https://doi.org/10.18593/ejjl.34773

PROTEÇÃO DE DADOS E POLÍTICAS PÚBLICAS DE SAÚDE: ALGUMAS APROXIMAÇÕES À LUZ DE EXEMPLO DA JURISPRUDÊNCIA DO SUPREMO TRIBUNAL FEDERAL

DATA PROTECTION AND PUBLIC HEALTH POLICIES: SOME APPROACHES IN LIGHT OF EXAMPLE FROM THE CASE LAW OF THE SUPREME FEDERAL COURT

Pedro Zanatta Silveira Borges[1]
Ingo Wolfgang Sarlet[2]

Resumo: Em um contexto no qual o processamento de informações por algoritmos e inteligência artificial manipula processos políticos, econômicos e sociais, a proteção dos dados pessoais é condição de possibilidade de uma democracia. Nesse cenário, este trabalho se propõe a analisar, à luz da teoria dos direitos fundamentais e de exemplo extraídos da jurisprudência constitucional brasileira, as tensões entre o direito fundamental à saúde e o direito fundamental à proteção de dados pessoais, especialmente no que diz respeito às políticas públicas na área da saúde.
Palavras-chave: direitos fundamentais; proteção de dados pessoais; direito à saúde. políticas públicas; Supremo Tribunal Federal.

Abstract: In a context where information processing by algorithms and artificial intelligence manipulates political, economic, and social processes, the protection of personal data is a condition for the possibility of democracy. In this scenario, this work aims to analyze, based on the assumptions of fundamental rights theory and an example of the Brazilian constitutional case law, the tensions between the right to health and the right to the protection of personal data, mainly considering public policies in the health sector.
Keywords: fundamental rights; personal data protection; right to health; public policies; Federal Supreme Court.

Recebido em 03 de maio de 2024
Avaliado em 29 de maio de 2024 (AVALIADOR A)
Avaliado em 15 de maio de 2024 (AVALIADOR B)
Aceito em 31 de maio de 2024

Introdução

Desde o final do século XX, o sistema capitalista passa por um processo de desenvolvimento em direção a um modo de produção que se organiza em torno da tecnologia da informação (Castells, 1999). Nesse contexto, a massiva digitalização representa verdadeira transformação nas condições de vida e na estrutura social que decorre, sobretudo, das tecnologias da informação específicas que processam dados digitais (Hoffmann-Riem, 2020).

[1] Graduando em Direito pela Pontifícia Universidade Católica do Rio Grande do Sul; Bolsista de Iniciação Científica PIBIC/CNPQ vinculado ao Grupo de Estudos e Pesquisa em Direitos Fundamentais (GEDF/CNPQ). https://orcid.org/0009-0006-2363-8826. pzsborges@gmail.com.

[2] Doutor e Pós-Doutor em Direito pela Universidade de Munique; Professor Titular da Escola de Direito da Pontifícia Universidade Católica do Rio Grande do Sul; Desembargador aposentado do Tribunal de Justiça do Estado do Rio Grande do Sul; Advogado e parecerista. https://orcid.org/0000-0002-2494-5805. iwsarlet@gmail.com.

O advento da inteligência artificial[3] destaca-se nessa conjuntura. Segundo a linguagem institucional da União Europeia, o termo refere-se a programas informáticos capazes de, a partir de determinados objetivos definidos por seres humanos, criar resultados, tais como conteúdos, previsões, recomendações ou decisões, que influenciam os ambientes com os quais interagem (Comissão Europeia, 2021). A tecnologia funciona a partir de algoritmos digitais. Contudo, ainda que suas etapas permaneçam controláveis, a adaptação independente dos processos de aprendizagem torna alguns sistemas infensos ao controle humano. Por esse motivo, são apontadas como características dos sistemas de inteligência artificial a opacidade, a complexidade, a dependência dos dados e o comportamento autônomo (Pedro, 2023).

As inovações advindas da aplicação desses sistemas de inteligência artificial são potencializadas a partir da combinação com a *Big Data*[4], que, utilizando um conjunto de técnicas digitais capazes de coletar, avaliar e processar um imenso volume e variedade de dados com alta velocidade, permite análises descritivas, preditivas e prescritivas com maior precisão (Sarlet, G.; Molinaro, 2020).

Não obstante, ao lado da possibilidade de aperfeiçoamento da prestação dos serviços públicos, a digitalização também cria ameaças à democracia e aos direitos fundamentais. Concretamente, esses riscos se manifestam, por exemplo, pela elaboração de perfis de comportamento de uma pessoa ou grupo. A técnica é conhecida como *profiling* e, com o auxílio de métodos estatísticos e de técnicas de inteligência artificial, permite a síntese de hábitos, preferências pessoais e outros registros da vida dos indivíduos. O resultado desse tratamento de dados é um quadro da personalidade do titular, que pode ser instrumentalizado para traçar tendências de futuras decisões, comportamentos e destino de uma pessoa ou grupo (Doneda, 2021).

O cenário é descrito por Byung-Chul Han como um *regime de informação* – forma de dominação na qual o processamento de informações por algoritmos e inteligência artificial manipula processos políticos, econômicos e sociais (2022). Isto é, diferentemente do regime disciplinar delineado por Michel Foucault (1989), as tecnologias políticas de submissão não direcionam-se apenas aos corpos, mas aos dados e informações. Dessa forma, conclui o autor, não é "a posse dos

[3] O termo não está imune a críticas, notadamente no que se refere à incapacidade desses modelos de apreender e replicar a complexidade humana – posição sarcasticamente exprimida na metáfora do neurocientista Miguel Nicolelis: *um computador digital não sobreviveria no estádio em uma noite de jogo do Palmeiras* (Teixeira, 2023), destacando sua insuficiência para exprimir a generalidade e complexidade de toda a capacidade do cérebro humano, notadamente de armazenar, experimentar e expressar. Ou seja, para Nicolelis, "não existe fluxo de S-info [modelo binário de informação descrito por Shannon], algoritmo matemático, computador digital ou qualquer forma de inteligência artificial que se aproxime de reproduzir ou emular aquilo que cada um de nós experimenta cotidianamente na nossa mente", cf. Nicolelis, (2020. p. 77).

[4] Cinco características são frequentemente utilizadas para identificar tecnologias de Big Data – os cinco "Vs":1 - Possibilidades de acesso a enormes quantidades de dados digitais ("High Volume"); 2 - Diferentes tipos e qualidade de dados, assim como diferentes formas de coleta, armazenamento e acesso ("High Variety"); 3 - A alta velocidade do seu processamento ("High Velocity"); 4 - O uso da inteligência artificial em particular torna possível novas e altamente eficientes formas de processamento de dados, bem como a verificação de sua consistência e garantia de qualidade ("Veracity"): 5 - Além disso, os Big Data são objeto e base de novos modelos de negócios e de possibilidades para diversas atividades de valor agregado ("Value"). Cf. Hofmann-Riem, (2022, p. 20).

meios de produção que é decisiva para o ganho de poder, mas o acesso a dados utilizados para vigilância, controle e prognóstico de comportamentos psicopolíticos" (Han, 2022)[5].

