FACULDADE DE DIREITO
PROGRAMA DE PÓS-GRADUAÇÃO EM DIREITO
MESTRADO INTERINSTITUCIONAL EM DIREITO (UNDB/PUCRS)

ISABELLA FURTADO BACELLAR FORTES BRAGA

PROTEÇÃO DE DADOS PESSOAIS SENSÍVEIS EM SAÚDE PÚBLICA: UMA ANÁLISE DOS LIMITES NO TRATAMENTO INDEPENDENTE DE CONSENTIMENTO

São Luís
2022

PÓS-GRADUAÇÃO - *STRICTO SENSU*

Pontifícia Universidade Católica
do Rio Grande do Sul

ISABELLA FURTADO BACELLAR FORTES BRAGA

PROTEÇÃO DE DADOS PESSOAIS SENSÍVEIS EM SAÚDE PÚBLICA: UMA ANÁLISE DOS LIMITES NO TRATAMENTO INDEPENDENTE DE CONSENTIMENTO

Dissertação apresentada como requisito para a obtenção do grau de Mestre pelo Programa de Pós-Graduação em Direito da Faculdade de Direito da Pontifícia Universidade Católica do Rio Grande do Sul.

Área de Concentração: Fundamentos Constitucionais do Direito Público e do Direito Privado
Linha de Pesquisa: Eficácia e Efetividade da Constituição e dos Direitos Fundamentais no Direito Público e Direito Privado.

Orientadora: Prof.ª Dr.ª Regina Luaden Ruaro

São Luís

2022

Ficha Catalográfica

B813p Braga, Isabella Furtado Bacellar Fortes

Proteção de Dados Pessoais Sensíveis em Saúde Pública : uma análise dos limites no tratamento independente de consentimento / Isabella Furtado Bacellar Fortes Braga. – 2022.

117 f.

Dissertação (Mestrado) – Programa de Pós-Graduação em Direito, PUCRS.

Orientadora: Profa. Dra. Regina Linden Ruaro.

1. Tratamento independente de consentimento. 2. Dados Sensíveis em Saúde. 3. Lei Geral de Proteção de Dados. 4. Limites Interpretativos. 5. Autoridade Nacional de Proteção de Dados. I. Ruaro, Regina Linden. II. Título.

Elaborada pelo Sistema de Geração Automática de Ficha Catalográfica da PUCRS
com os dados fornecidos pelo(a) autor(a).
Bibliotecária responsável: Clarissa Jesinska Selbach CRB-10/2051

ISABELLA FURTADO BACELLAR FORTES BRAGA

PROTEÇÃO DE DADOS PESSOAIS SENSÍVEIS EM SAÚDE PÚBLICA: UMA ANÁLISE DOS LIMITES NO TRATAMENTO INDEPENDENTE DE CONSENTIMENTO

Dissertação apresentada como requisito para a obtenção do grau de Mestre pelo Programa de Pós-Graduação em Direito da Faculdade de Direito da Pontifícia Universidade Católica do Rio Grande do Sul.

Área de Concentração: Fundamentos Constitucionais do Direito Público e do Direito Privado
Linha de Pesquisa: Eficácia e Efetividade da Constituição e dos Direitos Fundamentais no Direito Público e Direito Privado.

Aprovada em: 28 de Novembro de 2022.

BANCA EXAMINADORA:

_____

Profa. Dra. Denise Pires Fincato-PUCRS

_____

Prof. Dr. Paulo Caliendo-PUCRS

_____

Prof. Dr. Guilherme Wünsch-UNISINOS

Aos meus pais, que são o meu porto seguro e maiores incentivadores

AGRADECIMENTOS

A Deus, o autor máximo da minha vida e o meu maior auxiliar e porto seguro, a minha força e resiliência durante toda esta pesquisa deve-se exclusivamente ao Senhor.

Em segundo lugar, um agradecimento especial a minha família e especialmente aos meus pais, Jones e Patrícia. O estudo acadêmico é por vezes solitário e angustiantes, mas vocês deixaram de ser os meus fiéis incentivadores e intercessores, em oração e apoio emocional constante.

Às minhas tias Ruth e Grazielle, que tanto representam na minha formação, agradeço pelo apoio incondicional e constante desde os meus primeiros passos; seu amor e confiança sempre me permitem enfrentar a vida com coragem e determinação.

Aos meus tios Luciano e Frederico agradeço pelo carinho e incentivo constantes, e também pela referência de vida e de profissionais. Vocês me inspiram.

Aos meu avôs Armando e José Mercedes Braga (*in memorian*) que tanto acreditaram em mim, sempre me fortalecendo com palavras de apoio e carinho, declarando que meu futuro será abençoado e os quais levarei sempre no coração.

As minhas avós Madalena e Graça, referências de vida, exemplos a serem seguidos. Mulheres à frente de seu tempo e que sempre acreditaram nas preciosidade do investimento na educação, e a tiverem enquanto uma força de modificação social.

Aos meus irmãos Jones Fillipe, Guilherme, Rafael e Rebeca, os quais representam uma doçura e alento em meio a tantos momentos estressantes desse último ano.

Aos meus irmãos de fé e pastores, Pastora Penha e Pastor Josué, meu muito obrigada por todas as orações, conselhos e admoestações tão importantes durante todo este processo e todos os conflitos internos que despontaram.

A todos os meus companheiros de mestrado, que dividiram comigo essa experiência única, nunca esquecerei todos esses 2 anos de convívio e amizade constantes.

E aos meus professores com quem aprendi valoras lições durante todo este curso de pós-graduação, em especial a pessoa da minha orientadora, Profa. Regina Linden Ruaro, direcionadora e referência quanto a este tema que tanto me encantou.

Muito obrigada a todos.

“Caminhante, são tuas pegadas
o caminho e nada mais;
caminhante, não há caminho,
se faz caminho ao andar
Ao andar se faz caminho
e ao voltar a vista atrás
se vê a senda que nunca
se há de voltar a pisar."

-Antônio Machado

RESUMO

À partir da permissiva constante no Art.11, inciso II, alínea b, da Lei 13.709/2018, quanto a possibilidade de tratamento de dados sensíveis independente de consentimento, impera a necessidade da afixação das balizas interpretativas para o tratamento e compartilhamento de dado sensíveis em saúde voltados ao desenvolvimento de políticas públicas epidemiológicas. Partindo de tal questão central e da problemática propulsora quanto a quais limites interpretativos seriam estes, a investigação deste estudo, de ambiência qualitativa, a utilizar o método indutivo, monográfico, e a estar embasado em uma técnica exploratória bibliográfica e documental, imprime enquanto objetivos específicos, a análise dos fatores históricos, sociais e jurídicos a que culminaram com a gênese de um direito autônomo a proteção de dados e de uma lei protetiva específica no contexto brasileiro; a abordagem do parâmetro para o desenvolvimento de políticas públicas epidemiológicas por intermédio da informatização e operação com dados sensíveis e perante ao aparente conflito entre os direitos fundamentais à proteção de dados e à autodeterminação informativa e o direito à saúde e à vida; verificação do processo de implementação prática da Autoridade Nacional de Proteção de Dados, à luz da previsão legal e regimental e, neste sentido, aferir os limites atinentes ao tratamento independente do ato consentir do usuário, a destacar o papel que esta autoridade desempenha nesse processo. As concludentes despontadas apontam, inicialmente no sentido de que os limites adstritos ao Art.11, inciso II, b são os consonantes a uma própria interpretação integral da Lei Geral de Proteção de Dados, a revelar e promover efetividade aos princípios e fundamentos dispostos na lei, assim como uma interpretação compatível com os ditames constitucionais e a revelar uma ética racional em tal atividade de tratamento, preocupada em promover o maior zelo possível aos direitos fundamentais dos usuários e titulares de dados. No tocante a segunda consideração final asseverada é referente ao papel salutar que a autoridade nacional detém nesse contexto, tanto de contribuição para a afixação de tais contornos interpretativos do dispositivo, como também a promover a fiscalização de que, uma fez fixado, seja implementando também no plano prático, a promover uma atuação preventiva pedagógica e elucidativa para a sociedade em geral e, oportunamente, a administração pública a quem compete a promoção de políticas e prestação de serviços em saúde.

Palavras-chave: Proteção de Dados Pessoais. Dados Sensíveis. Consentimento. LGPD.ANPD.

ABSTRACT

Based on the permissive contained in Art.11, item II, subparagraph b, of Law 13,709/2018, regarding the possibility of processing sensitive data regardless of consent, there is a need to affix interpretative beacons for the treatment and sharing of sensitive data in health aimed at the development of epidemiological public policies.Starting from this central question and the driving problem as to which interpretative limits these would be, the investigation of this study, with a qualitative ambience, using the inductive, monographic method, and being based on a bibliographic and documentary exploratory technique, prints as specific objectives , the analysis of the historical, social and legal factors that culminated in the genesis of an autonomous right to data protection and a specific protective law in the Brazilian context; the parameter approach for the development of epidemiological public policies through computerization and operation with sensitive data and in the face of the apparent conflict between the fundamental rights to data protection and informational self-determination and the right to health and life; verification of the process of practical implementation of the National Data Protection Authority, in light of the legal and regimental provisions and, in this sense, to assess the limits regarding the independent treatment of the user's consent act, highlighting the role that this authority plays in that process. The concluding conclusions point out, initially in the sense that the limits attached to Art.11, item II, b are those in line with an integral interpretation of the General Data Protection Law , to reveal and promote effectiveness to the principles and foundations provided for in the law, as well as an interpretation compatible with the constitutional dictates and to reveal a rational ethics in such processing activity, concerned with promoting the greatest possible zeal for the fundamental rights of users and data subjects. With regard to the second final consideration asserted, it refers to the salutary role that the national authority has in this context, both as a contribution to the posting of such interpretative outlines of the device, as well as to promote the inspection that, once established, is also implemented in the practical, to promote a preventive pedagogical and enlightening action for society in general and, in due course, the public administration, which is responsible for the promotion of policies and provision of health services.

Keywords: Protection of Personal Data. Sensitive Data. Consent. LGPD.ANPD.

SUMÁRIO

1 INTRODUÇÃO 9

2 A Gênese de um direito a proteção de dados 12

2.1 OS MULTICONTORNOS HISTÓRICOS DO DIREITO À PRIVACIDADE E O SURGIMENTO DE UMA NOVA ACEPÇÃO 12

2.2 O RECONHECIMENTO DA AUTONOMIA DE UM DIREITO À PROTEÇÃO DE DADOS E DE UM DIREITO À AUTODETERMINAÇÃO INFORMATIVA E O CENÁRIO EUROPEU 24

2.3 O BRASIL, O SISTEMA PROTETIVO AOS DADOS PESSOAIS EM DESENVOLVIMENTO 37

2.3.1 Antes da concepção: Como sinalizava-se a questão de dados no Brasil antes da criação da Lei 13.709/2018? 38

2.3.2 O surgimento de uma Lei Geral de Proteção de Dados, o Art. 5°, LXXIX, da CRFB/88 e os dados sensíveis quanto a saúde 42

3 O SISTEMA NORMATIVO DE proteção de dados em saúde 50

3.1 ENTRE A PRIVACIDADE, A TUTELA DA SAÚDE E OS DESAFIOS DA IMPLANTAÇÃO DE SISTEMAS INFORMATIZADOS NO ÂMBITO DA SAÚDE 53

3.2 A NORMATIZAÇÃO ATINENTE AOS DADOS SENSÍVEIS EM SAÚDE E AOS DADOS EPIDEMIOLÓGICOS SITUADA NA LEI GERAL DE PROTEÇÃO DE DADOS 63

4 AS BALIZAS AO TRATAMENTO INDENPENDENTE DE CONSENTIMENTO E A ATUAÇÃO DA ANPD 76

4.1 O PAPEL FISCALIZATÓRIO ESTATAL E NO ESTABELECIMENTO DE UMA POLÍTICA PROTETIVA DE DADOS CONCISA 81

4.2 A ANPD E SEU PROCESSO DE IMPLEMENTAÇÃO À LUZ DA LEI GERAL DE PROTEÇÃO DE DADOS 90

4.3 A DEFINIÇÃO DOS LIMITES ÉTICOS E LEGAIS QUE TANGENCIAM O ARTIGO 11, INCISO II, ALÍNEA B, DA LEI 13.709/2018 96

5 CONSIDERAÇÕES FINAIS 106

REFERÊNCIAS 110

1 INTRODUÇÃO

O presente trabalho dedica-se à temática da Proteção de Dados Sensíveis referentes à saúde, especificamente aos dados epidemiológicos, e as limitações aos direitos fundamentais dos usuários nos esforços para o desenvolvimento e a articulação de políticas públicas epidemiológicas.

Com a entrada em vigor da Lei Geral de Proteção de Dados (LGPD), assim como da previsão expressa no texto constitucional de um direito à proteção de dados enquanto direito fundamental, observou-se o incremento de um sistema protetivo específico quanto aos dados pessoais.

Nesse sistema, a regra para a viabilização do tratamento quanto aos dados pessoais é que perpasse pelo devido consentimento do titular do dado, a promover a efetivação do chamado direito à autodeterminação informativa. No entanto, a própria lei geral apresenta algumas exceções, a que entre elas consta o Artigo 11, inciso II e, especificamente ao contexto deste trabalho, sua alínea b, que prevê a autorização para tratamento com a finalidade de desenvolvimento de políticas públicas.

Nesse empreendimento, parte-se de uma delimitação temática, a que concerne precipuamente analisar os contornos interpretativos balizadores atinentes ao Artigo 11, inciso II, alínea b, da Lei 13.709/2018. Portanto, analisa-se os limites para o tratamento independente de consentimento do indivíduo quanto aos dados sensíveis em saúde para a consecução de políticas públicas epidemiológicas, à luz da salvaguarda mínima dos direitos fundamentais dos usuários e titulares de tais dados, especialmente quanto ao direito à proteção de dados, à autodeterminação informativa, à privacidade e ao livre desenvolvimento de sua personalidade.

A utilização cada vez maior das tecnologias na vida humana e nas próprias instituições políticas e sociais, revela o fenômeno da informatização. Essa informatização promove a intensa produção de dados e informações pessoais, nesse sentido e pelos riscos atrelados às operações quanto aos dados pessoais nesses desdobramentos sociais, surge a necessidade da criação de padrões normativos e um verdadeiro sistema protetivo específico para regular a matéria.

Essa informatização passou a ser utilizada em larga escala nos últimos anos, especialmente no âmbito da prestação de serviços de saúde por parte do Estado. Neste sentido, é primordial a discussão quanto aos limites no tratamento destes dados sensíveis em saúde, enquanto ferramentas aptas ao desenvolvimentos de políticas públicas na seara epidemiológica,

à luz da própria LGPD e dos direitos fundamentais consagrados na Constituição Federal, o qual assume o objetivo central do presente.

A minuciar os objetivos específicos, o primeiro corresponde a análise dos fundamentos normativos e sociais para a consecução de um direito autônomo a proteção de dados pessoais, bem como na criação de uma regulação específica frente a matéria no Brasil. Apresenta-se também a identificação das principais ponderações e percepções quanto ao conflito entre os direitos constitucionais fundamentais incidentes no cerne do tratamento de dados independente de consentimento para o desenvolver de políticas em saúde.

No tocante ao outro objetivo específico do trabalho, atém-se a traçar as balizas e os limites éticos, legais e constitucionais que tangenciam a permissiva expressa no Artigo 11, inciso II, alínea b, da LGPD, observando a figura da Autoridade Nacional de Proteção de Dados (ANPD), seu processo de implementação no Brasil e o papel que vem exercer, especialmente nestes contornos interpretativos e limitativos.

Partindo de toda a contextualização quanto à atividade investigatória desenvolvida neste trabalho, relata-se que a problemática que a impulsiona é justamente: quais seriam os limites a balizarem o tratamento de dados sensíveis independente de consentimento para a articulação de políticas públicas epidemiológicas? De uma forma subsidiária e atrelada ao questionamento principal, deriva a suscitação do papel da ANPD nessa afixação dos limites atinentes.

Por conseguinte, são geradas hipóteses preliminares. Inicialmente é apontado que os limites a pautarem o tratamento de dados independente do consentir do usuário, na forma do Artigo 11, inciso II, alínea b[1], da LGPD, devem ser rigorosos e condizentes a própria aplicação dos princípios constantes na legislação protetiva e em vias a expressar uma compatibilização máxima entre os direitos constitucionais colidentes, tal qual a saúde e a autodeterminação informativa, de forma a preservar seus núcleos essenciais.

Quanto à suscitação subsidiária, parte da hipótese de que a ANPD compete à fiscalização quanto o cumprimento dos preceitos legais, assim viabiliza que os limites quanto à interpretação de seus dispositivos sejam de fato observados e seguidos.

Referente ao plano de investigação e desenvolvimento da pesquisa efetuada, sua composição é feita na forma de três capítulos, sendo cada um deles dividido em subtópicos, a

[1] Art. 11. O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses:
(...)
II - sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para:
(...)
b) tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos; (BRASIL, 2018)

facilitar o entendimento e devido destaque dos pontos centrais a serem abordados. Por oportuno, o primeiro capítulo dedica-se à análise do surgimento de um direito autônomo à proteção de dados, no mundo em geral e no contexto específico brasileiro, assim como ao processo de criação de um sistema legal protetivo específico quando aos dados pessoais no Brasil.

O segundo capítulo está relacionado ao sistema normativo brasileiro de dados, agora especificamente no que trata dos dados sensíveis em saúde. Para tal ênfase é que inicialmente apresenta o paradigma da privacidade confrontado com as diretrizes estruturantes do Sistema Único de Saúde (SUS), a que sinalizam uma informatização e compartilhamento de informações e, por fim, vem abordar as normas referentes aos dados em saúde epidemiológica no cerne da própria LGPD.

Quanto ao último capítulo desponta apresentar a Autoridade Nacional de Proteção de Dados, enquanto autarquia basilar na proteção de dados no âmbito brasileiro, a quem compete bem mais que um múnus fiscalizatório, como também regulatório. Nesse sentido, indica seu processo de implementação e o estágio a que se encontra atualmente, ademais seu nível de competência e o papel a que vem desempenhar quanto aos limites adstritos à permissiva prefixada no Artigo 11, inciso II, alínea b, da lei.

