UNIVERSIDADE FEDERAL DO RIO GRANDE DO SUL
FACULDADE DE DIREITO
PROGRAMA DE PÓS-GRADUAÇÃO EM DIREITO

Diego Dalbem Ribas Leal

SOCIEDADE DA INFORMAÇÃO E PROTEÇÃO DE DADOS NO ÂMBITO DA SAÚDE: um direito fundamental

Porto Alegre
2021

Diego Dalbem Ribas Leal

SOCIEDADE DA INFORMAÇÃO E PROTEÇÃO DE DADOS NO ÂMBITO DA SAÚDE: um direito fundamental

Dissertação apresentada ao Programa de Pós-Graduação em Direito da Universidade Federal do Rio Grande do Sul, na linha de pesquisa “Fundamentos da Integração Jurídica”, como requisito parcial para a obtenção do título de Mestre.

Orientador: Prof. Dr. Marcelo Schenk Duque

Porto Alegre

2021

Diego Dalbem Ribas Leal

SOCIEDADE DA INFORMAÇÃO E PROTEÇÃO DE DADOS NO ÂMBITO DA SAÚDE: um direito fundamental

Dissertação apresentada ao Programa de Pós-Graduação em Direito da Universidade Federal do Rio Grande do Sul, na linha de pesquisa “Fundamentos da Integração Jurídica”, como requisito parcial para a obtenção do título de Mestre.

Aprovada em 23 de agosto de 2021.

BANCA EXAMINADORA:

_____

Prof. Dr. Marcelo Schenk Duque

Orientador

_____

Profa. Dra. Caroline Vaz

_____

Prof. Dr. Fabiano Menke

_____

Profa. Dra. Daniela Copetti Cravo

AGRADECIMENTOS

Primeiramente agradeço à minha mãe, pelo amor incondicional e apoio em todos os momentos. Não menos importantes foram algumas pessoas, as quais mencionarei, que se tornaram extremamente imprescindíveis ao longo desta trajetória. Menciono então meu estimado orientador, Prof. Dr. Marcelo Schenk Duque, que, sem sombra de dúvida, com sua excelência e firmeza de caráter, tornou possível tal projeto; agradeço ao CDEA – Centro de Estudos Europeus e Alemães pelo suporte e projeto viabilizador de tal trabalho. Cumpre destacar o meu sincero agradecimento à equipe de colegas do PPGD da UFRGS, sempre solícitos e amigos, em especial em nome da colega Rosemari de Azevedo.

Por fim, mas não menos importante, meu profundo agradecimento à Profa. Dra. Claudia Lima Marques, Diretora da Faculdade de Direito da UFRGS, por absolutamente tudo.

Peço escusas por alguma falta que certamente haverá.

RESUMO

O presente trabalho tem por escopo analisar a proteção de dados, tema tão em voga atualmente, tanto no sistema jurídico brasileiro quanto no sistema jurídico alemão. Será abordada a questão dos dados sensíveis em matéria de saúde, direito fundamental à autodeterminação informativa, as novas tecnologias e seu impacto na proteção de dados. Falamos nesse sentir de "*big data*", inteligência artificial etc. Análise da legislação brasileira em matéria de proteção de dados, os riscos das novas tecnologias, assim como também, da mesma forma, será realizada uma análise comparativa no sistema jurídico alemão, de sorte que tenho certeza de que será possível chegar a resultados expressivos em avanços no que concerne ao tema ora apresentado.

Palavras-chave: Proteção de dados. Saúde. Autodeterminação informativa. Alemanha. Brasil.

ABSTRACT

The scope of this work is to analyze data protection, a topic that is currently in vogue, both in the Brazilian legal system and in the German legal system. The issue of sensitive data in health matters, the fundamental right to informational self-determination, innovative technologies and their impact on data protection will be addressed. We speak in this sense of “big data,” artificial intelligence etc. Analysis of Brazilian legislation on data protection, the risks of innovative technologies, as well as, similarly, a comparative analysis will be conducted in the German legal system. So I am sure we will be able to reach expressive results in advances regarding the topic presented here.

Keywords: Data protection. Health. Informative self-determination. Germany. Brazil.

SUMÁRIO

1 INTRODUÇÃO

Atualmente, há uma inconteste hipertrofia do ambiente digital/virtual. Na sociedade informacional, mediante o emprego sistemático das novas tecnologias, a compreensão acerca dos limites da vida privada tem se fragilizado, sobretudo em razão da infinidade de dados pessoais postados nas redes sociais e da produção irreflexiva de pegadas/rastros digitais.

Esse ambiente se constitui como um espaço compartilhado, ou seja, implica uma forma de participação instantânea; a segunda característica se refere à chamada "interface gráfica do usuário", pela qual se pode retratar o espaço visualmente a partir de vários estilos de imersão; a terceira é a imediatidade e, assim, as interações ocorrem em tempo real; como quarta característica apresenta-se a interatividade, que permite aos usuários alterarem, desenvolverem, construírem ou tornarem o conteúdo personalizado; a quinta é a persistência, uma vez que nesse ambiente, mesmo que o indivíduo não esteja conectado, suas informações seguem existindo; como sexta característica, apresenta-se a socialização participativa como estimulante do agrupamento de grupos sociais e de reivindicações comuns; por fim, agrega-se mais um atributo absolutamente indispensável, que se refere ao armazenamento em espaços, denominado comumente de "nuvem", e ao incremento no tratamento de dados fruto do alargado emprego de algoritmos e da Inteligência Artificial, bem como de *Big Data*[1].

É nesse ambiente, também chamado de meio ambiente digital/virtual, que se inserem os dados pessoais coletados, produzidos e transferidos pelos indivíduos. Dito de outro modo, trata-se de um ambiente permeado pela volatilidade, pela incerteza, pela complexidade e pela ambiguidade, devendo-se ressaltar que os dados pessoais, em suma, consubstanciam a vida das pessoas humanas atualmente.

Relevante ainda mencionar o padrão atual de crescente emprego do *Big Data* que, em rigor, persiste ainda como uma espécie de ponto cego no sistema protetivo,

[1] RUARO, Regina Linden; SARLET, Gabrielle Bezerra Sales. O direito fundamental à proteção de dados sensíveis no sistema normative brasileiro: uma análise acerca das hipóteses de tratamento e da obrigatoriedade do consentimento livre, esclarecido e informado sob o enfoque da Lei Geral de Proteção de Dados (LGPD). *In*: MENDES, Laura Schertel; DONEDA, Danilo; SARLET, Ingo Wolfgang; RODRIGUES JUNIOR, Otavio Luiz (org.). *Tratado de Proteção de dados pessoais*. Rio de Janeiro: Forense, 2021. p. 177-198.

ou seja, no mosaico legal brasileiro, apesar da nova legislação em vigor. *Big Data,* não custa rememorar, é um conceito primordial na atual conjuntura. Consiste, em suma, em um bloco algorítmico emulado para o tratamento de grandes quantidades de dados, que visa a reconhecer padrões e obter novas percepções a partir deles, caracterizando-se pela abundância, pela diversidade de dados e pela rapidez com que são coletados, analisados e reintroduzidos no sistema[2].

Oportuno afirmar que, em razão dos riscos, da irreversibilidade e, em particular, do grau de vulnerabilização das pessoas, torna-se essencial a proposição de parâmetros jurídicos com o intuito de garantir a coexistência da eficácia dos direitos humanos e fundamentais [3] constitucionalmente consagrados, compatibilizando-os entre si, uma vez que resultaram de um longo processo histórico para a sua afirmação, recaindo assim um novo enfoque sobre os dados pessoais.

Diante do exposto, o presente estudo tem dentre os seus objetivos analisar os fenômenos inerentes à proteção de dados, em especial dados sensíveis.

Importante salientar que, quando da escolha pelo tema do trabalho, em momento algum imaginou-se que ele seria feito em tempos tão “estranhos”, o que devido à atual situação da saúde mundial, torna-o de todo relevante, de forma que o aprofundamento de assuntos tão atuais e extremamente importantes no contexto presente se faz necessário de forma acurada e abrangente. Serão abordadas a conceituação de dados sensíveis, a autodeterminação informativa como direito fundamental, uma análise legislativa e principalmente a eficácia da proteção de dados.

Dando seguimento ao explanado, como objetivo central, pretende-se demonstrar a importância dos temas propostos em direito comparado, especificamente o direito alemão, tão caro como fonte de pesquisa ao ordenamento jurídico brasileiro. Sabe-se que o direito alemão, especialmente em decorrência dos acontecimentos históricos, procurou fornecer e curar de maneira bastante ampla os direitos fundamentais. No presente trabalho, terá especial atenção, por todos os

---

[2] MOLINARO, Carlos Alberto; SARLET, Gabrielle Bezerra Sales. 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, a. 13, n. 41, p. 183-212, jul./dez. 2019. p. 188.

[3] SARLET, Ingo Wolfgang. *A eficácia dos direitos fundamentais*. 12. ed. Porto Alegre: Livraria do Advogado, 2017. p. 405-406.

motivos mencionados, mais aqueles que são de conhecimento de todos, especialmente por ser um assunto extremamente polêmico.

Como objetivos secundários, mas não menos relevantes, o estudo almeja fornecer aos leitores embasamento das mazelas existentes em se tratando da proteção de dados no âmbito da saúde. Far-se-á necessário, devido à amplitude que o assunto possui, delimitar e decifrar os meandros do sistema de saúde no Brasil e na Alemanha. Com efeito, serão trazidas à baila a efetividade dos sistemas jurídicos alemão e brasileiro, comtemplando soluções à problemática existente em planos de saúde, laboratórios, hospitais etc.

O tema é de todo instigante, especialmente em tempos de pandemia. A pesquisa será realizada por intermédio do método dedutivo, utilizando-se de pesquisa bibliográfica e doutrinária. Realizar um estudo de direito comparado é realmente fascinante, ainda mais quando o ordenamento a ser estudado é deveras mais rico e eficiente, a servir de exemplo ao ordenamento pátrio.

Pretende-se oportunizar àqueles que se propuserem a ler o trabalho formar juízo de valor sobre a pesquisa deflagrada, a fim de enriquecer de alguma forma o conhecimento acerca do tema.

2 DADOS SENSÍVEIS EM MATÉRIA DE SAÚDE

Segundo as definições da Lei Geral de Proteção de Dados (LGPD), dado pessoal é “informação relacionada a pessoa natural identificada ou identificável” (art. 5º, I) e dado sensível é:

> Dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente a saúde ou a vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural (art. 5º, II).

Observa-se, assim, que o dado sensível é um tipo de dado pessoal, ou seja, todo dado sensível é pessoal, mas nem todo dado pessoal é sensível.

A marca característica do dado pessoal, em geral, é a identificabilidade da pessoa natural a que ele se refere, ou seja, o dado é considerado pessoal não somente se ele próprio servir a identificar o seu titular (por exemplo, o nome ou o número do CPF), mas também se, a partir da integração com outras informações, essa identificação for possível (por exemplo, o endereço ou o *Internet Protocol* – IP, o número que identifica o computador na rede). Sob esse conceito amplo de dado pessoal,

> Há dado pessoal não apenas quando houver a presença de identificadores diretos ou indiretos que diferem precisamente um indivíduo. Os dados que potencialmente conduzem à individuação da pessoa são igualmente tomados como informação pessoal.[4]

Assim, o dado pessoal contrapõe-se ao dado anonimizado, que é o “dado relativo a um titular que não pode ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento” (LGPD, art. 5º, III). Essa contraposição, todavia, vem sendo destacada pela doutrina como menos rigorosa do que pode parecer à primeira vista: “uma divisão binária e

[4] MACHADO, Diego; DONEDA, Danilo. Proteção de dados pessoais e criptografia: tecnologias criptográficas entre anonimização e pseudonimização de dados. *Revista dos Tribunais*, São Paulo, v. 998, dez. 2018.

estanque entre dado pessoal e dado anônimo e dos seus diversos perfis normativos não é mais critério seguro para garantir a privacidade dos titulares de dados".[5] Diversas falhas vêm sendo reveladas em técnicas de anonimização que até há poucos anos eram reputadas confiáveis[6], o que conduz à constatação de que a capacidade efetiva de desidentificar a informação é contingente ao avanço da tecnologia daquela época. Por essa razão, durante o trâmite do projeto de lei na câmara, a redação do dispositivo foi modificada para fazer referência a técnicas razoáveis, ante a constatação de que a anonimização perfeita é impossível.

Outro meio utilizado para impedir a identificação do titular do dado é a pseudonimização, que é "o tratamento por meio do qual um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo, senão pelo uso de informação adicional mantida separadamente pelo controlador em ambiente controlado e seguro" (LGPD, art. 13, § 4º). Assim, o titular do dado pseudonimizado só não é identificável por conta da separação entre ele e outra informação que levaria à identificação, razão pela qual Machado e Doneda defendem que, embora continue a ser reputada informação pessoal, pode se submeter a um regime jurídico modulado ou particularizado.[7]

Já no que tange à sensibilidade do dado, o legislador optou por uma conceituação exemplificativa, fazendo referência a informações de caráter racial, étnico, político, sindical, religioso, filosófico, sexual, de saúde, genético ou biométrico. Aponta-se que aqui também transparece novamente a influência da legislação europeia (GDPR) que, apesar de não utilizar expressamente a

---

[5] VIOLA, Mario; DONEDA, Danilo; ANDRADE, Norberto Nuno Gomes de. Dados Anônimos e tratamento de dados para finalidades distintas: a proteção de dados pessoais sob uma ótica civil-constitucional. *In*: TEPEDINO, Gustavo; FACHIN, Luiz Edson (org.). *Pensamento Crítico do direito civil brasileiro*. Curitiba: Juruá, 2011. p. 197-214. p. 198.

[6] MACHADO, Diego; DONEDA, Danilo. Proteção de dados pessoais e criptografia: tecnologias criptográficas entre anonimização e pseudonimização de dados. *Revista dos Tribunais*, São Paulo, v. 998, dez. 2018.

[7] "Muito embora com certa clareza seja reputado informação pessoal no GDPR, o dado pseudonimizado pode se submeter a um regime jurídico modulado ou particularizado, em linha de sintonia com esse mesmo estatuto: abrem-se portas para o tratamento de informações com finalidade diversa da original e não lastreada em consentimento expresso do titular dos dados, desde que o propósito ulterior seja compatível com o inicialmente consentido (GDPR, art. 6, 4, e). Semelhante raciocínio pode ter arrimo no sistema jurídico brasileiro a partir da previsão legal do art. 9, §2, da LGPD" (MACHADO, Diego; DONEDA, Danilo. Proteção de dados pessoais e criptografia: tecnologias criptográficas entre anonimização e pseudonimização de dados. *Revista dos Tribunais*, São Paulo, v. 998, dez. 2018.).

terminologia, define da mesma forma os dados submetidos à seção “Tratamento de categorias especiais de dados pessoais”.[8]

Comparando o regime imposto pela Lei 13.709/2018 ao tratamento dos dados pessoais em geral (art. 7º e ss.) com aquele imposto ao tratamento dos dados pessoais sensíveis (art. 11 e ss.), observa-se a repetição de diversas regras comuns. Em ambos o legislador estipulou o consentimento como base primordial para justificar qualquer tratamento de dados, mas especificou ainda outros interesses legítimos que autorizam o tratamento de dados mesmo sem o consentimento do titular[9]. Entre eles está justificado o tratamento de dados (sensíveis ou não) sem o consentimento de dados se ele servir: ao cumprimento de obrigação legal ou regulatória pelo controlador; ao tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos[10]; à realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis; ao exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral[11]; à proteção da vida ou da incolumidade física do titular ou de terceiro; e à tutela da saúde, em procedimento realizado por profissionais da área

[8] Art. 9, 1. “É proibido o tratamento de dados pessoais que revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas, ou a filiação sindical, bem como o tratamento de dados genéticos, dados biométricos para identificar uma pessoa de forma inequívoca, dados relativos à saúde ou dados relativos à vida sexual ou orientação sexual de uma pessoa”.

[9] A caracterização de “interesse legítimo” para fim de tratamento de dados não consentido vem sendo objeto de diversos estudos no âmbito da aplicação da GDPR, entre os quais se remete a AAVV. Parecer 06/2014 sobre o conceito de interesses legítimos do responsável pelo tratamento de dados na acepção do artigo 7 da Diretiva 95/46/CE.

[10] Em crítica ao legislador, afirma Mulholland: “Contudo, a LGPD permite que haja tratamento de dados sensíveis sem a necessidade de fornecimento de consentimento do titular de dados, quando for indispensável para o tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos (art. 11, II, b, LGPD), além de outras hipóteses que se referem, em grande medida, a interesses públicos. Neste último caso, o consentimento do titular dos dados sensíveis, seja genérico, seja específico, ficaria dispensado em decorrência de uma ponderação de interesses realizada pela Lei, aprioristicamente, que considera mais relevantes e preponderantes os interesses de natureza pública frente aos interesses do titular, ainda que estes tenham qualidade de Direito Fundamental. No entanto, críticas devem ser feitas a este posicionamento legislativo, especialmente se considerarmos que a proteção do conteúdo dos dados pessoais sensíveis é fundamental para o pleno exercício de Direitos Fundamentais, tais como igualdade, liberdade e privacidade”. (MULHOLLAND, Caitlin Sampaio. Dados pessoais sensíveis e a tutela de direitos fundamentais: uma análise à luz da Lei geral de proteção de dados (Lei 13.709/2018). *Revista de Direitos e Garantias Fundamentais*, Vitória, v. 19, n. 3, p. 159-180, set./dez. 2018. p. 170. DOI: https://doi.org/10.18759/rdgf.v19i3.1603.)

[11] Como explica Frazão, “a proteção de dados pessoais não compromete o necessário direito que as partes têm de produzir provas umas contra as outras, ainda que estas se refiram a dados pessoais do adversário” (FRAZÃO, Ana. Nova LGPD: as demais hipóteses de tratamento de dados pessoais. *Jota*, 19 set. 2018. Disponível em: www.jota.info/opiniao-e-analise/colunas/constituicao-empresa-e-mercado/nova-lgpd-as-demais-hipoteses-de-tratamento-de-dados-pessoais-19092018. Acesso em: 10 out. 2020.).

da saúde ou por entidades sanitárias. Vale observar que o art. 7º, III, admite a ausência de consentimento também para tratamento de dados pessoais voltados à execução de políticas públicas respaldadas em contratos, convênios ou instrumentos congêneres, o que não foi reproduzido no art. 11, II, b, que prevê a dispensa de consentimento para tratamento de dados sensíveis voltados à execução de políticas públicas previstas apenas em leis ou regulamentos. Por outro lado, a comparação entre os dispositivos revela também algumas regras distintas. De plano, o tratamento de dados autorizado pelo "consentimento do titular" dá lugar à necessidade de "consentimento pelo titular, de forma específica e destacada, para finalidades específicas", ou seja, impondo restrição formal quanto ao consentimento. Também se afasta o tratamento de dados sensíveis sem o consentimento do titular "quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados"; quando necessário para atender aos interesses legítimos do controlador ou de terceiro"[12] ou "para a proteção do crédito", hipóteses permitidas para os dados não sensíveis no art. 7º, V, IX e X, respectivamente, e não reproduzidas no art. 11. Para o legislador, os interesses patrimoniais envolvidos nesses casos não justificaram o risco intrínseco ao tratamento de dados sensíveis ao titular.

A Lei ressalva, todavia, a possibilidade de tratamento de dados sensíveis, sem consentimento do titular, como medida de segurança do titular e prevenção de fraude, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, como ocorre frequentemente com a utilização de impressão digital e palmar no ambiente bancário. A possibilidade é limitada ao prevalecimento de direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais.

No tocante a dados sensíveis referentes à saúde do titular, a lei comina regras ainda mais específicas. É vedado o compartilhamento desses dados para fins econômicos, exceto quando a portabilidade for consentida pelo titular ou quando for necessária para a adequada prestação de serviços de saúde suplementar (LGPD,

[12] A hipótese, aplicável aos dados pessoais não sensíveis, é obscura, como observa Frazão: "Como se pode observar, a hipótese enseja um duplo desafio: (i)compreender o que pode ser considerado legítimo interesse do controlador ou de terceiro e (ii) avaliar em que medida esse legítimo interesse pode ser alegado diante dos direitos e liberdades fundamentais do titular" (FRAZÃO, Ana. Nova LGPD: as demais hipóteses de tratamento de dados pessoais. *Jota*, 19 set. 2018. Disponível em: www.jota.info/opiniao-e-analise/colunas/constituicao-empresa-e-mercado/nova-lgpd-as-demais-hipoteses-de-tratamento-de-dados-pessoais-19092018. Acesso em: 10 out. 2020.)

art. 11, § 4º). Essa última ressalva foi inserida pela Medida Provisória 869, de 2018 e, embora não haja menção a esse ponto específico em sua exposição de motivos, foi observado pela doutrina na ocasião que "o texto original da LGPD se mostrava restritivo e poderia resultar na precarização da prestação de certos serviços relacionados à saúde, como aqueles oferecidos por planos de saúde, hospitais e clínicas médicas".[13]

Os dados possuem um inestimado valor pois, por meio deles, torna-se viável a formação de perfis de comportamento, consumo e até mesmo sobre características genéticas. Assim como muitos outros, o setor de saúde é dependente de dados e análises para proporcionar serviços mais rápidos e melhores. É um dos setores que atravessa um momento de grande inovação e transformação digital, utilizando-se da Inteligência Artificial, *Big Data*, *Machine Learning*, plataformas em nuvem etc. Ao longo dos anos, antes mesmo de a LGPD sequer começar a ser debatida, foram editadas normas e instituídos critérios técnicos para o compartilhamento de dados nos sistemas de saúde vigentes no país, tais como o Sistema de Saúde Único (SUS), a Saúde Suplementar e a Saúde Privada. Isso porque, segundo Bonafé, "o compartilhamento de dados em saúde é essencial para reduzir os custos assistenciais, seja ao disponibilizar dados mínimos do paciente aos que integram a cadeia de assistência à saúde, seja para viabilizar um tratamento mais assertivo"[14].

O Ministério da Saúde instituiu regras para os Sistemas de Informação, por meio da Portaria de Consolidação n. 01, de 28 de setembro de 2017 ("Portaria"), com um capítulo específico regulamentando o uso de padrões, informações em saúde e de interoperabilidade entre os sistemas de informação do SUS, incluindo também os sistemas privados e de saúde suplementar, com objetivo de permitir o compartilhamento de informações em saúde e a cooperação de todos os profissionais e de estabelecimentos de saúde. Dentre os principais itens na instituição de sistemas de informação, foi instituída a criação e padronização de codificação de dados, de forma a tornar célere o acesso a informações relevantes e fidedignas ao usuário dos serviços de saúde. A referida Portaria também estabelece

---

[13] LEMOS, Ronaldo; DOUEK, Daniel; ADAMI, Mateus Piva; LANGENEGGER, Natalia; FRANCO, Sofia Lima. A criação da Autoridade Nacional de Proteção de Dados pela MP n 869/2018. *Jota*, 29 dez. 2018. Disponível em: www.jota.info/opiniao-e-analise/artigos/a-criacao-da-autoridade-nacional-de-protecao-de-dados-pela-mp-869-2018-29122018. Acesso em 05 dez. 2020.

[14] BONAFÉ, Lucas Alves da Silva *et. al*. *LGPD na Saúde*. 2019. *E-book*.

que o sistema de informação permitirá a identificação dos usuários das ações e serviços em todo o país (art. 230, parágrafo único).

Organizado por meio do Sistema Cartão Nacional de Saúde[15] que, dentre vários benefícios, permite (i) a apuração do perfil epidemiológico dos usuários de acordo com seu domicílio residencial; (ii) a possibilidade de o usuário ter acesso aos seus dados de forma unificada; e (iii) a garantia de que os dados pessoais dos usuários sejam tratados de forma a respeitar os princípios constitucionais da intimidade, da integralidade das informações e da confidencialidade.

Além disso, essas informações e dados dos usuários do SUS compõem uma base de dados que poderão ser compartilhados entre os entes federativos e demais órgãos que executem políticas públicas, desde que sejam respeitadas as normas de segurança da informação. O DATASUS é o responsável por administrar a Base de Dados e encarregado de proporcionar um sistema que possibilite a transferência de informações para outros sistemas utilizados pelo poder público, privado contratado e de saúde complementar[16]. A Portaria de Consolidação n. 01/2017 previu uma série de critérios e requisitos que devem ser cumpridos por todos os envolvidos na cadeia como, por exemplo, o nível de segurança mínimo que deve ser observado para possibilitar a transmissão de dados de saúde, o órgão responsável pelo armazenamento e a necessidade de individualização da responsabilização do agente público ou privado que teve acesso aos dados, no caso de uma possível infração.

De igual forma, a Agência Nacional de Saúde Suplementar (ANS)[17] também depende do compartilhamento de informações a fim de que os serviços ofertados pelas operadoras de planos privados de assistência à saúde possam ser prestados aos seus beneficiários. Assim, através da Resolução Normativa n. 305/2012, foram estabelecidos parâmetros para Troca de Informações na Saúde Suplementar (TISS), sendo um deles a composição do registro eletrônico dos dados de atenção à saúde entre as operadoras, prestadores de serviço de saúde, o beneficiário de plano privado de assistência à saúde e a própria ANS[18].

---

[15] Portaria de consolidação nº 1, de 28 de setembro de 2017, arts. 255 e 256.
[16] BONAFÉ, Lucas Alves da Silva *et. al*. *LGPD na Saúde*. 2019. *E-book*.
[17] Instituída pela Lei nº 9.961/200 com objetivo de normatizar, controlar e fiscalizar as atividades das operadoras de planos privados de assistência à saúde.
[18] Portaria de consolidação n. 1, de 28 de setembro de 2017, arts. 255 e 256.

Assim, é possível verificar que antes mesmo da edição da LGPD o setor da saúde, tanto público quanto privado, já era pautado pelos princípios constitucionais de privacidade e intimidade, inclusive tratando de níveis de segurança da informação e regulamentação de ferramentas de tecnologia da informação. Para Bonafé, o setor de saúde será fortemente impactado com as obrigações dispostas na LGPD, principalmente no tocante ao direito do usuário do sistema de receber informações sobre o uso de seus dados[19].

Ao tratar dos dados da pessoa com deficiência, ganha relevo a proteção de seus dados médicos, que se inserem dentro da espécie de dados pessoais[20] sensíveis definidos no art. 5º, I e II, da LGPD. Os dados médicos abrangem os referentes à saúde, à vida sexual, ao dado genético ou biométrico do paciente, informações cujo conteúdo apresenta mais riscos discriminatórios que a média, tanto para a pessoa como para a própria coletividade. Isso porque, caso sejam conhecidas e processadas essas informações, os pacientes ficam suscetíveis a condutas de exclusão[21], que podem comprometer inclusive o acesso à saúde no âmbito público e privado, seu afastamento de meios familiares, sociais e corporativos, entre outras situações, que podem afetar a sua imagem e personalidade, acarretando danos nas esferas extrapatrimonial e patrimonial.