Uma das consequências de um modelo social construído sobre essas técnicas de elaboração de perfis digitais é a ascensão de projetos autoritários de poder, que usurpam a soberania popular e instauram estados de exceção (Valim, 2017), inclusive dentro de regimes formalmente democráticos. Trata-se de uma espécie de *tecno-autoritarismo* (Sarlet, I.; Sarlet, G., 2023), um sistema de dominação que se vale da tecnologia – como é o caso de *softwares* e algoritmos – para submeter a população à vigilância, controle e influência de Estados e mesmo de grandes corporações, ademais de se manifestar de diversas formas, por exemplo, a desinformação, a hiperconexão, a concentração de poder informacional, o vigilantismo, os discursos de ódio, novas formas de populismo, levando, dentre outros fatores, à deterioração da esfera pública e à manipulação de processos eleitorais, assim como à violação efetiva e potencial de direitos fundamentais de todas as dimensões.

Logo, considerando os riscos da digitalização, busca-se, a partir de uma pesquisa teórica, analisar as tensões entre direitos fundamentais decorrentes da aplicação de dados pessoais em políticas públicas de saúde. Especificamente, busca-se verificar em que medida o direito fundamental à proteção de dados constitui um limite à elaboração e execução de políticas públicas de saúde.

Quanto ao caminho a ser percorrido, inicia-se com um breve exame acerca do direito fundamental a saúde e da crescente digitalização das políticas públicas de saúde (i); em um segundo momento, analisa-se os fundamentos do direito à proteção de dados pessoais no Brasil (ii); para então, a partir da análise de uma decisão do Supremo Tribunal Federal (STF), examinar-se o alcance do direito à proteção de dados pessoais na elaboração e execução de políticas públicas no Brasil (iii); ao final, discute-se como a dogmática dos direitos fundamentais pode oferecer respostas constitucionalmente adequadas ao problema (iv).

1 **Digitalização e políticas públicas de saúde**

Ao consagrar a saúde como "direito de todos e dever do Estado, garantido mediante políticas sociais e econômicas que visem à redução do risco de doença e de outros agravos e ao acesso universal e igualitário às ações e serviços" (Brasil, 1988, art. 196), o constituinte originário eleva a saúde à condição de bem essencial do núcleo político na ordem jurídico-constitucional brasileira. Trata-se de um "direito fundamental à proteção e promoção da saúde", que abrange as dimensões preventiva, promocional e curativa da saúde (Sarlet; Figueiredo, 2018).

[5] Nesse ponto, cabe destacar a crítica de Jonathan Crary (2023, p. 50), no sentido de que "as mitologias de uma economia da informação pós-industrial também eclipsam a persistência de modos anteriores de produção no interior da atual corrida por recursos essenciais para os arsenais de alta tecnologia, para as redes de comunicação, para os produtos eletrônicos de consumo, para os sistemas de energia solar e eólica e muito mais". Segundo o professor da Universidade de Columbia, se for possível um futuro habitável e partilhado em nosso planeta, será um futuro offline, defendendo que a única resposta possível para superar a confluência de crises econômicas, sociais, políticas e ambientais decorrentes das ferramentas e serviços digitais é a rejeição de toda forma de vida baseada na internet.

A partir da forma de consagração, percebe-se que se trata de direito de titularidade universal que atua, simultaneamente, como uma norma definidora de direitos e de deveres de proteção. Na condição de direito subjetivo, o direito à saúde apresenta tanto a condição de direito de defesa (negativo), na medida em que veda ameaças e violações por parte do Estado e da sociedade, quanto de direito a prestações (positivo), que abrange a dimensão procedimental e as prestações materiais em sentido estrito, como o acesso a medicamentos, consultas, internações e exames (Sarlet; Figueiredo, 2018).

Já na condição de direito objetivo, a Constituição impõe ao poder público o dever de, inclusive preventivamente, assegurar a máxima efetividade possível ao direito à saúde, demandando a promoção de políticas sociais e econômicas. Trata-se de um comando constitucional de forte conteúdo programático, que vincula os poderes públicos, no sentido de que estes não apenas estão obrigados a concretizarem os programas, tarefas fins e ordens, mas também que não podem afastar-se do parâmetro preestabelecido na norma (Sarlet, I., 2021).

Na tentativa de concretização desses deveres de proteção, a aplicação de tecnologias de informação e comunicação vem crescendo exponencialmente ao longo dos anos na área da saúde, tanto para o tratamento direto do paciente ("uso primário"), quanto para fins de saúde pública, planejamento de políticas e pesquisas científicas ("uso secundário") (Campos; Xavier, 2022). O impressionante número de mortes diárias, o colapso dos sistemas de saúde, bem como as crises econômicas e sociais decorrentes da pandemia de covid-19 aceleraram o processo de inserção dessas tecnologias na sociedade, exigindo medidas rápidas dos Estados, a fim de antecipar demandas e alocar recursos de forma mais eficiente.

China, Alemanha, Estados Unidos, Austrália e Coreia do Sul – apenas para citar alguns exemplos – aplicaram mecanismos de inteligência artificial movidos por um imenso volume de dados na tentativa de conter a crise (Boffetta; Collatuzzo, 2022). As tecnologias foram utilizadas no aparelhamento de triagens, no rastreamento de casos, no monitoramento de quarentena, em diagnósticos e tratamento virtual, bem como na pesquisa, produção e distribuição de vacinas.

Levando em conta precisamente o caso brasileiro, também nota-se os impactos da pandemia na digitalização dos serviços. O Ministério da Saúde ofereceu acesso a aplicativo de rastreamento de infectados, que notificava os usuários sobre possível exposição ao vírus (Sarlet, G.; Fernandes; Ruaro, 2023). A tecnologia utilizava a aplicação dos sistemas *bluetooth* dos telefones celulares para monitorar e cruzar a localização dos usuários, identificando a possível extensão da contaminação a partir de um diagnóstico positivo da doença.

Portanto, ainda que a emergência de saúde pública referente à covid-19 tenha posto em evidência a necessidade dos dados pessoais para a elaboração de políticas públicas, bem como demonstrado a importância da digitalização de serviços para uma atuação mais eficiente, as contradições e problemas sociais decorrentes desse novo modelo social continuam demandando

novas respostas do Direito e colocando à prova sua capacidade de assegurar uma proteção efetiva dos direitos humanos e fundamentai, aqui, em especial, do direito à proteção de dados pessoais[6].