A metodologia utilizada coaduna-se com uma abordagem qualitativa, mediante uma técnica exploratória de acervos bibliográficos, por meio de livros, artigos quanto à temática, e documental, através das legislações, regulamentos e jurisprudências emblemáticas brasileiras, assim como também do direito europeu comparado. O método de abordagem empreendido é o indutivo, a que observa particularidades objetivando conclusões mais amplas referentes ao fenômeno em estudo, utilizando-se também do método procedimental monográfico.

Este processo de informatização e intensa produção e manejo de dados no âmbito da saúde foi muito bem vislumbrada quando da pandemia do Covid-19, mas a ela não se limita, em verdade trata-se de uma tendência a permanecer e de ser ainda mais utilizada, sob a prerrogativa de promoção de uma tutela mais eficaz ao direito à saúde. Apesar de antes da pandemia o Brasil contar com alguns sistemas já informatizados quanto à saúde, em 2020 houve a instituição de uma Rede Nacional de Dados em Saúde (RNDS), a que busca justamente amplificar este processo.

Por oportuno, a geração de dados informatizados em saúde será cada vez maior e incentivada pelo próprio Estado, e neste sentido impera a contemporaneidade e necessidade de enfrentar as indagações suscitadas e desenvolvidas no trabalho em questão.

2 A GÊNESE DE UM DIREITO A PROTEÇÃO DE DADOS

Os desdobramentos do direito à privacidade e a personalidade que abrem espaço a uma conotação autônoma[2] de um direito à proteção de dados é viabilizado e reivindicado, ante ao amplo desenvolvimento das ferramentas tecnológicas. Estas ferramentas, ao passo que vem facilitar a vida humana e interligar todo o mundo, à partir do fenômeno da globalização, de outra sorte imprimem uma intensa produção e circulação de dados pessoais de seus usuários.

A ampla produção e utilização massiva de dados nos meios digitais vem a trazer os contornos de uma problemática social e o desenvolvimento de uma verdadeira sociedade da vigilância[3]. Nesse sentido, frente as especificidades e buscando referendar uma esfera de disciplina e proteção mais adequada e ferrenha é que se abre espaço, tanto nas discussões doutrinárias e jurisprudenciais, e, posteriormente, no próprio campo legislativo, para o surgimento de um direito específico à proteção de dados pessoais.

2.1 OS MULTICONTORNOS HISTÓRICOS DO DIREITO À PRIVACIDADE E O SURGIMENTO DE UMA NOVA ACEPÇÃO

Ao focar em um estudo quanto a tutela mínima de dados é importante inicialmente abordar o que são efetivamente dados, para efeito de tal proteção, bem como quando surgem na sociedade humana e quando são institucionalizados nos seguimentos sociais.

Os dados enquanto produtos, ou seja, produzidos e armazenados dentro de uma sociedade não surgem apenas quando falamos das tecnologias informacionais. Em verdade, remetem a período muito anterior, inicialmente beiravam a informalidade e oralidade no seu método de produção e não eram efetivamente registrados.

Posteriormente, a demanda e o crescimento na produção de dados, fato este intimamente ligado ao crescimento da própria população, imprimiram uma necessidade de armazenamento e devido registro físico (RUARO; RODRIGUEZ, 2010). Sob essa inicial necessidade de escrita física de dados no tecido social, temos o exemplo clássico dos bancos de dados públicos.

---

[2] "As novas dimensões da coleta e do tratamento de informações provocaram a multiplicação de apelos à privacidade e, ao mesmo tempo, aumentaram a consciência da impossibilidade de confinar as novas questões que surgem dentro do quadro institucional tradicionalmente identificado por este conceito." (RODOTÀ, 2008, p. 23)

[3] Tal sociedade da vigilância tem seu delineio inicial já abordada por Foucalt em Microfísica do Poder, pois indica, segundo os pensamentos de Bentham, que indica o poder ligado a ideia de um "olhar dominador e vigilante. Ele faz funcionar o projeto de uma visibilidade universal, que agiria em proveito de um poder rigoroso e meticuloso." (FOUCALT, 1979, p. 215)

Esse suporte inicialmente físico e escrito, perante ao desenvolvimento das tecnologias, abre margem para o registro agora em ambiente virtual, a que viabiliza até mesmo uma forma de organizar, sistematizar esses dados alcançados e resguardados. O processo de transferência para os meios informacionais é algo natural a inserção das tecnologias na sociedade e na sua identificação com um veículo facilitador a vida humana na mais ampla gama de esferas da sociedade.

A doutrina indica que essa mudança de paradigma de transição do aporte dos dados de forma escrita à digital, relaciona-se com a revolução industrial e com a alteração até mesmo da forma das relações humanas que esse cenário veio desencadear (RUARO; RODRIGUEZ, 2011, p. 48). Nesse sentido, as relações intersubjetivas humanas antes detinham um caráter mais pessoal, ligadas a confiança na própria palavra dos sujeitos e, assim é que apoiava a oralidade inicial dos dados.

Posteriormente, ante à perda de tais características das relações intersubjetivas e especialmente das relações negociais, levou-se a necessidade da ampla produção de dados, com seu armazenamento em locais de fácil acesso e não sujeitos ao esquecimento que apenas a palavra, o dito entre as partes, poderia representar.

> O modelo de produção industrial fez necessários que se enrobustecesse o registro dos fatos e acontecimentos diários, como forma de auxílio à memória, como forma de fazer evidências e como ferramentas para o próprio planejamento da vida. A divisão de tarefas, bem como as máquinas e produtos tinham que ser planejados, controlados e dirigidos. Sem documentação e contabilidade nada disso seria possível. Ao contrário, antes desta era, tinha-se uma produção e estruturação "de boca em boca". Para o método adotado na produção industrial, que se impôs na Europa desde o fim do século XVIII, já não era mais suficiente este modo de armazenamento tradicional de informação." (RUARO; RODRIGUEZ, 2010, p. 48-49)

Chegando à fase do armazenamento físico de dados, seja em bancos públicos ou privados- estes a que os particulares controlavam e armazenavam as informações que lhe eram relevantes-, perante a curva ainda exponencial no crescimento da produção de dados, vistos como produtos claramente do próprio crescimento social e industrial, revelou-se uma necessidade de repensar este armazenamento tradicional de dados.

Da necessidade de rompimento com o armazenamento escrito até o armazenamento hodiernamente verificado, o ponto de virada ocorre com o surgimento dos computadores e, posteriormente, com o surgimento de inúmeras outras tecnologias que servem à serviço semelhante.

Os meios físicos[4] antes utilizados, seja pelas empresas ou mesmo pelo próprio Estado, através da fragilidade de uma maior chance de perda ou degradação, ou mesmo pela dificuldade em criar uma sistematização, ou seja, uma interligação entre todos os dados que viesse a facilitar o acesso e desbravamentos de informações relevantes, abriu espaço para o digital como melhor saída.

O digital figura então como um facilitador nas atividades humanas e, entre elas, a de armazenamento e alocação de dados. Armazenamento este que é muito mais dificultoso ocorrer uma degradação ao longo dos anos, como o papel imprimia, e que necessita de bem menos espaço físico, como não era o caso dos bancos de dados públicos outrora vigentes.

Na era digital continua-se a utilizar a dicção "Banco de Dados", que passaram a estar armazenados nos sistemas informatizados, por vezes no que chamamos rotineiramente de "nuvens". Nota-se que como aspectos positivos dessa transição, a facilidade de armazenamento, assim como uma facilidade também ao acesso e o alcance de novas informações, por meio a viabilidade de interação cada vez mais massiva entre dados.

Ao apresentar que o ponto de virada ocorreu quando do surgimento das tecnologias, sendo muito bem representada pela ilustração do computador, cabe algumas ponderações relevantes.

O surgimento dos computadores estão ligados de forma primária a estudos matemáticos e a tentativa de realizar tais cálculos em alta performance. Assim surgiu o projeto-piloto através das conhecidas "super calculadoras" que tinham resultados que superavam o do próprio homem (CONSENTINO, 2006).

Nos anos seguintes teve um desenvolvimento exponencial durante a II Guerra Mundial e também durante a Guerra Fria, a serviço da criptografia de mensagens e ao auxílio de serviços de espionagem (CARVALHO, 2006, p. 6). Para tanto, o protótipo inicial a serviços matemáticos e de cálculos, teve um desdobramento múltiplo e a cargo de outros serviços relevantes à época.

Posteriormente ao seu surgimento inicial, que ainda era monopolizado por centros de pesquisas e governos, é na década de 80 e 90 que há o que chamamos de um momento de popularização de seu uso, em que as máquinas anteriormente utilizadas apenas para viés técnico (matemático, pesquisa), passou a ter outros fins que serviam ao entretenimento e facilidades a população em geral (CONSENTINO, 2006, p. 62).

[4] Aponta-se que um dos exemplos dessa modificação nas empresas ficou por cargo da instituição dos cartões, denominados *Lochkarten*. A tradução da palavra alemã remete a "cartões perfurados". (RUARO; RODRIGUEZ, 2010, p. 49)

A este momento de utilização popular, ou alcance das massas a tais máquinas, divide-se didaticamente em duas fases o processo de interação verificado entre o homem e esta ferramenta tecnológica.

A primeira fase, chamada de Web 1.0, os usuários tinham um papel muito mais passivo em tal contato. Não que não havia a produção de dados, mas os utilizadores de tais computadores/ tecnologias não participavam tão ativamente na produção de novos dados e figuravam como leitores ou consumidores de dados previamente disponibilizados pelas grandes empresas e pelos grandes produtores de conteúdo nessa rede de internet. (COLOMBO, FACCHINI NETO, 2017, p. 60-61).

Já na conhecida Web 2.0 os produtores de conteúdo e de dados não estão mais vinculados apenas a grandes empresas, mas tem espaço aos próprios usuários, que não apenas são consumidores, mas geradores de dados e informações no meio digital (COLOMBO, FACCHINI NETO, 2017, p. 61). Esse contexto é especialmente viabilizado através das redes sociais, em que há um estímulo massivo na disponibilização de dados pessoais de seus "navegantes".

O exponente crescimento dos dados em ambientes virtuais e a gama de informações que podem ser desmembradas, inclusive com a formulação de perfis pessoais dos padrões de navegação dos indivíduos usuários, passa a ter, cada vez mais, uma valorização monetária (TOBBIN, CARDIN, 2020, p. 1265).

Esta valorização é refletida no contexto das transações astronômicas monetárias que objetivam disponibilizar acesso de grandes empresas, quanto aos dados que lhe são pertinentes no desenvolver de uma determinada atividade econômica. Assim, por vezes, comercializam informações condizentes com seu interesse de formulação de direcionamento de propaganda, a que esteja atentamente atrelada ao padrão de interesse e de consumo dos usuários.

Esse direcionamento é ajustado através das navegações anteriores destes usuários, através de suas curtidas, de seus comentários e até mesmo de seu histórico de acesso.

Nessa corrida do capital, o cenário conhecido como "capitalismo da vigilância" predita um contexto em que os produtores e os grandes conglomerados utilizam do artificie de acesso aos dados a converterem em ganhos ao seu negócio e em lucro efetivo. Através do processamento e manejo de tais dados, como bem explicita Shoshana Zuboff (2019, p. 23), podem até antecipar comportamentos futuros do indivíduo, pois não "apenas conhecem o nosso comportamento", mas através de tal fonte de informações podem incentivar adequadamente a fim de moldar os comportamentos futuros.

> [...] Pressões de natureza competitiva provocaram a mudança, na qual processos de máquina automatizados não só *conhecem* nosso comportamento, como também *moldam* nosso comportamento em escala. Com tal reorientação transformando conhecimento em poder, não basta mais automatizar o fluxo de informações *sobre nós*; a meta agora é *nos automatizar*. Nesta fase da evolução do capitalismo de vigilância, os meios de produção estão subordinados a "meios de modificação comportamental" cada vez mais complexos e abrangentes. Dessa maneira, o capitalismo de vigilância gera uma nova espécie de poder que chamo de *instrumentalismo*. O poder instrumentário conhece e molda o comportamento humano em prol das finalidades de terceiros. Em vez de armamentos e exércitos, ele faz valer sua vontade através do meio automatizado de uma arquitetura computacional cada vez mais ubíqua composta de dispositivos, coisas e espaços "inteligentes" conectados em rede. (ZUBOFF, 2019, p. 23)

Acessar dados e tentar efetivamente traçar padrões[5] e, a partir disso, formular, os já citados acima, perfis que em inúmeras vezes servem a oferta de produtos direcionados e contribuem para uma maior produção de riqueza estão por muita das vezes viabilizadas pelas chamadas tecnologias de *"big data"*.

Apesar da certa abertura que a terminologia *"big data"* aponta, esta teria sido utilizada inicialmente quando do início do século XXI aos casos de tão intensa produção de dados e informações que a memória desenhada originariamente aos computadores não seria suficiente (SZIVELSKI; ARCENO; FRANCISCO, 2019, p. 138).

Como características centrais do *"big data"*[6] há uma velocidade ímpar no tratamento de dados, assim como um volume exponencial dos mesmos, com a ampliação dos meios de coleta, gerando cada vez mais a produção e uma massiva mineração de dados. Outrossim, o acesso está relacionado não apenas a dados estruturados[7], o que imprime, como consequência,

---

[5] "Os perfis são composições, ou melhor dizendo, são mosaicos compostos pelas informações fornecidas pelos usuários em uma formatação igualmente constituída e circunstanciada pelo que é consciente e livremente disponibilizado e pelo que advém das pegadas digitais, dos cruzamentos e dos vazamentos de dados." (SARLET; RUARO, 2021, p. 87)

[6] Sobre o que é o big data e as modificações a que ele proporciona nos sistemas de informação e na própria sociedade, aponta: "Como resultado do barateamento das estruturas de coleta e armazenamento de dados, passaram a surgir novas possibilidades para análises e identificações de padrões em eventos aparentemente aleatórios.
Isto ocorre porque, fora dos limites humanos, o big data trabalha em conjuntos tão grandes de dados que permitem a identificação de correlações que, para um ser humano, parecem desconexas. [...]. As correlações, no mundo do big data, são infinitas, pois um mesmo conjunto de dados pode ser analisado por algoritmos distintos na busca por novos padrões. Os resultados dessas análises parecem completamente aleatórios em virtude de esses sistemas serem capazes de associais informações sem precedentes na história humana." (MENEZES NETO, 2016, p. 137-138)

[7] "Os dados coletos na web podem ser classificados em estruturados e não estruturados. Os dados estruturados são aqueles organizados, ou seja, estão tabulados em linhas e colunas. É o que se verifica, por exemplo, na coleta de dados decorrentes do Portal da Transparência, que identifica o servidor público federal, seu cargo e sua remuneração. Neste caso, não há necessidade de maior tratamento destes dados para que se possa atingir o estágio da informação e, por último, do conhecimento. Por sua vez, dados não estruturados são os textos, imagens, vídeos

uma necessidade de sofisticação das ferramentas tecnológicas para sua devida interpretação (MENEZES NETO, 2016, p. 166).

Quanto ao fenômeno e os reflexos que imprimem na sociedade, considera-se que permite o trabalhar com uma gama cada vez maior de dados, assim como a leitura e interação entre os dados, através de aparatos tecnológicos cada vez mais incrementados, de forma a viabilizar o acesso e detenção de uma nova gama de informações (SARLET; MOLINARO, 2019, p. 184).

> [...] o big data permite que o homem possa atribuir sentido a um conjunto de informações cada vez maior. A capacidade para analisar grandes conjuntos de dados torna-se um diferenciador para as entidades envolvidas- empresas e governos-, uma vez que melhores resultados podem ser obtidos através da elaboração de algoritmos de análise mais sofisticados. Esses algoritmos, contudo, pressupõem a existência de um sistema digital capaz de coletar esses dados, o que só pode ser feito em uma sociedade "mergulhada" no mundo tecnológico, onde todas as transações e interações típicas do cotidiano são mediadas, em algum momento, por uma estrutura virtual de dados. (MENEZES NETO, 2016, p. 167)

A este abundante desenvolvimento e a criação de um verdadeiro novo ambiente de convívio entre os seres humanos, o ambiente virtual, a que insere e integra cada vez mais o cotidiano e as atividades sociais, veicula, por outro lado, uma produção e disponibilização também abundante de dados pessoais nessa rede virtual. Assim é que o capitalismo passa a servir-se de tais interações e informações geradas pelos dados, no sentido de atender a seus próprios interesses.

Considerando as transformações sociais vivenciados nos últimos séculos, primordialmente pela inserção da tecnologia no mundo e a dispersão de seu acesso à população, reivindica um acompanhamento do Direito, em corresponder a proteção necessária e ante aos inúmeros problemas que foram surgindo e se instalando no manejo dessas operações.

Da mesma maneira que os dados pessoais dos "navegantes" das redes virtuais e dos participantes do "meio ambiente virtual" passam a ser considerados o "novo petróleo"[8] pelos detentores e geradores do capital, de outra parte, há a situação de fragilidade desse indivíduo frente a tais forças.

---

e sons. Dessa forma, é preciso maior custo, tempo e expertise para interpretação destes dados." (COLOMBO; FACCHINI NETO, 2017, p. 62-63, grifo nosso)

[8] "Nossos dados já são vistos como "o novo petróleo", sendo imprescindíveis para as articulações metodológicas na contemporaneidade." (COSTA; OLIVEIRA, 2019, p. 23)

A fragilidade que denota o posicionamento dos usuários de tais sistemas tecnológicos é efetivamente considerada pelo Direito e, como apontado, reivindicado uma espécie de solução perante a problemática de risco que esta atividade de operação de dados pode vir a gerar.

Apesar do papel de holofote que o direito e a jurisprudência europeia detiveram em vislumbrar os contornos problemáticos e assegurar um diploma de proteção específica, quando se trata de manejo de dados pessoais, o germine dessa disciplina, segundo Danilo Doneda (2020, p. 24), está ligado aos Estados Unidos da América.