Os dados pessoais, incluindo os dados médicos, são utilizados como um ativo econômico, por isso a falta de meios seguros de tratamento, proteção, guarda e custódia dos dados clínicos e genéticos dos pacientes tem possibilitado sua utilização sem filtros nas redes sociais. Além disso, propicia a comercialização dos dados, seja para pesquisas científicas[22], agências de emprego, planos de saúde e seguradoras, na maioria das vezes sem o devido consentimento livre e esclarecido do paciente.

Os pacientes com deficiência apresentam uma vulnerabilidade especial[23], e o uso indevido e sem autorização de seus dados médicos pode ter impactos ainda

---

[19] SALMEN, Caroline Salah; BELLÉ, Cathiane M. A Proteção de Dados Sensíveis e as Inovações da Área da Saúde. In: WACHOWICZ, Marcos (org.) *Proteção de Dados Pessoais em Perspectiva*: LGPD e RGDP na Ótica do Direito Comparado. Curitiba: Gedai, 2020. p. 242-270.

[20] Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, considerando 75.

[21] RODOTÀ, Stefano. *A vida na sociedade da vigilância*: A privacidade hoje. Rio de Janeiro: Renovar, 2008.

[22] A Resolução 466/2012 do CNS, que estabelece diretrizes e normas regulamentadoras de pesquisas envolvendo seres humanos trata da proteção dos dados dos participantes de pesquisa nos itens III.2, IV.3, e IV.7, IV.8, X.1, 3, a.

[23] KONDER, Carlos Nelson. Vulnerabilidade patrimonial e vulnerabilidade existencial: por um sistema diferenciador. *Revista de Direito do Consumidor*, São Paulo, v. 24, n. 99, p. 101-123, 2015.

maiores, afetando seu processo de inclusão e contrariando os princípios constitucionais e os preceitos cunhados pelo Estatuto da Pessoa com Deficiência (EPD) na busca de assegurar e promover, em condições de igualdade, o exercício de direitos e liberdades fundamentais.

Por isso, os dados médicos merecem proteção redobrada, a fim de evitar seu uso indevido nos setores a que deve ser assegurado o acesso prioritário, tais como saúde, educação, informação, lazer, trabalho, comunicação, locomoção, entre outros (arts. 8º e 9º do EPD).[24]

O surgimento de prontuários eletrônicos com a migração da forma física de tratamento e controle de dados para a forma virtual afetou diretamente a forma como os dados sensíveis dos pacientes resultantes da prestação de serviços médicos à distância[25] por meio das mídias sociais[26] circulam na internet, permitindo assim correlacionar uma série de dados que demonstram os perfis comportamentais do paciente, sua orientação sexual, estado de saúde, entre outras.

Portanto, faz-se necessário, diante da fragilidade constatada na era digital, desenvolver mecanismos efetivos de tutela dos dados sensíveis dos pacientes, que alcancem – tanto quanto possível – todos os participantes da cadeia de circulação dos dados, desde os profissionais da saúde, médicos, clínicas, hospitais, laboratórios, provedores de conteúdo, aplicativos na internet, controladores e até operadores. A não observância de medidas de restrição da transmissibilidade dos dados dos pacientes pode acarretar lesão à dignidade humana, à igualdade, à integridade psicofísica, à privacidade, direitos humanos fundamentais consagrados na Constituição Federal.

Diversas normas, de cunho ético e jurídico, no âmbito nacional e internacional[27], consagram o direito dos pacientes ao sigilo e à confidencialidade dos

---

[24] BARBOZA, Heloisa Helena; ALMEIDA, Vitor (Org.). *Comentários ao Estatuto da Pessoa com Deficiência à luz da Constituição da República*. Belo Horizonte, MG: Fórum, 2018. p. 74-90.

[25] PEREIRA, Paula Moura Francesconi de Lemos. O uso da internet na prestação de serviços médicos. In: MARTINS, Guilherme Magalhães (Org.) *Direito Privado e Internet*. São Paulo: Atlas, 2014. p. 259-299.

[26] A Resolução 1.974/2011, que trata da publicidade em Medicina regula divulgação de imagem nas mídias sociais (art. 13).

[27] No âmbito internacional destacam-se a Convenção para a proteção dos Direitos Humanos e Liberdades fundamentais – CEDH, art. 8, a Carta de Direitos Fundamentais da União Europeia, arts. 3,7,8, a Convenção do Conselho da Europa para a proteção de pessoas em relação ao tratamento automatizado de dados de caráter pessoal e as diretivas do Parlamento Europeu e do Conselho, como a diretiva 2002/58/CE, de 12 de julho de 2002, relativa ao tratamento de dados pessoais e à proteção da privacidade no setor das comunicações eletrônicas; Diretiva 96/9/CE do Parlamento

seus dados pessoais sensíveis, sendo estes reflexos do aspecto existencial da relação médico-paciente.[28]

2.1 APLICAÇÃO DO CONSENTIMENTO EM MATÉRIA DE SAÚDE

O consentimento informado na área de saúde é essencialmente reconhecido no contexto clínico e nas práticas de ética em pesquisas com seres humanos. Refere-se basicamente a um documento ético-jurídico, que se constitui no reconhecimento do valor da autonomia do paciente, mas que fundamentalmente observa regras institucionais e legais para formalizar a relação profissional de saúde e paciente.

A necessidade de representação eletrônica ou digital de Diretivas de consentimento surgiu a partir da disseminação do uso secundário das informações de saúde contidas nos diversos sistemas de Registro Eletrônico de Saúde. O Código de Ética da Associação Internacional de Informática Médica para Profissionais de Informática em Saúde - IMIA[29], traduzido pela Sociedade Brasileira de Informática em Saúde, estabelece que esses profissionais têm obrigação de assegurar que procedimentos apropriados sejam tomados, de modo que prontuários ou registros eletrônicos sejam estabelecidos ou transmitidos por meios de comunicação somente com o **consentimento voluntário,** competente e informado dos pacientes aos quais esses registros se referem.

Europeu e do Conselho, de 11 de março de 1996, relativa à proteção jurídica das bases de dados e o Regulamento Geral de Proteção de dados da União Europeia (GDPR), em vigor desde 2018.

[28] TEPEDINO, Gustavo José Mendes. A responsabilidade médica na experiência brasileira contemporânea. *Revista Trimestral de Direito Civil – RTDC*, Rio de Janeiro, a. 1, v. 2, p. 41-75, abr./jun. 2000.

[29] O código de ética da IMIA para profissionais de informática em saúde, traduzido pela Sociedade brasileira de Informática em Saúde (SBIS) está disponível em: http://www.sbis.org.br/images/ProTics/Codigo_Etica_IMIA_Brasil.pdf. Acesso em: 05 jun. 2021.

3 DA PRIVACIDADE À PROTEÇÃO DOS DADOS PESSOAIS SENSÍVEIS EM FACE DA DIGNIDADE DA PESSOA HUMANA

A princípio, pode-se esboçar a ideia do fim da privacidade, melhor dizendo, o fim da sua tradicional acepção. Deve-se salientar que o direito à privacidade, sobretudo na composição com o direito à identidade, está diretamente ligado à dignidade da pessoa humana[30]. O direito à privacidade é tutelado no art. 5º, X, da Constituição Federal brasileira, estando inserido no rol dos direitos de personalidade. Assim, a "esfera individual" é inerente à honra e diz respeito ao nome, à reputação e à imagem do titular. A esfera privada se refere à individualidade e, pois, à não intromissão externa na intimidade do titular, garantindo um certo isolamento do ser humano perante seus semelhantes[31].

Personalidade, destarte, inclui em sua estruturação um processo em que o indivíduo supera etapas com a intenção de reconhecer o ser humano em si e no outro. Em rigor, ser-pessoa é uma experiência integradora e deve, portanto, ser entendida além de uma síntese proteica, projetando-se em uma composição de essência e de existência. Trata-se, portanto, de uma categoria que expressa tanto a interioridade (relação para dentro) quanto a exterioridade (relação para fora) da pessoa humana. Em suma, pode-se trabalhar com uma esfera social (individual) e, em outra dimensão, com uma esfera privada. Os atos inerentes à esfera individual dizem respeito a comportamentos abertos – aqueles facilmente perceptíveis e valorados do indivíduo[32]. Tal esfera confunde-se com o direito à honra propriamente dito, protegendo o titular contra diversos tipos de agravos e, consequentemente de danos.

---

[30] SARLET, Ingo Wolfgang. *A eficácia dos direitos fundamentais*. 12. ed. Porto Alegre: Livraria do Advogado, 2017.
[31] VIEIRA, Tatiana Malta. *O direito à privacidade na sociedade da informação*: efetividade desse direito fundamental diante dos avanços da tecnologia da informação. Porto Alegre: Sergio Antonio Fabris, 2007. p. 22.
[32] COSTA JUNIOR, Paulo José da. *O direito de estar só*: tutela penal da intimidade. São Paulo: Revista dos Tribunais, 1970. p. 24.

Em contraposição, a esfera privada abarca os chamados comportamentos encobertos que o indivíduo pretende manter apartados do conhecimento e da interferência alheia, ou seja, diz respeito ao direito à privacidade[33]. E é justamente nesse tópico que se inserem os dados pessoais, notadamente os dados sensíveis que, em regra, têm sido considerados como *commodities* no panorama contemporâneo a despeito de sua relevância, uma vez que são geralmente irrenunciáveis e se encontram atrelados de modo insuperável à identidade pessoal. Assim, em razão da vedação ao seu emprego discriminatório, há sempre que se dedicar uma atenção redobrada.

Importa salientar, de toda sorte, que a privacidade, ainda que em franca reconfiguração no sistema jurídico e na vida cotidiana, pode ser dividida em diferentes categorias, interessando, no presente trabalho, principalmente a privacidade informacional ou autodeterminação informativa[34].

No que respeita à proteção de dados pessoais, mormente os dados sensíveis, esse feixe de direitos vem consubstanciado na Constituição Federal em diversos dispositivos, mas, mais especificamente, em seu art. 5º, XII, e está, embora em termos gerais, reforçado pela consagração do *Habeas Data*[35]. A delimitação de um direito fundamental autônomo e implícito no sistema normativo brasileiro implica uma compreensão que envolva o direito de acesso e de conhecimento dos dados pessoais existentes em registros (bancos de dados) públicos e privados; o direito ao não conhecimento, ao tratamento e à utilização e difusão de dados pessoais, particularmente no que concerne aos dados sensíveis pelo Estado ou por terceiros. Inclui-se, de toda maneira, um direito de sigilo quanto aos dados pessoais.

Fato inconteste é que, no Brasil, previsto tanto na Constituição quanto na legislação infraconstitucional, mais especificamente na LGPD, o direito à privacidade é considerado um direito fundamental e um dos direitos da personalidade, sendo um

---

[33] VIEIRA, Tatiana Malta. *O direito à privacidade na sociedade da informação*: efetividade desse direito fundamental diante dos avanços da tecnologia da informação. Porto Alegre: Sergio Antonio Fabris, 2007. p. 30.

[34] Cf. VIEIRA, Tatiana Malta. *O direito à privacidade na sociedade da informação*: efetividade desse direito fundamental diante dos avanços da tecnologia da informação. Porto Alegre: Sergio Antonio Fabris, 2007. p. 31-33.

[35] O *habeas data* é um dos mais importantes remédios constitucionais previstos na Constituição de 1988 por destinar-se a proteger a esfera íntima dos indivíduos. Por isso mesmo que tem status nas garantias fundamentais dispostas no art. 5. Dentre as suas finalidades, destacam-se as de proteger a intimidade das pessoas contra usos abusivos de registros de dados pessoais coletados por meios ilícitos e evitar a introdução dos já referidos dados sensíveis nestes arquivos. Visa também a desfazer a conservação de dados falsos ou com fins diversos dos previstos em lei.

instrumental jurídico que supera a dicotomia entre direito público e direito privado[36], essencial à formação da pessoa humana e indispensável na construção da identidade pessoal. Logo, é inegável a correspondência entre o princípio da dignidade[37] da pessoa humana com, de modo geral, os direitos fundamentais, observando-se com um destaque superior, em razão do tema dessa investigação, a garantia da liberdade, da intimidade, da privacidade e da proteção de dados pessoais sensíveis na sociedade informacional[38].

Com efeito, a LGPD dispõe, em seu art. 1º, sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e privacidade e o livre desenvolvimento da personalidade da pessoa natural. Do teor do art. 3º enfatiza-se, ainda, que se trata de uma proteção destinada aos dados que, independentemente do meio, referem-se ao fornecimento de bens ou serviços, notadamente, mas não exclusivamente, dos dados de indivíduos localizados em território nacional.

Tema de fundamental relevância, o consentimento livre, informado e esclarecido, e suas circunstâncias, passa a ser abordado. Exsurge inegavelmente da atual ideia de vigilância e de tecnocontrole a tarefa de reforçar a importância do consentimento, em especial em uma forma escrita, resgatando-o como um dos pontos nucleares do legado do século XX no sentido de valorização da autonomia privada, dos direitos humanos e fundamentais. Em especial, particulariza-se a sua natureza processual na medida em que devem ser garantidas todas as condições, inclusive temporais, circunstanciais e informacionais, para a tomada de decisão livre, esclarecida e autônoma em um cenário de liberdade, de solidariedade e de responsabilidade.

---

[36] Torna-se perceptível que a proteção à dignidade da pessoa humana envolve um aspecto negativo, no sentido de impedir violações, mas também um aspecto positivo, isto é, de assegurar o pleno desenvolvimento da personalidade de cada um dos indivíduos. Em função disso, a Constituição Federal de 1988 não se restringiu a uma elaboração em que a dignidade da pessoa humana ficasse restrita a um mero enunciado; de fato, considerou-a como fundamento que se reflete em todo o texto constitucional. Ainda digno de nota é enfatizar que a dignidade da pessoa humana é fonte primária que apresenta as diretrizes do ordenamento jurídico do Estado de Direito, representando vetor interpretativo e indicativo. E, em se tratando de direito brasileiro, apresenta-se como um dos fundamentos do próprio Estado Democrático de Direito.

[37] Sarlet destaca a complexidade inerente à conceituação jurídica da dignidade da pessoa humana. Cf. SARLET, Ingo Wolfgang. *A eficácia dos direitos fundamentais*. 12. ed. Porto Alegre: Livraria do Advogado, 2017. p. 70.

[38] SARLET, Ingo Wolfgang. *A eficácia dos direitos fundamentais*. 12. ed. Porto Alegre: Livraria do Advogado, 2017. p. 110.

Oportuno enfatizar que a atual relação entre a proteção de dados pessoais e o processo de elaboração de consentimento na vida digital corresponde à observância tanto de um direito/dever de informação dos usuários quanto de um dever por parte dos agentes públicos e privados de garantir a deliberação livre e, consequentemente, a revisão e a possibilidade de retirada da anuência a qualquer momento sem prejuízo algum, mediante a garantia de que o tráfego desses dados não implicará em danos de espécie alguma.

Em outras palavras, o consentimento deve ser efetuado nos moldes de um ato jurídico pleno, respeitando-se a ampliação de uma perspectiva de validade e de perfectibilidade em um panorama em que novos atores, advindos da era informacional, passam a ser cada vez mais corresponsáveis pela criação de um ambiente livre, seguro, minimamente estável nas fronteiras estabelecidas por sistemas auditáveis, compreensíveis e acessíveis. Segundo o art. 5º, XII, da LGPD, trata-se de uma manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada.

Ocorre que, atualmente, no Brasil, o tráfego de dados pessoais é realizado sem nenhuma espécie de consentimento. Caminha-se a passos lentos para tal regulamentação. Trata-se, com isso, de uma construção em que as fronteiras do processo de anonimização em face da reconfiguração do direito à privacidade e, consequentemente, do direito à proteção de dados sensíveis devem se encontrar em um movimento de consonância e de adequação com um padrão protetivo para o resguardo da identidade digital, tendo como base a dignidade e a autodeterminação informativa em face da hiperaceleração da tecnologia.

Por fim, urge salientar a importância do consentimento quando se trata de menores de idade. Nesse caso é imprescindível obter o consentimento inequívoco de um dos pais ou responsáveis. Outro aspecto primordial é quanto ao uso estrito dos dados, ou seja, deve ser empregado apenas o conteúdo estritamente necessário para a atividade econômica ou governamental em questão, vedado o repasse a terceiros. Na ausência do consentimento, só podem serem coletados dados em situações de urgência, devendo-se imediatamente entrar em contato com os pais ou com os responsáveis para garantir a maior e mais adequada proteção à criança e ao adolescente. Nesse ponto, observa-se uma relação clara entre a LGPD, o ECA (Estatuto da Criança e do Adolescente) e a principiologia constitucional.

Nesse último tópico cabe realizar uma análise pormenorizada. Concernente à relação entre a LGPD e o ECA, é fundamental mencionar o trabalho do Ministério Público, das Defensorias Públicas e demais agentes governamentais envolvidos. Entende-se extremamente eficaz a tutela aos menores, tornando assim uma realidade factível o "consentimento" no tratamento dos dados pessoais dos indivíduos.

3.1 AUTODETERMINAÇÃO INFORMATIVA COMO DIREITO FUNDAMENTAL

A LGPD elenca a autodeterminação informativa[39] como um dos fundamentos da disciplina da proteção de dados pessoais em seu artigo 2º, II. É possível dizer que dos fundamentos presentes no art. 2º da LGPD, a autodeterminação informativa é aquela que guarda, juntamente com o respeito à privacidade, a relação mais próxima com a disciplina da proteção de dados pessoais. Isso porque consiste no único fundamento presente no rol dos incisos do dispositivo que tem a sua origem atrelada a essa matéria.

Após essa explanação sobre a importância e relação do artigo 2º da LGPD, bem como sua correlação com a matéria da proteção de dados, segue-se, realizando um apanhado sobre as origens alemãs da autodeterminação informativa.

De acordo com Menke, "o direito à autodeterminação informativa, como âncora constitucional da proteção de dados, integra o denominado direito geral da personalidade[40]. Na Alemanha, o direito geral da personalidade tem origem na doutrina de Otto Von Gierke, no final do Século XIX, e posteriormente foi reconhecido pioneiramente pelo Tribunal Superior Federal (*Bundesgerichtshof – BGH)*, em decisão de 1954. Na sequência, foi e vem sendo desenvolvido pelo Tribunal Constitucional Federal (*Bundesverfassungsgericht),* e é derivado da combinação do art. 1, I (dignidade da pessoa) e art. 2, I (livre desenvolvimento da

[39] MENKE, Fabiano. As origens alemãs e o significado da autodeterminação informativa. *In*: MENKE, Fabiano; DRESCH, Rafael de Freitas Valle (org.). *Lei Geral de Proteção de Dados*: Aspectos Relevantes. 1. ed. Indaiatuba: Foco, 2021. p. 13-22.

[40] MENKE, Fabiano. As origens alemãs e o significado da autodeterminação informativa. *In*: MENKE, Fabiano; DRESCH, Rafael de Freitas Valle (org.). *Lei Geral de Proteção de Dados*: Aspectos Relevantes. 1. ed. Indaiatuba: Foco, 2021. p. 13-22.

personalidade) da Lei Fundamental[41], ou seja, a sua atuação em conjunto garante a cada indivíduo a possibilidade de desenvolver a sua própria personalidade.

O direito geral de personalidade protege elementos da personalidade que não estão cobertos pelas garantias especiais de liberdade da Lei Fundamental Alemã. Na dogmática do direito geral da personalidade, é possível distinguir três categorias ou implementações, conforme o desenvolvimento do Tribunal Constitucional Federal Alemão: o direito à autodeterminação (*Recht der Selbstbestimmung)*, o direito à autopreservação *(Recht der Selbstbewahrung)* e direito à autoapresentação (*Recht der Selbstdarstellung)*[42]*.* A seguir cumpre explicar pormenores da autodeterminação informativa.

A autodeterminação informativa pretende conceder ao indivíduo o poder de ele próprio decidir acerca da divulgação e utilização de seus dados pessoais". Nesse contexto, é usual que se utilize a expressão "controle"[43].

Dessa feita, diante do exposto, nota-se na Alemanha um pioneirismo no que tange à autodeterminação informativa. Por essa razão, no presente trabalho opta-se por concentrar esforços em trazer à baila relevante doutrina. Entende-se relevante na determinação conceitual saber em quais valores constitucionais a autodeterminação informativa encontra guarida[44]. A partir daí, constatado seu fundamento na *Grundgesetz*, trabalhá-lo como direito fundamental em suas dimensões, para que se possa determinar seu âmbito de proteção (*Schutzbereich*).

O direito geral de personalidade não tem em vista o individualismo sem vinculação social. Pelo contrário, ele parte de que a autodescoberta do indivíduo está integrada na sociedade. O ser humano tem uma necessidade de se mostrar na comunidade social, isto é, de determinar ele próprio quem fica a saber alguma coisa sobre si – mais precisamente também como, quando e por quem. Isso exige tanto aspectos positivos da autopreservação, como fatores negativos do retirar-se. Em um

---

[41] Art. 1º, I: A dignidade da pessoa é intangível. Respeitá-la e protegê-la é obrigação de todo poder público.
Art. 2º, I: Toda pessoa tem o direito ao livre desenvolvimento de sua personalidade, desde que os direitos dos outros não sejam violados e desde que não atente contra a ordem constitucional ou contra a lei moral. (Tradução livre da Lei Fundamental).

[42] MENKE, Fabiano. As origens alemãs e o significado da autodeterminação informativa. *In*: MENKE, Fabiano; DRESCH, Rafael de Freitas Valle (org.). *Lei Geral de Proteção de Dados*: Aspectos Relevantes. 1. ed. Indaiatuba: Foco, 2021. p. 13-22.

[43] DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*. 2. ed. São Paulo: Revista dos Tribunais, 2020. p. 170.

[44] ASSMANN, Jhonata. *A autodeterminação informativa no direito germânico e brasileiro*. 2014. 65f. Trabalho de Conclusão de Curso (Graduação em Direito) – Faculdade de Direito, Universidade Federal de Santa Catarina, Florianópolis, 2014.

sentido mais amplo, trata-se de informações sobre a identidade e a individualidade de cada indivíduo.

De importância particular é, neste caso, o levantamento e registro de dados relativos à pessoa por parte do Estado e de privados, por meio do processamento eletrônico de dados e da possibilidade a ele associada da transferência e da combinação de diferentes registros. A autonomia de utilização destes dados depende do indivíduo e é protegida pelo seu direito à autodeterminação informacional.

Essa expressão moderna do direito geral de personalidade foi, como mencionado no presente estudo, desenvolvida pelo Tribunal Constitucional Federal Alemão no contexto do censo da população no início de 1980. Neste âmbito, não se pode fazer uma distinção entre dados importantes e dados pretensamente insignificantes[45]. Também não se pode qualificar apenas o levantamento de dados, mas também o armazenamento, a utilização e a transmissão de dados como sendo, cada caso, uma ingerência independente, para a qual tem de haver respectivamente uma base legal especial. Disto faz parte também a liberdade de autoincriminação no processo penal como consequência jurídico-processual do direito de personalidade[46].

Direitos fundamentais são direitos públicos subjetivos de pessoas (físicas ou jurídicas), contidos em dispostos constitucionais e, portanto, encerram o caráter normativo supremo dentro do Estado, tendo como finalidade limitar o exercício do poder estatal em face da liberdade individual. O direito à autodeterminação informativa (*informationelles Selbstbestimmungsrecht*) não possui previsão textual na Lei Fundamental alemã (*Grundgesetz*): sua construção é jurisprudencial e dogmática[47], mas decorre de alguns de seus valores mais caros.

Para o *Bundesverfassungsgericht,* o livre desenvolvimento da personalidade, dadas as condições da manipulação de dados, pressupõe a proteção do indivíduo contra o levantamento, armazenagem, uso e transmissão irrestritos de seus dados pessoais. Essa proteção seria abrangida pelo direito fundamental do Art. 2 I[48] c. c.

---

[45] BVerfGE 65, 1, 45 – Volkszählung: não há “nenhum dado que não tenha interesse”.
[46] LOTHAR, Michael; MORLOK, Martin. *Direitos Fundamentais*. São Paulo: Saraiva, 2016.
[47] O *Bundesverfassungsgericht* enunciou-o quando do julgamento acerca da constitucionalidade da Lei de Censo (*Volkszahlungsurteil*), o qual merecerá atenção oportunamente.
[48] Art. 2 I, GG: *Jeder hat das Recht auf die freie Entfaltung seiner Persönlichkeit, soweit er nicht die Rechte anderer verletzt und nicht gegen die verfassungsmäßige Ordnung oder das Sittengesetz verstößt* (livre desenvolvimento da personalidade).

Art. 1 I[49] GG. O direito fundamental (a autodeterminação informativa) garante o poder do cidadão de determinar em princípio, ele mesmo, sobre a exibição e o uso de seus dados pessoais.

Essa ideia não se deve, contudo, à interpretação simplista de que a capacidade de disposição sobre seus próprios dados signifique o exercício à autodeterminação informativa e a encerre enquanto conceito[50].

> *What the expression 'informational self-determination' means is rather that an individual's control over the data and information produced about him is a (necessary but insufficient) precondition for him to live an existence that may be said 'self-determined.*[51]

Para que exista um livre desenvolvimento da personalidade se faz necessário um espaço de autonomia, enquanto "qualidade que a vontade tem de ser lei para si mesma (independentemente de uma qualidade qualquer dos objetos do dever)"[52], diferentemente da vontade heterônoma, jurídica. Essa definição kantiana de autonomia coincide com a definição de liberdade de Rousseau, entendida como "obediência à liberdade que cada um dá a si mesmo"[53]. A comunicação livre em uma sociedade democrática tem como requisito o livre desenvolvimento da personalidade para que haja um debate plural – cujas ideias postas em contraponto aperfeiçoam-se em um processo dialético. Instrumento necessário para concretização desses valores – constitucionalmente expressos – é o direito à autodeterminação informativa, que, enquanto direito fundamental, impõe limites ao Estado pela realização de suas dimensões negativa e positiva.

---

[49] Art. 1 I, GG: *Die Würde des Menschen ist unantastbar. Sie zu achten und zu schützen ist Verpflichtung aller staatlichen Gewalt*.(inviolabilidade da dignidade humana)

[50] O *Bundesverfassungsgericht* valeu-se da expressão *personbezogene Daten*, a qual, para PAHLEN-BRANT (2008), é relacionada à pessoa seja 1) por seu conteúdo, por meio de afirmações sobre a pessoa (*Aussage uber die Person*): "A possui uma carteira de motorista", por exemplo; 2) pela finalidade da manipulação de dados (*Zweck der Verarbeitung*), como no caso da vigilância por vídeo; ou 3) pelo resultado da manipulação, quando como consequência secundária de uma manipulação de dados seja possível formular afirmações sobre uma determinada pessoa. Neste último caso em especial é possível perceber a fragilidade da ideia de autodeterminação informativa como mera disposição sobre os próprios dados.