2 Da proteção do sigilo das comunicações e da privacidade a um direito autônomo à proteção dos dados pessoais

Como se sabe, há longa tradição de pelo menos algum nível de proteção da privacidade na história constitucional brasileira, ainda que durante muito tempo não se tenha feito expressa referência aos direitos à privacidade e intimidade. Desde a Constituição do Império, que assegurava o direito ao sigilo à correspondência (art. 179, XXVII), até a Constituição Federal de 1988 (Brasil, 1988) que, já desde a sua versão originária, garante o direito à intimidade e à vida privada (art. 5º, X), à inviolabilidade do domicílio (art. 5º, XI) e ao sigilo da correspondência e das comunicações (art. 5º, XII), ademais de ter previsto a ação constitucional do *habeas data* com status de direito e garantia fundamental (art. 5º, LXXII). Todavia, quanto ao reconhecimento de um direito fundamental à proteção de dados pessoais, uma longa trajetória ainda se faria necessária, tendo tal direito sido finalmente incorporado ao texto constitucional quando da promulgação da Emenda Constitucional (EC) 115/2022, como logo mais se verá.

Mas retornando, por ora, à privacidade, que, em primeira linha (mas não só, já que assume cada vez mais relevo a sua dimensão objetiva) opera como um direito subjetivo das pessoas naturais, há de se frisar que tal direito pressupõe, tal como reconhecido amplamente por muito tempo, uma separação entre as esferas pública e privada.

Não é à toa que, nos termos do clássico artigo escrito por Samuel D. Warren e Louis D. Brandeis (1890), o direito à privacidade é definido como o direito de ser deixado só (*the right to be let alone)*. Nessa perspectiva, a privacidade consiste em uma garantia de que os aspectos da vida pessoal e familiar serão publicizados somente na medida do interesse do indivíduo, reclamando uma abstenção dos poderes estatais e dos particulares, no sentido de não intervirem no âmbito de proteção desse direito fundamental.

A problemática envolvendo a proteção dos dados pessoais era considerada, na jurisprudência brasileira, como uma espécie de extensão desse direito à privacidade. Nesse sentido, predominava a posição representada por Tércio Sampaio Ferraz Júnior (1993), para quem – partindo do pressuposto de que a inviolabilidade do sigilo dos dados era condição de possibilidade do direito à privacidade – a proteção constitucional dos dados estaria adstrita ao momento da *comunicação*[7]. Isso fica claro, por

[6] Tamanho impacto das novas tecnologias nas diversas esferas da vida social, que já se fala, inclusive, em um "Constitucionalismo Digital". Nesse sentido: Mendes e Fernandes (2020); Celeste (2021); Saavedra, e Borges (2022). Em posição crítica ao conceito, no sentido de que o adjetivo teria se tornado mais importante que o substantivo, fragilizando-o teoricamente: Trindade e Antonelo (2023).

[7] Nesse sentido, segundo o autor "se alguém elabora para si um cadastro sobre certas pessoas, com informações marcadas por avaliações negativas, e o torna público, poderá estar cometendo difamação, mas não quebra sigilo de dados. Se estes dados, armazenados eletronicamente, são transmitidos, privadamente, a um parceiro, em relações mercadológicas, para defesa do

exemplo, no julgamento do RE 418.416-8/SC, de relatoria do Ministro Sepúlveda Pertence, em que o STF assentou que "a proteção a que se refere o art. 5º, XII, da Constituição, é da comunicação 'de dados' e não dos 'dados em si mesmos', ainda quando armazenados em computador", definindo que a inviolabilidade das comunicações não alcançaria a apreensão de base física de dados [8].

Nesse mesmo sentido, calha invocar a lição de Danilo Doneda (2021, p. 267-268) que aqui se toma a liberdade de transcrever:

> [Se,] por um lado, a privacidade é encarada como um direito fundamental, as informações pessoais em si parecem, a uma parte da doutrina, serem protegidas somente em relação à sua "comunicação", conforme art. 5, XII, que trata da inviolabilidade da comunicação de dados. Tal interpretação traz consigo o risco de sugerir uma grande permissividade em relação à utilização de informações pessoais. Nesse sentido, uma decisão do STF, relatada pelo Ministro Sepúlveda Pertence, reconheceu expressamente a inexistência de uma garantia de inviolabilidade sobre dados armazenados em computador com fulcro em garantias constitucionais...O sigilo, no inciso XII do art. 5º, está referido à comunicação, no interesse da defesa da privacidade.... Obviamente o que se regula é comunicação por correspondência e telegrafia, comunicação de dados e telefônica... A distinção é decisiva: o objeto protegido no direito à inviolabilidade do sigilo não são os dados em si, mas a sua comunicação restringida (liberdade de negação). A troca de informações (comunicação) privativa é que não pode ser violada por sujeito estranho... A decisão tem sido, desde então, constantemente mencionada como precedente em julgados nos quais o STF identifica que a natureza fundamental da proteção aos dados está restrita ao momento de sua comunicação.

Se o direito à proteção de dados pessoais não se confunde com o direito ao sigilo da comunicação de dados, também é verdade que, a despeito da proteção de dados pessoais ter conexão relevante com o direito à privacidade, tal relação igualmente não se traduz numa superposição completa dos respectivos âmbitos de proteção. A proteção de dados pessoais e, da mesma forma, autodeterminação informativa vão além da privacidade e de sua proteção, ao menos no sentido tradicional do termo, caracterizado por uma lógica de "recolhimento" e "exposição" (Ruaro; Rodriguez, 2010).

Uma primeira diferença que pode ser apontada reside no fato de que – na esteira das lições de Stefano Rodotà (2008) – a privacidade indica uma visão negativa e estática, em larga medida pautada na concepção de impossibilitar a interferência de terceiros. Em contrapartida, a proteção de dados confere ao titular poderes positivos e dinâmicos postos à sua disposição com vistas ao controle sobre a coleta e o processamento dos dados que lhe digam respeito. Assim – de acordo com Rodotà –,

mercado, também não haverá quebra de sigilo. Mas se alguém entra nesta transmissão, como um terceiro que nada tem a ver com a relação comunicativa, ou por ato próprio ou porque uma das partes lhe cede o acesso indevidamente, estará violado o sigilo de dados."