Nos Estados Unidos apontava-se a preservação da esfera íntima do indivíduo na forma de um direito à privacidade e já suscitava-se, de forma ainda primitiva, quanto a potencial lesividade nas circunstâncias de interação com as ferramentas tecnológicas.

No artigo "The right of privacy" de Samuel D. Warren e Louis D. Brandeis que datava de 1890 (p. 195) já se apresentava que as intensas mudanças dos negócios associadas as invenções verificadas chamariam a um "novo degrau" quanto a proteção da pessoa, justamente na identificação de um direito à privacidade.

Esse direito à privacidade vem abrir caminho perante a necessidade de demarcação de um espaço privado a ser controlado e livre de possíveis ingerências do âmbito público. Em síntese, trata-se de uma liberdade negativa (BIONI, 2021, p. 93) de que o indivíduo seja "deixado só", no sentido de uma abstenção de interferência dos demais sobre as questões sensíveis de sua vida que ditam e fazem parte, enquanto questões subjetivas, do livre desenvolvimento da personalidade daquele sujeito.

O conceito tradicional da privacidade nesse ambiente é compreendido como o "direito de ser deixado só", segundo a expressão apontada pelo juiz americano Cooley (WARREN; BRANDEIS, 1890, p. 195), perante o reconhecimento já na seara do direito americano que seria necessário um instrumento no *common law* em trazer uma resposta aplicável às situações de invasão íntima e sensível da esfera privada do indivíduo.

Ímpar assinalar que se já em 1890 tinha-se a detectação de um problema afeto a preservação dessa esfera íntima do sujeito, quando os invasores ferrenhos eram os jornais à época que figuravam como os grandes vilões, hoje, com as novas formas de adentrar a esfera íntima viabilizadas pelos aparatos tecnológicos, a reivindicação é ainda mais latente e justificável.

Nesse sentido, o *"next step"* (WARREN; BRANDEIS, 1890) reivindicado a proteção da pessoa e que culminou com o surgimento do próprio direito à privacidade, agora perante a energização e novos contornos de possíveis agressões, indicam a necessidade de ainda um novo

passo, ou melhor dizendo, um novo contorno na própria definição e esfera de proteção que tal direito à privacidade propõe.

O mero "direito de ser deixado só" não corresponde plenamente as demandas e novas reinvindicações[9] que o novo cenário instalado reivindicam (RODOTÀ, 2008, p. 23).

Sobre esse processo, Laura Schertel Mendes (2014, p. 29) bem sintetiza,

> No decorrer do século XX, a transformação da função do Estado, aliada à revolução tecnológica, contribuiu para modificar o sentido e o alcance do direito à privacidade. De um direito com uma dimensão estritamente negativa e com uma conotação quase egoísta, passou a ser considerado uma garantia de controle do indivíduo sobre as próprias informações e um pressuposto para qualquer regime democrático. É nesse sentido que se pode afirmar que o século passado vivenciou um "processo de inexorável reinvenção da privacidade.

Para tanto é que esse "novo degrau" quanto à privacidade é visto, em verdade, como um reforço[10] as situações de invasões a esfera sensível das pessoas, que apenas a acepção de "ser deixado só" não corresponderia e tutelaria plenamente.

O "desbravamento" para além do conceito tradicional de privacidade, segundo Stefano Rodotà (2008, p. 24) não se trata em essência ligado a acepção da palavra desbravar. O termo "desbravar", remete ao verbo descobrir segundo o Dicionário, mas o processo em questão em verdade sintetiza o verbo "explorar".

Isso porque essa nova acepção em comparação a definição clássica do direito à privacidade, e que irá melhor servir as novas situações sociais sensíveis, não se trata da gênese de algo totalmente novo. Em verdade, o que ocorre é que o centro de relevo, ou de gravidade, como bem nomeia Rodotà (2008), era voltado inicialmente ao "ser deixado só", mas que a releitura resgata aspecto que já podia ser dissociado do direito à privacidade e que apenas não tinha o devido destaque e desenvolvimento.

> [...] Não que este último aspecto estivesse ausente das definições tradicionais: nelas, porém, ele servia muito mais para sublinhar e exaltar o ângulo individualista, apresentando a privacidade como mero instrumento para

[9] Sobre esta necessidade de revisitar o conceito tradicional do conceito de privacidade e o expandir, Laura Schertel Mendes (2014, p. 27) aponta, "[...] como consequência da utilização de novas técnicas e instrumentos tecnológicos, que passaram a possibilitar o acesso e a divulgação de fatos relacionados à esfera privada do indivíduo de uma maneira anteriormente impensável."

[10] Sobre a necessidade de reforço, a trazer uma releitura do conceito tradicional de privacidade: *"It remains to consider what are the limitations of this right to privacy, and what remedies may be granted for the eforcement of the right. To determine in advance of experience the exact line at wich the dignity and convenience of the individual mut yield to the demands of the public welfare or of private justice would be a task."* (WARREN; BRANDEIS, 1890, p. 214)

> realizar a finalidade de ser deixado só; enquanto hoje chama a atenção sobretudo para a possibilidade de indivíduos e grupos controlarem o exercício dos poderes baseados na disponibilização de informações, concorrendo assim para estabelecer equilíbrios sócio-políticos mais adequados. (RODOTÀ, 2008, p. 24).

Quanto a um alargamento no conceito do direito à privacidade, para além das vestes clássicas iniciais, Stefano Rodotà (2008, p. 24) destaca que a informatização da sociedade não é algo que possa ser contido ou freado. Para tanto, urge ter espaço uma acepção que indique um protecionismo quanto a este poder o qual os controladores de dados são detentores, podendo levar a uma militância de verdadeira retomada de um poder que deveria ser unicamente subjetivo e pessoal e não colocado nas mãos de terceiros estranhos e que nem mesmo mostram quem são, inseridos e fantasiados pelos subterfúgios e tecnicidades da era digital.

Assim, esse alargamento pode gerar, como consequência, na configuração de uma privacidade esboçada na capacidade de determinação pelos próprios usuários, desses meios digitais, sobre a circulação dos dados que irão versar sobre eles mesmo. Frear, então, essa assimetria de poder verticalizada na preponderância dos controladores de dados.

Nesse sentido,

> O direito à privacidade abrange, hoje, não apenas à vida íntima do indivíduo, mas também a proteção de seus dados pessoais. Em outras palavras: o direito à privacidade hoje é mais amplo que o simples direito à intimidade. Não se limita ao direito de cada um ser "deixado só" ou de impedir a intromissão alheias na sua vida íntima e particular. Transcende essa esfera doméstica para alcançar qualquer ambiente onde circulem dados pessoais do seu titular, aí incluídos suas características físicas, código genético, estado de saúde, crença religiosa e qualquer outra informação pertinente à pessoa. Nesse sentido, a privacidade pode ser definida sinteticamente como o direito ao controle da coleta e da utilização dos próprios dados pessoais. (SCHREIBER, 2014, p. 138-139

O direito à privacidade é uma expressão do próprio direito de personalidade, tal qual, inclusive, consagrado em nosso ordenamento jurídico no artigo 5°, inciso X da Constituição Federal de 1988, sendo resguardado desde o nascimento com vida do indivíduo (BRASIL, 2002, Artigo 2°).

Perante este pressuposto e no esforço de conceituar o direito a personalidade, dado a sua aparente abrangência terminológica, é que Cíntia Rosa Pereira Lima (2020, p. 34) indica: "[...] são direitos subjetivos especiais, isto é, prerrogativas concedidas a uma pessoa pelo ordenamento jurídico, de fruir e dispor, dentro dos limites da lei, dos atributos essenciais da sua própria personalidade."

Os direitos à personalidade detém como natureza precípua o fato de serem direitos próprios e arraigados ao próprio homem (BITTAR, 2015, p. 35) e destinados a proteção mínima das projeções e contornos que são embutidos e característicos da sua própria condição enquanto homens[11].

Perante o desenvolver da sociedade, ao longo das décadas vão surgindo e se estabelecendo novas formas de expressão da proteção do amplo desenvolvimento da personalidade. Para tanto, essas novas formas de expressão, por vezes são dotadas de autonomia própria e positivação individualizada e específica, como se observa no caso da intimidade e a preservação da privacidade.

Com a influência da tecnologias e mineração de dados no últimos anos de forma a reivindicar novas formas de agressão mais sensíveis e profundas a intimidade das pessoas, abre-se espaço a esse processo de surgimento de novos direitos corolários ao próprio direito da personalidade enquanto necessidade protetiva à pessoa humana.

Nesse sentido, o processo de desenvolvimento de novos direitos corolários e dotados de autonomia é muito bem observado. Encontra-se, evidentemente, viabilizado pelo diagnóstico social latente das possíveis imbricações de problemas e preocupações de potenciais agressões.

Sobre tais "novos direitos", em verdade, caminham lado a lado como corolários de outros já consagrados, como o direito a personalidade, pois "concorrem a preservar um conteúdo densificado da pessoa humana, e de sorte a ampliar o raio de tutela de todas as suas renovadas virtualidades." (GODOY, 2019, p. 4)

A existência desses direitos de forma autônoma não mina a importância ou diminui a incidência e/ou razão de ser dos chamados direitos da personalidade. A clara abertura que indica a terminologia "direitos da personalidade", conduz a uma atividade do legislador, bem como do intérprete de articular a proteção mais ampla e completa possível desse direito, chegando até mesmo a tipificar novos direitos, mas que derivam daquele.

Ímpar considerar que a personalidade, assim como o próprio sujeito humano é indivisível (DONEDA, 2020), e que as novas expressões autônomas de direitos corolários vinculam-se a reivindicações sociais[12], assim como opções específicas a facilitarem os

[11] Essa noção inata ao próprio homem do direito a personalidade remete a contribuição dessa vertente jusnaturalista para o esforço inicial de sua conceituação e delimitação, notadamente os jusnaturalistas franceses e alemães. (SCHREIBER, 2014, p.5)

[12] Sobre a criação, em decorrência dos processos de modificações sociais e culturais na sociedade, de autônoma de um direito à proteção de dados como um corolário do direito à privacidade: "Elástica, flexível, fluida são alguns dos adjetivos que se pode utilizar para caracterizar a privacidade. Como demonstra-se, da antiguidade ao momento atual, as definições de público e privado sofreram profundas alterações, expandindo suas possibilidades, atingindo novos espaços e adaptando-se ao comportamento humano, também marcado pela liquidez." (CANCELIER, 2017, p. 229)

trabalhos e os esforços da proteção da personalidade humana em sua expressão dinâmica e de multicontornos.

O nascimento autônomo desses novos direitos são assim atrelados a própria asseguração e proteção das projeções amplas humanas assumidas. Nesse sentido, afirmam a denominada cláusula geral de personalidade que, conforme aponta Danilo Doneda, tem como função "orientar a interpretação e facilitar a aplicação e a tutela nas hipóteses em que a experiência ou a natureza dos interesses possam inspirar o legislador a tratá-las com maior detalhe." (2020, p. 73).

Por oportuno é que a nomenclatura empreendida é de que se trata de corolários ao próprio direito à personalidade, na medida em que caminham no mesmo sentido de proteção da pessoa humana e de sua dignidade em seu máximo exponencial.

Sob esse o esforço de reafirmar o livre desenvolvimento da personalidade e dignidade da pessoa humana e perante a onipresença da tecnologia, que ao enraizar-se no cotidiano tem o potencial de atingir a intimidade das pessoas a um novo nível, surge um processo de autonomia conferida a proteção de dados, como corolário do direito a personalidade e a própria privacidade. Viabiliza-se justamente por tocar nessa concepção de uma esfera íntima intangível própria do homem enquanto homem, em suas relações intersubjetivas ou subjetivas.

Apesar da clara identificação da raiz originadora, o direito à proteção de dados não pode ser confundido com o direito à privacidade e nem mesmo tratado simplesmente como apenas um salto evolutivo do mesmo, conforme bem destaca Ingo Sarlet (2021, p. 16 e 25). Seria errôneo e reducionista, a cercear sua incidência de proteção.

Há uma amplitude no objeto do direito à proteção de dados, englobando as variadas espécimes de dados que versam sobre um usuário e a atrelarem as inúmeras possibilidades de afetações a esfera sensível do indivíduo, não limitando apenas a esfera íntima, como também a social e familiar, por exemplo.

Dessa forma, a proteção dos dados impele um caráter protetivo atento e resolutivo a todas as peculiaridades que os desdobramentos tecnológicos e a massiva mineração de dados pode vir a gerar. Ademais, essa tutela protetiva parte do pressuposto do não descarte ou consideração de qualquer dado pessoal que seja como irrelevante, mas sim digno da devida proteção e a ter em vista seu potencial de lesividade a esfera íntima de indivíduos.

> É por tal razão, aliás, que a própria opção terminológica pela proteção de dados pessoais assume uma importância que vai muito além da mera novidade representada pela terminologia em si, porquanto, radica numa viagem concepcional, visto que parte do pressuposto de que dados, para efeitos de sua

> proteção jurídico-constitucional, devem ser compreendidos em sentido amplo, no sentido da inexistência de dados pessoais irrelevantes em face do processamento eletrônico na sociedade de informação, notadamente pelo fato de que, sendo os dados projeções da personalidade, o seu tratamento, seja qual for, potencialmente pode violar direitos fundamentais. (SARLET, 2021, p. 22)

Perpassando primeiramente pela razão de ser do reconhecimento de um direito a proteção de dados e sua relação próxima, mas não sinônima, com o direito à privacidade, impere também identificar como ocorreu tal movimento de autonomia no direito efetivamente e, posteriormente, analisar este processo no contexto especificamente brasileiro.

Justamente perante a já citada mudança de paradigma social pela exponencial inserção e relação de uma acentuada codependência na interação do ser humano com as tecnologias, gera-se uma intensa gama de dados a serem produzidos, coletados, armazenados e utilizados para fins diversos dentro dessa sociedade, como facilitadores de sistemas afins e/ou mesmo como uma "joia" monetizada à serviço das grandes empresas e conglomerados[13].

Nesse fluxo, perante as novas possibilidades apresentadas, por outro lado, também se desenham canais de invasão na esfera pessoal dos usuários de tais tecnologias nunca antes imaginados. Esses usuários encontravam-se, e encontram-se ainda hoje, em um patamar de intensa fragilidade, seja pela dependência social de adotar o uso de tais ferramentas ou mesmo pelo obscurantismo que os controladores de tais plataformas trabalham.

A fim de coadunar as considerações aduzidas alhures de Ingo Sarlet (2021, p. 22) e também de Danilo Doneda (2020, p. 164), assim com as conclusões próprias, o surgimento de um direito a proteção de dados trata-se de fluxo inerente à fenomenologia social e valorativa das relações humanas frente a esse novo cenário informacional que atuaram sobre as noções jurídicas já existentes, dentre elas o próprio direito à privacidade.

Esse fluxo, como já destacado, não se trata apenas de uma relação em que o direito à proteção de dados é uma evolução do direito à privacidade, pois se tratam de conceitos e esferas específicas de proteção distintas. Em verdade, faz uma espécie de atualização, com o alargamento e elasticidade do conceito de privacidade, com a promoção na delimitação desse novo direito das características que lhe são próprias (DONEDA, 2020, p. 164), especificas e geradoras de seu diferencial e autonomia.

[13] "Em consequência dessa realidade temos que, por ser o dados pessoal uma informação, quem a detém tem poder, o que acaba atribuir-lhe um valor econômico a ser comercializado em determinadas circunstância." (RUARO; MOLINARO, 2017, p. 14)

2.2 O RECONHECIMENTO DA AUTONOMIA DE UM DIREITO À PROTEÇÃO DE DADOS E DE UM DIREITO À AUTODETERMINAÇÃO INFORMATIVA E O CENÁRIO EUROPEU

A necessidade de reconhecimento de um direito autônomo relacionado à proteção de dados foi paulatina no direito a nível mundial. Não ocorreu de forma uniforme, visto que ainda hoje carece de plena afirmação por parte de alguns ordenamentos jurídicos.

Essa autonomia deriva justamente do cenário social, político e cultural afeto as relações humanas e ao novo desenho do globo, bem como da invocação de um sistema de proteção mais ferrenho e eficaz frente a tais mudanças e as possíveis agressões verificadas ao livre desenvolvimento da personalidade do homem de forma digna e plena.

O alargamento de tais discussões remete a década de 90 no eixo europeu, quando da Convenção de Estrasburgo de n. 108 de 1981 e das Diretrizes para a Proteção da Privacidade e dos Fluxos Transfronteiriços de Dados Pessoais de 1980 (GNOATTON, 2021, p. 24). Esta, de ano anterior a Convenção de Estrasburgo, foi de alcunha da Organização para a Cooperação e Desenvolvimento Econômico e já apontava princípios, como a necessidade de limitar-se a coleta e a operação a qualquer custo dos dados e a imperiosidade de sua utilização ser viabilizada perante o atendimento de finalidades específicas[14].

Tais princípios e limitações se desenvolveram e foram afixados de uma forma normativa, em um esforço de integração europeia, por intermédio desta Convenção de 1981. No bojo do artigo 1° do texto da convenção indicou como objetivo basilar a proteção mínima de direitos e liberdades individuais, notoriamente a vida privada, face aos desdobramentos que o tratamento automatizado de dados impõe.

Esses documentos, apesar de notória significância ao colocar em relevo tal temática e revelar a pungência do tema, não tinham caráter vinculativo aos países europeus e seguiam muito mais o aspecto de carta principiológica de recomendações a serem objeto de atenção interna pelos países.

Nessa mesma linha, também destituída de caráter forçoso e obrigatório apresentou-se a Diretiva 95/46/ CE de 24 de outubro de 1995, no cerne da União Europeia. Teve o atributo inegável de contribuição na concatenação de uma sistematização normativa e principiológica

[14] Na parte II de tal documento especifica os princípios que vão reger sua aplicação nos países limitando a atividade de coleta a balizas legais prévias, seguindo noções como do consentimento e alinhada *strictu sensu* com as finalidades que são a razão de ser de tal tratamento. O documento a que se refere pode ser encontrado em: https://www.oecd.org/sti/ieconomy/15590254.pdf.

cada vez mais concisa quanto a temática e, como aponta Laura Schertel Mendes (2014, p. 30), a “consolidação de um conceito de privacidade ligado à proteção de dados pessoais.”