[51] ROUVROY, Antoinette; POULLET, Yves. The Right to Informational Self-Determination and the Value of Self-Development: Reassessing the Importance of Privacy for Democracy. In: GUTWIRTH, Serge; POULLET, Yves; HERT, Paul; TERWANGNE, Cécile; NOUWT, Sjaak. *Reinventing Data Protection?* Heidelberg: Springer, 2009. p. 45-76. DOI: http://dx.doi.org/10.1007/978-1-4020-9498-9_2. p. 51.

[52] ASSMANN, Jhonata. *A autodeterminação informativa no direito germânico e brasileiro*. 2014. 65f. Trabalho de Conclusão de Curso (Graduação em Direito) – Faculdade de Direito, Universidade Federal de Santa Catarina, Florianópolis, 2014.

[53] BOBBIO, Norberto. *Direito e Estado no Pensamento de Emanuel Kant*. 4. ed. Brasília: Editora UnB, 1997. p. 62-63.

> O Estado Democrático de Direito baseia-se, em grande medida, na participação de todos os cidadãos e sua legitimidade lastreia-se no respeito à liberdade individual de cada pessoa. O direito à autodeterminação informativa não só é concedido para o bem do indivíduo, mas também em prol de um interesse público - para garantir um sistema de comunicação livre e democrático. Portanto, é possível, principalmente para justificar interferências no direito à autodeterminação informativa se uma consideração de ambos os princípios mostra que o público interesse prevalece sobre os interesses legítimos do indivíduo. No entanto, a ideia básica é sempre a mesma: a pessoa em causa é para manter o controle de seus próprios dados.[54]

Importante trazer à luna a Lei do Censo alemã (Volkszählunsgesetz) de 1983, que determinou que os cidadãos fornecessem uma série de dados pessoais para mensurar estatisticamente a distribuição espacial e geográfica da população[55]. A referida lei previa, contudo, a possibilidade de que os dados coletados fossem cruzados com outros registros públicos para a finalidade genérica de execução de "atividades administrativas"[56]. Tal vagueza e amplitude da lei de recenseamento foi o estopim para uma série de reclamações perante o Tribunal Constitucional alemão, que declarou a sua inconstitucionalidade parcial.

A Corte alemã considerou que eventual compartilhamento dos dados coletados deveria se destinar única e exclusivamente à finalidade de recenseamento (estatística)[57]. A relevância do julgado destaca-se por sua *ratio decidendi* sob dois aspectos: a) a proteção dos dados pessoais como um direito de personalidade autônomo e a compreensão do termo autodeterminação informacional para além do

---

[54] Cf. Hornung e Schnabel: "*The democratic constitutional state relies to a great extent on the participation of all citizens and its legitimacy is based on respecting each person's individual liberty. As said before, the right to informational self-determination is not only granted for the sake of the individual, but also in the interest of the public, to guarantee a free and democratic communication order. Therefore, itis primarily possible to justify interferences in the right to informational self-determination if a consideration of both principles shows that the public interest outweighs the legitimate interests of the individual. However, the basic idea is always the same: the data subject is to maintain control of his/her own data)*. (HORNUNG, Gerrit; SCHNABEL, Christoph. Data Protection in Germany I: The population census decision and the right to informational self-determination. *Computer Law and Security Review*, Kassel, n. 25, p. 84-88, 2009.) (Tradução Livre)

[55] MARTINS, Leonardo. Introdução à jurisprudência do Tribunal Constitucional Federal Alemão. In: MARTINS, Leonardo (org.) *Cinquenta anos de jurisprudência do Tribunal Constitucional Federal Alemão*. Montevidéu: Fundação Konrad Adenauer, 2005. p. 33-128.

[56] "O § 9 da Lei previa, entre outras, a possibilidade de uma comparação dos dados levantados com os registros públicos e também a transmissão de dados tornados anônimos a repartições públicas federais, estaduais e municipais para determinados fins de execução administrativa". (MARTINS, Leonardo. Introdução à jurisprudência do Tribunal Constitucional Federal Alemão. In: MARTINS, Leonardo (org.) *Cinquenta anos de jurisprudência do Tribunal Constitucional Federal Alemão*. Montevidéu: Fundação Konrad Adenauer, 2005. p. 33-128.)

[57] MARTINS, Leonardo. Introdução à jurisprudência do Tribunal Constitucional Federal Alemão. In: MARTINS, Leonardo (org.) *Cinquenta anos de jurisprudência do Tribunal Constitucional Federal Alemão*. Montevidéu: Fundação Konrad Adenauer, 2005. p. 33-128.

consentimento; e b) a função e os limites do consentimento do titular dos dados. Na primeira parte do julgado, estabelece-se a importante construção de que o cidadão deve ter o controle sobre os seus dados pessoais, a fim de que ele possa autodeterminar as suas informações pessoais. Cunha-se, então, a expressão "autodeterminação informacional ou autodeterminação informativa".

Para além dessa relevância terminológica, o julgado desenvolveu um direito autônomo e destacado do direito à privacidade para chegar à conclusão de inconstitucionalidade parcial da lei de recenseamento. Nesse sentido, as considerações iniciais do julgado são de contumaz importância, na medida em que contextualizam como o avanço tecnológico e, principalmente, o progresso qualitativo na organização das informações impactaram significativamente as liberdades individuais[58].

Baseado em tal premissa, o Tribunal Constitucional alemão delineia o direito da autodeterminação informacional, valendo-se do direito geral da personalidade[59]. A capacidade do indivíduo de autodeterminar seus dados pessoais seria parcela fundamental do seu direito em livremente desenvolver sua personalidade.

Por essa razão, o Tribunal Constitucional alemão argumenta recorrentemente que a atividade de processamento dos dados pessoais deve ter limites, impondo-se

---

[58] "Esse poder necessita, sob as condições atuais e futuras do processamento automático de dados, de uma proteção especialmente intensa. Ele está ameaçado, sobretudo porque em processos decisórios não se precisa mais lançar mão, como antigamente, de fichas e pastas compostos manualmente. Hoje, com ajuda do processamento eletrônico de dados, informações detalhadas sobre relações pessoais ou objetivas de uma pessoa determinada ou determinável (dados relativos à pessoa [cf. § 2 I BDSG – Lei Federal sobre a Proteção de Dados Pessoais]) podem ser, do ponto de vista técnico, ilimitadamente armazenados e consultados a qualquer momento, a qualquer distância e em segundos. Além disso, podem ser combinados, sobretudo na estruturação de sistemas de informação integrados, com outros bancos dedados, formando um quadro da personalidade relativamente completo ou quase, sem que a pessoa atingida possa controlar suficientemente sua exatidão e seu uso. Com isso, ampliaram-se, de maneira até então desconhecida, as possibilidades de consulta e influência que podem atuar sobre o comportamento do indivíduo em função da pressão psíquica causada pela participação pública em suas informações privadas". (MARTINS, Leonardo. Introdução à jurisprudência do Tribunal Constitucional Federal Alemão. In: MARTINS, Leonardo (org.) *Cinquenta anos de jurisprudência do Tribunal Constitucional Federal Alemão*. Montevidéu: Fundação Konrad Adenauer, 2005. p. 33-128.)

[59] "Quem não consegue determinar com suficiente segurança quais informações sobre sua pessoa são conhecidas em certas áreas de seu meio social, e quem não consegue avaliar mais ou menos o conhecimento de possíveis parceiros na comunicação, pode ser inibido substancialmente em sua liberdade de planejar ou decidir com autodeterminação. (...) Daí resulta: O livre desenvolvimento da personalidade pressupõe, sob as modernas condições do processamento de dados, a proteção do indivíduo contra levantamento, armazenagem, uso e transmissão irrestritos de seus dados pessoais. Esta proteção, portanto, é abrangida pelo direito fundamental do Art. 2 I c. c. Art. 1 I GG. O direito fundamental garante o poder do cidadão de determinar em princípio ele mesmo sobre a exibição e o uso de seus dados pessoais". (MARTINS, Leonardo. Introdução à jurisprudência do Tribunal Constitucional Federal Alemão. In: MARTINS, Leonardo (org.) *Cinquenta anos de jurisprudência do Tribunal Constitucional Federal Alemão*. Montevidéu: Fundação Konrad Adenauer, 2005. p. 33-128.)

"precauções organizacionais e processuais que combatam o perigo de uma violação do direito da personalidade" [60], não só considerando o consentimento como desdobramento desse novo direito da personalidade.

Assim, o Tribunal Constitucional não recorre ao discurso do que é público ou privado para criar o direito à autodeterminação informacional. Ao revés, a sua fundamentação acaba por transpor tal dicotomia, na medida em que estabelece que o uso das informações pessoais não deve afetar o desenvolvimento da personalidade das pessoas.

Para tanto, o controle exercido pelo cidadão sobre seus dados é de fundamental importância, bem como a prevenção de práticas de discriminação social[61]. Deslocou-se, por exemplo, a discussão sobre se um dado é sensível ou se esconderia algo íntimo da pessoa[62] para se considerar que qualquer dado pessoal pode angariar um efeito lesivo e daí então dar ênfase na garantia de que os dados pessoais sejam anonimizados[63], bem como que o seu uso seja restrito às finalidades estatísticas.

Portanto, o julgado é paradigmático na construção de um direito autônomo da personalidade relativo à proteção dos dados pessoais, o qual avança na compreensão de que a sua dinâmica se afasta da dicotomia entre público e privado.

A atestar tal afirmação, recorre-se à comparação da fundamentação do julgado sob análise (Lei do Recenseamento de 1983) frente a uma decisão pretérita

---

[60] MARTINS, Leonardo. Introdução à jurisprudência do Tribunal Constitucional Federal Alemão. In: MARTINS, Leonardo (org.) *Cinquenta anos de jurisprudência do Tribunal Constitucional Federal Alemão*. Montevidéu: Fundação Konrad Adenauer, 2005. p. 33-128.

[61] Essa é terminologia usada, mais de uma vez, ao longo do julgado. (MARTINS, Leonardo. Introdução à jurisprudência do Tribunal Constitucional Federal Alemão. In: MARTINS, Leonardo (org.) *Cinquenta anos de jurisprudência do Tribunal Constitucional Federal Alemão*. Montevidéu: Fundação Konrad Adenauer, 2005. p. 33-128.)

[62] "Com isso, um dado em si insignificante pode adquirir um novo valor :desse modo, não existem mais dados 'insignificantes' no contexto do processamento eletrônico de dados. O fato de informações dizerem respeito a processos íntimos não decide por si só se elas são sensíveis ou não. É muito mais necessário o conhecimento do contexto de utilização, para que se constate a importância do dado em termos de direito da personalidade". (MARTINS, Leonardo. Introdução à jurisprudência do Tribunal Constitucional Federal Alemão. In: MARTINS, Leonardo (org.) *Cinquenta anos de jurisprudência do Tribunal Constitucional Federal Alemão*. Montevidéu: Fundação Konrad Adenauer, 2005. p. 33-128.)

[63] "De especial importância para os levantamentos estatísticos são as eficazes regras de bloqueio em face do mundo exterior. Para a proteção do direito de autodeterminação sobre a informação é imprescindível a manutenção em sigilo absoluto dos dados individuais obtidos para fins estatísticos – e já desde o processo de levantamento – enquanto existir uma referência pessoal ou esta puder ser produzida (segredo estatístico); o mesmo vale para a obrigação de tornar, o mais cedo possível, anônimos (de fato) os dados, associada a precauções contra a quebra do anonimato". (MARTINS, Leonardo. Introdução à jurisprudência do Tribunal Constitucional Federal Alemão. In: MARTINS, Leonardo (org.) *Cinquenta anos de jurisprudência do Tribunal Constitucional Federal Alemão*. Montevidéu: Fundação Konrad Adenauer, 2005. p. 33-128.)

da própria Corte Constitucional alemã (Lei do Microcenso de 1957). Nessa última, a *ratio decidendi* centrou-se, diferentemente, na argumentação de que os dados pessoais coletados não deveriam atingir a esfera íntima dos cidadãos para daí então estabelecer a proteção de seus dados pessoais[64].

Por isso, a fundamentação construída pelo julgado sob análise – Lei do Recenseamento de 1983 – é paradigmática ao não tomar a proteção dos dados pessoais como uma evolução do direito à privacidade. Pelo contrário, trata-o como um direito de personalidade autônomo que reclama uma técnica de proteção desconectada da dicotomia entre público e privado.

Deriva daí, portanto, o primeiro aspecto relevante da releitura do julgado da Corte Constitucional alemã, em razão da construção dogmática da proteção dos dados pessoais como um direito de personalidade autônomo. Tal aspecto, se não é por vezes omitido, não angaria, ao menos, o merecido destaque por parcela da doutrina que estabelece a proteção dos dados pessoais como uma evolução do direito à privacidade.

Outro ponto a ser explorado na releitura do julgado diz respeito à ênfase de que os dados coletados dos cidadãos alemães sejam anonimizados e não utilizados para outra finalidade que não a estatística. Por se tratar de uma lei de recenseamento, era obrigatório o fornecimento de dados, não havendo a opção de recusa. Por isso, a ressalva de que se deveria garantir que o uso dos dados fosse restrito às finalidades estatísticas independentemente do consentimento dos seus titulares em sentido contrário.

E, nesse sentido, tornava-se ainda mais relevante que o Estado coletasse somente o que fosse realmente necessário[65]. Ainda que se reconhecesse que o

---

[64] "O TCF julgou presentes as condições processuais da apresentação judicial e no mérito confirmou a constitucionalidade dos dispositivos da lei do microcenso, que havia sido questionada pelo juízo representante. Na fundamentação, o TCF considerou, em suma, que os dados levantados não atingiam a esfera íntima intocável do indivíduo e que a intervenção estava justificada por ser formalmente permitida pelo Art. 2 I GG e materialmente proporcional em face do propósito de abastecer o Estado com dados necessários ao planejamento da ação estatal". (MARTINS, Leonardo. Introdução à jurisprudência do Tribunal Constitucional Federal Alemão. In: MARTINS, Leonardo (org.) *Cinquenta anos de jurisprudência do Tribunal Constitucional Federal Alemão*. Montevidéu: Fundação Konrad Adenauer, 2005. p. 33-128.)

[65] "A obrigação de fornecer dados pessoais pressupõe que o legislador defina a finalidade de uso por área e de forma precisa, e que os dados sejam adequados e necessários para essa finalidade. Com isso não seria compatível a armazenagem de dados reunidos, não anônimos, para fins indeterminados ou ainda indeterminável. Todas as autoridades que reúnem dados pessoais para cumprir suas tarefas devem se restringir ao mínimo indispensável para alcançar seu objetivo definido". (MARTINS, Leonardo. Introdução à jurisprudência do Tribunal Constitucional Federal

levantamento de dados estatísticos adquire múltiplas funções (e.g., densidade demográfica, espacial, geográfica etc.), isso não autorizava o seu uso ou transmissão para outra finalidade que não o recenseamento[66].

O que se extrai do julgado não é só a construção do princípio da especificação dos propósitos que orienta e limita a coleta e a utilização dos dados pessoais (finalidade estatística), mas, sobretudo, a sua prevalência em um contexto no qual o consentimento dos titulares de dados pessoais não teve um papel de protagonismo. Caso contrário, a pessoa poderia ser transformada em um "objeto de informação" decorrente da sua relação de assimetria de poder para com o Estado.

Não raras vezes a terminologia "autodeterminação informacional" implica a interpretação equivocada de que o consentimento do titular dos dados pessoais possui primazia e prevalência na proteção dos dados pessoais, a fim de que, justamente, o sujeito autodetermine as suas informações pessoais.

Do contrário, como adverte a própria decisão da Corte Constitucional alemã, desproteger-se-iam os dados pessoais provenientes de uma prática pouco ou nada transparente que feriria a confiança dos cidadãos alemães com relação ao contexto da coleta dos dados pessoais – i.e., estatística. A conclusão que se extrai da releitura do julgado é de que o consentimento poderia servir às avessas para a desproteção dos dados pessoais, na medida em que tornaria ilimitada a coleta e o processamento dos dados pessoais, tornando a pessoa, intermediada por seus dados, um objeto a ser ilimitadamente explorado.

A releitura do julgado impõe, portanto, não só reconsiderar a proteção dos dados pessoais como uma evolução do direito à privacidade, como também o próprio protagonismo do consentimento do titular dos dados pessoais. Esse último aspecto é de suma importância para a exata compreensão do conteúdo da

---

Alemão. In: MARTINS, Leonardo (org.) *Cinquenta anos de jurisprudência do Tribunal Constitucional Federal Alemão*. Montevidéu: Fundação Konrad Adenauer, 2005. p. 33-128.)

[66] "No levantamento de dados para fins estatísticos não se pode exigir uma vinculação estrita e concreta dos dados à finalidade. Segundo a essência da estatística, os dados devem ser utilizados para as tarefas mais diversas, não determináveis de antemão; consequentemente, existe também uma necessidade de armazenagem de dados. (...) O recenseamento deve ser levantamento e manipulação com múltiplas finalidades, portanto reunião e armazenagem de dados, para que o Estado possa enfrentar, estando para tanto preparado, o desenvolvimento da sociedade industrial. Também as proibições de transmissão e uso de dados preparados estatisticamente seriam contrárias à sua finalidade". (MARTINS, Leonardo. Introdução à jurisprudência do Tribunal Constitucional Federal Alemão. In: MARTINS, Leonardo (org.) *Cinquenta anos de jurisprudência do Tribunal Constitucional Federal Alemão*. Montevidéu: Fundação Konrad Adenauer, 2005. p. 33-128.)

autodeterminação informacional, bem como para a sua própria reavaliação dentro do quadro normativo da proteção dos dados pessoais.

3.2 OS RISCOS DAS NOVAS TECNOLOGIAS

Neste capítulo serão tradados a definição e os riscos que as novas tecnologias, como Inteligência Artificial (IA), *Big Data e Blockchain,* proporcionam à proteção de dados pessoais.

Embora seja uma tarefa ingrata tentar definir o que é Inteligência Artificial, de forma geral lida-se com um conjunto de técnicas e metodologias computacionais que possibilita a um *software* ou máquina realizar tarefas que requerem raciocínio ou aprendizagem, simulando ou encontrando soluções que normalmente requerem inteligência. A novidade e o desafio trazido pela inteligência artificial ao direito residem na dificuldade em lidar com um agente não dotado de personalidade jurídica, na acepção tradicional, mas que é capaz de realizar escolhas independentes (tomar decisões). No campo médico, estas escolhas podem levar a ações físicas, como no caso de um robô cirurgião, ou puramente cognitivas, como no caso de um sistema que gera diagnósticos a partir de informações relativas a um paciente[67]. No entanto, alguns problemas podem exsurgir em decorrência do uso das “novas tecnologias” na área da saúde.

O uso inadequado de inteligência artificial pode prejudicar a inteligibilidade de decisões médicas, lançar mão de dados pessoais excessivos, reproduzir práticas e padrões discriminatórios ou mesmo causar diretamente danos materiais, entre outras fontes de risco. A seguir serão abordadas questões éticas que podem surgir com a temática.

A principal abordagem de questões éticas ligadas à inteligência artificial tem sido a identificação, avaliação e explicação de princípios éticos capazes de lidar com preocupações levantadas pelo uso dessa tecnologia. Alguns estudos e relatórios recentes em âmbito internacional apontam haver alguma convergência em torno de um conjunto de princípios: transparência, tanto em relação ao uso de inteligência artificial quanto à explicabilidade de seus resultados; liberdade individual e

[67] MARANHÃO, Juliano Souza de Albuquerque; ALMADA, Marco. Inteligência Artificial no Setor de Saúde: ética e proteção de dados. *In*: DALLARI, Analluza Bolivar; MONACO, Gustavo Ferraz de Campos (coord.). *LGPD na Saúde*. 1. ed. São Paulo: Thomson Reuters Brasil, 2021. p. 357-372.

autonomia; não discriminação; não-maleficência; acurácia; responsabilidade; e proteção de dados e privacidade.

Há divergência e falta de consenso em torno do significado e alcance dos princípios abstratos. Estas são ainda maiores quando tratam objetos específicos como no caso da saúde. Nesse caso em particular, as abordagens éticas da inteligência artificial, com seus princípios abstratos, podem se beneficiar de um diálogo com os debates travados no campo da ética médica por uma perspectiva prática, orientada a casos e questões práticas dos diversos ramos da medicina[68].

Pela combinação da abordagem *top-down* típica da ética de IA com a orientação *bottom-up* da ética médica, passa a ser possível dar conteúdo aos princípios gerais da IA aplicada a problemas médicos, tornando sua aplicação factível.

Por outro lado, a conclusão elaborada pela IA pode estar inexata, partindo de evidências errôneas, o que acarreta danos às partes envolvidas bem como a toda operação iniciada. As limitações das evidências produzidas a partir da IA devem ser avaliadas em cada caso concreto, já que elas podem ser fruto tanto do sistema em si quanto do contexto de aplicação. Essa afirmação vai ao encontro do exposto anteriormente.

Há evidência de que seja inadequada por qualquer uma das formas existentes, reduz a transparência do processo de tomada de decisão médica, o que, por sua vez, também compromete a autonomia do paciente em tomar decisões relativas ao seu próprio tratamento. Além disso, os limites à transparência comprometem a acurácia e a robustez dos sistemas inteligentes, e até mesmo a não-maleficência, já que tornam mais difícil a identificação de potenciais efeitos nocivos do uso de um sistema em um determinado contexto.

Um sistema inteligente pode ter consequências éticas também em função dos resultados de suas operações. Por exemplo, um sistema inteligente pode ter efeitos transformadores na relação entre paciente e médico, alterando as expectativas das partes e impactando a relação de confiança entre elas[69].

---

[68] MARANHÃO, Juliano Souza de Albuquerque; ALMADA, Marco. Inteligência Artificial no Setor de Saúde: ética e proteção de dados. *In*: DALLARI, Analluza Bolivar; MONACO, Gustavo Ferraz de Campos (coord.). *LGPD na Saúde*. 1. ed. São Paulo: Thomson Reuters Brasil, 2021. p. 357-372.
[69] MORLEY, Jessica *et al*. The ethics of AI in health care: A mapping review. *Social Science § Medicine*, set. 2020. DOI: 10.1016/j.socscimed.2020.113172. p. 4.

Os princípios éticos indicados oferecem linhas gerais para a avaliação de questões éticas na aplicação da IA no campo da saúde. Além desses, devem ser levados em conta fatores relevantes a aplicações específicas, por exemplo, no caso de sistemas de telemedicina, muito em voga, especialmente em tempos de pandemia, surgem preocupações com a privacidade e o tratamento de dados de pacientes. Também as aplicações no domínio da saúde pública trazem suas próprias considerações, na medida em que os deveres em relação aos pacientes individuais podem se chocar com os deveres de construção de uma política pública que traga maiores benefícios gerais. Dessa forma, a aplicação dos critérios gerais de ética de IA deve ser sempre feita à luz das peculiaridades de cada caso particular, garantindo assim a atenção aos princípios relevantes da ética médica.

A tecnologia de *Blockchain* vem sendo testada – estando em nível experimental – em pesquisas na área da saúde para permitir a interoperabilidade dos sistemas de prontuários eletrônicos e, simultaneamente, o estabelecimento de um registro com índice único e acesso distribuído, garantindo a segurança e a privacidade dos pacientes.

Da mesma forma, a tecnologia de *Blockchain* tem sido pesquisada para estabelecer, em tempo real, sensores que se comunicam com um dispositivo inteligente, autorizados via contratos inteligentes (*smart contracts)*, para gravar registros de todos os eventos ocorridos no *blockchain*. A ideia desse sistema é criar uma forma de monitoramento de pacientes e de intervenções médicas, enviando notificações aos pacientes e aos médicos, além de manter um registro seguro de quem iniciou as atividades. A proposta desse sistema seria diminuir a insegurança associada ao monitoramento remoto de pacientes e automatizar a entrega de notificações a todas as partes envolvidas[70].

O tema relacionado à organização, à padronização, à proteção e à integração de dados armazenados nos prontuários eletrônicos é fonte de proposição internacional. Pode-se destacar como exemplo as políticas que estão sendo estabelecidas e discutidas na União Europeia e nos Estados Unidos.

A União Europeia, de modo exemplar, busca integrar prontuários eletrônicos dos cidadãos europeus, reconhecendo as fragilidades associadas aos diversos

[70] 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*: MENDES, Laura Schertel; DONEDA, Danilo; SARLET, Ingo Wolfgang; RODRIGUES JUNIOR, Otavio Luiz (org.). *Tratado de Proteção de dados pessoais*. Rio de Janeiro: Forense, 2021. p. 485-506.

aspectos correlacionados ao uso dos dados, sejam eles em prol da segurança, da proteção da privacidade, da adequação ética para utilização, gerenciamento, armazenamento e descarte e a interoperabilidade entre os sistemas de informação dos Estados. Essas medidas integram o propósito de criar um Mercado Digital Comum (Digital Single Market)[71].

Remover barreiras para estabelecer um Mercado Digital Comum para a União Europeia é uma das dez prioridades da Comissão Europeia. Nesse contexto, são formuladas as seguintes decisões: Decisão 922/2009/CE do Parlamento Europeu e do Conselho, de setembro de 2009, sobre soluções de interoperabilidade para as administrações públicas europeias (*e-Health European Interoperability Framework)* e a Decisão (UE) 2015/2240 do Parlamento Europeu e do Conselho, de novembro de 2015, que cria um programa sobre soluções de interoperabilidade e quadros comuns para as administrações públicas, as empresas e os cidadãos europeus (programa ISA), como meio de modernizar o setor público (*Refined e-Health European Interoprability Framework – ReEIF*)[72].

O *e-Health European Interoperability* está organizado em um modelo, considerando princípios, governança, acordos e casos, em quatro níveis de interoperabilidade: o legal, o organizacional, o semântico e o técnico. O legal inclui a dimensão advinda dos marcos legais e regulatórios; o organizacional subdivide-se entre a aplicação em políticas e cuidados com os processos; o semântico pauta a informação e a linguagem e o técnico subdivide-se entre a aplicação e a infraestrutura com as tecnologias de informação.

Em 2017, foram fixadas novas diretrizes (*New European Interoperability Framework*) para a administração pública melhorar e aperfeiçoar a governança relacionada às atividades concernentes à interoperabilidade e para estabelecer relacionamento interorganizacional, agilizar processos de suporte de ponta a ponta de serviços digitais e garantir que a legislação existente e a nova não comprometam os esforços de interoperabilidade.