[8] RE 418416, Relator Ministro Sepúlveda Pertence, Tribunal Pleno, julgado em 10/05/2006. Da mesma forma, no julgamento do HC nº 91.867/PA, Relator Ministro Gilmar Mendes, julgado em 24/04/2012, a partir de uma distinção entre comunicação telefônica e registros telefônicos, a Segunda Turma do STF entendeu que não haveria ilegalidade na identificação dos mandantes de crime por policiais através da verificação forçada do registro de chamadas nos celulares do executor do crime no momento da prisão em flagrante, repetindo a fórmula de que o direito fundamental previsto no artigo 5º, inciso XII, da Constituição Federal protegeria a *comunicação de dados* e não os *dados*.

o bem jurídico tutelado na privacidade gira em torno da informação e do sigilo, enquanto no direito à proteção de dados abarca a informação, a circulação e o respectivo controle (Rodotà, 2008).

Importante é que se tenha presente, nesse contexto, que, embora a proteção de dados tenha sido deduzida (associada), em diversos casos, do direito à privacidade (*v.g.*, nos EUA, o conceito de *informational privacy*) ou, pelo menos, também do direito à privacidade, como no caso da Convenção Europeia de Direitos Humanos (nos termos da exegese do art. 8.º levada a efeito pela CEDH), o fato é que o objeto (âmbito de proteção) do direito à proteção de dados pessoais é mais amplo, porquanto, com base num conceito ampliado de informação, abarca todos os dados que dizem respeito a uma determinada pessoa natural, sendo irrelevante a qual esfera da vida pessoal se referem (íntima, privada, familiar, social), descabida qualquer tentativa de delimitação temática (Karg, 2019).

O que se pode afirmar, sem temor de incorrer em erro, é que, seja na literatura jurídica, seja na legislação e jurisprudência, o direito à proteção de dados vai além da tutela da privacidade, cuidando-se, de tal sorte, de um direito fundamental autônomo, diretamente vinculado à proteção da personalidade. Aliás, não é à toa que Bruno Ricardo Bioni alertou para o fato de que o entendimento, hoje amplamente superado, de que o direito fundamental à proteção de dados consiste em mera evolução do direito à privacidade é uma "construção dogmática falha" (Bioni, 2018).

Percebe-se, portanto, que em virtude dos impactos das mudanças quantitativas e qualitativas no tratamento de dados pessoais decorrentes dos novos métodos, algoritmos e técnicas digitais desenvolvidas ao longo do século XX, em especial devido a velocidade de acesso, transmissão e cruzamento dos dados resultante das tecnologias de informação e comunicação, as possibilidades de afetação de direitos fundamentais são potencializadas, mediante o conhecimento e o controle de informações sobre a vida pessoal, privada e social (Sarlet, I., 2020), acarretando uma severa diminuição na capacidade de escolha e autodeterminação do titular dos dados.

Por isso, embora tardiamente, também acabou sendo reconhecido um direito fundamental autônomo à proteção de dados pessoais, o que, num primeiro passo, se deu na condição de direito implicitamente positivado e por força de decisão do STF, em maio de 2020, quando, por ampla maioria de 10 votos, o Plenário referendou medida cautelar concedida pela Ministra Relatora Rosa Weber e reconheceu que o tratamento de dados pelo poder público sem mecanismos de proteção e segurança viola o direito autônomo à proteção de dados pessoais, extraído a partir de uma leitura sistemática da Constituição. O direito fundamental também foi denominado "direito à autodeterminação informativa" por alguns Ministros, demonstrando a influência da decisão da famosa decisão do Tribunal Constitucional Federal da Alemanha, de 1983 (o assim conhecido caso do recenseamento), diversas vezes mencionada pelo STF.

Essa autonomia do direito à proteção de dados pessoais, contudo, deve ser bem compreendida, já que se trata de uma autonomia relativa, dada a intersecção com outros princípios e direitos fundamentais, tais como a privacidade e a intimidade, mas também do direito ao livre desenvolvimento da personalidade, da dignidade da pessoa humana e da autodeterminação

informacional. Assim, quando se fala em autonomia, o que está em causa é o fato de que o direito à proteção de dados pessoais tem um âmbito de proteção próprio e não se confunde com os direitos fundamentais referidos.

A decisão do STF abriu caminho para a promulgação da Emenda Constitucional 115/2022, que incorporou o direito à proteção de dados ao artigo 5º, (Brasil, 1988), de acordo com o qual "é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais" (inciso LXXIX). Com isso, foi assegurada a atribuição do regime jurídico-constitucional dos direitos fundamentais à proteção de dados pessoais, o que, em apertada síntese, significa que, além de fruir da supremacia característica das normas constitucionais, o direito à proteção de dados pessoais passou a assumir a condição de cláusula pétrea (art. 60, §§1º a 4º, CF) e, consequentemente, de limite material – mas também formal, temporal e circunstancial – à reforma constitucional, ademais de se tratar de direito veiculado por norma dotada de aplicabilidade imediata (art. 5º, §1º, CF) e que vincula diretamente todos os poderes públicos e, respeitadas as peculiaridades de cada situação, também os particulares (Sarlet, I., 2020).

Esse direito fundamental – como também restou assentado pelo STF, apresenta uma dupla dimensão subjetiva e objetiva. No concernente à primeira, o direito fundamental à proteção de dados pessoais assume a condição de um direito subjetivo atribuído às pessoas naturais, que se decodifica em uma série de posições jurídico-subjetivas, que, embora decorram da Constituição, foram previstas com detalhe e mediante lista não exaustiva, na legislação infraconstitucional[9], principalmente no Capítulo III da Lei Geral de Proteção de Dados Pessoais (LGPD), envolvendo: a) o direito ao acesso e ao conhecimento dos dados pessoais existentes em bancos de dados; b) o direito ao não conhecimento, tratamento, utilização e difusão de determinados dados pessoais pelo Estado ou por terceiros, incluindo um direito de sigilo; c) o direito ao conhecimento da identidade dos responsáveis pelo tratamento dos dados; d) o direito ao conhecimento da finalidade da coleta e da eventual utilização dos dados; e) o direito à retificação e, a depender do caso, à exclusão de dados pessoais armazenados em bancos de dados (Sarlet, I., 2020).

Além disso, o direito à proteção de dados – na condição de direito fundamental – constitui uma decisão valorativa de natureza jurídico-objetiva da Constituição, que produz efeitos em todo o ordenamento jurídico, ensejando o reconhecimento de novas funções e conteúdos normativos. Nesse aspecto, cabe destacar a *eficácia irradiante* (*Ausstrahlungswirkung*), que diz respeito a vinculação do legislador infraconstitucional às diretrizes impostas pelo direito fundamental, bem como eficácia nas relações privadas – também denominada eficácia horizontal (*Drittwirkung*). Ainda, não se pode desconsiderar que o direito a proteção de dados impõe aos poderes públicos deveres de proteção

[9] No plano infraconstitucional, ainda que o Código de Defesa do Consumidor (Lei 8.078/1990); a Lei de Acesso à Informação (Lei 12.527/2011) e o Marco Civil da Internet (Lei 12.965/2014), em alguma medida, já previssem mecanismos de proteção aos dados pessoais, a matéria foi detalhadamente regulada pela LGPD.