Ao mesmo tempo em que tais documentos ilustrados representavam um certo avanço, ao mesmo tempo, persistem na revelação de uma fragilidade. A não vinculação aos países pertencentes à União Europeia ainda espelhava uma falta de uniformidade normativa quanto a disciplina da proteção de dados.

Essa fragilidade tem especial destaque quando vislumbramos que as normativas em proteção de dados, muito mais do que conceder um aparato protetivo ao usuário das redes de internet e dos meios tecnológicos em geral, intenta disciplinar as relações que surgem à partir das interações nessa sociedade informacional, a promover o mínimo de segurança e confiabilidade para que se desenvolvam.

Portanto, implantar políticas e normas concisas e uniformes quando se trata do uso de dados, inclusive regulando uma utilização além das fronteiras de países, como é notoriamente natural ao ambiente globalizado dos dias atuais, promove segurança, ao traçar os limites legais pertinentes, bem como “confiança entre todos os atores desse ecossistema para que não haja paralisia nessas trocas econômicas” (BIONI, 2021, p. 108).

Não que esse motor de uniformidade das normas quanto a matéria estivesse totalmente ausente da Diretiva 95/46/ CE, em vias a conceder um instrumento de proteção e viabilizar uma segurança no mercado globalizado- e em especial o europeu, que tem a característica de uma interação mais próxima ainda devido a inegável proximidade territorial entre os países. No entanto, perante a necessidade de implementação interna, no ordenamento dos países, como bem se observa em seu artigo 1°, esse fator de uniformidade, e a consequência segurança que promove, é um tanto quanto fragilizado (EUROPEAN UNION LAW, 1995).

Porém, por intermédio da disciplina posterior quanto a matéria no contexto europeu, esses ideários de uniformidade, segurança e confiabilidade nas relações que se desenvolvem à partir do tratamento de dados são melhores articulados e viabilizados, vez que o aparato normativo já passa a ter um caráter vinculativo.

Nesse sentido, o Regulamento Europeu n. 2016/679 que data de 27 de abril de 2016, vem a revogar e suprir eventuais lacunas deixadas pela diretiva anteriormente em voga. Prefixou sua devida aplicação pelos países membros da União Europeia, conforme bem se delineia no artigo 3° respectivo, assim como prevê a criação de um comitê dotado de

personalidade jurídica e com a finalística máxima de promover a "aplicação coerente"[15] e efetiva do regulamento (EUROPEAN UNION LAW, 2016).

Em relação específica ao Regulamento 2016/679 é notório um certo grau evolutivo, ou melhor dizendo, de avanço nas discussões e reflexivas pertinentes a proteção de dados. No primeiro considerando de seu texto prevê e realça- com a devida importância a que merece- a existência de um direito autônomo e fundamental à proteção de dados pessoais.

A Diretiva n. 95/26 já encaminhava-se para uma interpretação de reconhecimento da relevância de uma protetiva específica e autônoma, mas ainda era tímida e muito mais lida no sentido de reconhece-la como um feixe inferido e conexo ao próprio direito à privacidade, conforme se vê pela própria articulação do texto[16] de seu artigo 1°.

> Os Estados-membros assegurarão, em conformidade com a presente directiva, a proteção das liberdades e dos direitos fundamentais das pessoas singulares, nomeadamente do direito à vida privada, no que diz respeito ao tratamento de dados pessoais. (EUROPEAN UNION LAW, 1995)

A autonomia e fundamentalidade do direito à proteção de dados pessoais, contudo, não remete em grau de inovação ao Regulamento n. 2016/679. De outra sorte, perante o grau lógico e paulatinamente evolutivo-assecuratório entre os documentos quanto ao tema, remete-se esse caminhar desde a Convenção de n.108, também intitulada Convenção de Estrasburgo, de 1981, e a ser assentado o entendimento perante a Carta de Direitos Fundamentais da União Europeia de 2000 (SARLET; MARINONI; MITIDIERO 2020, p. 16), assim como por intermédio do Tratado de Funcionamento da União Europeia no seu artigo 16[17].

Por tudo enquanto exposto, é digno de nota que perante tal tracejar de discussões e entendimentos, reflita-se já no Regulamento n. 2016/679 uma dicção que assegure um direito de proteção de dados de forma específica. Dessa forma, passou-se a não mais atrelar com terminologias que não expressam vividamente a intenção de apontar sua autonomia em relação a outros direitos que com ele guardem certa proximidade, mas que com que ele não se confundem, como a privacidade (EUROPEAN UNION LAW, 2016).

---

[15] Termo previsto no considerando de n. 139 do Regulamento Europeu 2016/679 e que versa especificamente sobre a criação de tal comitê e sua finalidade. A íntegra do documento pode ser encontra em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32016R0679.

[16] A íntegra do texto da Diretiva n. 95/26 encontra-se disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A31995L0046.

[17] O artigo 16 vem prever que: "Todas as pessoas têm direito à proteção dos dados de caráter pessoal que lhe digam respeito." A íntegra do documento encontra-se em: https://eur-lex.europa.eu/resource.html?uri=cellar:9e8d52e1-2c70-11e6-b497-01aa75ed71a1.0019.01/DOC_3&format=PDF.

Hoje, no primeiro ato de escrita do documento do citado regulamento em vigência da União Europeia e que substitui a anterior diretiva 95/26 não se abrem espaços para tais questionamentos,

> A proteção das pessoas singulares relativamente ao tratamento de dados pessoais é um direito fundamental. O artigo 8°, n° 1, da Carta dos Direitos Fundamentais da União Europeia e o artigo 16°, n° 1, do Tratado sobre o Funcionamento da União Europeia (TFUE) estabelecem que todas as pessoas têm direito à proteção dos dados de caráter pessoal que lhes digam respeito. (EUROPIAN UNION LAW, 2016)

No tocante a autonomia e fundamentalidade de um direito à proteção de dados, é válido ressaltar que já era possível ser demarcada ante as notórias discussões à época, as produções científicas atinentes e mesmo perante extração de posicionamento jurisdicional.

Remete à 1983 um julgado do Tribunal Constitucional Alemão que já se debruçava sobre a reflexiva e reconhecia a validade de uma autonomia no cerne protetivo de dados. No entanto, válido ressaltar que a jurisprudência em questão aponta a um direito autônomo à autodeterminação informativa e não especificamente um direito à proteção de dados.

A terminologia diferenciadora entre os direitos é importante e deve ser ponderada, conforme irá ser apontado ainda no desenvolver deste presente capítulo, mas não afasta a importância que o julgado representa em conferir o devido realce ao tema e a abrir espaço na elucidação da necessidade de um sistema protetivo normativo específico.

O *leading case* de 1983 reflete uma jurisprudência pioneira que, à partir de uma veia interpretativa, veio a reconhecer um direito autônomo à autodeterminação informativa. Esse resultado decisório partiu do julgamento de confronto da Lei do Censo de 25 de março de 1982 com o artigo 2° da Lei Fundamental Alemã (MENDES, 2020, p.10).

O artigo 2° da Lei Fundamental Alemã veiculava quanto um direito ao livre desenvolvimento da personalidade e à partir de uma fronte interpretativa, realizada pelo Tribunal Constitucional, indicou-se a existência de um direito implícito e autônomo à autodeterminação informativa.

No contexto jurisprudencial alemão já eram notáveis movimentos anteriores (SARLET, 2021, p. 23) ao julgamento da Lei do Censo, ocorrido 15 de dezembro de 1983, em reconhecer a importância da diretiva da proteção de dados pessoais. Tal cenário é, inclusive, perfeitamente justificável, na justa medida em que há um pioneirismo europeu da Alemanha em regular o tema, reconhecendo assim o caráter significativo da matéria desde o ano de 1970 com a Lei de Proteção de Dados Pessoais de Hesse.

Mesmo que essa lei pioneira tenha nível de regulação mais restrita, pois atrelada apenas ao estado de Hesse, a legislação ao nível nacional não tarda tanto e remete à 1977, após ser uma tendência a ser seguida pelos outros estados do país. (DONEDA, 2020, p. 192)

Levando em consideração que já havia lei quanto a proteção de dados desde 1977 no território alemão, mesmo que ainda bem simplificado esse arcabouço protetivo, e que o caso referente ao confronto da Lei do Censo com a Lei Fundamental Alemã é de 1983, já é perceptível que não havia estranheza total ao direito alemão em reconhecer o desdobramento da problemática suscitada e da necessidade mínima de um certo grau de proteção.

No entanto, mesmo diante de tais perspectivas e considerações, não há como negar o caráter evidentemente paradigmático de tal decisão.

Conforme apresentado anteriormente, cumpre ressaltar que nesse caso em especial não há o reconhecimento de um direito autônomo fundamental à proteção de dados pessoais, mas sim em um direito fundamental à autodeterminação informativa, que implica "na prerrogativa de cada indivíduo decidir em princípio e substancialmente sobre a divulgação e utilização de seus dados pessoais." (SARLET, 2021, p, 23)

E por que seria tão importante destacar que se trata do reconhecimento de um direito fundamental à autodeterminação informativa?

Para o seguinte questionamento cabe duas colocações. Inicialmente que a textualidade do julgado de 1983 faz referência justamente a esse poder de decisionismo nas mãos do próprio indivíduo na administração das informações e dados que fazem referência a ele mesmo, portanto, faz clara referência a noção de uma autodeterminação informativa,

> Assim declara o Tribunal que o processamento automático dos dados ameaçaria o poder do indivíduo em decidir por si mesmo se e como ele desejaria tornar públicos dados pessoais no sentido de que o processamento de dados possibilitaria a elaboração de um "quadro completo da personalidade" por meio de "sistemas integrados sem que o interessado possa controlar o suficiente sua correção e aplicação". Assim, aumentaria a influência do Estado sobre o comportamento do indivíduo, que não mais seria capaz de tomar decisões livres em virtude "da pressão psíquica da 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", seria contrária ao direito à autodeterminação informativa, o que prejudicaria tanto a personalidade quanto o bem comum de uma sociedade democrática. (MENDES, 2018b, p. 187 *apud* BVerfGE 27, 1(6) Microcenso (Mikrozensus)

A decisão e a posição do Tribunal Alemão Constitucional surgem à partir do defronte quanto a edição de uma lei, conhecida como lei do censo- e em alemão como "Volkszählungsgesetz" -, que datava de 25 de março de 1982.

A constitucionalidade e legitimidade da lei foram questionados quando em 1983 passa a imprimir em caráter vinculativo/ obrigatório um recenseamento do povo alemão. Para este proceder revestiu-se das justificativas de um interesse público, no sentido de identificação das características populacionais em ampla esfera, seja econômica, educacional, demográfica, e a viabilizar a adoção, *a posteriori*, e coordenação de melhores políticas públicas a serem desenvolvidas pelo Estado (LIVRE..., 2005).

Nesse sentido, ao apreciar tal aparente conflito e perante a inúmeras suscitações de inconstitucionalidade da lei por indivíduos que se sentiriam, em *última ratio*, direta e efetivamente atingidos pela norma em veiculação, houve a decisão no sentido de decretação de inconstitucionalidade de alguns de seus dispositivos, mas não totalmente. A decretação de inconstitucionalidade parcial foi justamente sob a argumentação expressa na *decisum* quanto a uma "autodeterminação informacional[18].

É imperioso destacar que o Tribunal Alemão entendeu que a lei não era totalmente inconstitucional. Essa atividade de pesquisa com o levante de dados populacionais necessários poderia ser viabilizada de acordo com o ordenamento incidente, se tal proceder fosse adstrito a um caráter eminentemente científico e, ademais, implantados as devidas medidas assecuratórias de um mínimo de segurança do indivíduo.

Válido transcrever o dispositivo da *decisium*, com especial ênfase no tocante ao ponto 1 e 2, que revelaram o ponto de decretação de inconstitucionalidade e reivindicaram uma regulamentação em caráter adicional no tocante ao procedimento de recenseamento articulado pela lei do censo, a fim de uma melhor congruência constitucional e segurança quanto à promoção de um livre desenvolvimento da personalidade.

> 1. Os § 2 I a VII e §§3 a 5 da Lei do Recenseamento da População, Profissão, Moradia e Trabalho (Lei do Recenseamento de 1983), de 25 de março de 1982 (BGBl. I, p. 369), são compatíveis com a Grundgesetz, mas o legislador deve providenciar regulamentação complementar sobre a organização e procedimento do recenseamento.
> 2. O §9 I a III da Lei de Recenseamento de 1983 é incompatível com o Art. 2 I c. c. o Art. 1 I GG, e, assim, é nulo.
> 3. Os direitos fundamentais dos reclamantes, decorrentes dos Art. 2 I e Art. 1 I GG, foram violados pela Lei do Recenseamento de 1983 em seus números 1

[18] "O livre desenvolvimento da personalidade pressupõe, sob as modernas condições do processamento de dados, a proteção de indíviduo contra levantamento, armazenagem, uso e transmissão irrestrito 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." (LIVRE..., 2005). Tradução encontrada em: http://www.mpf.mp.br/atuacao-tematica/sci/jurisprudencias-e-pareceres/jurisprudencias/docs-jurisprudencias/50_anos_dejurisprudencia_do_tribunal_constitucional_federal_alemao.pdf.

> e 2. De resto, as Reclamações Constitucionais são improcedentes. (SCHWABE *apud* LIVRE..., 2005, grifo nosso)

Nessa decisão, apesar de não estar expresso no dispositivo, com apenas a indicação dos artigos da Lei Fundamental Alemã confrontados, nas razões decisórias faz a devida remissão a um direito de se autodeterminar e ainda a considera-lo enquanto não dotado de um caráter absoluto. Para tanto, deve ser sopesado em vias de uma proporcionalidade, e analisado de forma congruente com preceitos como a dignidade da pessoa humana e o amplo desenvolvimento da personalidade dos indivíduos.

Quanto à segunda consideração ao questionamento anteriormente levantado, há que falar que essa autodeterminação informativa não é sinônimo de um direito à proteção de dados. Portanto, é válido sim fazer a devida distinção e apontar que enquanto a este julgado, apesar de abordar a questão de dados e o dever de um mínimo protetivo, inclusive fazendo referência a Lei Federal Alemã de Proteção de Dados, é reconhecido como emblemático por sublinhar e ter como ponto central o reconhecimento de um direito autônomo à autodeterminação informativa.

Conforme já pontuado, a partir do apresentado por Ingo Sarlet (2021, p. 22), esses direitos não se confundem, apesar de ser inegável sua margem de aproximação, ao que denomina a evidência de uma "zona de contato" entre os mesmos.

A proteção de dados como direito imprime uma noção de abrangência maior, a que a autodeterminação informativa enquanto uma feição de autonomia do indivíduo convive e caminha perfeitamente de forma conjunta. O âmbito diferenciador entre tais direitos existe, no entanto, a que será objeto de enfoque maior ao longo do presente capítulo.

Voltando a abordar quanto ao movimento de reconhecimento de um direito à proteção de dados, foi um processo notório e tendencial, tendo o continente europeu adotado um papel de alto-relevo e de inspiração para os demais países e regiões do globo.

Quanto às leis que disciplinam a matéria de proteção de dados, Danilo Doneda (2011, p. 97) as organiza e divide em 4 (quatro) estágios geracionais, em uma linha evolutiva dos dispositivos legais que foram surgindo ao longo dos anos nos países.

O primeiro estágio tem como característica o fato de uma certa primariedade nos dispositivos normativos, dotados de vernáculos técnicos e focados em si na atividade de processamento de dados. Trazia um limiar de proteção principalmente ao uso de dados pessoais por órgãos públicos, sem ainda sistematizar princípios mais específicos e com a centralidade ainda firmada na conferência de autorização a viabilizar a estruturação dos bancos de dados (DONEDA, 2011, p. 97).

A segunda geração tem como marcos exponenciais a Lei do Estado de Hesse da Alemanha do ano de 1977, já supracitada, assim como a Lei Francesa de 1978 – a denominada "*Informatique et Libertées"*[19]. Essa alteração geracional deu-se justamente pelo acrescer, no panorama encontrado, do número de dados agora tratados, com a existência de múltiplos centros de tratamento.

Assim, neste segundo momento, esse processo normativo anterior de autorização para o tratamento de dados não era mais possível. Inviável perante o alargamento dos bancos de dados, não só públicos, como também privados.

Esse recorte histórico das leis da segunda geração tinha como denominadores comuns o fato de que não mais detinha a centralidade voltada a atividade dos bancos de dados e a técnica informacional envolvida, mas estava atrelada ao indivíduo e o seu direito mínimo de privacidade, a conferir uma ferramenta para proteger seu direito, em caso de abusos[20].

Em contínuo a esse processo evolutivo, desponta a terceira geração de normativas quanto à proteção de dados. Como é natural de um influxo evolutivo se surge uma nova geração é por que, claramente, a anterior apresenta algumas problemáticas e há a tentativa de sua superação.

Nesse sentido, os problemas configurados remetem muito mais aos "colores" sociais que a utilização e o manejo de dados pessoais vêm paulatinamente assumindo. Em outras palavras, a considerar seriamente as devidas proporções que tal fenômeno imprime na sociedade e as feições de alteração que vem proporcionando.

A atividade de coleta e de tratamento de dados no decorrer do tempo passa a ser bem mais do que algo pontual identificado na sociedade, vem assumindo-se como algo cada vez mais arraigado e tão natural, como o próprio comer, dormir, respirar. Tal metáfora pode até ser entendida por alguns como uma hipérbole desmedida, mas está de acordo com um ser humano que ao acordar muito antes do desjejum já utiliza seus smartphones e, mesmo sem ter clara noção, está inserido nesse ciclo de tecnologias e de contínua "mineração de dados pessoais".

Por corresponder a um fenômeno tão fortemente presente na sociedade e a revestir as interações sociais de um novo caráter, a não adesão a estas tecnologias acaba por produzir uma espécie de exclusão. Exclusão ao próprio convívio social, vez que hodiernamente ele se desenvolve muito mais em uma via digital do que real.

---

[19] Com a tradução livre, tem como significado: "Informática e Liberdade".