As novas diretrizes conceituais definem a interoperabilidade como a capacidade das organizações de interagirem em prol de objetivos mutuamente

---

[71] EUROPEAN COMISSION. *Policies, information and services*. S.l. 2021. Disponível em: https://ec.europa.eu/digital-single-market/en. Acesso em: 20 jun. 2021.
[72] EUROPEAN COMISSION. *E-Health European Interoperability Framework*. Brussels, nov. 2015. Disponível em: https://ec. Europa.eu/health/sites/health/files/ehealth/docs/ev_20151123_co03_en.pdf. Acesso em: 20 jun. 2021.

benéficos, envolvendo a partilha de informação e conhecimento entre essas organizações, por meio dos processos empresariais que apoiam, pela troca de dados entre os seus sistemas de tecnologias de informação e comunicação (TIC).[73]

Os Estados Unidos, por meio do *Health Insurance Portability and Accountability Act of 1996* (HIPAA), estabeleceu regras e diretrizes para modernizar o fluxo de informações na área da saúde e determinar de que forma dados pessoais deveriam ser mantidos pelos serviços de saúde e seguradoras para fiscalizar atos fraudulentos. O HIPAA fixou padrões para o uso, a transmissão e o compartilhamento de dados e informações de assistência à saúde[74].

Atualmente, observa-se uma preocupação internacional na organização de normas, políticas preventivas e diretrizes especificamente relacionadas à garantia da proteção de dados pessoais em um ambiente de *Big Data*.

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, for suscitada 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[75] diversificados e relevantes para a saúde possibilitados por *big data* permite a criação de perfis de risco mais precisos. Isso 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[76], o que resultaria em consideráveis encargos suplementares para esta última. Toma-se, nessa altura, por evidente atualidade,

---

[73] EUROPEAN COMISSION. *New European Interoperability Framework*: promoting seamless services and data flows for European public administrations. Luxembourg, 2017. Disponível em: https://ec.europa.eu/isa2/sites/isa/files/eif_brochure_final.pdf. Acesso em: 20 jun. 2021.

[74] U.S. DEPARTMENT OF HEALTH § HUMAN SERVICES. *The HIPAA Privacy Rule*. Washington, D.C. S.d. Disponível em: https://www.hhs.gov/hipaa/for-professionals/privacy/index.html. Acesso em: 20 jun. 2021.

[75] MOLINARO, Carlos Alberto; SARLET, Gabrielle Bezerra Sales. 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, a. 13, n. 41, p. 183-212, jul./dez. 2019.

[76] 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.

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* 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)[77].

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[78]. 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[79].

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 são escassas as regras de

---

[77] Cf. LEDERBERG, Joshua. 'Ome Sweet 'Omics – A genealogical treasury of words. *The Scientist*, abr. 2001. Disponível em: https://www.the-scientist.com/commentary/ome-sweet-omics---a-genealogical-treasury-of-words-54889. Acesso em: 11 ago. 2020. Ainda: PLAZA, Noelia Clemente; GARCÍA-GALBIS, Manuel Reig; MARTÍNEZ-ESPINOSA, Rosa María. Impact of the "Omics Sciences" in Medicine: New Era for Integrative Medicine. *Journal of Clinical Microbiology and Biochemical Technology*, v. 3, n. 1, p. 9-13, 2017. http://dx.doi.org/10.17352/jcmbt.000018.

[78] GIOVANELLA, Ligia *et al*. Sistema universal de saúde e cobertura universal: desvendando pressupostos e estratégias. *Ciência § Saúde Coletiva*, Rio de Janeiro, v. 23, n. 6, p. 1763-1776, jun. 2018. DOI: http://dx.doi.org/10.1590/1413-81232018236.05562018.

[79] 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*. Aparecida/SP: Ideias § Letras, 2011. p. 76.

bom funcionamento para o intercâmbio de dados[80]. 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 pode ser disposta. 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 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 sejam reduzidos e as tentativas terapêuticas fúteis sejam 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 muitos 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 quando 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[81].

---

[80] MOLINARO, Carlos Alberto; SARLET, Gabrielle Bezerra Sales. 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, a. 13, n. 41, p. 183-212, jul./dez. 2019.

[81] 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: New York Civil Liberties Union (NYCLU), mar. 2012. Disponível em: https://bit.ly/305PT0F. Acesso em: 03 jul. 2020.

Além disso, deve-se apontar que uma ênfase no exagerado tecnicismo e, portanto, no adensamento do uso de abordagens baseadas em *big data*, pode resultar em danos de natureza ainda intangível, em particular quando se coloca a transparência do vidro, assim parecem os pacientes relativamente à exposição de seus dados, coloca 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* [82] do cuidado e da responsabilidade, elementar à área da saúde, particularmente quando se trata da afetação à individualidade e à singularidade da pessoa humana.

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 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 têm evidentemente um nítido interesse na saúde de seus contratantes[83]. 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 perspectiva, 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[84] não devem ser ignorados.

---

[82] CORTINA, Adela; MARTÍNEZ, Emilio. *Ética*. São Paulo: Loyola, 2009. p. 35-36.
[83] CONSELHO NACIONAL DE SAÚDE (MS). *Legislação*. Disponível em: https://bit.ly/2TtexFR. Acesso em: 12 dez. 2020
[84] 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.

Os ajustamentos ou advertências para o enquadramento de comportamentos nocivos, a título de exemplo, podem não ser, em um primeiro momento, do interesse dos respectivos 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 a direitos humanos e fundamentais.

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[85].

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[86]. 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 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

---

[85] 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, n. 10097, p. 882-897, out. 2020.

[86] 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. DOI: http://dx.doi.org/10.11606/issn.2316-9044.v19i1p166-187. 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 jan. 2021.

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 – as instituições de seguro de saúde estatutárias levam em consideração a responsabilidade e influenciam o comportamento de saúde de seus segurados é discutível[87]. Os sistemas de incentivo baseados em 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* 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[88], 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"[89].

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

---

[87] Cf. no Brasil, GIOVANELLA, Ligia *et al*. Sistema universal de saúde e cobertura universal: desvendando pressupostos e estratégias. *Ciência § Saúde Coletiva*, Rio de Janeiro, v. 23, n. 6, p. 1763-1776, jun. 2018. DOI: http://dx.doi.org/10.1590/1413-81232018236.05562018. Ainda, 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. *Ciência § Saúde Coletiva*, Rio de Janeiro, v. 23, n. 6, jun. 2018. DOI: http://dx.doi.org/10.1590/1413-81232018236.05732021.

[88] MOLINARO, Carlos Alberto; SARLET, Gabrielle Bezerra Sales. 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, a. 13, n. 41, p. 183-212, jul./dez. 2019.

[89] Cf. em outro sentido, WANG, Yichuan; KUNG, LeeAnn; BYRD, Terry Anthony. Big data analytics: Understanding its capabilities and potential benefits for healthcare organizations. *Technological Forecasting § Social Change*, 2016. DOI: http://dx.doi.org/10.1016/j.techfore.2015.12.019.

individuais[90]. 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 juntos deve ser evitada. Para que os provedores de dados individuais possam assumir a responsabilidade por seus dados mesmo em termos de *big data*[91], 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 na saúde, portanto sensível, também há maiores requisitos de *due diligence*[92], 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.

---

[90] Cf. WANG, Yichuan; KUNG, LeeAnn; WANG, William Yu Chung; CEGIELSKI, Casey G. Integrated big data analytics-enabled transformation model: Application to health care. *Information and Management*, 2017. DOI: http://doi.org/10.1016/j.im.2017.04.001.

[91] MOLINARO, Carlos Alberto; SARLET, Gabrielle Bezerra Sales. 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, a. 13, n. 41, p. 183-212, jul./dez. 2019.

[92] Cf. RICE, Kelley H. *Physician practice mergers*: the importance of due diligence and mutual trust for all involved. American College of Medical Practice Executives. 2018. Disponível em: https://bit.ly/2YMO7Vy. Acesso em: 23 jan. 2021.

Outra maneira de assumir a responsabilidade pelos direitos do indivíduo enquanto ainda salvaguarda interesses comerciais legítimos seria utilizar 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", que substituiria o gerenciamento de dados individuais por meio de uma administração programática, fornecendo aos indivíduos uma forma 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 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[93]. No entanto, se a confiabilidade funcional de tais algoritmos for bem documentada cientificamente, é preciso também ter em conta uma perspectiva ética de que o seu uso poderia, se necessário, prevenir 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

[93] MOLINARO, Carlos Alberto; SARLET, Gabrielle Bezerra Sales. 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, a. 13, n. 41, p. 183-212, jul./dez. 2019.

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.

É inequívoco que a proteção de dados, tal como inclusive deixa evidente a LGPD, não se restringe ao meio virtual, mas a todos os meios pelos quais dados podem ser coletados e utilizados. Entretanto, não há dúvida de que é no meio virtual que se concentram as maiores preocupações e os maiores desafios da proteção de dados.

Se os dados são os insumos e os *inputs* da economia digital, os algoritmos são os instrumentos por meio dos quais os dados são processados e podem ser revertidos em resultados (*outputs*) a serem utilizados para as mais diversas finalidades[94]. Muito além de aperfeiçoar estratégias econômicas já existentes, como seriam os casos do *marketing* personalizado (*Target marketing*) e das classificações ou perfilizações (*profiling*), tais aplicações podem levar à total modificação do cenário econômico, político e social.

Com efeito, entre as principais tarefas da chamada *Data Science*, estruturada a partir dos algoritmos, estão (i) a agregação ou segmentação de informações *(clustering ou segmentation*); (ii) a identificação de fraudes ou anomalias; (iii) a

[94] Para maiores discussões sobre os algoritmos, ver FRAZÃO, Ana. Dados, estatísticas e algoritmos: Perspectivas e riscos da sua crescente utilização. *Jota*, 28 jun. 2017. Disponível em: https://www.jota.info/opiniao-e-analise/colunas/constituicao-empresa-e-mercado/dados-estatisticas-e-algoritmos-28062017. Acesso em: 14 jul. 2021.

busca de associações e complementaridades (association – *rule mining e cross-selling*); e (iv) as predições[95].

A partir dessas funcionalidades, os algoritmos estão hoje sendo programados para a extração de padrões e inferências a partir dos quais serão tomadas, de forma automatizada, decisões sobre questões objetivas, mas que estão atreladas a importantes dados sensíveis, assim como decisões sobre questões subjetivas e que envolvem complexos juízos de valor, tais como (i) avaliar as características, a personalidade, as inclinações e as propensões de uma pessoa, inclusive no que tange à sua orientação sexual; (ii) identificar estados emocionais, pensamentos, intenções e mesmo mentiras; (iii) analisar o estado de ânimo ou de atenção de uma pessoa; (iv) detectar a capacidade e a habilidade para determinados empregos ou funções; (v) analisar a propensão à criminalidade; (vi) antever sinais de doenças, inclusive depressão, episódios de mania e outros distúrbios, mesmo antes da manifestação de qualquer sintoma.

Pode-se notar que algoritmos vêm sendo utilizados para análises complexas, que abarcam as respostas para nossas perguntas mais difíceis, como decisões e diagnósticos que além de representarem uma verdadeira devassa na intimidade das pessoas, ainda podem ter impactos nas possibilidades e no acesso destas a uma série de direitos e oportunidades. Não é novidade que algoritmos hoje podem decidir quem terá crédito e a que taxa de juros, quem será contratado para trabalhar em determinada empresa, qual a probabilidade de reincidência de determinado criminoso, quem deve ser atropelado em determinadas situações, entre outras circunstâncias.

De início, cabe destacar que dados e informação não se equivalem, ainda que sejam recorrentemente tratados na sinonímia e tenham sido utilizados de maneira intercambiável ao longo deste trabalho. O dado é o estado primitivo da informação[96], pois não é algo *per se* que acresce conhecimento. Dados são simplesmente fatos brutos que, quando processados[97] e organizados[98], convertem-se em algo

---

[95] Ver KELLEHER, John D.; TIERNEY, Brendan. *Data Science*. Cambridge: The MIT Press, 2018. p. 151.

[96] Veja-se, por exemplo, o instigante estudo, cujo título fala por si mesmo: BAMBERGER, Kenneth *et al*. Privacy on the books and on the ground. *Stanford Law Review*, v. 63, p. 247, jan. 2011.

[97] SMITIS, Spiros. Reviewing Privacy in an Information Society. *University of Pennsylvania Law Review*, v. 135, p. 736, 1987: "*the chimerical nature of the assumption that effective protection of privacy can be accomplished by simply entrusting the processing decision to the persons concerned (...) process of consent is no more than a 'mystification' that ignores the long-standing experience that*

inteligível, podendo ser deles extraída uma informação[99]. Tome-se o exemplo da multinacional Zara. A simples ação de coletar e acumular os fatos (dados) das vendas e saídas de seus produtos é algo que em si não é dotado de nenhum significado. Somente quando organizados, especialmente para o fim de identificar quais produtos foram os mais vendidos, extrai-se, então, uma informação útil. Especificamente, quais produtos tiveram melhor aceitação pelo mercado consumidor para (re)projetá-los de acordo com tal tendência. Por isso, a dinâmica de um banco de dados envolve a entrada (*input)* e o processamento de dados e a saída (*output*) de uma informação. É imprescindível, portanto, o gerenciamento, manual ou automatizado, de um banco de dados, para que dele seja extraído algum conhecimento[100]. A informática e a tecnologia da informação são cruciais, pois foi com os softwares que se automatizou, ainda que parcialmente, a gestão desses bancos de dados, havendo, por conseguinte, uma guinada de ordem qualitativa no processamento de tais informações brutas. Fala-se em automatização parcial, pois tais *softwares* não eliminaram a etapa prévia, conduzida por um ser humano, de estruturação dos dados. Por exemplo, quando se "alimenta" um banco de dados, que gerencia as contas a receber de uma empresa, devem ser inseridos corretamente: i) o nome do cliente: o núcleo principal donde derivam todos os demais dados, o que é chamado de entidade; ii) o valor do serviço, da linha de crédito e o endereço: todos os demais dados que são chamados de atributos. Somente assim é possível emitir faturas de cobrança, relatórios dos clientes inadimplentes, saldos devedores etc.[101] Esse é o chamado banco de dados operacional.

---

the value of a regulatory doctrine such as 'informed consent' depends entirely on the social and economic context of the individual activity."

[98] ACQUISTI, Alessandro. Nudging privacy: behavioral economics of personal information. *İEEE Security § Privacy*, p. 83, nov./dez. 2009.

[99] A expressão "dinâmica de poder" é de: CALO, Ryan. Consumer subject review boards: a thought experiment. *Stanford Law Review Online*, v. 97, p. 97-102, set. 2013.

[100] HOOFNAGLE, Chris Jay *et al*. Behavioral advertising: the offer you cannot refuse. *Harvard Law § Policy Review*, Harvard, v. 273, n. 6, 2012. p. 285: "*In the political debate, "paternalism" is a frequently invoked objection to privacy rules. Our work inverts the assumption that privacy interventions are paternalistic while market approaches promote freedom. (...) We argue that policymakers should fully appreciate the idea that consumer privacy interventions can enable choice, while the alternative, pure marketplace approaches can deny consumers opportunities to exercise autonomy*."

[101] Em sentido mais abrangente, cobrindo a chamada proteção dos vulneráveis: MARQUES, Claudia Lima; MIRAGEM, Bruno. *O novo direito privado e a proteção dos vulneráveis*. 2. ed. São Paulo: Revista dos Tribunais, 2014. p. 124: "São essas as bases do pensamento filosófico, ético-jurídico, as quais permitem que se identifique no direito privado a ressignificação da igualdade e reconhecimento da necessidade de proteção dos vulneráveis mediante produção normativa nova, mas especialmente

Interessam, contudo, os chamados data *warehouses*, que seguem a mesma lógica acima delineada, mas são utilizados para uma tomada de decisão. Tal sistema de gerenciamento permite, por exemplo, identificar um fator que será determinante para adoção ou não de uma ação de *marketing*, como a classificação daqueles clientes que têm maior probabilidade de ser seduzidos por uma "mala direta" ou por outro tipo de abordagem publicitária[102]. Ou, ainda, no exemplo antes mencionado, se a linha de crédito deverá ser expandida de acordo com a inadimplência acumulada dos clientes-devedores.

É essa dinâmica que possibilita que uma montanha de fatos (dados) sobre os usuários da Internet seja gerenciada (informação) para lhes direcionar mensagens publicitárias personalizadas (conhecimento)[103]. Trata-se, portanto, de um fator crítico e viabilizador da publicidade comportamental.

Portanto, um banco de dados deve ser necessariamente atrelado à ideia de um sistema de informação[104], cuja dinâmica explicita, sequencialmente, um processo que se inicia pela coleta e estruturação dos dados, perpassa a extração de uma informação e, por fim, agrega conhecimento.

Por isso, os bancos de dados não são somente um agrupamento lógico e inter-relacionado do estado primitivo da informação[105], mas são, também, uma

---

a partir de uma nova perspectiva dos juristas na construção das soluções jurídicas concretas, mediante interpretação e aplicação das normas jurídicas".

[102] Neste trabalho, reconhece-se não ter uma opinião formada se as políticas de privacidade seriam consideradas contratos de adesão ou condições gerais de contratação. Isto porque os termos de uso acabam por disciplinar um número indeterminado de relações contratuais do consumidor, na medida em que, por exemplo, seria capaz de regulamentar o fluxo dos dados pessoais dos consumidores com outras aplicações com os famigerados "parceiros comerciais". Por esse viés, as políticas de privacidade enquadrar-se-iam nessa última espécie do fenômeno da massificação contratual. A indecisão é decorrente do próprio impasse na doutrina no que diz respeito à utilidade de tal diferenciação entre contratos de adesão e condições gerais de contratação. A favor: MARQUES, Claudia Lima. *Contratos no código de defesa do consumidor*: o novo regime das relações contratuais. 9. ed. São Paulo: Revista dos Tribunais, 2020. p. 74-75;86-87. Em sentido contrário: GOMES, Orlando. *Contratos de adesão*: condições gerais dos contratos. São Paulo: Revista dos Tribunais, 1972. p. 5-9.

[103] Essa é, em síntese, a "gênese" dos contratos de adesão que é marcada pela transição de uma economia artesanal e familiar por uma economia industrial em massa. Nesse sentido: MIRANDA, Custódio da Piedade Ubaldino. *Contrato de Adesão*. São Paulo: Atlas, 2002. p. 13-16.

[104] Veja-se, nesse sentido, a própria ressalva terminológica de que os contratos seriam por adesão e não de adesão. "Afinal, a aceitação em bloco de cláusulas preestabelecidas significa que o consentimento sucede por adesão, prevalecendo a vontade do predisponente (...)". (GOMES, Orlando. *Contratos de adesão*: condições gerais dos contratos. São Paulo: Revista dos Tribunais, 1972. p. 5.)

[105] "A expressão contrato de adesão resulta inicialmente do fato de que o que impressiona nessa figura, em relação à estrutura normal de um contrato, é a posição do aderente que não tem a possibilidade de discutir as cláusulas, até mesmo as que lhe sejam desfavoráveis, quer sejam ilegais, quer não, sob pena de ser excluído o círculo dos possíveis contratantes". (MIRANDA, Custódio da Piedade Ubaldino. *Contrato de Adesão*. São Paulo: Atlas, 2002. p. 20.)

ferramenta que deve criar uma interface para quem a manipula analisar e descobrir informações para a tomada de decisões. Tais decisões vão desde a concepção de um bem de consumo ao direcionamento da mensagem publicitária. Possibilita-se, pois, identificar e precisar o perfil do potencial consumidor, seus hábitos e outras "informações necessárias à tomada de decisões táticas e estratégicas"[106]. É o que se convencionou chamar de mineração de dados ou *data mining*.

Em conclusão, não se trata somente de dados ou de bancos de dados, mas, necessariamente, da dinâmica de um sistema de informação, que é o que permite a um manancial de fatos (dados) ser estruturado, organizado e gerenciado para produzir um conhecimento que possa ser revertido para tomada de uma decisão (e.g., direcionamento da ação publicitária).

A tecnologia da informação (dos *bits* ao sistema de informação) permitiu agregar e acumular dados que revelam muitas informações sobre todos. É por tal razão que não se poderia prosseguir sem antes tratar daquilo que pode ser tido como o êxtase e o estado da arte dessa matéria: *Big Data*.

[106] Realmente, no contrato de adesão, não há liberdade contratual de definir conjuntamente os termos do contrato, podendo o consumidor somente aceitá-lo ou recusá-lo. É o que os doutrinadores anglo-americanos denominam em uma *take-it-or-leave-it*". (MARQUES, Claudia Lima. *Contratos no código de defesa do consumidor*: o novo regime das relações contratuais. 9. ed. São Paulo: Revista dos Tribunais, 2020. p. 79.)

4 A EFETIVIDADE DA PROTEÇÃO DA AUTODETERMINAÇÃO INFORMATIVA

Inicialmente cabe salientar a importância acerca do “legítimo interesse” como ferramenta capaz de controlar o tratamento de dados dos indivíduos. Alguns apontamentos seguem.

É fato que a LGPD acompanha um movimento global pelo qual os países começaram a regulamentar a proteção de dados de forma cada vez mais robusta, incorporando legislações com alcance extraterritorial, inclusive[107]. Nesse contexto, o grande desafio desse movimento regulatório é equilibrar a necessidade de proteger os direitos dos titulares, ao mesmo tempo em que se garante o livre fluxo desse tipo de informação, que é reconhecidamente o insumo/ativo mais valioso para o desenvolvimento da economia global.

A realidade brasileira não era diferente. Era necessário proteger os direitos dos titulares de dados, bem como garantir que essa proteção não impediria o livre fluxo de dados pessoais no país. É nesse contexto que a LGPD foi construída sobre dois fundamentos, cuja harmonia é essencial para o referido objetivo: a autodeterminação informativa e o desenvolvimento econômico, financeiro e incentivo à inovação.

Para sustentar essa equação, a LGPD trouxe uma série de garantias, tais como: os princípios de tratamento (art. 6º), os direitos dos titulares (arts. 17 a 22) e principalmente, a Autoridade Nacional de Proteção de Dados – ANPD como órgão independente para fiscalizar e cumprir a lei (capítulo IX), inclusive com possibilidade de aplicação de penalidades (art. 52). Outra dessas garantias trazidas pela LGPD é de somente permitir o tratamento de dados pessoais nas hipóteses previstas em Lei, no caso, nos seus arts. 7º e 11. São as conhecidas bases legais para tratamento de dados pessoais.

Uma dessas hipóteses de tratamento é o legítimo interesse do controlador ou de terceiros. É importante perceber que a hipótese de tratamento pelo legítimo interesse, além de estar no rol de proteção para os titulares (como base legal),

[107] Como exemplo, o artigo 3 do General Data Protection Regulation do Parlamento Europeu e do Conselho.

também garante a possibilidade de utilização dos dados pessoais quando há interesse do negócio ou mesmo da sociedade de maneira mais ampla[108].

Alguns aspectos relevantes para a devida aplicação do legítimo interesse são necessários. Para que o tratamento[109] de um dado pessoal seja lícito, é preciso que esteja enquadrado em uma das bases legais trazidas pela LGPD[110], isto é, em uma das hipóteses em que a lei autoriza o tratamento de dados pessoais[111].

Uma dessas hipóteses é o legítimo interesse do controlador, previsto no art. 7º, IX, da LGPD:

> Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:
> (…)
> IX – quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais;

O desafio inicial para a aplicação prática (tema sempre interessante) dessa base legal é compreender o que efetivamente significa legítimo interesse. Primeiro porque essa abrangência pode fazer com que o controlador[112] caia na tentação de utilizá-la como uma base legal periférica, isto é, que pode abarcar todo e qualquer tipo de tratamento, sem maiores critérios.

A seguir, para que o tópico não se alongue demais, aborda-se outra questão de fundamental relevância ao tema da efetividade da autodeterminação informativa. Note-se que tanto o legítimo interesse quando a Autoridade Nacional de Proteção de Dados são meios eficazes e afins à autodeterminação informativa. A ANPD foi

---

[108] FRANCOSKI, Denise de Souza L.; TASSO, Fernando Antonio. *A Lei Geral de Proteção de Dados Pessoais LGPD*: Aspectos Práticos e Teóricos relevantes no setor público e privado. 1. ed. São Paulo: Thomson Reuters Brasil, 2021.

[109] Art. 5º. Para os fins desta lei, considera-se:
X – tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação, ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

[110] As bases legais para o tratamento de dados pessoais estão indicadas no art. 7º da LGPD; para tratamento de dados sensíveis, no art. 11; e para tratamento de dados de crianças no art. 14.

[111] BLUM, Renato Opice; FURTADO, Tiago Neves. Legítimo Interesse: Nuances e limites para aplicações práticas no âmbito da LGPD. *In*: FRANCOSKI, Denise de Souza L.; TASSO, Fernando Antonio. *A Lei Geral de Proteção de Dados Pessoais*: Aspectos Práticos e Teóricos relevantes no setor público e privado. 1. ed. São Paulo: Thomson Reuters Brasil, 2021. p. 304-308.

[112] Art. 5º. Para os fins desta lei, considera-se:
(…)
VI – controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais.

inspirada em órgãos reguladores internacionais, especialmente no Regulamento Europeu de Proteção de Dados.

Os modelos de regulação de proteção de dados pessoais dos cidadãos oscilam em um espectro mais liberal, presente no ordenamento jurídico norte-americano, que valoriza a escolha individual, até uma forte regulamentação estatal dos ordenamentos jurídicos europeus[113]. Com efeito, a doutrina sinaliza uma variedade de instrumentos – internacionais, regulatórios e técnicos – como ferramentas mais comuns exaradas em políticas, leis e práticas de um número crescente de países. Uma característica proeminente dos instrumentos regulatórios é a existência de autoridades de proteção de dados, ou órgãos de supervisão. Nesse sentido, o estudo a respeito da ANPD, instituída pela LGPD, deve ser realizado nesse contexto, ou seja, como um instrumento regulatório importante na salvaguarda da proteção de dados pessoais e todas as repercussões sobre a proteção do indivíduo e da dignidade da pessoa humana[114]. A seguir, serão abordados a ANPD e o CNPDP.

A atuação de uma autoridade de proteção de dados merece atenção dado que, nesse caso, a simples atuação do indivíduo para a proteção de seus interesses – o controle individual, que pode se materializar em algumas das concepções de proteção de dados pessoais – em muitas ocasiões não é capaz de proporcionar uma tutela adequada. A impossibilidade de que os direitos que hoje estão relacionados à proteção de dados sejam contemplados unicamente pela ação singular de seu interessado é patente em vista da desproporção entre as possibilidades do indivíduo e as estruturas hoje dedicadas ao tratamento de seus dados[115].

A evocação dos direitos relacionados à proteção de dados pela atuação específica do cidadão, além de não se configurar realista para grande parte dos casos de maior relevância, ressoa como uma tradição de certa maneira elitista do

---

[113] GEDIEL, José Antonio Peres; CORREA, Adriana Espíndola. Proteção jurídica de dados pessoais: a intimidade situada entre o Mercado e o Estado. *Revista da Faculdade de Direito UFPR*, Curitiba, n. 47, p. 141-143, 2008. DOI: http://dx.doi.org/10.5380/rfdufpr.v47i0.15738. p. 143.