(*Schutzplichten*), no sentido de que devem intervir, inclusive preventivamente, contra agressões por parte dos órgãos estatais e de particulares (Sarlet, I., 2020).

À vista dessa sumária apresentação do direito fundamental à proteção de dados como direito (relativamente) autônomo no Brasil, importa agora passar a analisar os desdobramentos de seu reconhecimento no caso específico das políticas públicas de saúde, à luz da acima mencionada decisão do STF.

3 **Dados pessoais e deveres de proteção em políticas públicas de saúde**

A decisão do STF no *caso IBGE* não é importante apenas pelo reconhecimento da fundamentalidade e da autonomia do direito à proteção de dados pessoais, mas também porque representou, por outro lado, um suposto revés para o Poder Executivo no que diz respeito à elaboração e execução de políticas públicas de saúde.

Para relembrar, o caso versava sobre a constitucionalidade do artigo 2º, *caput*, da Medida Provisória nº 954 de 17 de abril de 2020, que atribuiu às empresas de telefonia fixa e móvel o dever de disponibilizar, durante a pandemia da Covid-19, a relação de nomes, números de telefone e endereço de seus consumidores com o Instituto Brasileiro de Geografia e Estatística (IBGE). A medida foi publicada em um cenário inicial da crise sanitária, muito embora o Brasil já estivesse enfrentando um agravamento do quadro, com o crescimento no número de casos e mortes[10].

De acordo com o ato normativo, os dados seriam utilizados exclusivamente pela Fundação IBGE para a produção de estatística oficial, com o objetivo de realizar entrevistas domiciliares em caráter não presencial (art. 2º, §1º) e seriam eliminados quando superada a emergência de saúde pública de importância internacional decorrente do coronavírus (art. 4º).

A questão jurídico-constitucional submetida ao STF envolvia, portanto, a legitimidade da restrição ao direito a proteção de dados decorrente do compartilhamento de informações pessoais. A constitucionalidade da norma impugnada foi analisada mediante aplicação do assim chamado teste de *proporcionalidade*.

A aplicação da proporcionalidade, na sua condição de técnica para dar uma solução constitucionalmente adequada aos conflitos (colisões) entre direitos fundamentais, como se sabe, é originária do direito administrativo alemão, tendo sido posteriormente incorporada ao direito constitucional e desenvolvida pela jurisprudência do Tribunal Constitucional Federal da Alemanha ao longo da segunda metade do Século XX, e acabou por ser recepcionada em um número cada vez maior de Países e mesmo na esfera dos Tribunais Internacionais, com destaque para a Corte Europeia de Direitos Humanos e o Tribunal de Justiça da União Europeia.

[10] Segundo dados divulgados pelas secretarias estaduais de saúde, até o dia 17 de abril de 2020 o Brasil já havia atingido a grave marca de 34.221 casos confirmados e 2.171 mortes. (Casos [...], 2020).

No caso do Brasil, embora durante muito tempo tenha prevalecido o recurso ao instituto da razoabilidade, por fora da influência do direito norte-americano nesse particular, a partir da promulgação da atual Constituição Federal, em 1988, e do gradual fortalecimento da influência da doutrina e jurisprudência constitucional da Alemanha, inclusive no âmbito da jurisprudência do STF, a utilização da proporcionalidade como parâmetro do controle material da constitucionalidade de medidas restritivas de direitos fundamentais foi cada vez mais difundido, em que pese – há que anotar – as críticas assacadas contra uma ainda presente confusão e uso assistemático das categorias da razoabilidade e da proporcionalidade como se fungíveis fossem, ademais da objeção de um frequente manejo superficial e voluntarista de ambas as técnicas.

De todo modo, retornando ao caso do compartilhamento de dados com o IBGE, anota-se que o STF, mediante recurso à proporcionalidade, considerou que a medida provisória que determinou o compartilhamento de dados não cumpriu suficientemente as exigências de adequação e necessidade, as duas das três etapas (critérios e exigências) do teste de proporcionalidade, que inclui, além das duas já mencionadas, a assim chamada proporcionalidade em sentido estrito. Primeiramente, a medida foi considerada *inadequada* pela Corte em virtude da imprecisão do conceito de "produção de estatística oficial". A ausência de definição apropriada da finalidade e do modo de utilização dos dados impediria um exame acerca da *correspondência entre a coleta e a finalidade pretendida*, violando, pois, o devido processo legal – entendido na dimensão substantiva.

Da mesma maneira, a restrição foi considerada *desnecessária*, por não prever qualquer mecanismo de proteção contra o tratamento indevido de dados – como acessos não autorizados, vazamentos ou emprego diverso do estabelecido –, bem como não assegurar o anonimato das informações coletadas, a medida provisória desrespeitaria o *mandamento da intervenção menos gravosa*. Isso ocorre, também, segundo a Corte, pela previsão de armazenamento dos dados por trinta dias após a decretação do fim da situação de emergência de saúde pública (art. 4º, parágrafo único), tempo manifestamente excedente ao estritamente necessário para o atendimento da sua finalidade declarada, de modo que a medida viola de modo excessivo o direito à proteção de dados pessoais.

A *proporcionalidade em sentido estrito*, terceiro nível do teste de proporcionalidade na tradição germânica (Alexy, 2009), sequer acabou sendo examinada, porquanto a inexistência de definição precisa da finalidade pretendida com a medida (compartilhamento de dados) e a extensão da restrição ao direito fundamental à proteção de dados pessoais foram suficientes para a formação do entendimento de que inexistia interesse público legítimo no compartilhamento dos dados pessoais dos usuários dos serviços de telefonia. A Corte entendeu que a medida era inadequada e desnecessária e, portanto, inconstitucional.

Muito embora a decisão tenha sido amplamente aplaudida, em especial no que toca ao reconhecimento em si de um direito fundamental autônomo à proteção de dados pessoais, não faltou quem tivesse lançado um olhar crítico, como foi o caso de Ivar Hartmann, que focou especialmente no fato de que existiria um déficit de compreensão dos juristas, e que acabou repercutindo na decisão

do STF, posto que, para fins estatísticos, a amostra gerada é muito pequena e que apenas a partir do conhecimento de determinadas características do universo dos cerca de cem milhões de pessoas naturais e jurídicas, o IBGE poderia tomar decisão segura sobre o tamanho adequado da amostra e/ou seus diferentes estratos (Hartmann, 2020).