[20] "[...] Assim, criou-se um sistema que fornecia instrumentos para o cidadão identificar o uso indevido de suas informações pessoais e propor a sua tutela." (DONEDA, 2011, p. 98)

A alusão a imagens tão comuns nos dias atuais, de uma mesa em um ambiente que conta com cada um dos indivíduos dialogando com seus *smarthphones* e não com as pessoas ao seu derredor confirma a criação de um meio ambiente digital, onde as relações sociais virtuais parecem cada vez mais sacrificar ou suprimir as relações reais.

Indicar uma exclusão, remete a que os indivíduos que optam por estarem desatrelados desse meio ambiente virtual, perdem grande interação com outros humanos. E essa perda acaba por ser tão grandiosa e a gerar uma espécie de exclusão, vez que a relações sociais e interações reais são bem menos intensas, hoje, e menores em comparação as desenvolvidas por intermédio das tecnologias e as redes sociais instrumentalizadas.

Esse processo de informatização além de trazer puramente uma transformação nas interações interpessoais humanas, também altera o próprio meio de produção capitalista no século XXI (SARLET; CALDEIRA, 2019, p. 6-7). O capitalismo, tendo sempre como matéria-prima uma busca incessante pelo lucro, passa a ver nos dados um vetor de monetarização de grande serviço nos novos desenhos empresariais do globo e, assim, abre espaço e alargamento na atividade de mineração de dados, sob a sustentação do denominado capitalismo da vigilância.

> O capitalismo de vigilância recrutava as maravilhas do mundo digital para atender às nossas necessidades referentes a levar uma vida efetiva, prometendo a mágica de informação ilimitada e milhares de maneiras de antecipar nossas necessidades e facilitar as complexidades das nossas perturbadas vidas. [...], devido ao capitalismo de vigilância é que os recursos para a vida efetiva que buscamos no mundo digital vêm sobrecarregados por um novo tipo de ameaça. Sob esse novo regime, o momento preciso em que nossas necessidades são atendidas também é o momento preciso em que a nossa vida é saqueada em busca de dados comportamentais, e tudo isso para o lucro alheio. O resultado é um perverso amálgama de empoderamento inextricavelmente sobreposto ao enfraquecimento. (ZUBOFF, 2019, p. 73, grifo nosso)

As leis que refletem uma terceira geração remetem à década de 80, e além de continuarem centradas na conferência de uma garantia ao cidadão, frente a possíveis abusos de direitos, indicam um novo espectro nessa frente de proteção ao indivíduo.

Assim, segundo Danilo Doneda (2011, p. 2011), para além de proteger esses dados, surge-se também o direito de autodeterminação informativa, como a incrementar o regime de proteção e conferir efetividade mais ampla a própria proteção de dados- inicialmente reconhecida nas gerações anteriores.

> A autodeterminação informativa surgiu basicamente como uma extensão das liberdades presentes nas leis de segunda geração, e são várias as mudanças específicas nesse sentido que podem ser identificadas na estrutura dessas novas leis. O tratamento dos dados pessoais era visto como um processo, que não se encerrava na simples permissão ou não da pessoa à utilização de seus dados pessoais, porém procurava incluí-la em fases sucessivas do processo de tratamento e utilização de sua própria informação por terceiros, além de compreender algumas garantias, como o dever de informação. (DONEDA, 2011, p. 97-98)

A quarta fase geracional apresenta a perspectiva de que apenas o reconhecimento de uma autodeterminação informativa não seria suficiente ao nível protetivo, vez que ainda vislumbravam-se alguns pormenores conturbados. Indicou que a centralidade da proteção de dados não pode ser apenas visto de forma individual, mas a nível coletivo, que tem como consequência o reconhecimento da vulnerabilidade e da assimetria da relação entre controladores e usuários, bem como a garantia de mecanismos aptos a filtrarem o tratamento de dados como um todo.

As leis que se afiliam a essa fase reconhecem balizas rígidas a possibilitar um sistema amplo de proteção de dados, a englobar qualquer tipo de interface com dados pessoais (DONEDA, 2011, p. 98). Essa rigidez deve ser ainda mais elevada no caso de dados dotados de características sensíveis, outrossim também abre-se espaço para normas específicas a determinadas formas de tratamento de dados que por serem reiteradas e dotadas de algumas singularidades, assim requerem e viabilizam.

Segundo tal divisão feita pelo supracitado autor, é possível fazer uma conexão e interpretação e identificar que a lei hodierna brasileira, assim como o já abordado Regulamento Europeu de n° 679 de 2016 estariam posicionados já nesta quarta geração. Tais normativas já concebem essa diferença de regramento quanto a dados sensíveis e um certo enfoque não apenas em liberdade negativa do cidadão frente a possíveis intervenções de particulares ou do Estado, mas em um microssistema protetivo voltado a regulação e proteção de toda uma coletividade, com a afixação de princípios que firmam verdadeiros compromissos a pautarem todo o tipo de tratamento de dados com um pressuposto de transparência e segurança.

Como as considerações acima revelam, há o surgimento de um direito à autodeterminação informativa que é atribuído ao momento da terceira geração de leis quanto à matéria. Sua atribuição, enquanto direito autônomo em relação ao direito à proteção de dados tem um sentido, no entanto.

O direito à autodeterminação informativa cuida de uma esfera específica, que é quanto ao próprio indivíduo ter em suas mãos o poder de decidir quanto a circulação e manipulação de

dados referentes a ele mesmo. Parte-se do princípio de que toda a atividade de disponibilização de tratamento e gerência quanto aquele dado há que ser feita de acordo com a anuência prévia do titular do dado.

Assim, esse direito à autodeterminação informativa, apesar de ter uma zona de contato com o direito à proteção de dados (SARLET, 2021, p. 22), com ele não se confunde.

Quanto à relação da autodeterminação informativa com a proteção de dados, como já elucidado alhures, o termo a ser utilizado não é confusão e sim complementação. Portanto, surge um direito de forma autônoma para enriquecer esse microssistema protetivo.

Observou-se à partir das inúmeras mudanças sociais e da difusão do uso e codependência da tecnologia na vida das pessoas que para que de fato houvesse um núcleo de proteção de dados era indispensável que se dispensasse a esse titular dos dados "o controle sobre o seu armazenamento e transmissão" (CACHAPUZ; JOBIM, 2021, p. 68).

Esse direito à autodeterminação, conforme também já apontado, tem seu surgimento historicamente demarcado de forma autônoma e destacado ao nível de direito fundamental através da jurisprudência do Tribunal Constitucional Alemã.

Válido é, no entanto, destacar os pontos paradigmáticos que levaram ao Tribunal em questão decretar a inconstitucionalidade da Lei do Censo de 25 de março de 1982 não com base apenas no direito à privacidade ou personalidade- já unânimes em reconhecimento no direito daquele país-, ou mesmo na dicção simples do direito à proteção de dados- já também reconhecido internamente, com a presença de lei federal, desde 1977, assim como leis de cunho estadual, como é o caso de Hesse, desde 1970.

Os pontos nevrálgicos considerados, a propiciar uma *decisium* nesse sentido, conforme bem sintetiza Laura Schertel (2018, p. 188), foi que naquele caso em prospecto, "o risco do processamento de dados residiria mais na finalidade do processamento e nas possibilidades de processamento do que no tipo dos dados mesmos (ou no fato de quão sensíveis, ou íntimos são)".

Sem dúvidas é possível fazer uma analogia com o processo de redefinição e elasticidade conferida ao direito à privacidade, bem elucidada no artigo "The Right of privacy" (WARREN; BRANDEIS, 1980). Assim, passa-se a compreender uma nova acepção quanto à privacidade e preservação do livre desenvolvimento da personalidade de um sujeito, que seria a de controlar as informações disponibilizadas à respeito da sua própria pessoa.

Essa nova acepção de privacidade foi demarcada e conferido tal enfoque perante as mudanças sociais que vieram insurgir a devida resposta do direito. Nota-se que a mesma pode

ser desmembrada e aludida do próprio conceito inicial de privacidade, ao qual permite tal viés interpretativo, como mui bem ilustra Stefano Rodotà (2008).

Pelas peculiaridades das transformações sociais e ao despontar o fenômeno da informatização e a articulação de uma verdadeira sociedade da vigilância, erige-se a articulação de um sistema protetivo dotado das devidas especificidades e mecanismos eficientes de proteção, ao que gera ambiência fértil para articular-se tanto um direito à proteção de dados, como também um direito à autodeterminação informativa.

Ímpar apontar que mesmo que se considere que um direito deu espaço, ou melhor dizendo, abertura para que outro direito, de forma autônoma, surgisse e fosse consagrado, é certo firmar que com ele não se confunde e não reduz o outro a um mero braço seu ou extensão sua. Em verdade, seu desenvolvimento e surgimento reivindicam especificidades, bem como são respostas no direito aos novos fenômenos sociais de forma muito mais adequada e completa[21].

Voltando ao desenvolvimento de um conceito e de um direito de autodeterminação informativa, à luz do julgado alemão de 1983, aponta-se que seu surgimento tem um caráter revolucionário à época e a influenciar definitivamente as normativas que iriam surgir à partir de então, não só na realidade europeia, mas em todo o mundo, como o próprio caso brasileiro indica.

Esse julgado teve um caráter de mudança de paradigmas, pois de forma distinta de outros anteriores[22], tem sua fundamentação pautada não apenas na defesa da privacidade, mas sob a defesa da autodeterminação informativa. Esse proceder, com a indicação de um novo direito, deu-se por que a mera proteção de uma esfera privada não era mais entendida como suficiente quando confrontada com a análise de constitucionalidade da Lei do Censo de 1982,

> Duas foram as principais críticas da doutrina alemã à fórmula da esfera privada que acabaram por motivar a evolução desse conceito. A primeira crítica refere-se à relatividade da esfera privada, isto é, ao fato de que os desejos de privacidade podem diferir muito fortemente de pessoa para pessoa. Assim, espaços não poderiam ser designados rigidamente de esfera privada ou

[21] "De certo modo já adiantado no segmento anterior, o conteúdo (no sentido do âmbito de proteção normativo) de um direito fundamental à proteção de dados pessoais, embora fortemente articulado com o princípio da dignidade da pessoa humana e de outros direitos fundamentais, em especial o direito ao livre desenvolvimento da personalidade e alguns direitos especiais de personalidade, como é o caso, entre outros, do direito à privacidade e do assim chamado direito à autodeterminação informativa, não se confunde com o do objeto de proteção de tais direitos." (SARLET, 2021, p. 22)

[22] Outros julgados anteriores na Alemanha tocavam a matéria de dados e da necessidade de um viés protetivo, mas não sob a defesa e a consagração de um novo direito denominado de autodeterminação informativa. Nesse sentido, cita-se o julgado da decisão do mirocenso e do divórcio, na forma ponderada por Laura Schertel Mendes (2018b, p. 189).

> íntima, "pois os espaços vitais, nos quais o indivíduo se refugia para descansar das exigências sociais, preparar um comportamento social e fazer tudo o que não pode ser trazido para a sociedade e representado diante dela são relativos". A segunda crítica, estreitamente relacionada ao princípio da relatividade da esfera privada, refere-se ao contexto de aplicação. Ela se refere à ideia básica de que "a sensibilidade e o significado das informações dependem do respectivo contexto de aplicação" e não podem ser definidos *a priori* somente pelo conteúdo da informação, isto é, se é íntimo, privado ou público. Assim, a finalidade do levantamento e o destinatário da informação são muito mais decisivos para a avaliação da constitucionalidade do processamento de dados do que a classificação de dados em esfera privada e íntima. (MENDES, 2018b, p. 189)

As considerações expressas na citação acima apontam duas chaves centrais, onde a segunda deriva efetivamente da compreensão e validação da primeira.

Para tanto, a primeira implica o reconhecimento de uma relatividade do que constitui-se como esfera privada de um indivíduo. O que pode ser considerado como algo privado e íntimo pode sofrer divergência no âmbito de consideração de cada pessoa.

Partindo desse primeiro pressuposto, reconhece-se então que a definição do que é uma informação a que cabe ser efetivamente entendida como sensível, e com intenso potencial lesivo a esfera íntima dos usuários, depende do contexto de sua aplicação e, mais precisamente, da finalidade em sua utilização.

Em outras palavras, o julgado imprime que a defesa da privacidade ou apenas proteger o conteúdo *priori* dos dados e informações não são mais suficientes frente aos desdobramentos do fenômeno. Considera-se que um dado inicialmente definido como não sensível ou não referente a esfera íntima pode, durante a operação de tratamento de dados e interação com outros semelhantes, assumir um novo papel e uma nova classificação.

Nesse sentido, para além da proteção do conteúdo inicial de um dado, alerta-se para a proteção em torno de toda a operação quanto a dados. Está concludente é justamente o que abre margem ao reconhecimento de um direito de autodeterminação informativa e a compreensão mais ampla do direito à proteção de dados, vislumbrada na terceira geração das leis quanto à temática e também no julgado paradigmático em alusão.

A sofisticação cada vez mais primorosa no contexto de operação de dados viabiliza o armazenamento e reiteração entre inúmeros outros dados semelhantes, a fim de alcançar informações novas e traçar perfis comportamentais das pessoas. De tal sorte, é inegável o viés problemático em pauta que vem a exigir do direito uma resposta compatível.

A resposta compatível não poderia ter vazão adequada apenas na diretiva da privacidade e de uma proteção de dados centrada na definição apriorística do que é considerado como íntimo

e privado[23]. Essa é a veia interpretativa que o Tribunal Constitucional Alemão segue para traçar a existência de um novo direito a melhor corresponder a tais anseios sociais e contornos conflituosos do fenômeno em relevo.

Esse reconhecimento, à luz de uma interpretação dos integrantes do Tribunal Constitucional Alemão, apresenta-se claramente um agir criativo no exercício dessa atividade jurisdicional, pois há o reconhecimento de um "novo" direito, sem perpassar por um processo tipicamente legislativo para tanto.

Essa atividade de exegese é viabilizada por dispositivos já resguardados na Lei Fundamental Alemã, como é o caso do artigo 2°, que tutela o livre desenvolvimento da personalidade. Ademais, também por uma interpretação deste artigo de forma conjunta com o também artigo 1° da lei em questão que, por sua vez, resguarda a dignidade da pessoa humana (CUNHA, 2022, p. 85).

Perante a conjugação de tais dispositivos e o vislumbre de novos riscos à sociedade, com o ressurgir de dados dimensionados monetariamente pelas empresas e a necessidade de resguardar um reequilíbrio da relação entre o usuário da rede de internet e os controladores de dados, é tão importante criar-se e ter-se um efetivo sistema protetivo de dados.

2.3 O BRASIL, O SISTEMA PROTETIVO AOS DADOS PESSOAIS EM DESENVOLVIMENTO

Inicialmente é válido abordar o porquê da nomenclatura referente a este subtópico. Trata-se da análise do sistema de normas existentes hodiernamente no Brasil, a consagrarem os esforços em conferir uma proteção de dados aos usuários das tecnologias ou dos demais indivíduos sujeitos as suas interferências.

A abordagem não é restrita as normas vigentes quando da elaboração do presente trabalho, mas as anteriores que abriram espaço e/ou que eram aplicáveis na falta de norma mais

[23] Sobre as mudanças sociais, as tecnologias e o desenvolver de novos direitos, como é o caso da proteção de dados e da autodeterminação informativa: "Atualmente, o fenômeno das modernas formas de gigantesca coleta de dados pessoais alterou a visão tradicional da privacidade em vários aspectos. Em primeiro lugar, as questões relacionadas à privacidade, que classicamente envolviam um indivíduo isolado (o clássico *right to be let alone*), envolvem simultaneamente milhões de pessoas, considerando a coleta de dados pessoais de [...] de todos nós. Em segundo lugar, vários dispositivos são capazes de transmitir informações a nosso respeito- celulares, GPS, cartões de crédito, redes sociais, etc- de forma a se poder reconstituir quem nós somos, por onde circulamos, o que consumimos e o que pensamos. Em terceiro lugar, todas essas informações podem ser utilizadas não só para compreender quem nós somos e o que fazemos, mas principalmente para influenciar nossas condutas [...]. o fenômeno deixou de ser territorial para ser global, já que o tratamento de dados passou a envolver elementos transnacionais e globais, envolvendo pessoas localizadas em várias partes do mundo, sujeitas a jurisdições diversas." (COLOMBO; FACCHINI NETO, 2017, p. 66, *grifos nossos*)

específica. Ademais, o termo “em desenvolvimento”, refere-se não ao fato de que a norma está em elaboração, mas que os contornos interpretativos da mesma na prática, bem como as experiências vindouras e que culminam na sua exegese, ainda estão em desenvolvimento.

Por oportuno, este tópico será dividido em dois subtópicos distintos em vias de elucidação do sistema normativo referente a dados no Brasil. O primeiro subtópico dedica-se a apresentar o momento anterior a entrada em voga da Lei Geral de Proteção de Dados (Lei 13.709/2018), com as leis esparsas e setoriais que tocam quanto à matéria de dados no Brasil.

O subsequente dedica-se a apresentar justamente esse contexto de implementação da LGPD, assim como da asseguração do direito à proteção de dados no âmbito constitucional brasileiro. Por fim, em antecipação ao capítulo seguinte, alcunha-se desenhar os contornos iniciais que a lei disciplina quanto ao tratamento de dados sensíveis e notoriamente os dados que versam sobre a saúde.

2.3.1 Antes da concepção: Como sinalizava-se a questão de dados no Brasil antes da criação da Lei 13.709/2018?

O Brasil, direcionado por sua Constituição Federal do ano de 1988 possui uma carta de direitos fundamentais, os quais possuem a garantia de aplicabilidade imediata (art. 5°, §1°, da CF/88), e que em algum nível já traziam diretrizes relevantes quanto à proteção do indivíduo e de seus dados pessoais.

Assim, já havia a garantia de um direito à personalidade e seu amplo desenvolvimento no artigo 5°, inciso X, da CF/88, tendo já o vislumbre das esferas de proteção da intimidade e vida privada do cidadão. Tais direitos devem ser interpretados de forma coadunada com o princípio da dignidade da pessoa humana, que na Constituição Federal está estruturado como um dos fundamentos do Estado Democrático de Direito Brasileiro.