[114] SILVA, Amanda Rodrigues da. Autoridade Nacional de Proteção de Dados: Aspectos Institucionais da Autoridade Brasileira em Comparação com os Requisitos estabelecidos no Regulamento Europeu. MENKE, Fabiano; DRESCH, Rafael de Freitas Valle (org.). *Lei Geral de Proteção de Dados*: Aspectos Relevantes. 1. ed. Indaiatuba: Foco, 2021. p. 285-314.

[115] DONEDA, Danilo. A autoridade nacional de proteção de dados e o conselho nacional de proteção de dados. In: MENDES, Laura Schertel; DONEDA, Danilo; SARLET, Ingo Wolfgang; RODRIGUES JUNIOR, Otavio Luiz (org.). *Tratado de Proteção de dados pessoais*. Rio de Janeiro: Forense, 2021. p. 459-471.

direito à privacidade, pelo qual este seria um direito efetivamente direcionado para aqueles que possuam meios para o seu exercício.

Para a efetiva proteção dos direitos em questão na amplitude necessária, seja esta individual ou coletiva, cabe a devida consideração das características da matéria de proteção de dados pessoais a partir dos desafios específicos à implementação de um sistema adequado de tutela[116]. Conforme observa-se, trata-se de seara na qual os danos de reduzidíssima monta são comuns, o que diminui a propensão para que se postule individualmente sua reparação a partir dos institutos tradicionais de responsabilidade civil. A utilização de uma tutela baseada na responsabilidade não é, por si só, um instrumento que tutele na medida necessária o direito fundamental à proteção de dados pessoais, podendo inclusive vir a incentivar a consolidação de práticas de utilização indevida de dados pessoais. A ação de uma autoridade para a proteção de dados pessoais representa, portanto, instrumento necessário para a efetivação de uma garantia fundamental. A fim de que uma ANPD seja realmente eficaz, deverá ela ter especialmente dois atributos: autonomia e independência.

A independência, atributo intrínseco à própria razão de ser de uma autoridade de proteção de dados, pode ser garantida por meio de mecanismos que busquem isolar sua atuação da influência dos poderes estatais constituídos na administração pública direta. Para tal, entre suas normas constituidoras, costumam estar presentes mecanismos que lhes garantam, por exemplo, gerência sobre seu próprio orçamento e estrutura, a limitação da discricionariedade na escolha de seus membros (por meio, por exemplo, da exigência de determinada formação ou atuação profissional), a incompatibilidade de atuação destes membros com outras atividades, atuais ou mesmo futuras (a conhecida “quarentena” para os diretores egressos antes de que iniciem novas atividades), entre outras. Igualmente fundamental para a sua independência é a ausência de ingerência governamental (muito importante no

[116] Sem se referir à hipótese de uma autoridade independente, Antonio Herman Benjamin acena à necessidade de um controle plural para os dados pessoais: “Os organismos, privados ou públicos, que armazenam informações sobre os consumidores clamam, pois, por controle rígido, seja administrativo, seja judicial, este ora penal, pra civil.” (BENJAMIN, Antonio Herman *et al*. *Código Brasileiro de defesa do consumidor*: comentado pelos autores do anteprojeto. 6. ed. Rio de Janeiro: Forense Universitária, 1999. p. 328.)

cenário em que se opera atualmente) sobre seus atos, ao não colocar tais órgãos em uma posição de vinculação hierárquica em relação ao governo[117].

A independência dessas autoridades é também causa de um aparente paradoxo, presente em seu próprio código genético: ela implica um afastamento hierárquico da administração pública direta, legitimada pelo voto. Torna-se necessário, portanto, definir a sua independência a partir do princípio democrático, e não somente por meio dos ditames da prática e da necessidade. O problema da legitimação pelas autoridades independentes é o desdobramento de um problema clássico da democracia, que é a existência de organismos de vultuosa importância institucional que eventualmente não são diretamente legitimados pelo voto popular[118].

Essa não é, no entanto, uma solução institucional arbitrária, visto que procura abordar demandas cuja crescente complexidade e conteúdo técnico exigem ações que dificilmente obteriam resposta adequada e célere da administração direta, conforme anteriormente citado. Na verdade, o problema muitas vezes é menos a legitimidade democrática em si do que a forma de implementá-la, de modo que existem mecanismos de controle como a estrita atribuição e delimitação de competências por lei, a constante referência central aos seus valores constitucionais e objetivos específicos, além de um correto equilíbrio entre a sua independência e os fundamentos de sua legitimidade.

A independência dessas autoridades é um atributo fundamental para que sua missão seja exitosa. Essa independência é importante não somente para a tutela do cidadão, mas também para a estruturação de todo o sistema normativo de proteção de dados, que compreende aspectos da regulação do próprio fluxo de dados. Assim, também para o setor privado uma autoridade independente afigura-se útil por diversos motivos, como a uniformização da aplicação da lei em um mesmo território e em circunstâncias nas quais eventualmente tribunais ou reguladores setoriais tendam a produzir soluções heterogêneas quanto à interpretação da legislação de proteção de dados. Essa consistência também é importante para impedir que

---

[117] DONEDA, Danilo. A autoridade nacional de proteção de dados e o conselho nacional de proteção de dados. In: MENDES, Laura Schertel; DONEDA, Danilo; SARLET, Ingo Wolfgang; RODRIGUES JUNIOR, Otavio Luiz (org.). *Tratado de Proteção de dados pessoais*. Rio de Janeiro: Forense, 2021. p. 459-471.

[118] Conforme observa Stefano Rodotà em prefácio à obra de Fiorella Schioppa (Le autorità indipendenti e il buono funzionamento dei mercati. Milano: Il Sole 24, 2002, p. 13-14)

empresas que eventualmente não cumpram a LGPD acabem por ter vantagens competitivas em relação às demais, com prejuízo para os cidadãos[119].

Ainda, a autoridade possui um arsenal específico de medidas regulatórias à sua disposição maior do que os tribunais, inclusive com medidas que visam a incutir e fomentar boas práticas no tratamento de dados por meio das regras de *accountability*, além de possuir um regime sancionatório próprio, adaptado à natureza da matéria e com metodologia própria. Isso, somado ao fato de que a centralização da matéria em uma autoridade evita o risco da fragmentação da interpretação da lei entre tribunais e mesmo outros órgãos administrativos com competências eventualmente concorrentes, garante a uniformidade dos direitos do cidadão e a segurança jurídica na aplicação da LGPD.

Para que se caracterize esta necessária independência da autoridade, portanto, suas atividades fiscalizatória, sancionatória e decisional não devem se subordinar hierarquicamente a outros órgãos. A autoridade ainda deverá contar com as prerrogativas necessárias, como por exemplo a existência de mandato fixo de seus dirigentes, para que executem suas funções de forma autônoma e isonômica para quaisquer setores e modalidades de tratamento de dados pessoais.

Desse imperativo, aliás, deriva a opção de a LGPD estabelecer que, em até dois anos de sua estruturação, seja realizada revisão para que se atribua, eventualmente, natureza de autarquia especial à Autoridade Nacional de Proteção de Dados (art. 55-A, I e II, da LGPD).

Uma autoridade independente, com autonomia técnica e dotada dos meios necessários para realizar suas funções, é, portanto, condição orgânica para que as garantias presentes na LGPD sejam eficazes. E, ainda, é uma peça indispensável para que o Brasil obtenha as vantagens econômicas e políticas derivadas da LGPD: por exemplo, a obtenção da adequação europeia, que pode garantir o livre fluxo de dados pessoais entre o Brasil e os países do bloco, depende inexoravelmente do estabelecimento de uma autoridade independente[120]; o ingresso do Brasil na OCDE

---

[119] DONEDA, Danilo. A autoridade nacional de proteção de dados e o conselho nacional de proteção de dados. In: MENDES, Laura Schertel; DONEDA, Danilo; SARLET, Ingo Wolfgang; RODRIGUES JUNIOR, Otavio Luiz (org.). *Tratado de Proteção de dados pessoais*. Rio de Janeiro: Forense, 2021. p. 459-471.

[120] Uma breve descrição dos requisites e do processo de adequação aos padrões de proteção de dados da legislação europeia, pode ser consultada no “Adequacy referential”, documento produzido pelo grupo de autoridades de proteção de dados europeias WP29 e posteriormente referendado pelo EDPB (European Data Protection Board). Disponível em: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614108. Acesso em 05 jul.2021.

pode ser facilitado, entre outros. De forma geral, o comércio internacional vem apresentando requisitos mais concretos quanto à proteção de dados, sendo um destes a existência de uma autoridade independente como condição para que empresas ou órgãos brasileiros possam participar livremente de fluxos internacionais de dados, tão caros à nova economia da informação. A seguir serão abordadas a estrutura organizacional da ANPD e do CNPDP.

O Decreto 10.474/2020 define a estrutura organizacional da ANPD e estabelece parâmetros necessários para a instalação do Conselho Nacional de Proteção de Dados e da Privacidade (CNPDP). A efetiva criação de ambos, no entanto, ainda está pendente da nomeação do diretor-presidente da ANPD, que é condição suspensiva para a entrada em vigor do referido Decreto.

A estrutura definida pelo Decreto para a ANPD prevê, no art. 3º do Anexo I do Decreto, além do seu Conselho Diretor já previsto na LGPD como composto pelos seus cinco diretores, um deles Diretor-Presidente, que este será assistido por uma Secretaria-Geral, uma Coordenação-Geral de Administração e uma Coordenação-Geral de Relações Internacionais e Institucionais. Como órgãos seccionais, a ANPD terá uma Corregedoria, uma Ouvidoria e uma Assessoria Jurídica; finalmente como órgãos específicos singulares, a ANPD terá três Coordenações-Gerais: a de Normalização, a de Fiscalização e a de Tecnologia e Pesquisa.

Entre outros aspectos cuja regulamentação será necessária na entrada em operação da ANPD, o Decreto esclareceu alguns aspectos referentes ao Conselho Nacional de Proteção de Dados e da Privacidade (CNPDP), indispensáveis para a sua efetividade. Dentre estes, destaque-se a previsão de que a presidência do CNPDP é fixada na pessoa do conselheiro indicado pela Casa Civil da Presidência da República (art. 15, I, do Anexo I do Decreto), ao qual incumbe, com exclusividade, convocar, coordenar e dirigir as reuniões do Conselho, além de convocar eventuais sessões extraordinárias para além das três sessões anuais, também previstas no Decreto.

Essa concentração de poderes quanto à operacionalização do CNPDP exclusivamente nas mãos da Casa Civil da Presidência da República, junto ao fato de os conselheiros setoriais que formarão o CNPDP deverem ser escolhidos por ato discricionário do Conselho Diretor da ANPD e posteriormente referendados pela mesma Casa Civil da Presidência da República, abre a possibilidade de que a representatividade setorial no CNPDP possa ser diluída caso haja a eventual

seleção e nomeação de conselheiros que não estejam plenamente identificados com as demandas do seu respectivo setor – possibilidade esta que é plausível, vista a inexistência de qualquer mecanismo que proporcione a cada setor indicar os representantes que julgar mais adequados por mecanismos de escolha próprios. Nesse sentido, verifica-se que o Decreto torna possível um eventual esvaziamento do modelo multissetorial que, em última análise, seria extremamente bem-vindo para induzir as diferentes visões e abordagens dos vários setores da sociedade que estarão diretamente afetados com a normativa de proteção de dados pessoais – esta foi, aliás, a própria razão de ser da criação do CNPDP[121].

[121] DONEDA, Danilo. A autoridade nacional de proteção de dados e o conselho nacional de proteção de dados. In: MENDES, Laura Schertel; DONEDA, Danilo; SARLET, Ingo Wolfgang; RODRIGUES JUNIOR, Otavio Luiz (org.). *Tratado de Proteção de dados pessoais*. Rio de Janeiro: Forense, 2021. p. 459-471.

5 PARA ALÉM DA AUTODETERMINAÇÃO INFORMATIVA: PROTEÇÃO DE DADOS PESSOAIS E SALVAGUARDA DA CONFIDENCIALIDADE E DA INTEGRIDADE DOS SISTEMAS TÉCNICO-INFORMACIONAIS

A dinâmica na esfera da evolução das tecnologias de informação e a necessidade de reações regulatórias adequadas para o efeito da proteção de direitos fundamentais, inclusive na seara da proteção de dados pessoais, acabaram confirmando a insuficiência de um direito à autodeterminação informativa, que de qualquer sorte, não substituiu pura e simplesmente outros direitos, como é o caso da privacidade.

Por essa razão, é de se trazer à colação, nesse contexto, outra contribuição importante da jurisprudência constitucional alemã, designadamente, o reconhecimento, pelo Tribunal Constitucional Federal, de um direito fundamental à garantia da confiabilidade e integridade dos sistemas técnico- informacionais (*Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität Informationstechnischer Systeme*), também conhecido como Direito Fundamental – TI (*IT – Grundrecht*), deduzido, a exemplo da autodeterminação informativa, como direito implícito especial de personalidade, a partir do direito geral de personalidade e do princípio da dignidade da pessoa humana[122].

No caso julgado pela Corte Constitucional Alemã, estava em causa a legitimidade constitucional de lei do estado alemão de Nordhein – Westfalen, que autorizava as autoridades policiais a adotar medidas sigilosas de vigilância e monitoramento remoto da internet (incluindo correspondência eletrônica – e-mail) bem como acesso secreto e remoto a sistemas de tecnologias de informação (computadores), incluindo o monitoramento de todas as atividades de suspeitos da prática de ilícitos penais na internet, medidas que tinham por escopo a proteção da ordem constitucional estatal em face da crescente criminalidade, destaque para o crime organizado e o terrorismo[123].

---

[122] Cf. decisão de 27.02.2008, publicada em BVerfGE 120, 274 e ss.

[123] Cf. MENKE, Fabiano. A proteção de dados e o novo direito fundamental à garantia da confidencialidade e da integridade dos sistemas técnico-Informacionais no direito alemão. *In*:

Uma das lacunas possivelmente mais importantes não cobertas pelo direito à autodeterminação informativa diz respeito ao fato de que terceiros que acabam tendo acesso a dados armazenados em algum sistema técnico-informático não se encontram sujeitos às regras sobre a coleta e tratamento de tais dados, de tal sorte que uma das diferenças entre os dois direitos reside na circunstância de que a autodeterminação informativa se refere a um dado ou a um conjunto de dados, ao passo que o direito à garantia da confiabilidade e integridade dos sistemas técnico-informacionais tem por objeto a proteção do sistema como um todo (e por isso a confiança na sua utilização) e os dados em sentido amplo, evitando que terceiros possam se apropriar até mesmo de um perfil da personalidade do usuário dos sistemas[124].

MENDES, Gilmar Ferreira; SARLET, Ingo Wolfgang; COELHO, Alexandre Zavaglia P. (coord.). *Direito, Inovação e tecnologia*. São Paulo: Saraiva, 2015. p. 205-230. p. 205 ss.

[124] Cf. MENKE, Fabiano. A proteção de dados e o novo direito fundamental à garantia da confidencialidade e da integridade dos sistemas técnico-Informacionais no direito alemão. *In*: MENDES, Gilmar Ferreira; SARLET, Ingo Wolfgang; COELHO, Alexandre Zavaglia P. (coord.). *Direito, Inovação e tecnologia*. São Paulo: Saraiva, 2015. p. 205-230. p. 219.

6 DIREITO FUNDAMENTAL À SAÚDE

6.1 A SAÚDE COMO DIREITO FUNDAMENTAL

Sarlet, ao analisar o direito à saúde, entende que ele pode ser considerado como norma jusfundamental que constitui, além do clássico direito prestacional que impõe ao Estado a realização de políticas públicas, um direito de defesa, que afasta intervenções estatais indevidas na integridade psicofísica do indivíduo[125]. Considera-se, desse modo, que o direito à saúde significa que o sujeito tem a faculdade de resistir a ingerências em seu corpo, inclusive no sentido de decidir sobre como preservar e recuperar sua saúde. Essa possibilidade de decisão significa ser informado acerca da sua situação de saúde e das recomendações para seu tratamento, e, diante delas, poder escolher livre e conscientemente.

Nesse mesmo sentido, o Código de Ética Médica, em seu art. 31, IV, estabelece que é vedado ao médico "desrespeitar o direito do paciente ou de seu representante legal de decidir livremente sobre a execução de práticas diagnósticas ou terapêuticas, salvo em caso de iminente risco de morte." Parece bastante pertinente tal discussão, especialmente em tempos de pandemia, em que muito se fala sobre a autonomia médica no que tange à prescrição de medicamentos não comprovados cientificamente como parte de um pseudotratamento precoce.

Os deveres fundamentais, por sua vez, são também de extremo relevo, pois imprescindíveis para a garantia dos direitos fundamentais. A ideia de dever fundamental geralmente advém da concepção prévia de determinado direito fundamental como comportamento obrigatório por parte do Estado – ou de particulares, em casos específicos e expressos – para que o direito ao qual se vincula possa ser realizado, ainda que potencialmente. Alguns encontram-se

[125] RESENDE, José Renato Venâncio; ALVES, Cândice Lisbôa. A vacinação obrigatória como um dever jurídico decorrente do direito fundamental à saúde. *Revista da Faculdade de Direito UFPR*, Curitiba, v. 65, n. 2, maio/ago. 2020. DOI: http://dx.doi.org/10.5380/rfdufpr.v65i2.69582.

expressos na própria Constituição (por exemplo, dever de alistamento obrigatório), outros são decorrentes do texto constitucional, ainda que implícitos[126].

6.2 PROTEÇÃO E COMPARILHAMENTO DE DADOS NA SAÚDE SUPLEMENTAR

A constituição Federal assegura que a saúde é direito de todos e dever do Estado (art. 196), mas também prevê a atuação da iniciativa privada (art. 199) na assistência à saúde de forma complementar ao Sistema Único de Saúde (SUS)[127]. Assim, o sistema de saúde brasileiro pode ser acessado pelo cidadão por meio de dois subsistemas:

a) O SUS – serviço público e universal, financiado pelo Estado nos níveis federal, estadual e municipal, podendo ainda a iniciativa privada complementar os serviços oferecidos pelo SUS, quando suas disponibilidades forem insuficientes para garantir a cobertura assistencial à população de uma determinada área; e
b) O Sistema de Saúde Privado[128] – seja por meio da contratação de planos privados de assistência junto a operadoras de planos de saúde (Sistema de Saúde Suplementar), seja mediante a contratação direta de serviços de saúde junto aos prestadores privados.

Por sua vez, a Operadora de Planos de Saúde (OPS) é a pessoa jurídica, obrigatoriamente registrada na ANS, que opera ou comercializa planos privados de assistência à saúde. Já os contratantes de seguros ou planos de saúde podem ser pessoas físicas ou jurídicas, sendo o beneficiário do contrato a pessoa física, titular ou dependente, que usufrui dos serviços de saúde nele estabelecidos. Os valores das mensalidades são calculados conforme o risco do beneficiário, o que pode ser um método inexato e discriminatório, ocasionando uma forte fiscalização dos órgãos reguladores a fim de evitar abusos.

Uma vez que a cobertura do SUS é universal, o beneficiário da saúde suplementar também está coberto pelo sistema público. Além disso, os dois

[126] RESENDE, José Renato Venâncio; ALVES, Cândice Lisbôa. A vacinação obrigatória como um dever jurídico decorrente do direito fundamental à saúde. *Revista da Faculdade de Direito UFPR*, Curitiba, v. 65, n. 2, maio/ago. 2020. DOI: http://dx.doi.org/10.5380/rfdufpr.v65i2.69582.
[127] Regulada pela Lei n. 8080, de 19 de setembro de 1990, que dispõe sobre as condições para a promoção, proteção e recuperação da saúde, a organização e o funcionamento dos serviços correspondentes e dá outras providencias.
[128] A regulação da saúde suplementar foi iniciada 1999, quando entrou em vigor a Lei 9.656/1998, que dispõe sobre os planos de saúde.

sistemas possuem uma rede de prestadores em comum, formada por clínicas, hospitais e médicos, entre outros, que apesar de conveniados ao SUS, prestam serviços às operadoras de planos e seguros de saúde, assim como há prestadores de serviços privados que atendem a usuários do SUS[129].

Todo esse sistema privado é regulado por três órgãos: a Agência Nacional de Vigilância Sanitária (ANVISA) é responsável pela regulação sanitária e econômica do mercado de compra e venda de insumos hospitalares; a Agência Nacional de Saúde (ANS) tem como competência regular o fluxo financeiro e de serviços entre operadoras, beneficiários e prestadores; e o Sistema Brasileiro de Defesa da Concorrência (SBDC) deve garantir a competitividade do setor.

De forma geral, os agentes econômicos do setor da saúde sempre estiveram muito preocupados com o sigilo dos dados de saúde dos usuários (dados de saúde), restringindo o compartilhamento de dados médicos, com o objetivo de não gerar constrangimento ou discriminação do paciente e propiciar o acesso à saúde[130].

O Conselho Federal e os Conselhos Regionais de Medicina foram instituídos pelo Decreto-lei n. 7.955/1945, ganharam o *status* de autarquia em 1957 por meio da Lei n. 3.268 e sempre tiveram a competência de supervisionar a ética profissional no território nacional, além de julgar e disciplinar a classe médica. O Código de Ética Médica (Resolução CFM n. 2.217/2018, modificada pelas Resoluções CFM n. 2.222/2018 e 2.226/2019) traz a obrigação de sigilo como princípio e dever do médico, prevendo como exceção apenas o dever legal e o consentimento dado pelo paciente. Da mesma forma prevê o Código de Ética de Enfermagem (Resolução COFEN n. 0564/2017, art. 52). A obrigação de confidencialidade das informações também está presente na Lei n. 13.787/2018, que trata do prontuário médico.

---

[129] FAVERO, Walquiria Nakano Eloy. Proteção e Compartilhamento de Dados na Saúde Suplementar. In: DALLARI, Analluza Bolivar; MONACO, Gustavo Ferraz de Campos (coord.). *LGPD na Saúde*. 1. ed. São Paulo: Thomson Reuters Brasil, 2021. p. 171-194.

[130] A primeira publicação com referência à proteção da privacidade na *Common Law* ocorreu em 1890, em um artigo publicado na Harvard Business Review por Samuel D. Warren e Louis D. Brandeis, denominado "*The right to Privacy*". Em 1948, a Declaração Universal dos Direitos Humanos previu como Direito Fundamental o Direito à Privacidade. Em 1981, o Conselho Europeu adota a Convenção de Proteção de Dados (Tratado 108), prevendo privacidade como um direito legal. Com as novas tecnologias, a comunicação por redes iniciada na década de 1990, o tratamento intensivo de dados pessoais no setor privado para segmentar produtos e serviços e aumentar a eficiência de seu processo produtivo e o uso de *Big Data*, é criada em 1995 a Diretiva Europeia de Proteção de Dados, refletindo os avanços tecnológicos e a introdução de novos termos, como processamento, dados sensíveis e consentimento, sendo sucedido em 2016 pelo Regulamento Geral de Proteção de Dados, a denominada GDPR. Neste interim, diversos escândalos como "Cambridge Analytica", investigações e vazamentos de dados pessoais reforçaram a necessidade no cuidado com a privacidade e um sistema que efetivasse a proteção de dados pessoais dos indivíduos.

No Brasil, a lei que regulamenta os planos de saúde não permite discriminar esses valores de acordo com o sexo, com a existência de doença antes do contrato ou outras características do beneficiário que influenciem no padrão de utilização do serviço contratado[131]. O único atributo individual admitido para a fixação de preços diferenciados em lei é a idade[132]. Interessante notar esse ponto, pois na realidade o cenário é bem diferente. Não todos, mas vários planos de saúde desrespeitam a lei, utilizando-se de critérios próprios a fim de fixar preço que impossibilita ao usuário aderir a tal serviço.

Segundo dados do Cenário Saúde publicado pelo Sistema Abramge/Sinamge/Sinog em 2020, a taxa de cobertura de planos médico-hospitalares atingiu o ápice nos anos 2014 e 2015, quando 24,7% da população brasileira tinha acesso à saúde suplementar. Desde então, o setor vem amargando sucessivas quedas, que acarretaram uma redução da ordem de 1,7% entre 2015 e 2020. Hoje, 23% da população conta com cobertura suplementar. Nota-se que nem um quarto da população brasileira conta com serviços de qualidade ou agilidade. Não há necessidade de expor as mazelas do Sistema Único de Saúde brasileiro.

Cabe trazer a lume algumas iniciativas na área da saúde que possuem um forte impacto na temática da privacidade, entre as quais está a integração de dados de saúde com dispositivos médicos, com a telemedicina, com a inteligência artificial, com a internet das coisas, com os aplicativos de saúde e com a coordenação de cuidados dos pacientes, para que mantenha um comportamento preventivo, de forma que a prioridade seja a manutenção da saúde e não simplesmente o tratamento de uma doença, entre outros. Além disso, o acesso à medicina personalizada, ou à medicina do futuro, promete oferecer pelo seu *framework*: um diagnóstico precoce e preciso, o monitoramento e atendimento à distância, planos de atendimento individualizado, melhoramento da gestão de riscos, opções de

[131] A Lei n. 8.080/90, em suas razões expositivas, sempre teve o intuito de proteger os cidadãos, para evitar a discriminação e dar acesso ao sistema, independentemente do seu histórico de saúde – "Art. 2 A saúde é um direito fundamental do ser humano, devendo o Estado prover as condições indispensáveis ao seu pleno exercício. Inciso 1 O dever do Estado de garantir a saúde consiste na formulação e execução de políticas econômicas e sociais que visem à redução de riscos de doenças e de outros agravos e no estabelecimento de condições que assegurem acesso universal e igualitário às ações e aos serviços para a sua promoção, proteção e recuperação". O acesso à saúde está intimamente ligado à proteção dos dados de saúde que, por sua própria natureza e sensibilidade das informações, pode levar ao cerceamento ao acesso ao sistema de saúde em decorrência das condições e custos para tratamento de um paciente.

[132] Os beneficiários de planos de saúde são divididos em dez faixas etárias, e o valor fixado para a última faixa não pode ser superior a seis vezes o valor da primeira. Além disso, a variação acumulada entre a 7 e a 10 faixa não poderá ser superior a variação acumulada entre a 1 e a 7 faixa.

tratamento personalizado e a mudança de paradigma "*one-size fits all*", e, assim não só gerar o acesso à medicina personalizada como também melhorar a função do sistema de saúde como um todo – sendo um dos seus principais desafios para implantação a coleta e o armazenamento de informação de forma integrada, especialmente nos registros eletrônicos de saúde, bem como pelos próprios dispositivos de monitoramento do indivíduo[133].