Seja como for, o fato é que independentemente de eventuais críticas (ainda que fundadas em boas razões) que possam ser endereçadas à decisão do STF na ADI 6387/2020, sublinha-se que, nos termos do voto da Ministra Rosa Weber, a Corte assentou que a urgência decorrente da crise social e sanitária causada pela pandemia de Covid-19 e a necessidade de utilização de dados específicos para a elaboração de políticas públicas não podem ser invocadas como pretextos para justificar o enfraquecimento de direitos e garantias fundamentais. Isto é, embora a formulação de políticas públicas demande dados específicos para o desenho de formas de enfrentamento à emergência, o poder público deve garantir o tratamento adequado e seguro dos dados compartilhados.

Dessa forma, verifica-se que o STF assentou que o Governo Federal descumpriu os seus *deveres de proteção* com relação aos dados pessoais na elaboração e execução de políticas públicas. Ainda que a forma como o Estado assume os seus deveres de proteção e os efetiva esteja, em princípio, dentro do espectro de definição política – considerando as diferentes alternativas de ação, a limitação dos meios disponíveis, os interesses colidentes e a necessidade de estabelecer prioridades (Sarlet, I., 2020) –, motivo pelo qual é difícil falar de um dever específico de agir, é certo que há um dever de adotar medidas impeditivas de agressão (Canotilho, 2023) ao direito à proteção de dados.

Sem adentrar aqui o exame mais detalhado deste tema, importa destacar que o reconhecimento de deveres de proteção atribui ao Estado a obrigação juridicamente vinculante de zelar, inclusive de forma preventiva, contra agressões provindas de particulares, dos próprios órgãos públicos e até mesmo de outros Estados (Sarlet, I., 2021). Trata-se de uma exigência de maximização da eficácia dos direitos fundamentais decorrente de sua função como imperativos de tutela (Canaris, 2003). Essa incumbência de proteção efetiva do direito fundamental, por sua vez, desemboca na obrigação de o Estado adotar medidas positivas da mais diversa natureza, inclusive organizacional e procedimental, a fim de evitar os riscos de uma redução do significado de seu conteúdo material (Sarlet, I., 2021).

Portanto, ainda que a coleta e o tratamento dados sejam necessários à garantia de outros direitos fundamentais, é dever do Estado assegurar mecanismos de proteção e segurança, bem como limitar o tratamento e o compartilhamento ao mínimo necessário e em observância à estrita a finalidade informada.

Isso, contudo, não quer dizer que exista um necessário e permanente conflito entre o direito fundamental e correspondente dever estatal de proteção dos dados pessoais e a realização, pelo poder público, do seu dever de, mediante políticas públicas adequadas e eficazes, proteger e mesmo promover o direito à saúde, fixando-nos no aqui no foco do presente texto. Pelo contrário, não se trata de uma equação à feição da proteção de dados pessoais vs. o direito fundamental à saúde,

mas sim, de uma relação de convivência que, embora não imune a tensões, não apenas é conciliável, como também pode resultar no fortalecimento constitucionalmente adequado do recurso a dados pessoais para uma inteligente e bem-informada formatação de políticas públicas, não só, mas também na área da saúde.

Considerações finais

No paradigma do Estado Democrático de Direito, o papel da Constituição ultrapassa o de mero freio à vontade das maiorias, uma vez que passa a estabelecer um modo de a sociedade ser transformada a partir do Direito, com a incorporação das promessas incumpridas da modernidade (Streck, 2020). Tal compromisso é representado no artigo 3º da Constituição que, ao reconhecer as desigualdades, estabelece o núcleo político essencial para a construção de um Estado Social, a partir de vinculações para concretização dos direitos prestacionais e proibição de retrocesso social (Streck, 2011).

Na ordem jurídico-constitucional brasileira, o direito à saúde representa um dos pilares desse núcleo político, porquanto se traduz em elemento central para a proteção da vida, da dignidade humana e mesmo de condição de possibilidade para o exercício dos demais direitos fundamentais e viabilização de um desenvolvimento sustentável. De outra parte, trata-se de um direito fundamental marcado por uma forte relação de interdependência com outros bens e direitos fundamentais (Sarlet, 2021), apresentando, nas palavras de João Loureiro, "zonas de sobreposição com esferas que são autonomamente protegidas" (2006), como é o caso da vida, integridade física e psíquica, privacidade, educação, ambiente, moradia, alimentação, trabalho, dentre outras. Isto é, a saúde constitui uma pré-condição para o exercício de uma série de direitos fundamentais, assumindo a condição de um verdadeiro direito a ter direitos (Sarlet, 2021).

Portanto, dada a importância e sensibilidade do direito à saúde, a demarcação dos *limites* – e, sobretudo, dos *limites dos limites* – à atuação do Estado na elaboração e execução de políticas públicas deve ser realizada com muita cautela, na medida em que exerce papel central na sua concretização.

De outro lado, não se pode menosprezar os impactos decorrentes da digitalização das condições de vida e da estrutura social e, em especial, do incremento do emprego das Tecnologias de Informação e Comunicação na sociedade atual. Os riscos decorrentes de uma forma de governança baseada nos dados crescem com as novas possibilidades advindas do processamento eletrônico de informações por algoritmos e sistemas de inteligência, demandando novas respostas do Direito.

Assim, diante das novas formas de violação da personalidade e da tendência de agravamento das desigualdades promovida pela inteligência artificial, o Direito, para além de controlar as opções das políticas públicas, não poderá "ficar alheio às mudanças sociais e económicas que a IA tenderá a provocar, devendo surgir como nivelador e garantidor das diferentes variações e desenvolvimentos da dignidade da pessoa humana" (Pedro, 2023). Em outras palavras, uma vez que esse conjunto de

informações pessoais é a matéria prima de novas formas de controle social, a proteção de dados passa a ser a proteção da pessoa humana (Sarlet, G.; Caldeira, 2019).

Em razão dessas exigências, o direito à proteção dos dados pessoais ganha autonomia frente ao direito à intimidade e à vida privada, assegurando posições jurídicas subjetivas e objetivas próprias. Além disso, o direito à proteção de dados pessoais exige deveres de proteção, no sentido de que o Estado deve zelar preventivamente pela sua efetividade, promovendo medidas contra agressões de particulares e dos próprios poderes públicos.

No caso específico das políticas públicas de saúde, conforme decidiu o Supremo Tribunal Federal no Caso IBGE, as restrições ao direito à proteção de dados pessoais devem passar pelo crivo da proporcionalidade. Isto é, ainda que os dados pessoais sejam indispensáveis à elaboração e execução de políticas públicas de saúde, o manejo dessas informações deve guardar estrita relação com a finalidade da medida e limitar-se ao mínimo necessário. Caso contrário, a proteção será insuficiente e a medida será inconstitucional.

