Informed Consent: General Considerations for Physicians. *Mayo Clin Proc.*, v. 83, n. 3, p. 313-319, mar. 2008. Disponível em: https://mayocl.in/31FSmPK. Acesso em: 2 ago. 2019.

PLAZA, N. C.; GARCÍA-GALBIS, M. R. Impact of the "Omics Sciences" in Medicine: New Era for Integrative Medicine. *J Clin Microbiol. Biochem Technol*, v. 3, n. 1, p. 9-13, 2017.

PURTOVA, Nadezhda. The law of everything. Broad concept of personal data and future of EU data protection law. *Law, Innovation and Technology*, v. 10, n. 1, p. 40-81, 2018. Disponível em: https://bit.ly/2w3iKFu. Acesso em: 2 ago. 2019.

RHODES, Richard. *Visions of technology*: a century of vital debate about machines systems and the human world. New York: Simon and Schuster, 2000.

RICE, Kelley H. *Physician practice mergers*: the importance of due diligence and mutual trust for all involved. American College of Medical Practice Executives. Disponível em: https://bit.ly/2YMO7Vy. Acesso em: 1º dez. 2018.

ROBERTS, Jessica L. Progressive Genetic Ownership. University of Houston Law Center. *Notre Dame L. Rev.*, v. 93, n. 1105, 2018. Disponível em: https://bit.ly/31Jk7qB. Acesso em: 18 dez. 2018.

SCHERMER, B. W.; CUSTERS, B.; VAN DER HOF, S. The crisis of consent: how stronger legal protection may lead to weaker consent. *Data Protection, Ethics & Information Technology*, v. 16, n. 2, p. 171-82, 2014.

SOLOVE, Daniel J. A taxonomy of privacy. *University of Pennsylvania Law Review*, v. 154, n. 3, jan. 2006. Disponível em: https://ssrn.com/abstract=667622. Acesso em: 21 jul. 2018.

SOLOVE, Daniel J. Conceptualizing privacy. *California Law Review*, v. 90, p. 1087-1155, 2002.

TRETTEL, Daniela Batalha; KOZAN, Juliana Ferreira; SCHEFFER, Mario César. Judicialização em planos de saúde coletivos: os efeitos da opção regulatória da Agência Nacional de Saúde Suplementar nos conflitos entre consumidores e operadoras. *Revista de Direito Sanitário*, v. 19, n. 1, p. 166-187, 2018. Disponível em: http://dx.doi.org/10.11606/issn.2316-9044.v19i1p166-187. Acesso em: 23 jan. 2019.

WANG, Y. *et al.* Big data analytics: Understanding its capabilities and potential benefits for healthcare organizations. *Technol. Forecast. Soc. Change*, 2016. Disponível em: http://dx.doi.org/10.1016/j.techfore.2015.12.019. Acesso em: 11 jul. 2019.

WANG, Y.; KUNG, L.; WANG, Y. C. W.; CEGIELSKI, C. G. Integrated big data analytics-enabled transformation model: Application to health care. *Information and Management*, 2017. Disponível em: http://doi.org/10.1016/j.im.2017.04.001. Acesso em: 23 jan. 2019.

WESTIN, Alan F. *Privacy & Freedom*. London, Sydney, Toronto: The Bodley Head, 1967.

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

SARLET, Gabrielle Bezerra Sales; MOLINARO, Carlos Alberto. Questões tecnológicas, éticas e normativas da proteção de dados pessoais na área da saúde em um contexto de big data. *Direitos Fundamentais & Justiça,* Belo Horizonte, ano 13, n. 41, p. 183-212, jul./dez. 2019.

Recebido em: 06.11.2019
Pareceres: 11.11.2019, 08.11.2019, 19.11.2019, 24.11.2019
Aceito para publicação: 24.11.2019