Portanto, partindo desse prisma, o compartilhamento de dados de saúde é, além de uma necessidade, uma realidade cada vez mais presente no dia a dia, e discutir a sua realização, seguindo os princípios e requisitos da LGPD nos diversos elos da cadeia, tendo o interesse e o cuidado com o paciente no centro efetivamente, para lhe propiciar um cuidado real com a sua saúde e o protegendo não só de quaisquer ameaças à sua personalidade e dos riscos de sua discriminação e estigmatização de mercado[134], mas também viabilizando um sistema que possibilite ao titular dos dados o gerenciamento dos seus dados e o exercício dos seus direitos, concretiza assim a efetiva proteção de dados pessoais.

Neste sentido, Doneda afirma que

> A privacidade assume, portanto, posição de destaque na proteção da pessoa humana, não somente tomada como escudo contra o exterior- na lógica da exclusão – mas como elemento indutor da autonomia, da cidadania, da própria atividade política sem sentido amplo e dos direitos de liberdade de uma forma geral. Nesse papel, ela é pressuposto de uma sociedade democrática moderna, da qual o dissenso e o anticonformismo são componentes orgânicos.[135]

6.3 COMPARTILHAMENTO DE DADOS DE SAÚDE E AGENTES DO TRATAMENTO DE DADOS NA REDE SUPLEMENTAR

Os agentes envolvidos na cadeia da saúde suplementar são: i) o paciente; ii) os médicos e demais profissionais da saúde que atuam na assistência ao paciente; iii) os prestadores de serviço/fornecedores; iv) a Operadora de Plano de Saúde (OPS) e as Agências Reguladoras, a Agência Nacional de Saúde Suplementar

---

[133] FAVERO, Walquiria Nakano Eloy. Proteção e Compartilhamento de Dados na Saúde Suplementar. In: DALLARI, Analluza Bolivar; MONACO, Gustavo Ferraz de Campos (coord.). *LGPD na Saúde*. 1. ed. São Paulo: Thomson Reuters Brasil, 2021. p. 171-194.
[134] MENDES, Laura Schertel. *Privacidade, proteção de dados e defesa do consumidor*: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014. p. 236.
[135] DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*. 2. ed. São Paulo: Revista dos Tribunais, 2020.

(ANS) e a Agência Nacional de Vigilância Sanitária (ANVISA). As relações jurídicas firmadas entre esses agentes de tratamento nesta cadeia são basicamente as seguintes:

i) Operadora de Plano de Saúde (OPS) celebra um contrato de plano de saúde com o paciente, por meio do qual se obriga, mediante remuneração, a oferecer a cobertura estabelecida em contrato;

ii) Operadora de Plano de Saúde (OPS) celebra um contrato de credenciamento com os prestadores de serviços/fornecedores, por meio do qual os prestadores se obrigam a atender o grupo de vidas da Operadora de Plano de Saúde (OPS) nas condições estabelecidas no contrato;

iii) Prestadores de serviços celebram contratos de prestação de serviços com os pacientes, para atendimento de consultas médicas, internações, medicina diagnóstica, dentre outros.

Essas relações jurídicas estão sujeitas às normas da ANS e da Anvisa. Antes de adentrar na análise do posicionamento de cada um dos agentes de tratamento conforme a LGPD, de se rememorar alguns conceitos básicos trazidos pela LGPD.

Primeiramente, relevante lembrar que, nos termos do art. 5º, I, da lei, dado pessoal é qualquer informação relacionada a pessoa natural identificada ou identificável. Já o dado pessoal sensível (art. 5º, II) é o dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural.

A lei é aplicável tanto para pessoa natural quanto pessoa jurídica de direito público ou privado, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados, desde que: i) trate dados no território nacional; ii) a atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional. A lei só não se aplica ao tratamento de dados pessoais e se realizado por pessoa

natural para fins exclusivamente particulares e não econômicos, como uma pesquisa *pro bono*[136].

O tratamento de dados é toda operação realizada com dados pessoais, como coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração (art. 5º, X).

De acordo com a LGPD, as organizações podem ser controladoras (art. 5º, VI, e arts. 37-40) e/ou operadoras de dados pessoais (art. 5º, VII e arts. 37-40), bem como cocontroladoras. São:

i) controladoras quando determinam os objetivos e tomam decisões a respeito do uso e tratamento de dados pessoais, por exemplo, uma OPS, ou quando decidem coletar dados para a criação de uma plataforma de saúde para guardar o histórico de saúde dos seus pacientes ou oferecer serviços de telemedicina;

ii) tais controladores podem fazer uso de operadores para realizar algum tratamento em seu nome (um médico contrata uma plataforma de prontuário eletrônico para manter o prontuário digital de seus pacientes). Portanto, os operadores sob as instruções processam dados em nome dos controladores. Os controladores também podem utilizar operadores de dentro do seu grupo econômico, por exemplo, quando todas as entidades de um grupo econômico utilizam um *help desk* de TI administrado por uma entidade específica desse mesmo grupo;

iii) as organizações também podem ser simultaneamente controladoras e operadoras, por exemplo, um prestador de medicina diagnóstica ou serviços hospitalares é operador perante a OPS no modelo padrão de atuação por "*fee for service*", porém, é um controlador de dados ante o paciente;

iv) as organizações podem ser cocontroladoras quando determinam conjuntamente os objetivos do tratamento de dados pessoais (e podem utilizar terceiros como operadores), por exemplo uma OPS e um prestador hospitalar celebram um contrato no modelo de remuneração de pacote, para o cuidado de

[136] FAVERO, Walquiria Nakano Eloy. Proteção e Compartilhamento de Dados na Saúde Suplementar. In: DALLARI, Analluza Bolivar; MONACO, Gustavo Ferraz de Campos (coord.). *LGPD na Saúde*. 1. ed. São Paulo: Thomson Reuters Brasil, 2021. p. 171-194.

pacientes oncológicos, em que há o compartilhamento de dados e a tomada de decisão nos protocolos de cuidados ou seus resultados de vidas cobertas;

v) por fim, as organizações, sejam controladoras ou operadoras, devem nomear um encarregado de dados, que deverá atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD).

6.4 DIGNIDADE DA PESSOA HUMANA, LIVRE DESENVOLVIMENTO DA PERSONALIDADE, AUTODETERMINAÇÃO INFORMACIONAL

As conexões entre o princípio da dignidade da pessoa humana e o direito fundamental à proteção de dados pessoais são intensas, embora nem sempre compreendidas do mesmo modo no âmbito das diferentes ordens jurídicas. Os dois principais pontos de contato, todavia, são o princípio autonômico (autodeterminação) e os direitos da personalidade, representados pelo direito ao livre desenvolvimento da personalidade e os direitos especiais à privacidade e à autodeterminação informativa, igualmente conectados entre si, mas que não esgotam o leque de alternativas[137].

Em que pese não se tratar de premissa válida para todos os direitos fundamentais, porquanto nem todo direito fundamental tenha um fundamento direto e um conteúdo em dignidade, no caso do direito à proteção de dados pessoais, o princípio da dignidade da pessoa humana pode e deve ser acionado, seja para a justificação da fundamentalidade daquele direito, seja para a determinação de parte de seu conteúdo, com destaque para a identificação de alguns pontos de contato com outros princípios e direitos fundamentais.

Para a compreensão dessa relação e pela sua relevância para a proteção de dados pessoais, segue atual retornar à Alemanha, porquanto é lá que se costuma situar o reconhecimento, pela primeira vez, do assim chamado direito à autodeterminação informativa, não no texto constitucional, mas por conta da paradigmática decisão do Tribunal Constitucional Federal, de 1983, sobre a constitucionalidade de aspectos da lei do censo aprovado pelo Parlamento Federal,

[137] SARLET, Ingo Wolfgang. Fundamentos Constitucionais: O direito fundamental à proteção de dados. *In*: MENDES, Laura Schertel; DONEDA, Danilo; SARLET, Ingo Wolfgang; RODRIGUES JUNIOR, Otavio Luiz (org.). *Tratado de Proteção de dados pessoais*. Rio de Janeiro: Forense, 2021. p. 21-60.

cuja realização foi suspensa liminarmente pela Corte em 13.04.1983, muito embora a existência de decisões anteriores envolvendo, ao fim e ao cabo, a proteção de dados pessoais[138]. Cuida-se de uma construção que tem sido tida como a "verdadeira chave" para a compreensão da concepção alemã relativamente à proteção de dados, tendo, além disso, influenciado um expressivo número de outras ordens jurídicas, inclusive o direito europeu.

Na sua decisão, o Tribunal Constitucional, contudo, não reconheceu diretamente um direito fundamental à proteção de dados pessoais, mas, deduziu, em uma leitura conjugada do princípio da dignidade da pessoa humana e do direito ao livre desenvolvimento da personalidade, um direito fundamental implícito à autodeterminação informativa, que consiste, em suma e de acordo com o Tribunal, na prerrogativa de cada indivíduo decidir, em princípio e substancialmente, sobre a divulgação e a utilização de seus dados pessoais[139].

O próprio Tribunal Constitucional, contudo, na mesma decisão, alertou para o fato de que o direito à autodeterminação informativa não assegura a cada cidadão um controle absoluto sobre seus dados, visto que, dadas a inserção e a responsabilidade comunitária e social do ser humano, este deve tolerar eventuais limitações do direito quando em prol do interesse geral[140].

De acordo com Hans-Peter Bull, primeiro encarregado da agência federal de proteção de dados alemã, o cerne moral e político das preocupações do Tribunal Constitucional foi, e ainda é, o da garantia da liberdade dos cidadãos em face da repressão por parte do Estado, de modo que a argumentação deduzida na decisão foi orientada de acordo com o objetivo da proteção da liberdade de ação do ser humano, sendo a transparência da coleta de informações um meio para alcançar tal finalidade.

Na condição de direito de defesa (direito à não intervenção arbitrária), o direito à autodeterminação informativa consiste em um direito individual de decisão, cujo objeto (da decisão) são dados e informações relacionados a determinada pessoa – indivíduo[141].

---

[138] Aqui costuma ser referida, dentre outras, decisão de 16.07.1969 ("*Mikrozensus – Entscheidung*"), na qual o Tribunal Constitucional assentou que a Lei Fundamental proíbe que o ser humano tenha sua inteira personalidade registrada e catalogada compulsoriamente (v. BVerfGE 27, p. 6).
[139] Cf. BVerfGE 65, p. 42 e ss.
[140] Cf. BVerfGE 65, p. 44.
[141] SARLET, Ingo Wolfgang. Fundamentos Constitucionais: O direito fundamental à proteção de dados. *In*: MENDES, Laura Schertel; DONEDA, Danilo; SARLET, Ingo Wolfgang; RODRIGUES

A relação do direito à autodeterminação informativa com o princípio da dignidade da pessoa humana, portanto, é, em certo sentido, dúplice, pois se manifesta tanto pela sua vinculação com a noção de autonomia quanto com a do livre desenvolvimento da personalidade e de direitos especiais de personalidade conexos, de tal sorte que a proteção dos dados pessoais envolve também a salvaguarda da possibilidade concreta de tal desenvolvimento, para o qual a garantia de uma esfera privada e íntima é indispensável.

De qualquer sorte, a ancoragem de um direito à proteção de dados pessoais no direito geral de personalidade, como se deu desde o início na tradição constitucional alemã, não quedou imune a críticas, sobrelevando o argumento de Spiros Simitis, no sentido de que se trata de uma moldura insuficiente para dar conta de todos os problemas, fragilidade que também se estende à conhecida teoria das três esferas da proteção da personalidade (íntima, privada ou individual e social ou pública), visto não dar conta e não considerar as diversas possibilidades de inter-relação e combinação prática entre as esferas[142].

Tal crítica, todavia, não é partilhada por todos, a exemplo do que novamente argumenta Hans-Peter Bull, para quem uma compreensão suficientemente flexível e na condição de critérios indicativos para uma diferenciação em concreto entre as esferas é possível e útil, inclusive quando se trata de avaliar a legitimidade constitucional de uma intervenção restritiva na própria autodeterminação informativa[143].

Outrossim, cabe ressaltar que o direito à autodeterminação informativa – que no concernente à sua estrutura normativa, assume condição de princípio – também não se sobrepõe ao direito à privacidade e mesmo outros direitos especiais de personalidade. Isso já se dá – mas não exclusivamente – pelo fato de o direito à autodeterminação informativa apresentar dupla dimensão individual e coletiva, no sentido de que garantida constitucionalmente não é apenas (embora possa ser, como direito subjetivo individual, o mais importante) a possibilidade de cada um decidir sobre o acesso, uso e difusão de seus dados pessoais, mas também – e aqui a dimensão metaindividual (coletiva) – se trata de destacar que a autodeterminação

---

JUNIOR, Otavio Luiz (org.). *Tratado de Proteção de dados pessoais*. Rio de Janeiro: Forense, 2021. p. 21-60.

[142] SCHIEDERMAIR, Stephanie. Einleitung. In: SIMITIS, Spiros; HORNUNG, Gerrit; SPIECKER GENANNT DÖHMANN, Indra (Coord.). *Datenschutzrecht*. Baden-Baden: Nomos, 2019. p.169 e ss.

[143] BULL, Hans Peter. *Informationelle Selbstbestimmung*: Vision oder Illusion? 2. ed. Tübingen: Mohr Siebeck, 2011. p. 41-42.

informativa constitui precondição para uma ordem comunicacional livre e democrática, distanciando-se, nessa medida, de uma concepção de privacidade individualista e mesmo isolacionista à feição de um direito a estar só (*right to be alone*)[144]. Dito de outro modo, "a proteção de dados é enquanto proteção de direitos fundamentais, espinha dorsal de uma democracia liberal"[145].

Diante do supra exposto, é possível afirmar que o direito à autodeterminação informativa, fundado na dignidade da pessoa humana e no direito ao livre desenvolvimento da personalidade, guarda, já em virtude de seus fundamentos, uma íntima e indissociável conexão com o princípio autonômico e, portanto, a noção de dignidade como autonomia, razão da extrema importância do consentimento também no domínio da proteção de dados pessoais.

6.5 O CONSENTIMENTO LIVRE, INFORMADO E ESCLARECIDO.

A noção de consentimento informado surgiu, historicamente, na medicina (e em suas respectivas pesquisas clínicas), tendo sido referenciada já por Hipócrates[146]. À época, a principal preocupação que se buscava endereçar com a coleta do consentimento era a divulgação de informações que causariam danos ou aborrecimentos aos pacientes.

Posteriormente, entre as décadas de 1950 e 1960, a jurisprudência norte-americana fez evoluir tal noção, associando-a, ainda no campo da medicina, ao dever dos médicos de informar pacientes acerca de possíveis riscos e tratamentos alternativos, para além das já estabelecidas determinações de informar a natureza do tratamento e suas consequências[147]. Voltava-se, assim o foco da discussão à qualidade e adequação das informações prestadas.

Seguiu-se então uma série de decisões judiciais nos anos seguintes voltadas a estabelecer padrões de divulgação de informações orientados pelas demandas e necessidades dos pacientes. O dever de informação passa a ser delineado pelo

---

[144] HORNUNG, Gerrit; SCHNABEL, Christoph. Data Protection in Germany I: The populational census decision and the right to informational self-determination. Computer Law § Security Review, v. 25, n. 1, p. 84-88, 2009. DOI: https://doi.org/10.1016/j.clsr.2008.11.002. p. 85-86.
[145] SPIECKER GENNANT DÖHMANN, Indra. *Kontexte der demokratie*: Parteien, Medien und Sozialstrukturen. Berlin: De Gruyter, 2018. p. 55-56.
[146] BEAUCHAMP, Tom L. *Informed consent*: its history, meaning, and present challenges. v. 20. Cambridge: Quarterly of Healthcare Ethics, 2011. p. 515.
[147] BEAUCHAMP, Tom L. *Informed consent*: its history, meaning, and present challenges. v. 20. Cambridge: Quarterly of Healthcare Ethics, 2011. p. 516.

direito à autodeterminação do paciente, que só poderia ser exercido com o fornecimento das informações necessárias para tanto[148].

Na década de 1970, passou-se a conceber um dever moral e uma obrigação legal de obtenção de consentimento informado para certos procedimentos de pesquisa, estabelecendo-se, para isso, balizas qualificadoras para sua coleta. A comunidade médica reagiu, argumentando serem as exigências de validação do consentimento quase impossíveis de serem atingidas, e, por vezes, até distantes do bem-estar dos pacientes[149].

A preocupação em cumprir tais exigências e evitar as sanções pelo seu descumprimento transferiu o foco da discussão do consentimento informado da sua substância, i.e., o oferecimento das informações necessárias à autodeterminação dos pacientes, para sua forma – a obtenção do consentimento dos pacientes como requisito meramente formal da prática médica. A doutrina jurídica construída sobre a noção do "consentimento informado" deixava, assim, de corresponder às práticas realizadas no plano concreto – o que teria sido apontado empiricamente como uma alteração no agente do médico, e não do paciente, de decidir a respeito do tratamento.

A trajetória histórica do "consentimento informado" brevemente descrita parece indicar dois significados históricos para o termo. O primeiro refere-se a uma autorização autônoma, dada pelo titular apenas quando este, com o necessário conhecimento e liberdade, intencionalmente autoriza algo (autodeterminação). No âmbito judicial da responsabilidade civil médica, o consentimento acabou por ser reduzido a dois elementos: o dever de informar e de obter o consentimento por parte dos médicos.

A obrigação judicial estabelecida por essa nova doutrina acabou afastando a noção de "consentimento informado" da autodeterminação dos pacientes enquanto detentores de papel decisivo no processo de decisão médica[150]. Esse contexto teria estabelecido o segundo significado histórico do termo, o "consentimento informado" como prática social fundada em determinados contextos institucionais. Assim, o

[148] BEAUCHAMP, Tom L. *Informed consent*: its history, meaning, and present challenges. v. 20. Cambridge: Quaterly of Healthcare Ethics, 2011. p. 516.
[149] BEAUCHAMP, Tom L. *Informed consent*: its history, meaning, and present challenges. v. 20. Cambridge: Quartel of Healthcare Ethics, 2011. p. 517-518.
[150] LUCIANO, Maria; BIONI, Bruno Ricardo. O Consentimento como processo: em busca do consentimento válido. *In*: MENDES, Laura Schertel; DONEDA, Danilo; SARLET, Ingo Wolfgang; RODRIGUES JUNIOR, Otavio Luiz (org.). *Tratado de Proteção de dados pessoais*. Rio de Janeiro: Forense, 2021. p. 149-162.

consentimento será válido se estiver em conformidade com as regras que regem determinado contexto social e institucional, independentemente da autonomia do titular. Esse tem sido, por exemplo, o sentido adotado por agências reguladoras norte-americanas[151]. E a ele se relacionam também as práticas iniciais de coleta de consentimento para tratamento de dados pessoais por aplicações de internet.

O campo da proteção de dados inclusive retomou o debate do consentimento em seu primeiro sentido histórico, como enquadramento teórico da extensão da personalidade do indivíduo que constitui esse tipo de dado. No contexto de uma economia de dados (como se verá adiante), o potencial de causar danos aos titulares conferido ao tratamento de dados pessoais, bem como seus complexos e diversos desdobramentos, reacendeu o debate em torno da coleta do consentimento como um processo. Um diálogo dinâmico em que as informações necessárias à autodeterminação informacional do titular são fornecidas e atualizadas, e o fornecimento do consentimento deste é garantido e sempre passível de revogação e revisão. Esses novos contornos parecem transcender, inclusive, o dever de informação, postulado principalmente após a entrada em vigor do Código de Defesa do Consumidor[152].

Tendo em vista o desenvolvimento peculiar que o tema vem repercutindo, busca-se a seguir tratar do consentimento a partir dos preceitos da LGPD.

O consentimento é fruto de uma relação cognoscente em que as capacidades cognitivas são ativadas em maior ou menor grau em relação às informações disponibilizadas. Não custa reforçar que as informações devem guardar diferenciação quanto à pertinência, à finalidade, à adequação, ao tempo de 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.

Afirma-se, em termos reais, o protagonismo do sujeito na dimensão linguística e discursiva aberta pela tecnologia para a condução e para a construção de sua própria vida. Interessante, nesse sentido, é a busca em garantir ainda a proteção apropriada contra os riscos de danos materiais e imateriais, e.g., em casos de

---

[151] FADEN, Ruth R.; BEAUCHAMP, Tom L. *A history and Theory of informed consent*. New York: Oxford University Press, 1986. p. 276.

[152] GUZ, Gabriela. O consentimento livre e esclarecido na jurisprudência dos tribunais brasileiros. *Revista de Direito Sanitário*, São Paulo, v. 11, n. 1, p. 95-122, mar./jun. 2010. DOI: https://doi.org/10.11606/issn.2316-9044.v11i1p95-122.

criação de perfis falsos, de violação da privacidade, de retenção e de manipulação de dados, sobretudo para fins de estigmatização, de discriminação[153], direta ou indireta.

O que não se pode perder de vista a essa altura é a necessidade de investir na composição de pautas de enfrentamento dessa nova modulação de privacidade e da confidencialidade, em que, à guisa do exemplo, o uso de processamento de linguagem natural possa ser aproveitado para a construção de uma radiografia de um Estado ou de uma região e, dessarte, de mapas de índices/indicadores referentes a um grupo ou a uma população, produzidos a partir de dados anonimizados.

Exsurge daí a atual ideia de vigilância e de tecnocontrole que, como anteriormente apontado, implica a urgência na tarefa de reforçar a importância do consentimento individual e de grupos, resgatando-o como um dos pontos nucleares da abordagem no âmbito da tecnologia, pautada pelos direitos humanos. Particulariza-se a sua natureza processual em que devem ser garantidas todas as condições, inclusive temporais, circunstanciais e informacionais, para a tomada de decisão livre, esclarecida e autônoma em um cenário de responsabilidade[154].

Oportuno enfatizar que a atual relação entre a proteção de dados pessoais e o processo de elaboração de consentimento na vida digital corresponde à observância de um dever de garantir a deliberação livre e, isso posto, a revisão e a possibilidade de retirada da anuência a qualquer momento sem prejuízo algum, mediante a garantia de que o tráfego desses dados não implicará danos de qualquer espécie.

Em outras palavras, o consentimento deve ser efetuado nos moldes de um ato jurídico pleno, respeitando-se a ampliação de uma perspectiva de validade e de perfectibilidade em um panorama em que os novos atores, advindos da era informacional[155], passam a ser cada vez mais corresponsáveis.

Em razão disso, pertinente é relembrar que, a despeito da extrema relevância do consentimento como instrumental para a reafirmação da economia, atualmente há outros aspectos que emolduram o cotidiano e, assim, enfraquecem-no, tais como

---

[153] ALMEIDA, Silvio Luiz de. *O que é racismo estrutural?* Belo Horizonte: Letramento, 2018. p. 56.
[154] BRÜGGEMEIER, Gert. Protection of Personality rights in the law of delict/torts in Europe: mapping out paradigms. *In*: BRÜGGEMEIER, Gert; CIACCHI, Aurelia Colombia; O' CALLAGHAN, Patrick (Ed.). *Personality rights in European tort law*. Cambridge: Cambridge University Press, 2010. p. 5-37.
[155] CUKIER, Kenneth; MAYER-SCHÖNBERGER, Viktor. *Big Data*: a revolution that will transform how we live, work and think. Boston, New York: Mariner Books, 2014. p. 176.

o volume e o fluxo de informações que elevam a velocidade das transações a níveis exponenciais, comprometendo o processo de formação da vontade consciente; o excesso de pegadas/sombras digitais que são geradas por todas as pessoas, independentemente de sua anuência; e, por fim, a incapacidade de o Estado, em sua configuração atual, enfrentar a crise de soberania que o fenômeno da sociedade informacional revelou e, dessa forma, a incontestável precarização da garantia da dignidade da pessoa humana que se tem testemunhado.

O ato de consentir apresenta-se nesse contexto como um ato posto na condição de *standard* mínimo, uma vez que em sua totalidade, ou seja, em uma condição de autonomia absoluta, torna-se impossível de ser experienciado, tanto no que se refere ao mundo real quanto ao mundo digital. Com efeito, a ideia acerca de uma racionalidade absoluta, a despeito dos vieses cognitivos que eivam qualquer decisão humana, ainda ampara significativamente o conceito de sujeito de direito, em particular ao arrepio das contribuições científicas, destacando-se as advindas das pesquisas em neurociências.

Entende-se que a idealização do ser humano racional enfraquece a possibilidade de uma atuação consciente, responsável e solidária no âmbito da tecnologia. De modo geral, há a necessidade do enfrentamento dos vieses como uma realidade inevitável e, em razão disso, o aprofundamento da investigação sobre o funcionamento cerebral vai propiciar e expor os aspectos relacionados com as modalidades de regulação factíveis e com os graus de amadurecimento e conscientização, seja do consumidor, do usuário do sistema de saúde público ou privado, do paciente e/ou participante de pesquisas com seres humanos.[156]

De qualquer forma, o processo de consentir permanece como um dos ícones nessa era digital, essência da expressão da autonomia privada e da dignidade da pessoa humana, devendo ser valorizado e, na medida do possível, adequado às novas circunstâncias oriundas da velocidade, da fluidez e da flexibilização de fronteiras, ou seja, com relação ao potencial de empregabilidade da *privacy by design.*

[156] 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*: MENDES, Laura Schertel; DONEDA, Danilo; SARLET, Ingo Wolfgang; RODRIGUES JUNIOR, Otavio Luiz (org.). *Tratado de Proteção de dados pessoais*. Rio de Janeiro: Forense, 2021. p. 485-506.

6.6 ENTRE O ACESSO À INFORMAÇÃO E A PROTEÇÃO DE DADOS NA ADMINISTRAÇÃO PÚBLICA: CRITÉRIOS DE COMPATIBILIZAÇÃO

O direito administrativo da proteção de dados refere-se às regras que autorizam, limitam e controlam o tratamento de dados pessoais por órgãos e entes públicos no exercício de suas atividades. Nesse contexto, a interação entre o direito de acesso às informações administrativas e a proteção de dados pessoais constitui a principal questão que o direito administrativo da proteção de dados precisa resolver. Ao mesmo tempo em que a Administração Pública é obrigada a dar publicidade de seus atos e fornecer acesso às informações administrativas, exige-se a proteção dos dados pessoais contra qualquer operação de tratamento de dados ilegítima (incluindo a divulgação). O conflito exige uma ponderação, na forma de uma restrição recíproca aos direitos fundamentais[157].

A ponderação precisa compatibilizar a realização conjunta do direito de acesso à informação e a proteção de dados pessoais. De um lado, reconhece-se que a própria realização do dever de transparência[158] pode ameaçar direitos fundamentais, como a proteção de dados pessoais. De outro lado, a ampliação irrestrita à proteção de dados pessoais poderia tornar opacas as atividades da Administração Pública, prejudicando a transparência e os demais direitos e interesses públicos que ela instrumentaliza[159]. Nesse caso, seria inadmissível recusar acesso a informações sobre atividades administrativas que eventualmente contenham informações pessoais, mas cujo risco ao titular seja inexpressivo, como é o caso da divulgação de informações gerais sobre os agentes públicos[160]. Como tal

---

[157] HEINEN, Juliano. *Comentários à Lei de Acesso à informação*. 2. ed. Belo Horizonte: Fórum, 2015. p. 259.