Assim, ao estabelecer a imposição de condições ao tratamento de dados pessoais pelo poder público para planejamento e execução de políticas públicas, uma Suprema Corte não estará, apenas por isso, inibindo e limitando o direito à proteção da saúde. Muito pelo contrário, o respeito às condições constitucionais e legais, ao passo que garante a efetividade de outros direitos fundamentais – como a dignidade humana, a autodeterminação informativa e o livre desenvolvimento da personalidade –, assegura a utilização exclusiva desses dados na elaboração de políticas públicas e, consequentemente, a tutela da saúde, em suas variadas dimensões.

Logo, considerando que a Constituição é limite e condição de possibilidade em um regime democrático, políticas públicas que envolvam a restrição de direitos fundamentais devem passar por um filtro de constitucionalidade, como forma de resguardar os interesses envolvidos. Assim, uma interpretação constitucionalmente adequada dos limites à atuação do Estado na elaboração e execução de políticas públicas de saúde não pode prescindir do diálogo e da interação com outros princípios e direitos fundamentais, que auxiliam a determinar o seu âmbito de proteção, inclusive mediante o estabelecimento de limites diretos e indiretos (Sarlet, I.; Sarlet, G., 2023). No caso do compartilhamento de dados com o poder público, sem qualquer pretensão de esgotamento do tema, isso se passa pela garantia de mecanismos de proteção e segurança, bem como pela limitação do tratamento ao mínimo necessário e em observância à estrita a finalidade informada.

REFERÊNCIAS

ALEXY, Robert; tradução: Virgílio Afonso da Silva. Teoria dos direitos fundamentais. 1. ed. 3. tir. São Paulo: Malheiros Editores LTDA., 2009.

BIONI, Bruno Ricardo. **Proteção de dados pessoais**: a função e os limites do consentimento. 2. ed. Rio de Janeiro: Forense, 2020.

BOFFETTA, P.; COLLATUZZO, G. Application of P4 (Predictive, Preventive, Personalized, Participatory) Approach to Occupational Medicine. **La Medicina del Lavoro | Work, Environment and Health**, [S. l.], v. 113, n. 1, 2022. DOI: https://doi.org/10.23749/mdl.v113i1.12622. Disponível em: https://www.mattioli1885journals.com/index.php/lamedicinadellavoro/article/view/12622. Acesso em: 9 maio 2023.

BRASIL. [Constituição (1988)]. Constituição da República Federativa do Brasil de 1988. **Diário Oficial da União**: seção 1, Brasília, DF, n. 191-A, p. 1, 5 out. 1988. Legislação Informatizada – Constituição de 1988 – Publicação Original. Disponível em: w2.camara.leg.br/legin/fed/consti/1988/constituicao-1988-5-outubro-1988-322142-publicacaooriginal-1-pl.html.

BRASIL. Supremo Tribunal Federal, **Ação Direta de Inconstitucionalidade nº 6.387/DF**, Relatora Ministra Rosa Weber, Decisão Monocrática 24/04/2020. Decisão do Plenário da Corte: 07/05/2020.

CAMPOS, Ricardo; XAVIER, Carolina. eHealth: apontamentos sobre a centralidade dos dados pessoais. **Revista de Direito da Saúde Comparado**, São Paulo, v. 1 ed. 1, p. 82-97, dez. 2022. Disponível em: https://revistas.unisa.br/index.php/direitosaude/article/view/394. Acesso em: 09 maio 2023.

CANARIS, Claus-Wilhelm; tradução: Ingo Wolfgang Sarlet; Paulo Mota Pinto. **Direitos fundamentais e direito privado**. Coimbra: Alamedina, 2003.

CASOS de coronavírus e número de mortes no Brasil em 17 de abril. Bem-Estar. G1. Globo.com. Disponível em: https://g1.globo.com/bemestar/coronavirus/noticia/2020/04/17/casos-de-coronavirus-e-numero-de-mortes-no-brasil-em-17-de-abril.ghtml. Acesso em: 20 fev. 2024.

CASTELLS, Manuel; tradução: Roneide Venâncio Majer. **A Era da Informação**: economia, sociedade e cultura. Volume I. 3. Ed. São Paulo: Paz e Terra, 1999.

CELESTE, Edoardo. Constitucionalismo digital: mapeando a resposta constitucional aos desafios da tecnologia digital. **Revista Brasileira de Direitos Fundamentais & Justiça**, v. 15, n. 45, p. 63–91, 2021.

COMISSÃO EUROPEIA. **Proposta da Comissão Europeia para harmonização dos regulamentos sobre inteligência artificial**. COM(2021) 206 final. Artigo 3º, nº 1. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:52021PC0206. Acesso em: 27 ago. 2023.

CRARY, Jonathan; Tradução: Humberto do Amaral. **Terra arrasada**: além da era digital, rumo a um mondo pós-capitalista. São Paulo: Ubu Editora, 2023.

DONEDA, Danilo. **Da Privacidade à Proteção de Dados Pessoais** [livro eletrônico]. 2. ed. São Paulo: Thomson Reuters Brasil, 2021.

FERRAZ JÚNIOR, T. S. Sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do Estado. **Revista da Faculdade de Direito**, Universidade de São Paulo, [S. l.], v. 88, p. 439-459, 1993. Disponível em: https://www.revistas.usp.br/rfdusp/article/view/67231. Acesso em: 9 set. 2023.

FOUCAULT, Michel. **Vigiar e punir**: história da violência nas prisões. 7 ed. Editora Vozes: 1989.

HAN, Byung-Chul; tradução: Gabriel S. Philipson. **Infocracia**: digitalização e crise da democracia. Petrópolis, RJ: Vozes, p. 7, 2022.

HARTMANN, Ivar. Suspensão do repasse de dados ao IBGE é boa e má notícia, analisa Ivar A. Hartmann. **Poder 360**. 2020. Disponível em: https://www.poder360.com.br/opiniao/suspensao-do-repasse-de-dados-ao-ibge-e-boa-e-ma-noticia-analisa-ivar-a-hartmann/. Acesso em: 27 abr. 2024.

HOFFMANN-RIEM, W. BIG DATA E INTELIGÊNCIA ARTIFICIAL: desafios para o Direito. **REI - REVISTA ESTUDOS INSTITUCIONAIS**, [S. l.], v. 6, n. 2, p. 431–506, 2020. DOI: 10.21783/rei.v6i2.484. Disponível em: https://www.estudosinstitucionais.com/REI/article/view/484. Acesso em: 2 set. 2023.

KARG, Moritz. Artikel 4, Nr. 1. *In*: SIMITIS, Spiros; HORNUNG, Gerrit; SPIECKER GENANNT DÖHMANN, Indra. **Datenschutzgesetz**. Baden-Baden: Nomos, p. 287-290, 2019.