No âmbito constitucional já existia uma especial guarita normativa de tutela aos direitos à personalidade e à privacidade. Ou seja, apesar de ainda em um primeiro momento não haver explicitamente um direito autônomo à proteção de dados pessoais, o mínimo de sua defesa podia ser feito com base na interpretação sistêmica desses outros dispositivos constitucionais,

> [...] o fundamento constitucional direito mais próximo de um direito fundamental à proteção de dados seja mesmo o direito ao livre desenvolvimento da personalidade, radicado diretamente no princípio da dignidade da pessoa humana e no direito geral de liberdade, o qual também assume a condição de cláusula geral de proteção de todas as dimensões da personalidade humana, que, de acordo com tradição jurídica já consolidada no

> direito constitucional estrangeiro e no direito internacional (universal e regional) dos direitos humanos, inclui o (mas não se limita ao!) direito à livre disposição sobre os dados pessoais, o assim designado direito à livre autodeterminação informativa. (SARLET, 2021, p. 18)

No entanto, conforme já bem tratado ao longo deste trabalho, o fenômeno social e informacional de mineração de dados veio a exigir uma proteção específica, a que além de conferir a especial relevância ao tema também pudesse disciplinar todos os desdobramentos e riscos assumidos (MENDES, 2018b, p. 195), bem como um esforço de reequilíbrio entre a distância de forças que a relação de usuários e controladores representa.

Anteriormente a este processo de reconhecimento e afirmação, não só implícita, como também expressa, de um direito à proteção de dados no Brasil, bem como com a regulamentação específica, por intermédio da Lei Geral de Proteção de Dados (LGPD), existiam certos dispositivos entendidos como aplicáveis, por extensão, as situações que envolviam o tratamento de dados pessoais.

Os direitos constitucionais já consagrados da privacidade e personalidade, como também a garantia da inviolabilidade de correspondência, dados e comunicações telefônicas, eram aplicáveis em uma vertente extensiva ou por analogia a questão dos dados[24].

Ademais, a garantia do *Habeas Data*, ao disciplinar o acesso a informações referentes à pessoa do impetrante, traz a relevo constitucional a noção de tutela de informações pessoais e não apenas aquelas de foro íntimo (MENDES, 2014, p. 168-169)

Ao nível legal, bem se sabe que a LGPD apenas surge no ano de 2018, porém antes de sua égide também eram aplicadas outras normativas já existentes no ordenamento pátrio.

A Lei de Acesso à Informação (BRASIL, 2011b) do ano de 2011, que em seu artigo 6° já vinha a guarnecer uma proteção da informação sigilosa e também da informação pessoal, assim como outra série de dispositivos que revelam preocupações com o manejo de informações.

Outrossim, o Código de Defesa do Consumidor também compete um certo destaque pelo fato, de que não obstante ser de 1990, ilustra um movimento de inovação no cenário brasileiro com os dispositivos que o integram. Entre estes o artigo 43, por exemplo, que com destaque a seu caput e §§1°[25] ao 3° trazem já um aspecto protetivo ao consumidor, aos dados

[24] "Dessa forma, embora os dados pessoais em si não se enquadrem no inciso XII do art. 5° da Constituição, eles se inserem no âmbito de proteção do direito à inviolabilidade da intimidade e da vida privada, garantido pelo inciso X do art. 5° da Constituição, interpretado de forma sistemática com o princípio da dignidade humana e à luz da garantia do habeas data." (MENDES, 2014, p. 169)

[25] Art. 43. O consumidor, sem prejuízo do disposto no art. 86, terá acesso às informações existentes em cadastros, fichas, registros e dados pessoais e de consumo arquivados sobre ele, bem como sobre as suas respectivas fontes.

relativos a eles e a formação de bancos de dados, com o dever de transparência, linguagem de fácil compreensão e de não viabilizar um armazenamento *ad eternum*, mas que não ultrapasse um período de 5 anos.

Existiam também outras legislações referentes a questões mais setoriais e a outras matérias que não propriamente a proteção de dados, mas que também continham certas noções proveitosas ao tema e as problemáticas que despontavam, como é o caso da Lei de Cadastro Positivo (BRASIL, 2011a), a Lei quanto a identificação criminal do civilmente identificado (BRASIL, 2009) e também o denominado Código Brasileiro de Telecomunicações (BRASIL, 1962). (GNOATTON, 2021, p. 111)

Esses diplomas apresentados detinham uma certa limitação a ser aplicado nas situações controvérsias à proteção de tratamento de dados, justamente por que não era o seu foco preponderante e não havia ainda a estruturação e sistematização de princípios e normas pertinentes. No entanto, na falta de uma lei específica quanto a temática, havia a aplicação extensiva de outras leis que tocavam e guardavam certa conexão com a sistemática de proteção de dados pessoais e as operações de seu tratamento.

No caso do Código de Defesa do Consumidor (CDC) em uma interpretação extensiva já havia a sinalização ao princípio da finalidade, especialmente na coleta de dados sensíveis e não só quanto a banco de dados de consumidores, mas em âmbito geral (DONEDA, 2020, p. 271).

O caráter impactante das normas constantes no CDC possibilita em se falar em uma outra análise do conceito de privacidade e de proteção à personalidade do consumidor no âmbito brasileiro já no ano de 1990, que é quando a referida lei foi publicada. É inegável um patamar evolutivo a que remete essa legislação, a fazer um viés protetivo ao consumidor até mesmo referente às suas informações pessoais e que acaba gerando um impacto dentro do olhar do direito à privacidade e personalidade no direito brasileiro como um todo.

> Um dos precursores e catalizadores no processo de evolução do conceito de privacidade foi certamente o Código de Defesa do Consumidor, que estabeleceu uma proteção integral da pessoa nas relações de consumo, seja dos seus interesses econômicos, seja da sua integridade e personalidade. Ademais, o caráter principiológico das suas normas tem se mostrado aberto o suficiente para oferecer soluções para os novos conflitos relacionados à tecnologia da informação, servindo de base para a jurisprudência referente à violação dos dados pessoais, [...].

§ 1° Os cadastros e dados de consumidores devem ser objetivos, claros, verdadeiros e em linguagem de fácil compreensão, não podendo conter informações negativas referentes a período superior a cinco anos. (BRASIL, 1990a)

> Vê-se, assim, que a capacidade do Código de Defesa do Consumidor de se adaptar a novas demandas e de oferecer novas respostas foi fundamental para o desenvolvimento contínuo de mecanismos de proteção da personalidade do consumidor, inclusive contra os riscos advindos do processamento de dados pessoais. (MENDES, 2014, p. 200)

A importância e o contexto vanguardista da legislação de 11 de setembro de 1990 é reafirmado na medida em que traz uma proteção da personalidade do consumidor de forma ampla, inclusive sobre o aspecto protetivo de tratamento de seus dados pessoais. Esse vetor passa a servir de parâmetro interpretativo extensivo para aquelas situações que não veiculam propriamente uma relação consumerista, mas que referem-se à dados pessoais no cerne brasileiro.

Outra legislação também desponta nesse contexto e é relevante por convergir com certas questões referentes a dados. O denominado Marco Civil da Internet, refere-se a Lei de n. 12.965 de 23 de abril de 2014 e tinha como objeto central a fixação dos parâmetros e das normas mínimas a regerem o uso da internet no Brasil, como bem colaciona a dicção de seu artigo 1° (BRASIL, 2014).

Já detinha em seu corpo normativo, especificamente no artigo 3°, inciso II e III, os princípios da privacidade e à proteção de dados pessoais, sob a intitulação de princípios incidentes quanto o uso da internet. O princípio à proteção de dados, no entanto, remetia que deveria ser equalizado e efetivado, “na forma da lei”.

No âmbito de sua seção III veiculava quanto a proteção do registro e dados pessoais, no entanto, ainda de forma bem distante da necessidade pátria. Sob uma normativa bem aberta e a que cabia várias brechas, viabilizava e legitimava agressões perpetradas aos usuários e o amplo desenvolvimento de sua personalidade e privacidade.

É inequívoco a contribuição de tal legislação, a que também já ponderava o consentimento como requisito viabilizador de tratamento e disponibilização de dados à terceiros (BRASIL, 2014, Artigo 7°, VII e IX). Denota-se, no entanto, que perante certas lacunas e brechas, assim como o fato de restringir apenas as situações de uso ativo de rede de internet (GNOATTON, 2021, p. 111), acabava por exigir-se cada vez mais a existência de uma normativa específica quanto à questão de tratamento de dados pessoais no Brasil.

Ímpar salientar que o Marco Civil da Internet não tinha como centralidade tratar de dados pessoais, mas sim disciplinar o uso da internet, com a fixação dos direitos e deveres pertinentes, assim em muito faltava a ponderar quanto às múltiplas especificidades da questão de tratamento de dados devido a própria finalidade assumida pela lei.

Conforme já bem tratado, as outras legislações outrora existentes, não incidiam centralmente à proteção de dados pessoais e tocavam na matéria apenas em caráter paralelo, como é o caso do Código de Defesa do Consumidor e o próprio Marco Civil da Internet.

Essa sociedade da informação e o capitalismo da vigilância não tinham uma tendência de serem freados, mas ao contrário, de serem ainda mais implementados. Com o consequente surgimento de novas questões ao direito e ao judiciário a serem resolucionadas utilizavam-se as inúmeras legislações esparsas que tocavam de certa forma na questão de dados, a realizar uma atividade interpretativa sistêmica e por vezes extensiva, para deliberar as soluções.

Essa atividade interpretativa cada vez mais foi carecendo, perante a densificação e surgimento de novas categorias digitais e de métodos de manipulação de dados, como é o caso do Big Data ou do *ubiquituous computing*[26] – na tradução livre, computação ubíqua-. Fez-se necessário uma sistematização de princípios e normativas específicas, a fim de que o direito de fato não se tornasse omisso perante os fenômenos sociais despontantes.

Imperiosa a edição de uma legislação específica a que viesse tratar e reger especificamente o fenômeno de manejo com dados pessoais e especificamente os sensíveis, que demandam um nível protetivo ainda maior.

2.3.2 O surgimento de uma Lei Geral de Proteção de Dados, o Art. 5°, LXXIX, da CRFB/88 e os dados sensíveis quanto a saúde

A legislação que atualmente regula a matéria de dados no Brasil (Lei n. 13.709/2018) teve aprovação em 14 de agosto de 2018, sendo conferida a devida vigência apenas em 2020. Tentou-se postergar o momento de entrada em vigor, por intermédio da Medida Provisória de n° 959/2020, mas teve sua vigência devidamente garantida em 18 de setembro de 2020, com suas sanções sendo aplicáveis apenas à partir de agosto de 2021 (LEME; BLANK, 2021, p. 212).

A lei em questão entrou em vigor no Brasil em um momento bem problemático, marcado pela pandemia do Covid-19. No entanto, não é relativizado sua importância, inclusive

[26] Sobre a definição dessa sofisticação das tecnologias de computação: "A computação ubíqua ou pervasiva é caracterizada pela disponibilidade onipresente e móvel dos serviços de aplicativos reais, independente da plataforma alvo real. (...). é vista menos como um campo de tecnologia independente, mas como uma nova aplicação de tecnologia de informação e comunicação, que é integrada muito mais fortemente no mundo cotidiano do que nunca. O objetivo é realizar a reinvindicação tudo, sempre, em todos os lugares em relação ao processamento e transmissão de dados pelas onipresença dos sistemas de TIC." (SALES; MOLINARO, 2017, p. 331)

neste momento, a que as tecnologias muito foram utilizadas como forma de proporcionar o exercício de atividades básicas mesmo na constância de medidas como o distanciamento.

Assim, o trabalho, as compras, os contatos com outros seres humanos, muito mais do que antes, passaram a ser intermediados por tecnologias. Em uma era a que a mineração de dados e sua produção já remetia a níveis elevados, passa-se a níveis estratosféricos.

Outrossim, salutar a existência de uma legislação específica a que conste a sistematização de normas e princípios mínimos quanto às operações que tratem dados pessoais.

A legislação pátria tem forte inspiração no regulamento europeu[27] (LEME; BLANK, 2021, p. 211) e intenta conferir uma tutela específica à proteção de dados e a qualquer tipo de tratamento efetuado, seja aquele realizado por pessoa física ou jurídica, pública ou privada. Em seus dispositivos normativos fica evidente a amplitude de sua proteção, a considerar enquanto tratamento de dados, "toda atividade realizada com dados pessoais" (BRASIL, 2018, Artigo 5°, X)

A importância da criação de um sistema conciso e não segmentado, mas sistêmico e generalista é elementar, a que proporciona uma operação quanto aos dados segura em todo o tempo de vida das operações de caracterizadas como tratamento (SARLET; RUARO, 2021, p. 86).

A própria criação de um sistema protetivo específico quanto à dados, como já apresentado ao longo deste capítulo, é resultado da fomentação de um problema e de um esforço em reequilibrar as tensões de poder entre a relação do usuário das tecnologias e do controlador (BIONI, 2021).

Por oportuno é ilustrar o que a lei precipuamente entende enquanto controlador, operador, bem como titular de dado- este que versa a essência de uma proteção ferrenha. Neste sentido, o Artigo 5° da Lei indica como

> V - titular: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento;
> [...]
> VI - controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;
> VII - operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador; (BRASIL, 2018)

[27] "O Regulamento Europeu de Proteção de Dados consolida o posicionamento de vanguarda no Continente no sentido de conferir especial proteção à esfera pessoal de seus membros. Quer dizer, desde as primeiras normatizações, sabidamente do movimento contra a Lei do Estado de Hesse, na Alemanha, até o atual Regulamento n° 2016/679, a União Europeia vem ditando os padrões a serem seguidos nessa matéria." (RUARO; SILVA, 2021, p. 913)

O controlador e o operador são ambos definidos como agentes de tratamento de dados, conforme previsão do artigo sublinhado.

Para o efeito de tal legislação há a proteção dos chamados dados pessoais. Conforme a própria terminologia de “titular” acima explicitada indica, os dados pessoais são aqueles que traduzem uma carga de informação referentes a pessoais naturais identificadas ou passíveis de identificação, e todos estes tipos de dados detém uma valoração legal, no sentido de serem dignos de proteção.

> Na Lei Geral de Proteção de Dados, parte-se da ideia de que todo dado pessoal tem importância e valor. [...] Dados que pareçam não relevantes em um momento ou que não façam referência a alguém diretamente, uma vez transferidos, cruzados ou organizados, podem resultar em dados bastantes específicos sobre determinada pessoa, trazendo informações inclusive de caráter sensível sobre ela.” (VIOLA; TEFFÊ, 2020, p. 131)

Dentre esses encargos protetivos de dados pessoais, enquanto afeto a pessoa passível de identificação é que emergem técnicas como a anonimização, também indicadas no bojo da LGPD. Essa técnica empreende justamente a perda da possibilidade de ligar um dado, de forma direta ou indireta, a uma pessoa especificamente (Art. 5°, XI).

Mediante a sofisticação das tecnologias, uma anonimização totalmente eficaz e que rompa totalmente com a possibilidade de identificar a que pessoa, outrora, fazia referência é algo utópico. Assim, o que hoje temos como uma técnica eficaz, daqui há algum tempo com o surgimento de uma nova tecnologia, pode ser revertido.

Para tanto, a legislação fez a devida consideração em seu Artigo 12, a indicar que os dados anonimizados não serão considerados dados pessoais enquanto esse processo de anonimização não for revertido.

Primordial ressaltar que a Lei 13.709/2018 faz a distinção entre os dados meramente pessoais e os denominados dados sensíveis (BRASIL, 2018). A estes o critério diferenciador tem como objetivo a disposição de normas mais rígidas, a conferir uma proteção mais elevada em seu tratamento.

Em síntese, todo dado sensível é um dado pessoal, mas nem todo dado pessoal é entendido e classificado como sensível (KONDER, 2019, p. 452). Os dados sensíveis são aqueles indicados no teor do Artigo 5°, inciso II e que traduzem informações quanto a origem racial, étnica, religião, filiação política e/ou sindical, filosófica, dados genéticos, sexuais, biométricos e também os dados quanto à saúde.

Por oportuno, os dados sensíveis serão mais extensamente analisados e abordados quando do capítulo posterior, no recorte quanto aos dados em saúde, por serem o objeto da presente pesquisa.

Mas, ainda quanto à este ponto, é importante apresentar a consideração de que este rol de dados sensíveis indicados no artigo 5° não haveria por ser entendido como um rol taxativo. Em verdade, a definição de um dado enquanto dado sensível atine para o potencial ofensivo, discriminatório e de segregação a que pode gerar, justificando assim um maior rigor protetivo. (KONDER, 2019, p. 455-456)

Outros tipos de dados, a *priori* não denominados como sensíveis podem propiciar um potencial lesivo a nível sensível ao longo da operação de tratamento ou mesmo ao longo do desenvolvimento das relações sociais no recorte histórico.

Está concludente pode ser retirada da própria ponderação aduzida por Laura Schertel Mendes quando da análise do julgado paradigmático de 1983 pelo Tribunal Constitucional Alemão, citado em tópico anterior do trabalho. A análise de que muito mais do que a definição da informação enquanto pública ou privada *a priori*- a que aqui se desenvolve extensamente para definição enquanto dado pessoal ou sensível de forma fixa e fechada, no momento inicial -, durante as operações de tratamento esse dado e essa informação podem assumir uma nova feição e, assim, cabe que esses critérios classificatórios não sejam tão rígidos.

Quanto aos princípios que orientam não só a aplicação da lei, como também a interpretação de seus dispositivos, apresentam-se a finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação, responsabilização, prestação de contas e boa-fé (BRASIL, 2018, Art. 6°).

Os fundamentos basilares da própria lei expressam uma ponderação entre a tutela da privacidade, autodeterminação informativa, liberdade de expressão e informação, desenvolvimento econômico e tecnológico, livre desenvolvimento da personalidade e dignidade da pessoa humana.

Observa-se que a lei não intenta frear a informatização da sociedade e o uso de aparatos digitais, mas implicar em parâmetros mínimos que promovam a defesa dos direitos constitucionais da privacidade, personalidade e proteção de dados pessoais.