[158] MARRARA, Thiago. *Manual de Direito Administrativo*. v. I. fundamentos, organização e pessoal. São Paulo: KDP, 2017. *E-book*.

[159] Cf. decisão do STF, "a insuficiente limitação ao direito à privacidade revelar-se-ia, por outro ângulo, desproporcional, porquanto lesiva aos interesses da sociedade de exigir do Estado brasileiro uma atuação transparente". (BRASIL. Supremo Tribunal Federal. Mandado de Segurança 33340. Impetrantes: Banco Nacional de Desenvolvimento Econômico e Social – BNDES e outros. Impetrado: Tribunal de Contas da União. Relator: Min. Luiz Fux. Brasília, 26 maio 2015. DJe 03 ago. 2015.)

[160] A esse respeito, STF decidiu que "a divulgação de dados referentes aos cargos públicos não viola a intimidade e a privacidade, que devem ser observadas na proteção de dados de natureza pessoal", (BRASIL. Supremo Tribunal Federal. Agravo Regimental no Recurso Extraordinário 766390. Agravante: Sindicato dos Médicos do Distrito Federal – Sindmedico. Agravado: Distrito Federal. Relator: Min. Ricardo Lewandowski. Brasília, 24 jun. 2014. DJe 15 ago. 2014.)

divulgação é importante para a realização de outros direitos e interesses públicos, deve-se privilegiar o acesso nesses casos[161].

A maior dificuldade na compatibilização desses direitos fundamentais é realizar uma leitura conjunta da LAI com a LGPD. A LAI estabelece a transparência das atividades administrativas como regra geral e a restrição dessas informações apenas em casos excepcionais. Dessa forma, as exceções reconhecidas pela LAI devem ser interpretadas de forma restritiva para garantir a realização do dever de transparência. A LGPD, por sua vez, regula o fluxo informacional referente a pessoas naturais, permitindo o tratamento de dados pessoais apenas de acordo com as hipóteses estabelecidas em lei.

Com a entrada em vigor da LGPD, a necessidade de uma orientação jurisprudencial dos tribunais superiores, a estabelecer parâmetros e critérios objetivos bem delineados, já se faz sentir intensamente. Em caso noticiado por veículo de imprensa brasileiro, identificou-se que o Gabinete de Segurança Institucional da Presidência da República (GSI) recusou, baseando-se em preceitos da LGPD, pedidos de acesso à informação sobre os registros de entrada no Palácio do Planalto de certos familiares do atual chefe do governo federal e de lobistas do segmento de armas de fogo. Na motivação da rejeição aos pedidos formulados, o GSI afirmou que "o tratamento de dados só poderá ser feito para propósitos legítimos, específicos, explícitos e informados e com consentimento do titular ou proteção da vida do titular ou de terceiros", além do fato de que os registros dos visitantes à sede do governo federal "cumpre a finalidade específica de segurança da mais alta autoridade do Poder Executivo".[162]

De acordo com a LAI, a Presidência da República tem o dever de garantir o direito de acesso (CF, art. 5º, XXXIII; LAI, art. 5º), podendo recusar o acesso apenas em três situações: i) se as informações forem consideradas imprescindíveis à segurança da sociedade ou Estado (CF, art. 5º, XXXIII; LAI, art. 23); ii) se a

---

[161] GASIOLA, Gustavo Gil; MACHADO, Diego; MENDES, Laura Schertel. O tratamento de dados pessoais pela Administração Pública: Transparência, bases legais e limites constitucionais. *In*: FRANCOSKI, Denise de Souza Luiz; TASSO, Fernando Antonio (coord.) *A lei geral de proteção de dados pessoais*: aspectos práticos e teóricos relevantes no setor público e privado. 1. ed. São Paulo: Thomson Reuters Brasil, 2021. p. 137-162.

[162] AMADO, Guilherme. Presidência usa Lei de Proteção de Dados para negar informações de visitas de lobistas de armas e advogados ao Planalto. *O Globo*, 14 jan. 2021. Disponível em: https://oglobo.globo.com/epoca/guilherme-amado/presidencia-usa-lei-de-protecao-de-dados-para-negar-informacoes-de-visitas-de-lobistas-de-armas-advogados-ao-planalto-24833164. Acesso em: 20 maio 2021.

informação é protegida por hipótese legal de sigilo, segredo de justiça e segredo industrial (art. 22, LAI); ou iii) se as informações forem pessoais (art. 31, LAI).

Diante do supracitado, torna-se relevante abordar o direito fundamental à proteção de dados e o controle de constitucionalidade dos atos da administração que permeiem o tratamento de dados.

Em certas hipóteses, o tratamento de dados no setor público necessita de edição de lei ou medida provisória (MP). Nesse caso, o controle de mérito realizado pela LGPD não será suficiente, em razão de se tratar de atos normativos de mesmo nível hierárquico. Assume, pois, função central nesse contexto a tutela constitucional dos dados pessoais, seja na forma de um direito à autodeterminação informativa ou de um direito fundamental à proteção de dados.

Aqui, mais uma vez, devido à importância e ao marco histórico na cronologia e desenvolvimento dos direitos fundamentais, passa-se a abordar brevemente o julgado do Tribunal Federal Constitucional Alemão.

Pois bem, o Tribunal asseverou que o processamento indevido de dados pessoais poderia ampliar a influência do Estado sobre o comportamento do indivíduo, que não mais seria capaz de tomar decisões livres em virtude “da pressão psíquica de participação pública”. Uma sociedade “na qual os cidadãos não mais são capazes de saber quem sabe o que sobre eles, quando e em que situação” é contrária ao direito à autodeterminação informativa, prejudicando tanto a personalidade quanto o bem comum de uma sociedade democrática.[163]

Nesse julgamento, a Corte julgou inconstitucionais dispositivos da Lei de recenseamento que autorizavam um amplo compartilhamento de dados pessoais entre órgãos administrativos, sem prever garantias de proteção adequadas. O julgamento é um marco, ao consolidar a tutela constitucional dos dados pessoais e possibilitar o controle dos atos normativos que estabelecem a coleta, o uso ou qualquer compartilhamento de dados pela Administração.

Nota-se, portanto, o relevante papel que o direito fundamental à proteção de dados exerce no ordenamento: ele possibilita que todos os atos normativos que autorizem um determinado tratamento de dados tenham o seu conteúdo controlado para avaliar a adequação do referido tratamento. Isso ocorreu no famoso caso acima citado, assim como em outros julgados importantes na Alemanha, como por exemplo

[163] BverfGE 65, 1 (42).

no caso de retenção de dados (BverfGE *Vorratsdatenspeicherung*) e no caso de busca pela polícia de perfis suspeitos a partir do cruzamento de dados (*BverfGE Rasterfahndung*).

Cumpre destacar ainda que, no âmbito europeu, tem-se um direito fundamental à proteção de dados estabelecido de forma expressa no art. 8 da Carta de Direitos Fundamentais da União Europeia. A tutela constitucional no âmbito europeu também foi fundamental para o controle de constitucionalidade de normas autorizativas, como no emblemático julgamento que determinou a invalidade da Diretiva 2006/24/EC sobre retenção de dados.

No Brasil, apenas em 2020 o STF finalmente respondeu de forma afirmativa e contundente a essa questão, ao reconhecer um direito fundamental à proteção de dados[164] e suspender a validade da Medida Provisória 954, que determinava às operadoras de telefonia o envio dos dados de telefone fixo, celular e endereço de seus consumidores para a Fundação IBGE, para a realização de suposta pesquisa por telefone[165].

A referida decisão, proferida nos dias 6 e 7 de maio, foi histórica para o desenvolvimento da disciplina jurídica relativa à proteção de dados pessoais no Brasil. Com a impressionante maioria de 10 votos favoráveis, o Plenário da Suprema Corte referendou a Medida Cautelar concedida pela Ministra Rosa Weber, relatora das Ações Diretas de Inconstitucionalidade (ADIs) n. 6387, 6388, 6389,6390 e 6393, e reconheceu a tutela constitucional dos dados pessoais de forma autônoma em relação a outros direitos fundamentais.

No julgamento, o STF endossou o amplo conceito de dado pessoal já estabelecido na LGPD, bem como reconheceu a sua tutela pela Constituição Federal, a partir da constatação de que não existem dados insignificantes no contexto automatizado e massificado de dados pessoais. Conforme afirmou o Min. Ricardo Lewandowski,

---

[164] MENDES, Laura Schertel. Habeas Data e Autodeterminação Informativa: os dois lados da mesma moeda. *Direitos fundamentais e justiça*, Belo Horizonte, a. 12, n. 39, p. 185-216, jul./dez. 2018. Cf. também: MENDES, Laura Schertel; RODRIGUES, Otavio; FONSECA, Gabriel. O Supremo Tribunal Federal e a proteção constitucional de dados pessoais: rumo a um direito fundamental autônomo. *In*: MENDES, Laura Schertel; DONEDA, Danilo; SARLET, Ingo Wolfgang; RODRIGUES JUNIOR, Otavio Luiz (org.). *Tratado de Proteção de dados pessoais*. Rio de Janeiro: Forense, 2021. p. 61-72.

[165] GASIOLA, Gustavo Gil; MACHADO, Diego; MENDES, Laura Schertel. O tratamento de dados pessoais pela Administração Pública: Transparência, bases legais e limites constitucionais. *In*: FRANCOSKI, Denise de Souza Luiz; TASSO, Fernando Antonio (coord.) *A lei geral de proteção de dados pessoais*: aspectos práticos e teóricos relevantes no setor público e privado. 1. ed. São Paulo: Thomson Reuters Brasil, 2021. p. 137-162.

> é preciso ficar claro, portanto, que não se está a falar de informações insignificantes, mas da chave de acesso a dados de milhões de pessoas, com alto valor para execução de políticas públicas, é verdade, mas também com provável risco de adoção de expedientes, por vezes, dissimulados, obscuros, que possam causar desassossego na vida diária do indivíduo.[166]

O significado histórico da decisão do STF para o Brasil é, portanto, comparável ao referido julgamento do Tribunal Constitucional Federal Alemão, em 1983[167]. Ao fazer referência ao julgado, o STF expressamente mencionou o conceito de autodeterminação informativa, já positivado na LGPD, a fim de ressaltar o necessário protagonismo exercido pelo cidadão no controle do que é feito com seus dados.

A despeito da construção desenvolvida desse direito fundamental, ele não pode ser concebido de forma absoluta, pois as informações pessoais integram a órbita de representação da pessoa no corpo social. A limitação desse direito fundamental, no caso concreto, exige i) uma base jurídica segura, ii) com a clareza necessária à finalidade do tratamento de dados, para que se avalie o nível de intervenção no direito fundamental, iii) que seja também proporcional, adequada e necessária à finalidade pretendida, adotando, ainda, iv) as providências preventivas mínimas de cunho procedimental e organizacional, orientadas à segurança dos cidadãos envolvidos e à diminuição dos riscos de danos a seus direitos da personalidade. Em verdade, quanto mais grave for essa restrição, mais contundentes devem ser as justificativas, os critérios e as precauções para tal fim, sob pena de se legitimar intervenções na vida privada em nome de fins genéricos ou necessidades coletivas abstratas.[168]

Diante do analisado, demonstra-se que o tratamento de dados pela Administração Pública depende não apenas de um ato normativo formal, mas também da avaliação de conteúdo quanto à adequação desse tratamento. Isso pode ser feito a partir de um controle pela LGPD para os atos infralegais e de um controle de constitucionalidade para os atos legais autorizativos. Em ambos os casos, entende-se ser fundamental a atuação da Autoridade Nacional de Proteção de

---

[166] BRASIL. Supremo Tribunal Federal. Medida Cautelar na Ação Direta de Inconstitucionalidade 6387. Requerentes: Rede Sustentabilidade e outros. Relatora: Min. Rosa Weber. Brasília, 07 maio 2020. DJe 12 nov. 2020.

[167] BverfGE 65, I, "Recenseamento" (*Volkszählung*)

[168] MENDES, Laura Schertel. Habeas Data e Autodeterminação Informativa: os dois lados da mesma moeda. *Direitos fundamentais e justiça*, Belo Horizonte, a. 12, n. 39, p. 185-216, jul./dez. 2018.

Dados (ANPD) na qualidade de órgão de supervisão e implementação da proteção de dados no país.

6.7 AUTODETERMINAÇÃO INFORMACIONAL MUITO ALÉM DO CONSENTIMENTO

Após uma abordagem analítica dos dados pessoais como um novo ativo econômico, como um novo direito da personalidade e de como isso foi acomodado pelas legislações de proteção de dados pessoais, reavaliou-se, em duas frentes, o produto desse diagnóstico: a função e os limites do consentimento para compreender o que é autodeterminação informacional, um dos fundamentos da LGPD.

A primeira demonstra que a falácia do consentimento pode ter como causa a ausência de uma tomada regulatória que disponibilize formas efetivas ao cidadão para autodeterminar as suas informações pessoais[169].

6.8 COMPLIANCE NA SAÚDE

A expressão "*compliance*" vem do inglês "*to comply with*", que pode ser traduzido como conformar-se a, ou adequar-se a, ou seja, quando se fala de "*compliance*", quer se dizer conformidade de modo geral. E essa conformidade é tanto em relação às disposições legislativas vigentes a respeito das mais variadas matérias quanto relativamente às disposições normativas infralegais e até mesmo éticas e morais.

As políticas de *compliance*, assim, ocorrem de forma ampla e devem buscar abranger todos os setores da atuação empresarial que ofereçam possibilidades de risco, novamente compreendidos da forma mais vasta possível: riscos legais, jurídicos, trabalhistas, éticos e morais.

Com a importância cada vez maior conferida aos dados e com o reconhecimento de seu valor econômico intrínseco – pois ainda que tal valor não decorra deles diretamente, advém de suas possíveis aplicações –, e na esteira da legislação da União Europeia sobre o tema, especialmente o GDPR (*General Data*

[169] BIONI, Bruno Ricardo. *Proteção de Dados Pessoais*: a função e os limites do consentimento. 3. ed. Rio de Janeiro: Forense, 2021.

Protection Regulation) que, em 2018, não só definiu amplamente as políticas de proteção de dados, como também restringiu a realização de relações comerciais com países que não oferecessem o mesmo nível de proteção estabelecido por aquela legislação, a questão da proteção de dados passou a ter uma mais significativa importância que reflete, em contrapartida, deveres de proteção cada vez mais amplos e resulta em preocupações concretas com a sua observância, criando novas facetas das políticas de conformidade empresariais[170].

Assim, tendo que se adaptar a essa nova realidade de proteção a dados sensíveis, as políticas de *compliance* existentes precisam se conformar, o que pode ser feito mediante a aplicação da própria lei, que sugere e dispõe de instrumentos que têm precisamente esta função, a respeito dos quais se passa a debater.

O primeiro instrumento de *compliance* fornecido pela LGPD é coincidente com o que se pode entender como um dos principais elementos de qualquer política de conformidade empresarial: a criação de um programa de governança em privacidade ou, mais simplificadamente, uma política de privacidade. Em seu art. 50, § 2º, I, 'c', a Lei dispõe que o controlador poderá – notando-se daí não uma obrigação, mas uma sugestão – implementar um programa de governança em privacidade, o que deve ser feito observando a estrutura, a escala e o volume de suas operações, bem como a sensibilidade dos dados tratados e a probabilidade e gravidade dos danos para os titulares dos dados.

A legislação ainda estabelece que referido programa de governança deve atender a requisitos específicos que demonstrem, por exemplo: "comprometimento do controlador em adotar processos e políticas internas que assegurem o cumprimento, de forma abrangente, de forma abrangente, de normas e boas práticas" (art. 50, § 2º, I, 'a') e que "tenha o objetivo de estabelecer relação de confiança com o titular, por meio de atuação transparente e que assegure mecanismos de participação do titular".

Importante destacar que a implementação do Programa de Governança não é importante apenas para demonstrar à Autoridade Nacional de Proteção de Dados o comprometimento da companhia com a legislação em questão e com os direitos dos

[170] SANTORO, Raquel Botelho. A LGPD como ferramenta de compliance na área da saúde: política de privacidade e relatório de impacto à proteção de dados pessoais. In: DALLARI, Analluza Bolivar; MONACO, Gustavo Ferraz de Campos (coord.). *LGPD na Saúde*. 1. ed. São Paulo: Thomson Reuters Brasil, 2021. p. 249-262.

titulares dos dados que lhe são apesentados[171]. Essa implementação é ainda mais crucial internamente, pois vai depender dela a criação de uma cultura de proteção de dados que, no âmbito empresarial, conscientize os funcionários e colaboradores para a importância dessas novas políticas e para efetivar o grau de proteção que se deve conferir a dados, sejam eles sensíveis ou não, mas especialmente nestes últimos casos.[172]

Aliás, é indispensável que essa Política de Governança, para que atenda devidamente ao objetivo, seja escrita em uma linguagem acessível e didática, e que para tanto preveja todos os aspectos essenciais de sua aplicação, desde a identificação e classificação de seu objeto de proteção – especificando quais são os dados passíveis de proteção –, até a estipulação de regras para seu tratamento de forma ampla – acesso, proteção, compartilhamento, políticas de segurança e outras – e a previsão de consequências internas para o descumprimento das referidas regras.

Com o advento da Lei e com a estipulação de regras claras e muitas vezes exemplificativas com referência ao objeto de proteção e da forma pela qual tal proteção deve ser implementada, facilita-se a criação interna, no meio empresarial, dessa cultura que até então não é natural e que, portanto, precisa ser incutida em cada um dos indivíduos responsáveis pelo tratamento dos dados.

Assim, a Política de Governança se mostra duplamente relevante como instrumento de *compliance* no que concerne à proteção de dados, pois ela: i) demonstra uma preocupação efetiva da companhia em relação a conformar-se com as normas que determinam as políticas de proteção de dados que devem ser implementadas; e ii) contribui para a criação de uma cultura empresarial de proteção de dados, o que permite que tal política não só seja efetivamente executada

---

[171] SANTORO, Raquel Botelho. A LGPD como ferramenta de compliance na área da saúde: política de privacidade e relatório de impacto à proteção de dados pessoais. In: DALLARI, Analluza Bolivar; MONACO, Gustavo Ferraz de Campos (coord.). *LGPD na Saúde*. 1. ed. São Paulo: Thomson Reuters Brasil, 2021. p. 249-262. p. 252.

[172] Na esteira do reconhecimento da importância em se criar uma cultura de *compliance* voltada à proteção de dados no ambiente empresarial, é interessante notar o apontamento de Ustaran a respeito do elemento que deveria motivar uma empresa a implementar referido programa de compliance direcionado à proteção de dados. Para ele, "*successful legal compliance is, more often than not, the result of presenting dry and costly legal obligations as something else. In particular, something that provides tangible benefits*."
Dessa forma, sugere que, por meio da implementação das referidas políticas, a empresa busque encarar os custos e esforços envolvidos pela ótica dos benefícios que certamente obterá, seja porque protege os direitos fundamentais envolvidos, seja porque também pode tirar vantagens econômicas deste tratamento de dados ético e legalmente adequado. (USTARAN, Eduardo. How to encourage Privacy Compliance. *Managing Intellectual Property*, v. 244, p. 36-37, 2014.)

internamente, como também que ela contribua para a educação interna dos funcionários, permitindo, em última instância, uma maior eficácia da lei.

No mais, a Política de Governança bem implementada diminui consideravelmente os riscos de que haja a aplicação de penalidades pela ANPD. E, ainda que situações eventuais de aplicação de sanções venham a ocorrer, ela serve como uma atenuante na aplicação de ocasionais penas, o que mais uma vez demonstra a sua importância e essencialidade para as empresas com atuação na área de saúde, tendo em vista o volume de dados pessoais sensíveis que são por elas administrados e tratados diariamente e que são essenciais para o próprio exercício das suas atividades[173].

6.9 O RELATÓRIO DE IMPACTO À PROTEÇÃO DE DADOS.

Enquanto a Política de Governança é um instrumento geral que serve como diretriz na atuação dos mais diversos setores internos e que tem por objetivo não só estabelecer as regras de conduta relativamente ao tratamento de dados, mas também conceituar quais são exatamente os dados protegidos e como tal política deve ser implementada e executada no dia a dia de cada um dos funcionários e áreas da empresa, o Relatório de Impacto à Proteção de Dados Pessoais (RIAPD) se revela como um documento de cunho mais técnico, inclusive passível de revisão pela ANPD.

De acordo com a definição legal, o RIAPD é uma “documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco” (art. 5º, XVII).

Ainda, conforme o que dispõe a legislação (art. 10, § 3º, e art. 38), a ANPD possui a competência e a possibilidade de solicitar ao controlador que lhe forneça acesso ao RIAPD para que possa verificar a sua conformidade aos ditames da lei, o que revela mais uma vez a sua importância.

Todavia, esse é um relatório com viés técnico e não funciona como um documento que fornece diretrizes, definições e normas de conduta para aqueles que

[173] SANTORO, Raquel Botelho. A LGPD como ferramenta de compliance na área da saúde: política de privacidade e relatório de impacto à proteção de dados pessoais. In: DALLARI, Analluza Bolivar; MONACO, Gustavo Ferraz de Campos (coord.). *LGPD na Saúde*. 1. ed. São Paulo: Thomson Reuters Brasil, 2021. p. 249-262.

terão acesso aos dados tratados pela empresa, como é o papel da Política de Governança.

Referido relatório, é bom que se indique, deve ter o seu modelo fornecido pela própria ANPD que, uma vez devidamente instalada e em funcionamento, não só será responsável por regulamentar esse ponto da Lei, mas também vários outros que necessitem diretrizes mais específicas[174].

Contudo, enquanto isso não ocorre, a obrigação de elaboração do RIAPD já está vigente, de modo que é possível às empresas que desejam se conformar a esse ponto da nova legislação buscar aplicar o modelo desenvolvido no âmbito europeu pela GDPR que, como já explicitado no presente estudo, serviu de parâmetro para a LGPD e que já tem tido aplicação prática.

A própria GDPR, aliás, também criou um documento equivalente ao RIAPD, que é conhecido como DPIA (*Data Protection Impact Assessment*).[175] A observância dos parâmetros adotados pela União Europeia na elaboração do seu DPIA pode trazer diretrizes que contribuam para concretizar os requisitos de um Relatório de Impacto e as informações que efetivamente precisam estar contidas nele.

Assim como o DPIA, o Relatório de Impacto somente é obrigatório caso haja o tratamento de dados que possam gerar riscos às liberdades civis e aos direitos fundamentais do seu titular. Portanto, o primeiro passo é o de identificar os dados que serão tratados e os riscos que esse tratamento pode oferecer.

Em um segundo momento, mostra-se necessário descrever como se dará o tratamento de dados naquele projeto específico, levando em conta as atividades exercidas com aquelas informações. Nesse ponto, o controlador precisa se perguntar quais atos, além da coleta, ele irá realizar. Assim, deve saber se irá compartilhar os dados, armazená-los, por quanto tempo o fará e qual a finalidade a ser atingida mediante essa atividade específica. É essencial que o controlador possa prever como se dará o fluxo de dados dentro de sua empresa, para que possa

---

[174] SANTORO, Raquel Botelho. A LGPD como ferramenta de compliance na área da saúde: política de privacidade e relatório de impacto à proteção de dados pessoais. In: DALLARI, Analluza Bolivar; MONACO, Gustavo Ferraz de Campos (coord.). *LGPD na Saúde*. 1. ed. São Paulo: Thomson Reuters Brasil, 2021. p. 249-262. p. 255.

[175] Sobre a importância da estipulação do DPIA pela GDPR e sobre a necessidade de se adaptarem as práticas empresariais para a definição do que viria a se configurar a hipótese de "alto risco" a exigir a elaboração do documento – questão essa já levantada antes mesmo da entrada em vigor do Regulamento -, vide: VOSS, Gregory W. Internal Compliance Mechanisms for Firms in the EU General Data Protection Regulation. *Revue Juridique Themis*, v. 50, n. 03, p. 783-820, 2016.

avaliar especificamente os riscos inerentes a cada uma das atividades de tratamento que serão exercidas.

Finalizada a etapa de ampla análise de dados, procedimentos e riscos, é chegada a hora de consultar os demais setores empresariais que possam ter participação não apenas no tratamento de dados, mas na sua proteção e na garantia das políticas de conformidade, lembrando sempre que a política de proteção de dados deve fazer parte da cultura empresarial e, como tal, não fica restrita a um único setor.

Especificamente no que diz respeito ao setor da saúde, o RIAPD certamente haverá de fazer constar em seus itens a forma pela qual deverão ser tratados prontuários, dados pessoais, receituário, resultados de laudos e exames, comunicações eventuais com pacientes, assim como resultados e informações sobre cirurgias e demais procedimentos médicos e hospitalares, intercorrências, internações, planos de saúde, formas utilizadas para pagamento de consultas, dados genéticos, histórico de saúde e demais informações que, neste âmbito, são sempre consideradas sensíveis.

E, por mais que, à primeira vista, o tratamento destes dados não pareça acarretar riscos à liberdade civil de seus titulares, é evidente que eles são por definição própria hipóteses de risco a direitos fundamentais, já que informações relacionadas à saúde invariavelmente dizem respeito a direitos de privacidade, dignidade e intimidade.

Portanto, ainda que seja incluído na Lei Geral como uma obrigação, o RIAPD apresenta-se também como uma importante ferramenta de *compliance* ao auxiliar as empresas a se conformarem com as exigências da nova LGPD e, em consequência, a se protegerem de eventuais sanções que possam decorrer de sua inadimplência, sejam elas administrativas, judiciais ou até mesmo reputacionais.

6.10 DOS RISCOS ESPECÍFICOS DE COMPLIANCE

Por fim, não é demais destacar a importância da efetiva implantação de uma eficiente política de *compliance* na área de proteção de dados, a fim de evitar a responsabilização tanto do controlador quanto do operador, pessoa física ou jurídica, responsáveis pelo tratamento de dados de terceiros.

Além dos riscos de aplicação de pesadas sanções pela ANPD com fulcro no *quantum* estabelecido pela própria lei (art. 52), nas quais estão incluídas multas no montante de até R$ 50 milhões (art. 52, II), há ainda que se considerar o risco reputacional a que estão sujeitas as empresas de saúde que descumprirem as normas e que venham a ser punidas.[176]

Ora, os agentes da área da saúde – sejam eles empresas ou pessoas físicas – tratam cotidianamente de alguns dos dados mais sensíveis que qualquer indivíduo pode disponibilizar. E sabe-se que um dos principais incentivos que os indivíduos têm de disponibilizar tais dados sensíveis aos cuidados dos agentes de saúde é a garantia de que seu sigilo é uma das principais obrigações éticas e morais de todos aqueles agentes (previstas não apenas na LGPD, mas desde sempre tratadas pelo Código de Ética, por Resoluções do Conselho Federal de Medicina e por normas esparsas da legislação).