LOUREIRO, João. Direito à (protecção da) saúde. *In*: **Estudos em Homenagem ao Professor Doutor Marcello Caetano**, Coimbra: Coimbra Editora, 2006.

MENDES, Gilmar Ferreira; FERNANDES, Victor. Constitucionalismo digital e jurisdição constitucional: uma agenda de pesquisa para o caso brasileiro. **Revista Brasileira de Direito**, v. 16, n. 1, p. 1-33, 2020. DOI: https://doi.org/10.18256/2238-0604.2020.v16i1.4103.

NICOLELIS, Miguel. **O verdadeiro criador de tudo**: Como o cérebro humano esculpiu o universo como nós o conhecemos. São Paulo: Planeta, 2020.

PEDRO, Ricardo. Inteligência artificial, políticas públicas e direito público: apontamentos introdutórios e exploratórios no contexto português. *In*: SARLET, Gabrielle Bezerra Sales *et al*. (coord**.). Inteligência Artificial e Direito**. Porto Alegre: Editora Fundação Fênix, 2023. DOI: https://doi.org/10.36592/9786554600200. Disponível em: https://www.fundarfenix.com.br/ebook/206iaedireito. Acesso em: 11 maio 2023.

RUARO, Regina Linden; RODRIGUEZ, Daniel Piñeiro. O direito à proteção de dados pessoais na sociedade de informação. **Direito, Estado Sociedade**, n. 36, jan.-jun. 2010.

RODOTÀ, Stefano. **A vida na sociedade de vigilância**: a privacidade hoje. Organização, seleção e apresentação de Maria Celina Bodin de Moraes. Rio de Janeiro: Renovar, 2008.

SAAVEDRA, Giovani; BORGES, Gabriel. Constitucionalismo digital brasileiro. **Revista da Ajuris**, v. 49, n. 152, p. 157-180, 2022.

SARLET, Gabrielle Bezerra Sales; FERNANDES, Márcia Santana; RUARO, Regina Linden. A proteção de dados no setor de saúde em face do sistema normativo brasileiro atual. *In*: DONEDA, Danilo *et al*. (org.). **Tratado de proteção de dados pessoais**. 2. Ed. Rio de Janeiro: Forense, p. 487-512, 2023.

SARLET, Ingo Wolfgang. **A eficácia dos direitos fundamentais**: uma teoria geral dos direitos fundamentais na perspectiva constitucional. 13. ed. rev. e atual. 2. tir. Porto Alegre: Livraria do advogado, 2021.

SARLET, Ingo Wolfgang. Proteção de dados pessoais como Direito Fundamental Na Constituição Federal Brasileira de 1988: Contributo Para A Construção De Uma Dogmática Constitucionalmente Adequada. **Revista Brasileira de Direitos Fundamentais & Justiça**, [S. l.], v. 14, n. 42, p. 179–218, 2020. DOI: 10.30899/dfj.v14i42.875. Disponível em: https://dfj.emnuvens.com.br/dfj/article/view/875. Acesso em: 14 out. 2023.

SARLET, Ingo Wolfgang; FIGUEIREDO, Mariana Filchtiner. Art. 196. *In*: CANOTILHO, J. J. Gomes; SARLET, Ingo Wolfgang; STRECK, Lenio Luiz; MENDES, Gilmar Ferreira. **Comentários à Constituição do Brasil**. 2. Ed. São Paulo: Saraiva Educação, p. 2012-2018, 2018.

SARLET, Ingo Wolfgang; SARLET, Gabrielle Bezerra Sales. *In*: SARLET, Gabrielle Bezerra Sales *et al*. (coord.). **Inteligência Artificial e Direito.** Porto Alegre: Editora Fundação Fênix, 2023. DOI: https://doi.org/10.36592/9786554600200. Disponível em: https://www.fundarfenix.com.br/ebook/206iaedireito. Acesso em: 11 maio 2023.

SARLET, G.; SARLET, Gabrielle Bezerra SalesMOLINARO, Carlos Alberto. A. Questões tecnológicas, éticas e normativas da proteção de dados pessoais na área da saúde em um contexto de big data. **Revista Brasileira de Direitos Fundamentais & Justiça**, [S. l.], v. 13, n. 41, p. 183–212, 2020. DOI: 10.30899/dfj.v13i41.811. Disponível em: https://dfj.emnuvens.com.br/dfj/article/view/811. Acesso em: 4 set. 2023.

SARLET, G.; SARLET, Gabrielle Bezerra SalesCALDEIRA, Cristina. O consentimento informado e a proteção de dados pessoais de saúde na internet: uma análise das experiências legislativas de Portugal e do Brasil para a proteção integral da pessoa humana. **civilistica.com**, v. 8, n. 1, p. 1-27, 29 abr. 2019. Disponível em: https://civilistica.emnuvens.com.br/redc/article/view/411. Acesso em: 09 maio 2023.

STRECK, Lenio Luiz. **Dicionário de Hermenêutica**: 50 verbetes fundamentais da Teoria do Direito à luz da Crítica Hermenêutica do Direito. 2. ed. Belo Horizonte: Casa do Direito, 2020.

STRECK, Lenio Luiz. **Verdade e consenso**: constituição, hermenêutica e teorias discursivas. 4. ed. São Paulo: Saraiva, 2011.

TEIXEIRA, Pedro S. **IA não é inteligência e sim marketing para explorar trabalho humano, diz Nicolelis**. Folha de São Paulo, 8 jul. 2023. Disponível em: https://www1.folha.uol.com.br/tec/2023/07/ia-nao-e-inteligencia-e-sim-marketing-para-explorar-trabalho-humano-diz-nicolelis.shtml. Acesso em: 26 ago. 2023.

TRINDADE, André Karam; ANTONELO, Amanda. Constitucionalismo digital: um convidado (in)esperado. **Revista Brasileira de Direito**, Passo Fundo, v. 18, n. 1, p. e4816, maio 2023. ISSN 2238-0604. Disponível em: https://seer.atitus.edu.br/index.php/revistadedireito/article/view/4816. Acesso em: 11 set. 2023. DOI: https://doi.org/10.18256/2238-0604.2022.v18i1.4816.

VALIM, Rafael. Estado de Exceção: a forma jurídica do neoliberalismo. São Paulo: Editora Contracorrente, 2017.

WARREN, Samuel D.; BRANDEIS, Louis D. The Right to Privacy. **Harvard Law Review**, vol. 4, no. 5, pp. 193–220. JSTOR, 1890. Disponível em: https://www.jstor.org/stable/1321160. Acesso em: 17 out. 2023.