Inicialmente não havia um reconhecimento expresso na Constituição Federal de 1988 que viesse a outorgar o *status* de direito fundamental à proteção de dados pessoais. Quando confrontado com tal questionamento, o Supremo Tribunal Federal já havia se posicionado no sentido de reconhecer a fundamentalidade implícita de tal direito, que poderia ser deduzido da

leitura sistemática da Constituição e dos direitos da personalidade, privacidade, bem como do próprio princípio da dignidade humana. (BRASIL, 1988)

Tal posicionamento emergiu do julgamento conjunto das ADI's 6387, 6388, 6389, 6390 e 6393, que impugnavam a medida provisória de n° 954/2020. Essa medida provisória buscava possibilitar o acesso pelo Instituto Brasileiro de Geografia e Estatística (IBGE) de dados pessoais dos usuários dos serviços de telecomunicações, durante o período de emergência em saúde ocasionado pela pandemia do Covid-19.

No bojo de tal julgamento fica reconhecido o direito de proteção de dados[28] como um direito autônomo constitucional, ou seja, independente de uma garantia da personalidade ou mesmo da privacidade. Aqui abre espaço a uma consideração do professor Ingo Sarlet (2021, p. 16) que predita que, muito embora esse direito à proteção possa ser deduzido de outros direitos fundamentais, não há como confundi-los.

Digno de nota é o voto do Ministro Gilmar Mendes no julgamento das supracitadas ações de inconstitucionalidade na defesa da ordem de um direito fundamental à proteção de dados,

> O quadro fático contemporâneo deve ser internacionalizado na leitura e aplicação da Constituição Federal de 1988. Aliás, ousaria a dizer que nunca foi estranha à jurisdição constitucional a ideia de que os parâmetros de proteção dos direitos fundamentais devem ser permanentemente abertos à evolução tecnológica. (BRASIL, 2020).

Parte da ideia norteadora em reconhecer uma releitura do direito à privacidade, conforme já apresentado alhures, e à partir da influência comparada do direito alemão e a própria tendência normativa interna, a que cita o Código de Defesa do Consumidor, o Marco Civil da Internet, a Lei do Cadastro Positivo e recente Lei de n° 13.709/2018[29], bem como mediante outros entendimentos do próprio STF a referendar[30].

---

[28] Quanto aos efeitos de tal reconhecimento pelo STF e sob o que implica um direito à proteção de dados e da vertente de um direito à autodeterminação informativa: "De um lado, essa proteção se desdobra como liberdade negativa do cidadão oponível perante o Estado, demarcando seu espaço individual de não intervenção estatal (dimensão subjetiva). De outro lado, ela estabelece um dever de atuação estatal protetiva no sentido de estabelecer condições e procedimentos aptos a garantir o exercício e a fruição desse direito fundamental (dimensão objetiva)." (MENDES; FONSECA, 2020, p. 473)

[29] Sobre a influência dessas leis no ordenamento jurídico interno como passos para o reconhecimento constitucional de um direito à autodeterminação informativa: "Ao mesmo tempo em que todas essas iniciativas normativas não implicam formalmente alterações dos textos constitucionais, elas consagram materialmente categorias de direitos, princípios e normas de governança para a internet, limitando drasticamente o poder de autoridades públicas e de atores privados nas suas relações com os usuários. (BRASIL, 2020)

[30] BRASIL. Supremo Tribunal Federal. **RE 673.707**. Relator: Min. Luiz Fux, 17 jun. 2015. DJe 30.9.2015. Disponível em: https://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=754357629. Acesso em: 28 out, 2022.

Hodiernamente viabilizado pelo Projeto de Emenda à Constituição de n. 17/ 2019 foi aprovada a alteração constitucional no sentido de também reconhecer expressamente um direito fundamental autônomo à proteção de dados pessoais, assegurando também a competência privativa da União para legislar sobre a matéria de proteção e tratamento de dados pessoais.

O direito fundamental à proteção de dados pessoais assim hoje, para além de implicitamente reconhecido, está explícito na Constituição Federal Brasileira em seu Artigo 5°, inciso LXXIX. (BRASIL, 1988)

Apesar das anteriores legislações setoriais e que de certa forma eram aplicadas a casos atinentes a dados na circunscrição brasileira, a edição de uma lei específica, bem como o reconhecimento não só implícito, como também expresso, de um direito autônomo à proteção de dados pessoais ressalta não só a contemporaneidade do tema e a imersão do Direito em fixar as balizas e normativas necessárias, mas também o próprio destaque que o Estado Brasileiro confere em tratar seriamente as agressões e arbitrariedades no campo de tratamento de dados.

Ainda sobre os dados sensíveis no parâmetro legal, especificamente os dados que versam quanto a saúde, é válido assinalar algumas ponderações para efeitos introdutórios, a que serão melhores desenvolvidos no capítulo posterior, vez que se dedica a uma análise aprofundada quanto a tal recorte.

Perpassando pela classificação atinente aos dados, vislumbra-se claramente o contexto situacional dos dados em saúde enquanto dados pessoais sensíveis. Nesse viés, a LGPD dedica a sua Seção II a tratar do rigor a proteção dos dados sensíveis.

A sistemática legal assenta como regra que o tratamento de dados pessoais deve estar firmado em um prévio consentimento do titular do dado, a efetivar um direito à autodeterminação informativa. E não qualquer consentimento, como bem destaca Regina Linden Ruaro (2020), mas um consentimento na forma que já vinha expressa no Regulamento Europeu e a que lei brasileira adota moldes parecidos, de ser livre, informado e inequívoco (BRASIL, 2018, Art.5°, XII).

Se já salientamos que a proteção de dados pessoais sensíveis, pelas próprias características e potencial ofensivo, remete a um regime de proteção ainda mais rigoroso, no que tange a tais dados a regra também é o consentimento. Não por outra sorte, os dados em relação à saúde também, em regra, devem possuir o consentimento do titular.

No entanto, a própria legislação traz a permissiva, em seu Artigo 11, inciso II, de hipóteses no tratamento de dados sensíveis independente do consentimento do titular. Entre estas hipóteses está resguardada a elaboração de políticas públicas em saúde, como bem se

destacam as políticas epidemiológicas, vez que se trata eminentemente da defesa e ponderação com um interesse público.

Partindo do pressuposto de que a Lei 13.709/2018 viabiliza o uso compartilhado de dados para execução destas políticas públicas através da administração pública (BRASIL, 2018, Art.7°, inciso III) e que esse tratamento, independe de um consentimento (BRASIL, 2018, Artigo 11, inciso II, b), deve-se delinear os limites da aplicação de tal permissiva, em vias a não fulminar ou restringir significativamente o direito à proteção de dados e à autodeterminação informativa.

Por sorte, a pandemia do Covid-19 fez emergir uma tendência- já sinalizada e em aplicação no Brasil, apenas não ainda com todo esse rigor-, de informatização dos dados em saúde, como mecanismo para uma melhor articulação da prestação do serviço em saúde. Assim também quanto aos dados epidemiológicos, para a coordenação dos insumos necessários e das políticas públicas epidemiológicas em geral.

Coaduna-se essa informatização com os preceitos da própria instituição do SUS, onde no Artigo 47 da Lei 8.080/1990 o propósito de estruturação de um sistema nacional de informações em saúde fica evidente. A criação do Departamento de Informática do Sistema Único de Saúde em 1991 caminha nesse sentido, com seu desenvolvimento e incremento nos últimos anos implementando o alargamento da informatização dos dados em saúde em todo o país.[31]

É inegável que a pandemia do Covid-19 acelerou esse processo de informatização, especialmente quando referente aos dados epidemiológicos, a que se pode observar através da Portaria 1.434/2020 instituidora da Rede Nacional de Dados em Saúde, assim como a Lei 13.979/2020 que prevê a obrigatoriedade de compartilhamento de dados atinentes a identificação de pessoas infectadas entre os órgãos e entes da administração pública.

Mesmo a considerar a situação transitória emergencial da pandemia, ela revelou e acelerou, de forma inegável, essa tendência de informatização em saúde.

Como as questões de doenças, sejam virais, bacterianas ou outras, são rotineiras no âmbito mundial e nacional, surgindo sempre outras que desconhecidas *a priori*, apresentou-se

[31] Conforme as informações disponibilizadas no site oficial do Datusus, indica-se que detém o software e estrutura de armazenamento de dados Storage, a que se serve de duas salas cofre- uma em Brasília e outra no Rio de Janeiro-, e a fazer interface com todo o território brasileiro e os diversos serviços atinentes ao SUS. Ademais, aponta a tendência e diretriz de plena informatização quanto a saúde, quando indica que tem "condições de armazenar as informações em saúde de toda a população brasileira". Informações coletadas em: https://datasus.saude.gov.br/sobre-o-datasus/.

e sedimentou-se o compartilhamento dos dados epidemiológicos como veículo facilitador na articulação de medidas eficazes de enfrentamento.

Perante a todo este contexto e a possibilidade de tratamento independente de consentimento quanto aos dados epidemiológicos, com o fim de desenvolvimento das políticas públicas em saúde correspondentes, é importante assinalar os limites nessa execução do permissivo legal, bem como identificar a quem incumbe a responsabilidade de fixar tais balizas interpretativas.

3 O SISTEMA NORMATIVO DE PROTEÇÃO DE DADOS EM SAÚDE

A Lei Geral de Proteção de Dados disciplina que os dados pessoais são aqueles que tem como característica principal o fato de serem correspondentes a informação sobre pessoa natural já identificada ou que possa ser identificada. Seriam aqueles que transmitem informações a guardarem um vínculo objetivo e direito com uma pessoa, a exprimir suas características ou suas próprias ações (DONEDA, 2011, p. 93).

Os dados pessoais sensíveis figuram enquanto uma classificação quanto aos dados pessoais. Nesse sentido, os dados pessoais sensíveis são a espécie de dados pessoais que detém um potencial ofensivo ainda mais elevado quanto ao tipo de informações pessoais que guardam[32],

> [...] a LGPD traz a diferenciação do tratamento de certa categoria de dados pessoais: os chamados "dados sensíveis". Com efeito, se o tratamento de qualquer dado pessoal tem o potencial de atingir o seu titular, alguns dados apresentam potencial de dano qualificado no que tange à pessoa humana. A distinção de tratamento normativo, envolvendo a incidência de regras próprias, justifica atenção especial a essa nova categoria normativa.
> Para proceder a essa qualificação, propõe-se chave de leitura fundada na abertura e dinamicidade do princípio da dignidade da pessoa humana, em especial com a conjugação de três de suas mais populares manifestações nos últimos tempos: privacidade, identidade pessoal e vedação a discriminação. A partir dessa perspectiva, identifica-se quando determinada informação pode ser considerada dado sensível e passa-se a aplicação do conjunto de normas próprio a reger o seu tratamento. (KONDER, 2019, p. 446)

No tocante aos dados pessoais sensíveis, a Legislação Geral de Proteção de Dados contém em seu artigo 5° uma espécie de lista do que viria a ser considerado dotado de tal sensibilidade,

> Art. 5° Para os fins desta Lei, considera-se:
> [...]
> II- dado pessoal sensível: 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; (BRASIL, 2018)

[32] "São dados que quase sempre uma pessoa só revela para aqueles com quem tem vínculo de confiança e intimidade. O dado pessoal sensível é aquele relacionado ao âmago do indivíduo, associado a elementos muito mais aprofundados da sua intimidade e vida privada e que, por isso, deve ser merecedor de maior proteção legal." (ALMEIDA, 2020, p. 171)

O rigor protetivo diferenciado ao campo dos dados pessoais dotados de sensibilidade é justamente pelo reconhecimento do potencial discriminatório e maior risco ao livre desenvolvimento da personalidade dos indivíduos que teriam suas informações desveladas. Por entender que "entre os diversos dados associáveis à pessoa, alguns são especialmente aptos a favorecer processos sociais de exclusão e segregação" (KORKMAZ, 2019, p. 42) é que cabe uma classificação diferenciada como a de dado sensível e, por consequência, um sistema mais rígido de tutela.

> Estes dados, pela sua índole, carecem de maior proteção pois são essencialmente sensíveis do ponto de vista dos direitos e liberdades fundamentais, já que do tratamento dos mesmos podem surgir danos para os direitos e liberdades fundamentais." (NUNES, 2019, p. 19)

Os dados referentes à saúde, neste sentido, estão claramente situados nesta classificação de dados sensíveis. Essa topologia situacional de tais dados imprime um maior rigor no sistema protetivo afeto ao seu tratamento.

Os dados referentes a saúde, já classificados topologicamente no rol de dados pessoais sensíveis, devem ser oportunamente conceituados. Apesar da legislação brasileira não se dedicar a fazer tal conceituação, pode ser empregada a constante no Regulamento Europeu Geral de Proteção de Dados (RGPD) 2016/679, que em seu Artigo 4°, alínea 15 entende que são "os dados relacionados com a saúde física ou mental de uma pessoa singular, incluindo a prestação de serviços de saúde, que revelem informações sobre o seu estado de saúde."

É necessária uma amplitude e cautela a pautar a devida consideração de dados e informações como referentes à saúde dos indivíduos. Em diversas situações um dado individualizado a *prima facie* não se revela como afeto a saúde, mas combinado com outra rede de dados trazem uma carga de informações valiosas quanto à saúde de indivíduos, como se explicita o caso do peso e altura[33], (GONÇALVES, 2020, p. 128).

[33] Sobre as possíveis integrações de dados e a abrangência do que pode se chegar em informações quanto a saúde: "Saliente-se que alguns dados, quando isolados, não necessariamente revelam informação sobre o estado de saúde do titular como, por exemplo, a altura, o peso e a idade. No entanto, uma vez combinados estes dados com informações, por exemplo, de um Fitness Tracker sobre a atividade diária do indivíduo, podem configurar dados pessoais relativos à saúde. Sublinhe-se que até mesmo o fato de uma pessoa ter lesionado um pé constitui um dado pessoal relativo à saúde, pois no condão da jurisprudência do Tribunal deve a expressão "dados relativos à saúde" ser interpretada de forma abrangente, lata.
A abrangência dos dados relativos à saúde é muitas vezes subestimada. Por exemplo, se um usuário individual acessa um provedor de buscas e pesquisa sobre determinada doença, a probabilidade de que esse usuário ao menos tenha receio de tê-la contraído não é baixa. Esta busca, associada a demais informações do usuário, pode, então, ser classificada como dado de saúde". (GONÇALVES, 2020, p.128)

Portanto, é importante ter a compreensão de tal conceito com a devida cautela e amplitude necessárias.

Os dados que trazem informações relativas à saúde, justamente por conta de uma possibilidade de agressão em um nível mais profundo à direitos mínimos e constitucionais dos indivíduos, direcionam ao artigo 11 da Lei 13.709/2018. Evidencia-se esse maior rigor nas regras de tratamento ao fixar que quanto aos dados sensíveis só é viabilizado mediante consentimento do titular e, quando independente de consentimento, apenas nas linhas taxativas previstas em seu inciso II.

> II - sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para:
> a) cumprimento de obrigação legal ou regulatória pelo controlador;
> b) tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos;
> c) realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis;
> d) exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral, este último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem) ;
> e) proteção da vida ou da incolumidade física do titular ou de terceiro;
> f) tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; ou
> g) garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no art. 9º desta Lei e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais. (BRASIL, 2018)

Cumpre salientar, que os dados pessoais sensíveis em saúde pública podem assim, referendados pela legislação em questão, serem tratados independente de consentimento para a consecução destes casos previstos no inciso II, sublinhado acima. Nesse campo, os casos afetos à dados sensíveis a serem tratados independente de consentimento destacam-se os constantes nas alíneas b, c, e, f, justamente por corresponderem a potenciais hipóteses a que caberia utilizar-se de dados sensíveis em saúde.

A utilização dos dados em saúde, especialmente nos casos legais em que independe o consentimento, reverbera a existência da preservação de um interesse coletivo e um interesse público. A consecução de uma prestação mais efetiva, articulada e eficaz de um direito à saúde oportuniza um certa flexibilização, neste casos, do direito à privacidade e da autodeterminação informativa.

> Os dados pessoais na saúde cumprem, indubitavelmente, uma outra função que vai além da proteção da privacidade em prol da produção de um bem comum. O interesse coletivo é intrínseco à compreensão de bem comum na saúde, e determina os valores e parâmetro que devem orientar o uso e a disponibilização dos dados pessoais enquanto bem jurídico tutelado, de forma a garantir, preponderantemente, a satisfação de necessidades coletivas.
> Essa dinâmica ressignificação do direito à privacidade e à informação na saúde requer uma regulamentação e governança que articule virtuosamente proteção da privacidade e promoção do acesso à informação em compasso com as referidas necessidades coletivas e as possibilidades tecnológicas disponíveis. (VENTURA; COELI, 2018, p. 2)

As tecnologias possibilitam uma melhor articulação no tocante a uma prestação eficiente no âmbito do direito à saúde, seja pela interoperabilidade de dados a garantir um acompanhamento mais completo e até mesmo preventivo e programado.

No entanto, como bem destacado, ao tratar-se de um dado classificado como essencialmente sensível é imperiosa essa devida parcimônia em congregar esses dois pesos da balança. Sopesar, por um lado, a necessidade de acesso aos dados para a promoção do direito à saúde e efetividade aos interesses públicos e, por outro, considerar um dever de proteção mínima da privacidade e da autodeterminação informativa dos titulares de dados.

Outrossim, conforme a citação em destaque indica, há que se articular uma regulamentação e uma governança que ressoe a ponderação adequada entre os direitos constitucionais em relevo, tal qual a tutela de uma autodeterminação e também da saúde.

Essa regulamentação apesar de efetivada por parte da Lei Geral de Proteção de Dados, há que consubstanciar quais seriam os limites claros interpretativos de tal texto legal, a afixar as balizas nessas operações de compartilhamento entre dados sensíveis e, em específico, dos dados epidemiológicos em saúde.