Ao saber, no entanto, que tal sigilo foi violado por algum destes agentes – seja por dolo, culpa, imperícia ou negligência –, dificilmente o titular dos dados recuperará a confiança naquele agente, ou poderá vir a criar essa relação de confiança, o que certamente pode ser muito mais prejudicial, na prática e ao longo do tempo, do que a aplicação de uma sanção administrativa, pecuniária ou não.

Da mesma forma, a reparação judicial deste tipo de violação (seja por danos materiais e/ou morais que podem decorrer de uma falha deste tipo) ou inclusive de eventual perquirição criminal de um agente responsável por essa violação de sigilo (o que pode vir a configurar, em tese, o crime do artigo 154 do Código Penal, que trata da violação do sigilo profissional) pode não ser tão prejudicial à imagem de um agente de saúde quanto a divulgação de que falhou na proteção dos dados que lhe foram confiados para tratamento.

Adicionalmente aos riscos já bastante consideráveis de cunho administrativo, civil e penal, cabe destacar os concretos riscos reputacionais a que estão sujeitos os agentes de saúde, tornando-se ainda mais importante a implementação de todas as ferramentas de *compliance* que a própria LGPD nos apresenta.

---

[176] SANTORO, Raquel Botelho. A LGPD como ferramenta de compliance na área da saúde: política de privacidade e relatório de impacto à proteção de dados pessoais. In: DALLARI, Analluza Bolivar; MONACO, Gustavo Ferraz de Campos (coord.). *LGPD na Saúde*. 1. ed. São Paulo: Thomson Reuters Brasil, 2021. p. 249-262.

7 CONSIDERAÇÕES FINAIS

O presente estudo teve como objetivo abordar as nuances do direito à proteção de dados em matéria de saúde. É importante mencionar que atualmente não há muita doutrina escrita sobre o tema. Contudo, foi possível realizar uma abordagem técnica perpassando diversos aspectos da proteção de dados como direito fundamental.

Dessa feita, alguns institutos jurídicos, como a autodeterminação informativa, vêm evoluindo na sua aplicabilidade, ou seja, tornando-se mais eficazes do ponto de vista prático. A questão do consentimento também tem especial relevo, mesmo que ainda careça de esclarecimentos e previsão regulatória eficaz. Na Alemanha por exemplo, a matéria, por seus diversos aspectos previsionais, incluindo culturais, assumiu uma abordagem diferente. A preventiva abordagem que os cidadãos expõem diante de situações do cotidiano envolvendo a matéria serviriam de exemplo ao Brasil.

Foi possível atestar também que os direitos fundamentais e as liberdades civis são extremamente afetados e estão inexoravelmente ligados à proteção de dados como direito fundamental, de sorte que foi possível notar tal intrinsecabilidade durante as diversas vezes em que foram abordados temas preciosos como a autodeterminação informativa, o consentimento livre e esclarecido e a privacidade em termos de proteção à dados sensíveis.

Cabe salientar a questão do *compliance* em proteção de dados na saúde, cada vez mais necessária e preventiva a aspectos da regulação nas empresas principalmente. Outro ponto que não se poderia deixar de citar é o compartilhamento de dados entre operadores e controladores da saúde, tema de fundamental importância.

Como conclusão, acredita-se que o Brasil ainda está dando passos iniciais, porém em uma direção correta. A ANPD e o CNPDP são instituições imprescindíveis a uma eficaz aplicação de medidas restritivas e preventivas em termos de abusos no tema.

Por fim, de acordo com o descrito, oportuno dizer que a matéria é infinita e ainda carece de profissionais que se dediquem a ela. No entanto, devido a todos os percalços que a pandemia ocasionou, acredita-se ter sido possível realizar um trabalho de pesquisa interessante e esclarecedor em vários aspectos.

REFERÊNCIAS

ACQUISTI, Alessandro. Nudging privacy: behavioral economics of personal information. *İEEE Security & Privacy*, p. 83, nov. /dez. 2009.

ALLAMEL-RAFFIN, Catherine; LEPLÈGE, Alain; MARTIRE JÚNIOR, Lybio. *História da Medicina*. Aparecida/SP: Ideias & Letras, 2011.

ALMEIDA, Silvio Luiz de. *O que é racismo estrutural?* Belo Horizonte: Letramento, 2018.

AMADO, Guilherme. Presidência usa Lei de Proteção de Dados para negar informações de visitas de lobistas de armas e advogados ao Planalto. *O Globo*, 14 jan. 2021. Disponível em: https://oglobo.globo.com/epoca/guilherme-amado/presidencia-usa-lei-de-protecao-de-dados-para-negar-informacoes-de-visitas-de-lobistas-de-armas-advogados-ao-planalto-24833164. Acesso em: 20 maio 2021.

ASSMANN, Jhonata. *A autodeterminação informativa no direito germânico e brasileiro*. 2014. 65f. Trabalho de Conclusão de Curso (Graduação em Direito) – Faculdade de Direito, Universidade Federal de Santa Catarina, Florianópolis, 2014.

BAMBERGER, Kenneth *et al*. Privacy on the books and on the ground. *Stanford Law Review*, v. 63, p. 247, jan. 2011.

BARBOZA, Heloisa Helena; ALMEIDA, Vitor (Org.). *Comentários ao Estatuto da Pessoa com Deficiência à luz da Constituição da República*. Belo Horizonte, MG: Forum, 2018.

BEAUCHAMP, Tom L. *Informed consent*: its history, meaning, and present challenges. v. 20. Cambridge: Quarterly of Healthcare Ethics, 2011.

BENJAMIN, Antonio Herman *et al*. *Código Brasileiro de defesa do consumidor*: comentado pelos autores do anteprojeto. 6. ed. Rio de Janeiro: Forense Universitária, 1999.

BIONI, Bruno Ricardo. *Proteção de Dados Pessoais*: a função e os limites do consentimento. 3. ed. Rio de Janeiro: Forense, 2021.

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.

BLUM, Renato Opice; FURTADO, Tiago Neves. Legítimo Interesse: Nuances e limites para aplicações práticas no âmbito da LGPD. *In*: FRANCOSKI, Denise de Souza L.; TASSO, Fernando Antonio. *A Lei Geral de Proteção de Dados Pessoais*: Aspectos Práticos e Teóricos relevantes no setor público e privado. 1. ed. São Paulo: Thomson Reuters Brasil, 2021. p. 304-308.

BOBBIO, Norberto. *Direito e Estado no Pensamento de Emanuel Kant*. 4. ed. Brasília: Editora UnB, 1997.

BONAFÉ, Lucas Alves da Silva *et. al*. *LGPD na Saúde*. 2019. *E-book*.

BRASIL. Supremo Tribunal Federal. Agravo Regimental no Recurso Extraordinário 766390. Agravante: Sindicato dos Médicos do Distrito Federal – Sindmedico. Agravado: Distrito Federal. Relator: Min. Ricardo Lewandowski. Brasília, 24 jun. 2014. DJe 15 ago. 2014.

BRASIL. Supremo Tribunal Federal. Mandado de Segurança 33340. Impetrantes: Banco Nacional de Desenvolvimento Econômico e Social – BNDES e outros. Impetrado: Tribunal de Contas da União. Relator: Min. Luiz Fux. Brasília, 26 maio 2015. DJe 03 ago. 2015.

BRASIL. Supremo Tribunal Federal. Medida Cautelar na Ação Direta de Inconstitucionalidade 6387. Requerentes: Rede Sustentabilidade e outros. Relatora: Min. Rosa Weber. Brasília, 07 maio 2020. DJe 12 nov. 2020.

BRÜGGEMEIER, Gert. Protection of Personality rights in the law of delict/torts in Europe: mapping out paradigms. *In*: BRÜGGEMEIER, Gert; CIACCHI, Aurelia Colombia; O' CALLAGHAN, Patrick (Ed.). *Personality rights in European tort law*. Cambridge: Cambridge University Press, 2010. p. 5-37.

BULL, Hans Peter. *Informationelle Selbstbestimmung*: Vision oder Illusion? 2. ed. Tübingen: Mohr Siebeck, 2011.

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, n. 10097, p. 882-897, out. 2020.

CALO, Ryan. Consumer subject review boards: a thought experiment. *Stanford Law Review Online*, v. 97, p. 97-102, set. 2013.

CAREY, Corinne A.; STERN, Gillian. *Protecting patient privacy*: strategies for regulating electronic health records exchange. New York: New York Civil Liberties Union (NYCLU), mar. 2012. Disponível em: https://bit.ly/305PT0F. Acesso em: 03 jul. 2020.

CORTINA, Adela; MARTÍNEZ, Emilio. *Ética*. São Paulo: Loyola, 2009.

COSTA JUNIOR, Paulo José da. *O direito de estar só*: tutela penal da intimidade. São Paulo: Revista dos Tribunais, 1970.

CUKIER, Kenneth; MAYER-SCHÖNBERGER, Viktor. *Big Data*: a revolution that will transform how we live, work and think. Boston, New York: Mariner Books, 2014.

DONEDA, Danilo. A autoridade nacional de proteção de dados e o conselho nacional de proteção de dados. In: MENDES, Laura Schertel; DONEDA, Danilo; SARLET, Ingo Wolfgang; RODRIGUES JUNIOR, Otavio Luiz (org.). *Tratado de Proteção de dados pessoais*. Rio de Janeiro: Forense, 2021. p. 459-471.

DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*. 2. ed. São Paulo: Revista dos Tribunais, 2020.

EUROPEAN COMISSION. *E–Health European Interoperability Framework*. Brussels, nov. 2015. Disponível em: https://ec. Europa.eu/health/sites/health/files/ehealth/docs/ev_20151123_co03_en.pdf. Acesso em: 20 jun. 2021.

EUROPEAN COMISSION. *New European Interoperability Framework*: promoting seamless services and data flows for European public administrations. Luxembourg, 2017. Disponível em: https://ec.europa.eu/isa2/sites/isa/files/eif_brochure_final.pdf. Acesso em: 20 jun. 2021.

EUROPEAN COMISSION. *Policies, information and services*. S.l. 2021. Disponível em: https://ec.europa.eu/digital-single-market/en. Acesso em: 20 jun. 2021.

FADEN, Ruth R.; BEAUCHAMP, Tom L. *A history and Theory of informed consent*. New York: Oxford University Press, 1986.

FAVERO, Walquiria Nakano Eloy. Proteção e Compartilhamento de Dados na Saúde Suplementar. In: DALLARI, Analluza Bolivar; MONACO, Gustavo Ferraz de Campos (coord.). *LGPD na Saúde*. 1. ed. São Paulo: Thomson Reuters Brasil, 2021. p. 171-194.

FRANCOSKI, Denise de Souza L.; TASSO, Fernando Antonio. *A Lei Geral de Proteção de Dados Pessoais LGPD*: Aspectos Práticos e Teóricos relevantes no setor público e privado. 1. ed. São Paulo: Thomson Reuters Brasil, 2021.

FRAZÃO, Ana. Dados, estatísticas e algoritmos: Perspectivas e riscos da sua crescente utilização. *Jota*, 28 jun. 2017. Disponível em: https://www.jota.info/opiniao-e-analise/colunas/constituicao-empresa-e-mercado/dados-estatisticas-e-algoritmos-28062017. Acesso em: 14 jul. 2021.

FRAZÃO, Ana. Nova LGPD: as demais hipóteses de tratamento de dados pessoais. *Jota*, 19 set. 2018. Disponível em: www.jota.info/opiniao-e-analise/colunas/constituicao-empresa-e-mercado/nova-lgpd-as-demais-hipoteses-de-tratamento-de-dados-pessoais-19092018. Acesso em: 10 out. 2020.

GASIOLA, Gustavo Gil; MACHADO, Diego; MENDES, Laura Schertel. O tratamento de dados pessoais pela Administração Pública: Transparência, bases legais e limites constitucionais. *In*: FRANCOSKI, Denise de Souza Luiz; TASSO, Fernando Antonio (coord.) *A lei geral de proteção de dados pessoais*: aspectos práticos e teóricos relevantes no setor público e privado. 1. ed. São Paulo: Thomson Reuters Brasil, 2021. p. 137-162.

GEDIEL, José Antonio Peres; CORREA, Adriana Espíndola. Proteção jurídica de dados pessoais: a intimidade situada entre o Mercado e o Estado. *Revista da Faculdade de Direito UFPR*, Curitiba, n. 47, p. 141-143, 2008. DOI: http://dx.doi.org/10.5380/rfdufpr.v47i0.15738.

GIOVANELLA, Ligia *et al*. Sistema universal de saúde e cobertura universal: desvendando pressupostos e estratégias. *Ciência & Saúde Coletiva*, Rio de Janeiro,

v. 23, n. 6, p. 1763-1776, jun. 2018. DOI: http://dx.doi.org/10.1590/1413-81232018236.05562018.

GOMES, Orlando. *Contratos de adesão*: condições gerais dos contratos. São Paulo: Revista dos Tribunais, 1972.

GUZ, Gabriela. O consentimento livre e esclarecido na jurisprudência dos tribunais brasileiros. *Revista de Direito Sanitário*, São Paulo, v. 11, n. 1, p. 95-122, mar./jun. 2010. DOI: https://doi.org/10.11606/issn.2316-9044.v11i1p95-122.

HEINEN, Juliano. *Comentários à Lei de Acesso à informação*. 2. ed. Belo Horizonte: Fórum, 2015.

HOOFNAGLE, Chris Jay *et al*. Behavioral advertising: the offer you cannot refuse. *Harvard Law & Policy Review*, Harvard, v. 273, n. 6, 2012.

HORNUNG, Gerrit; SCHNABEL, Christoph. Data Protection in Germany I: The populational census decision and the right to informational self-determination. *Computer Law & Security Review*, v. 25, n. 1, p. 84-88, 2009. DOI: https://doi.org/10.1016/j.clsr.2008.11.002.

KELLEHER, John D.; TIERNEY, Brendan. *Data Science*. Cambridge: The MIT Press, 2018.

KONDER, Carlos Nelson. Vulnerabilidade patrimonial e vulnerabilidade existencial: por um sistema diferenciador. *Revista de Direito do Consumidor*, São Paulo, v. 24, n. 99, p. 101-123, 2015.

LEDERBERG, Joshua. ‘Ome Sweet ‘Omics – A genealogical treasury of words. *The Scientist*, abr. 2001. Disponível em: https://www.the-scientist.com/commentary/ome-sweet-omics---a-genealogical-treasury-of-words-54889. Acesso em: 11 ago. 2020.
PLAZA, Noelia Clemente; GARCÍA-GALBIS, Manuel Reig; MARTÍNEZ-ESPINOSA, Rosa María. Impact of the “Omics Sciences” in Medicine: New Era for Integrative Medicine. *Journal of Clinical Microbiology and Biochemical Technology*, v. 3, n. 1, p. 9-13, 2017. http://dx.doi.org/10.17352/jcmbt.000018.

LEMOS, Ronaldo; DOUEK, Daniel; ADAMI, Mateus Piva; LANGENEGGER, Natalia; FRANCO, Sofia Lima. A criação da Autoridade Nacional de Proteção de Dados pela MP n 869/2018. *Jota*, 29 dez. 2018. Disponível em: www.jota.info/opiniao-e-analise/artigos/a-criacao-da-autoridade-nacional-de-protecao-de-dados-pela-mp-869-2018-29122018. Acesso em 05 dez. 2020.

LOTHAR, Michael; MORLOK, Martin. *Direitos Fundamentais*. São Paulo: Saraiva, 2016.

LUCIANO, Maria; BIONI, Bruno Ricardo. O Consentimento como processo: em busca do consentimento válido. *In*: MENDES, Laura Schertel; DONEDA, Danilo; SARLET, Ingo Wolfgang; RODRIGUES JUNIOR, Otavio Luiz (org.). *Tratado de Proteção de dados pessoais*. Rio de Janeiro: Forense, 2021. p. 149-162.

MACHADO, Diego; DONEDA, Danilo. Proteção de dados pessoais e criptografia: tecnologias criptográficas entre anonimização e pseudonimização de dados. *Revista dos Tribunais*, São Paulo, v. 998, dez. 2018.

MARANHÃO, Juliano Souza de Albuquerque; ALMADA, Marco. Inteligência Artificial no Setor de Saúde: ética e proteção de dados. *In*: DALLARI, Analluza Bolivar; MONACO, Gustavo Ferraz de Campos (coord.). *LGPD na Saúde*. 1. ed. São Paulo: Thomson Reuters Brasil, 2021. p. 357-372.

MARQUES, Claudia Lima. *Contratos no código de defesa do consumidor*: o novo regime das relações contratuais. 9. ed. São Paulo: Revista dos Tribunais, 2020.

MARQUES, Claudia Lima; MIRAGEM, Bruno. *O novo direito privado e a proteção dos vulneráveis*. 2. ed. São Paulo: Revista dos Tribunais, 2014.

MARRARA, Thiago. *Manual de Direito Administrativo*. v. I. fundamentos, organização e pessoal. São Paulo: KDP, 2017. *E-book*.

MARTINS, Leonardo. İntrodução à jurisprudência do Tribunal Constitucional Federal Alemão. In: MARTINS, Leonardo (org.) *Cinquenta anos de jurisprudência do Tribunal Constitucional Federal Alemão*. Montevidéu: Fundação Konrad Adenauer, 2005. p. 33-128.

MENDES, Laura Schertel. Habeas Data e Autodeterminação Informativa: os dois lados da mesma moeda. *Direitos fundamentais e justiça*, Belo Horizonte, a. 12, n. 39, p. 185-216, jul./dez. 2018.

MENDES, Laura Schertel. *Privacidade, proteção de dados e defesa do consumidor*: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014.

MENDES, Laura Schertel; RODRIGUES, Otavio; FONSECA, Gabriel. O Supremo Tribunal Federal e a proteção constitucional de dados pessoais: rumo a um direito fundamental autônomo. *In*: MENDES, Laura Schertel; DONEDA, Danilo; SARLET, Ingo Wolfgang; RODRIGUES JUNIOR, Otavio Luiz (org.). *Tratado de Proteção de dados pessoais*. Rio de Janeiro: Forense, 2021. p. 61-72.

MENKE, Fabiano. A proteção de dados e o novo direito fundamental à garantia da confidencialidade e da integridade dos sistemas técnico-Informacionais no direito alemão. *In*: MENDES, Gilmar Ferreira; SARLET, Ingo Wolfgang; COELHO, Alexandre Zavaglia P. (coord.). *Direito, Inovação e tecnologia*. São Paulo: Saraiva, 2015. p. 205-230.

MENKE, Fabiano. As origens alemãs e o significado da autodeterminação informativa. *In*: MENKE, Fabiano; DRESCH, Rafael de Freitas Valle (org.). *Lei Geral de Proteção de Dados*: Aspectos Relevantes. 1. ed. Indaiatuba: Foco, 2021. p. 13-22.

MIRANDA, Custódio da Piedade Ubaldino. *Contrato de Adesão*. São Paulo: Atlas, 2002.

MOLINARO, Carlos Alberto; SARLET, Gabrielle Bezerra Sales. 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, a. 13, n. 41, p. 183-212, jul./dez. 2019.

MORLEY, Jessica *et al*. The ethics of AI in health care: A mapping review. *Social Science & Medicine*, set. 2020. DOI: 10.1016/j.socscimed.2020.113172.

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 jan. 2021.

MULHOLLAND, Caitlin Sampaio. Dados pessoais sensíveis e a tutela de direitos fundamentais: uma análise à luz da Lei geral de proteção de dados (Lei 13.709/2018). *Revista de Direitos e Garantias Fundamentais*, Vitória, v. 19, n. 3, p. 159-180, set./dez. 2018. p. 170. DOI: https://doi.org/10.18759/rdgf.v19i3.1603.

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. *Ciência & Saúde Coletiva*, Rio de Janeiro, v. 23, n. 6, jun. 2018. DOI: http://dx.doi.org/10.1590/1413-81232018236.05732021.

PEREIRA, Paula Moura Francesconi de Lemos. O uso da internet na prestação de serviços médicos. In: MARTINS, Guilherme Magalhães (Org.) *Direito Privado e Internet*. São Paulo: Atlas, 2014. p. 259-299.

RESENDE, José Renato Venâncio; ALVES, Cândice Lisbôa. A vacinação obrigatória como um dever jurídico decorrente do direito fundamental à saúde. *Revista da Faculdade de Direito UFPR*, Curitiba, v. 65, n. 2, maio/ago. 2020. DOI: http://dx.doi.org/10.5380/rfdufpr.v65i2.69582.

RICE, Kelley H. *Physician practice mergers*: the importance of due diligence and mutual trust for all involved. American College of Medical Practice Executives. 2018. Disponível em: https://bit.ly/2YMO7Vy. Acesso em: 23 jan. 2021.

RODOTÀ, Stefano. *A vida na sociedade da vigilância*: A privacidade hoje. Rio de Janeiro: Renovar, 2008.

RODRIGUES, José Carlos. *Higiene e ilusão*: o lixo como invento social. Rio de janeiro: NAU, 1995.

ROUVROY, Antoinette; POULLET, Yves. The Right to Informational Self-Determination and the Value of Self-Development: Reassessing the Importance of Privacy for Democracy. *In*: GUTWIRTH, Serge; POULLET, Yves; HERT, Paul; TERWANGNE, Cécile; NOUWT, Sjaak. *Reinventing Data Protection?* Heidelberg: Springer, 2009. p. 45-76. DOI: http://dx.doi.org/10.1007/978-1-4020-9498-9_2.

RUARO, Regina Linden; SARLET, Gabrielle Bezerra Sales. O direito fundamental à proteção de dados sensíveis no sistema normative brasileiro: uma análise acerca das hipóteses de tratamento e da obrigatoriedade do consentimento livre, esclarecido e informado sob o enfoque da Lei Geral de Proteção de Dados (LGPD). *In*: MENDES, Laura Schertel; DONEDA, Danilo; SARLET, Ingo Wolfgang;

RODRIGUES JUNIOR, Otavio Luiz (org.). *Tratado de Proteção de dados pessoais*. Rio de Janeiro: Forense, 2021. p. 177-198.

SALMEN, Caroline Salah; BELLÉ, Cathiane M. A Proteção de Dados Sensíveis e as Inovações da Área da Saúde. In: WACHOWICZ, Marcos (org.) *Proteção de Dados Pessoais em Perspectiva*: LGPD e RGDP na Ótica do Direito Comparado. Curitiba: Gedai, 2020. p. 242-270.

SANTORO, Raquel Botelho. A LGPD como ferramenta de compliance na área da saúde: política de privacidade e relatório de impacto à proteção de dados pessoais. In: DALLARI, Analluza Bolivar; MONACO, Gustavo Ferraz de Campos (coord.). *LGPD na Saúde*. 1. ed. São Paulo: Thomson Reuters Brasil, 2021. p. 249-262.

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*: MENDES, Laura Schertel; DONEDA, Danilo; SARLET, Ingo Wolfgang; RODRIGUES JUNIOR, Otavio Luiz (org.). *Tratado de Proteção de dados pessoais*. Rio de Janeiro: Forense, 2021. p. 485-506.

SARLET, Ingo Wolfgang. *A eficácia dos direitos fundamentais*. 12. ed. Porto Alegre: Livraria do Advogado, 2017.

SARLET, Ingo Wolfgang. Fundamentos Constitucionais: O direito fundamental à proteção de dados. *In*: MENDES, Laura Schertel; DONEDA, Danilo; SARLET, Ingo Wolfgang; RODRIGUES JUNIOR, Otavio Luiz (org.). *Tratado de Proteção de dados pessoais*. Rio de Janeiro: Forense, 2021. p. 21-60.

SCHIEDERMAIR, Stephanie. Einleitung. In: SIMITIS, Spiros; HORNUNG, Gerrit; SPIECKER GENANNT DÖHMANN, Indra (Coord.). *Datenschutzrecht*. Baden-Baden: Nomos, 2019.

SILVA, Amanda Rodrigues da. Autoridade Nacional de Proteção de Dados: Aspectos Institucionais da Autoridade Brasileira em Comparação com os Requisitos estabelecidos no Regulamento Europeu. MENKE, Fabiano; DRESCH, Rafael de Freitas Valle (org.). *Lei Geral de Proteção de Dados*: Aspectos Relevantes. 1. ed. Indaiatuba: Foco, 2021. p. 285-314.

SMITIS, Spiros. Reviewing Privacy in an Information Society. *University of Pennsylvania Law Review*, v. 135, p. 736, 1987.

SPIECKER GENNANT DÖHMANN, Indra. *Kontexte der demokratie*: Parteien, Medien und Sozialstrukturen. Berlin: De Gruyter, 2018.

TEPEDINO, Gustavo José Mendes. A responsabilidade médica na experiência brasileira contemporânea. *Revista Trimestral de Direito Civil – RTDC*, Rio de Janeiro, a. 1, v. 2, p. 41-75, abr./jun. 2000.

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. DOI: http://dx.doi.org/10.11606/issn.2316-9044.v19i1p166-187.

U.S. DEPARTMENT OF HEALTH & HUMAN SERVICES. *The HIPAA Privacy Rule*. Washington, D.C. S.d. Disponível em: https://www.hhs.gov/hipaa/for-professionals/privacy/index.html. Acesso em: 20 jun. 2021.

USTARAN, Eduardo. How to encourage Privacy Compliance. *Managing Intellectual Property*, v. 244, p. 36-37, 2014.

VIEIRA, Tatiana Malta. *O direito à privacidade na sociedade da informação*: efetividade desse direito fundamental diante dos avanços da tecnologia da informação. Porto Alegre: Sergio Antonio Fabris, 2007.

VIOLA, Mario; DONEDA, Danilo; ANDRADE, Norberto Nuno Gomes de. Dados Anônimos e tratamento de dados para finalidades distintas: a proteção de dados pessoais sob uma ótica civil-constitucional. *In*: TEPEDINO, Gustavo; FACHIN, Luiz Edson (org.). *Pensamento Crítico do direito civil brasileiro*. Curitiba: Juruá, 2011. p. 197-214.

VOSS, Gregory W. Internal Compliance Mechanisms for Firms in the EU General Data Protection Regulation. *Revue Juridique Themis*, v. 50, n. 03, p. 783-820, 2016.

WANG, Yichuan; KUNG, LeeAnn; BYRD, Terry Anthony. Big data analytics: Understanding its capabilities and potential benefits for healthcare organizations. *Technological Forecasting & Social Change*, 2016. DOI: http://dx.doi.org/10.1016/j.techfore.2015.12.019.

WANG, Yichuan; KUNG, LeeAnn; WANG, William Yu Chung; CEGIELSKI, Casey G. Integrated big data analytics-enabled transformation model: Application to health care. *Information and Management*, 2017. DOI: http://doi.org/10.1016/j.im.2017.04.001.