3.1 ENTRE A PRIVACIDADE, A TUTELA DA SAÚDE E OS DESAFIOS DA IMPLANTAÇÃO DE SISTEMAS INFORMATIZADOS NO ÂMBITO DA SAÚDE

A permeação das tecnologias na realidade cotidiana das pessoas e nos mais vastos campos da vida em sociedade é produto de sua identificação como um veículo facilitador e transformador na vida humana. Assim também apresenta-se no desenvolvimento dos serviços estatais e, por tal sentido, cada vez está mais inserida nestes setores e nesse múnus público.

Dentre as diversas áreas da sociedade que passam a utilizar-se de tais ferramentas, o campo da saúde não é diferente. Destaca-se que esse processo não limita-se apenas as redes

particulares, mas, hodiernamente, também está sendo implementado no Sistema Único de Saúde de forma geral e paulatina.

> Se o mote geral do discurso relacionado à proteção de dados reserva atenção especial à privacidade e intimidade do indivíduo, quando a discussão volta-se ao universo dos dados em saúde, mormente dos sistemas sanitários, a análise extrapola, em muito, a mera tutela individual de direitos. Um dos aspectos a ser debatido nesses casos é a dicotomia entre a legítima busca de proteção das informações sensíveis e as necessidades e dificuldades práticas de gestão, contradição aparentemente inalienável. Se do ponto de vista teórico esse limite parece bastante claro à vista do contido na Lei 13.709/2018, sob a ótica da práxis das rotinas dos serviços de saúde, a tarefa vislumbra-se mais complexa. A evolução rápidas das TIC, especialmente com o uso intensivo da internet, ilimitado no tempo e no espaço, levou ao crescimento do volume e variedade de informações que podem ser combinadas, aumentando o risco de vazamentos e re-identificação, mesmo após a anonimização ou desidentificação de bases de dados de saúde. (ARAGÃO; SCHIOCCHET, 2020, p. 698)

Volta-se a ponto já discutido em tópico anterior, a que aponta a amplitude que a experiência prática pode conferir no que de fato consistem os dados em saúde. Isto pela possibilidade de ressignificação que a conjunção de dados que *a priori* não versavam sobre questões de saúde, mas que à partir de uma interação, revelam uma variada fonte de novas informações.

A dificuldade prática na devida proteção dessa esfera de dados, inicia-se pela própria identificação dos mesmos. Assim deve-se atentar para o reconhecimento e a devida proteção, enquanto dado sensível sobre saúde, não apenas aqueles micro dados que podem ser de pronto ligados a questões quanto à saúde do indivíduo, mas a englobar também aqueles que integrados com outros, acabam trazendo informações nesse campo e, para tanto, são também dignos da proteção necessária.

Quanto a inserção e interação das tecnologias com o campo da saúde, indica-se que o chamado movimento da reforma sanitária teve grande aporte nesse sentido, ao trazer a pauta de um sistema único de saúde, distante da, outrora vigente, gestão centralizada. Pleiteava-se um sistema que se compatibilizaria com o acesso de todos os indivíduos à saúde (FORNAZIN, 2015, p. 53)

Nesse sentido, a informatização em saúde surge justamente como uma corrente correlata a veia de pensamento a indicar que é necessário uma promoção mais universalizada do direito à saúde e mais descentralizada em sua gestão. Para tanto, “a partir desse enfoque, as pesquisas

revelam que a produção de informação em saúde não é neutra, faz parte de uma luta política pela saúde e pelo direito à cidadania.” (FORNAZIN, 2015, p. 53)

Desde de o processo de redemocratização brasileira e da criação de um Sistema Único de Saúde (SUS) há uma propensão do Ministério de Saúde em desenvolver uma política em nível nacional de informatização em saúde, na tangente de coletar e armazenar dados migrando de uma via física para digital e a garantir uma interoperabilidade dos dados. Parte do entendimento de que tal atuação resta compatibilizada com uma gestão descentralizada, tal qual funda-se o próprio SUS.

> Nesse contexto, foi instituído o Sistema Nacional de Informações em Saúde (SNIS), cuja organização coube ao Ministério da Saúde (MS), em parceria com estados e municípios. Para dar conta dessa atribuição, em 1990 foi criado o Datasus, a partir do desmembramento do Dataprev. A gestão descentralizada, fundamento básico do SUS, orientou ações objetivando prover SIS aos níveis regionais e locais. Ou seja, passou-se a produzir SIS para apoiar as ações de secretarias estaduais e municipais de saúde. (DANIEL; PEREIRA; MACADAR, 2014, p. 23)

Essa gestão descentralizada seria marcada justamente pelo objetivo máximo de implantar sistemas informatizados em cada nível estadual e municipal. A que essas informações e esses dados viriam a alimentar todo o sistema de saúde nacional, a conter uma rede de informação de cada gestão.

Quanto à existência de tais SIS (Sistemas de Informação em Saúde) de forma regional e local[34], desponta a necessidade da interface das informações fornecidas por cada um deles- a chamada interoperabilidade- a fim de que os objetivos gerais para a própria criação de tal rede informatizada fossem alcançados.

O aludido Datasus, a que refere-se ao Departamento de Informática do Ministério da Saúde, é instaurado por meio do Decreto de n° 100 que data de 16 de abril de 1991 e o prevê como integrante da estrutura básica da Fundação Nacional de Saúde, na forma de seu artigo 3°. Nesse contexto, pode-se atrelar o panorama de informatização na saúde pública ao próprio processo de promulgação da Carta Magna de 1988 e da previsão de um sistema universal de saúde, conforme a especial atenção conferida ao direito de saúde, como um direito do cidadão e dever do Estado (BRASIL, 1988, Art. 6° e Art. 196).

[34] “Considerando a complexidade informacional existente na área da saúde, surgem desafios para avançar na integração dos SIS. Integração esta que favorece tanto o planejamento e a gestão como o controle social comprometido com o avanço da democracia e da melhoria da condição de saúde da população brasileira.” (FORNAZIN, 2015, p. 54)

As bases fundantes de uma rede integralizada de informações em saúde e, o seu manejamento em prol da tutela da saúde, remete ao próprio influxo da instituição de um Sistema Único de Saúde. Nessa justa medida, quando da análise da Lei 8.080, há a previsão no artigo 47 da instituição em um prazo exímio de um sistema nacional de informações em saúde, conforme já até mesmo abordado ao fim do capítulo anterior.

Não obstante as problemáticas inerentes a propagação de informações, mediante os princípios de descentralização na rede de prestação do serviço e a promoção de um acesso universal, em um país de base territorial como o Brasil, o influxo de informações à partir de sistemas informatizados cumpria muito mais aos propósitos então colacionados.

De tal sorte, é que em 1991 surge um Departamento de Informática do Ministério de Saúde, imprimindo justamente essa integração de informações atinentes ao usuários dos serviços de saúde de maneira piamente informatizada, facilitando o acesso, a fidedignidade das mesmas, e sua serventia.

Quanto à existência desses, denominados Sistemas de Informação em Saúde, a promover justamente este ideário de informatização nas redes e serviços de saúde,

> Os Sistemas de Informação em Saúde (SIS) são instrumentos usados para processar os dados e produzir a informação. Podem ser entendidos como instrumentos usados para adquirir, organizar e analisar dados necessários à definição de problemas e riscos para a saúde, avaliar a eficácia, eficiência e influência que os serviços prestados possam ter no estado de saúde da população, além de contribuírem para a produção de conhecimento acerca da saúde e dos assuntos a ela ligados. (SANTOS; PEREIRA, SILVEIRA, 2017, p. 3)

Mormente a existência de sistemas de informações em saúde, o desafio maior consistiu na devida integração entre os mesmos, o que vem avançando e sendo enfrentado nos últimos anos. A falta de interoperabilidade entre as informações atinentes a cada sistemas específico é altamente indesejada e caminha para uma não articulação precisa da fronte de atendimento em saúde, tanto de forma preventiva –nas políticas públicas e pesquisas correspondentes-, como na forma de enfrentamento de enfermidades.

Sobre a existência já firmada de sistemas de informação em saúde e a falta de uma interoperabilidade real, analisada quando do ano de 2014, apontou-se de forma latente a problemática,

> No Brasil, existem diversos sistemas de informação para atender demandas específicas, por exemplo, sistema de controle de natalidade, sistema de informação de mortalidade, sistema de informações socioeconômicas, sistema

> de informação para controle de doenças- tuberculose, Aids, hepatite, etc. (Brasil, 2010). Desse modo, a falta de integração entre tais sistemas acarreta inconsistência nas informações, afetando o entendimento adequado da situação de saúde da população brasileira. Isso se deve ao fato de que, não obstante haver um olhar específico acerca das doenças, não é possível observar a situação de saúde dos indivíduos. (FORNAZIN, 2015, p. 53)

Diante de tudo enquanto exposto, esse processo paulatino de informatização de informações em saúde, caminha objetivando a interoperabilidade dos dados atinentes. Interoperabilidade esta que viabiliza o real diagnóstico quanto a situação da saúde no âmbito nacional.

Como analogia ao caso dos dados epidemiológicos, à partir da interoperabilidade entre as inúmeras redes informatizadas à nível municipal, estadual, consegue-se alimentar o sistema nacional e capacita-se a retratar o panorama precípuo quanto as doenças existentes e seu grau de dispersão. Para tanto, é que agiliza-se e promove um parecer mais assertivo no desenvolvimento das políticas públicas epidemiológicos necessárias.

À respeito da importante inicial definição do que constitui como interoperabilidade, empresta-se o conceito:

> [...], interoperabilidade é a capacidade de diferentes sistemas de informação trabalharem juntos para acessar, trocar, integrar e usar dados de forma cooperativa de maneira coordenada, dentro e através das fronteiras organizacionais, regionais e nacionais, fornecendo portabilidade oportuna e contínua das informações, otimizando a saúde de indivíduos e populações globalmente, promovendo a prestação eficaz de cuidados de saúde para indivíduos e comunidades. (FANTONELLI; CELUPPI; OLIVEIRA; BURIGO; DALMARCO; WAZLAWICK, 2020, p. 167)

Válido é também ponderar as dificuldades que refletem esse processo de informatização no âmbito do Sistema único de Saúde. As maiores dificuldades coadunam com aquelas elencadas na Tese de Marcelo Fornazin (2015) e que predita os obstáculos verificados na implementação de sistemas de informação em saúde nos países em desenvolvimento, ao passo que vem destacando caminhos alternativos viáveis.

Assim, focar não apenas nas sofisticações tecnológicas a esse serviço, mas também em fornecer uma capacitação dos indivíduos que irão lidar com esses sistemas, seja o alimentando ou retirando informações deles. Essa capacitação indicada[35] deve abranger não apenas os

[35] "[...] a implantação dos SIS não deve concentrar-se somente no enfoque tecnológico. [...] Tais projetos também devem considerar o ambiente local, provendo capacitação aos recursos humanos para sustentação dos SIS ao longo do tempo." (FORNAZIN, 2015, p. 51). Aqui pontua-se que para além dessa capacitação servir para

profissionais da comunicação que irão operacionalizar esses novos sistemas, como também os gestores municipais, estaduais e federais, a que esse campo de informações detém um papel salutar.

Uma rede de interoperabilidade eficiente, a que integre outros demais sistema de informação menores e que, vistos a densidade demográfica brasileira, atenda a devida coleta e interface dos dados em saúde coletados, a fim de promover como resultado a prestação mais satisfatória na diversa gama de serviços de saúde também pondera-se como caminho necessário.

Doravante a tônica de exponencial crescimento das técnicas informatizadas de integração de dados em saúde do SUS, ante a pandemia vivenciada, surge a edição da Portaria de n° 1.434 de 28 de maio de 2020. Esta prevê a criação de um sistema denominado *Conect* SUS, bem como prevê a instituição de uma Rede Nacional de Dados em Saúde e a afixação de padrões atinentes a interoperabilidade supracitada.

A Lei 13.979/2020, que predita as medidas para o enfrentamento da emergência em saúde pública, em seu artigo 6° assenta como de seus pilares justamente o compartilhamento de dados epidemiológicos e outros dados sensíveis em saúde perante a administração pública.

Apesar das atenuações dos efeitos nefastos do Covid-19, impõe assinalar que as medidas de compartilhamento de dados, bem como outros sistema informatizados, como a Rede Nacional de Dados e o próprio Conect Sus não foram afastados e não serão afastados com o fim da pandemia.

De forma diametralmente oposta, na verdade a Rede Nacional de Dados em Saúde vem sendo incrementada, como mesmo informa o Plano Estratégico do Ministério da Saúde 2022-2028[36]. Há um esforço de informatização e integração entre os dados atinentes a todos os setores da saúde, com o envolvimento de todos os atores necessários.

Não caberia pensar que tais mecanismos emergiram apenas por conta da crise em saúde pelo Covid-19 e que com o seu fim serão totalmente derrocados. Em verdade, a integração de tais dados remete à período em muito anterior a vivência excepcional contemporânea pandêmica, ademais são justificadas com a consecução finalística de facilitar a tutela da saúde, não estando restrita sua implementação a um recorte temporal específico.

Assim, o regime da coleta e integração dos dados em saúde, e que são notoriamente sensíveis, está para além do cenário pandêmico atual e trata-se precipuamente de uma tendência

sustentação desses sistemas informatizados, tem um especial papel na utilidade e proveito máximo das informações agregadas e compartilhadas pelos mesmo.

[36] Documento disponibilizado na plataforma: https://bvsms.saude.gov.br/bvs/publicacoes/estrategia_saude_digital_Brasil.pdf.

mundial, a que o Estado cumpre regular e resolver os eventuais aspectos problemáticos revelados.

Entre uma de tais tensões, é apresentada o ideário protetivo de dados sensíveis em saúde e a possibilidade do tratamento independente de consentimento nas hipóteses legais traçadas- conforme o artigo 11, inciso II, da Lei 13.709/2018 prevê.

Dentre as hipóteses constantes no Inciso II, contém a previsão para a elaboração de políticas públicas estatais. É sabidamente conhecido a intensa carga de importância, inclusive plenamente válida, de políticas públicas no campo da saúde, assim como especificamente nas políticas públicas epidemiológicas.

A redação constante do citado artigo 196 atrela a previsão do desenvolvimento de políticas públicas em saúde, a própria tutela fidedigna do direito à saúde,

> Art. 196. A saúde é direito de todos e dever do Estado, garantido mediante políticas sociais e econômicas que visem à redução do risco de doença e de outros agravos e ao acesso universal e igualitário às ações e serviços para sua promoção, proteção e recuperação. (BRASIL, 1988).

Nessa senda, a previsão de políticas estatais, conforme expressamente consta, indica também a articulação e coordenação de medidas para a redução do risco de doenças, a que engloba, por certo, o caráter epidemiológico, de contenção e prevenção de doenças.

Ao prever o compartilhamento de dados independente do consentimento como técnica para o desenvolvimento de políticas públicas, preceitua-se a discussão dos limites em tal tratamento específico no desenvolvimento de medidas integradas em saúde e, oportunamente, aquelas ligadas ao controle epidemiológico.

A dispersão de doenças contagiosas e a instauração de um cenário de crise epidêmica ou pandêmica, como o caso do Covid-19, leva a pensar e põe em relevo que ante as situações de urgência muitas vezes são realizadas ações arbitrárias e em violação à direitos fundamentais. Nesse ressurgir, a preocupação com o compartilhamento de dados sensíveis e ainda assoberbada pela inexistência de um consentimento, é plenamente justificável e primordial.

Para tanto, o enfrentamento e combate de doenças não é algo singular ao Covid-19, que limita o presente estudo a um recorte temporal específico, mas algo cíclico na história mundial.

Por exemplo, epidemia do Ebola que remete a um surgimento de um vírus em 1976 e a classificante de epidemia em 2014, com a morte de 11.299 pessoas, nos territórios apenas de

Guiné, Serra Leoa e Libéria[37].Ou mesmo, em um cenário mais próximo, a difusão pelo mosquito *Aedes aegypti* de um vírus identificado como Zika, a que remete uma propagação e instalação no Brasil de um contexto emergencial em 2015, pós-evento da Copa do Mundo de Futebol recepcionado pelo país ,outrora, identificado em casos na região do pacífico, e a que gerou não só um alto índice de contaminação, como também de sequelas nos infectados[38].

Nesse sentido, o desenvolvimento de políticas epidemiológicas é algo contingente a atuação estatal, do Ministério da Saúde, e das Secretária de Saúde, na esfera tanto estadual, como municipal, na medida em que os serviços de saúde integram uma rede regionalizada e hierarquizada, na forma da previsão constitucional do SUS (Art. 198 da CF/88). Evoca-se que a participação das instituições privadas de saúde é feita de uma forma eminentemente suplementar.

Outrossim, a descentralização fundante de sua atuação e a universalidade de acesso à saúde encontram-se como princípios motores do próprio Sistema Único de Saúde, na forma da Lei 8.080 de 1990. Converge com tais diretrizes a criação de um sistema informacional de saúde e a facilitação do compartilhamento dos dados para a estruturação de políticas estatais, mediante o desiderato de facilitar um acesso universal e tutelar efetivamente a saúde.

Dentro da mesma lei supracitada, em seu artigo 6° que prevê o campo de atuação do SUS, encontra-se a vigilância epidemiológica. Não poderia ser diferente, dito o seu papel salutar na defesa da saúde e na prevenção de doenças, na forma que o próprio conceito legal expõe no parágrafo 2° do dito dispositivo,

> § 2º Entende-se por vigilância epidemiológica um conjunto de ações que proporcionam o conhecimento, a detecção ou prevenção de qualquer mudança nos fatores determinantes e condicionantes de saúde individual ou coletiva, com a finalidade de recomendar e adotar as medidas de prevenção e controle das doenças ou agravos. (BRASIL, 1990a)

A possibilidade de um compartilhamento de dados nos moldes do sistema informatizado de saúde, ainda mais assoberbado ante a Portaria de n° 1.424/2020 e o surgimento de uma Rede Nacional de Dados de Saúde e ferramentas como o *Conect* SUS, bem como a permissiva de um tratamento independente de consentimento para a adoção de políticas em saúde e articulação

[37] Informações encontradas no endereço eletrônico da Agência Fiocruz; FIOCRUZ. **Ebola**. Disponível em: https://agencia.fiocruz.br/ebola. Acesso em 06/10/2021.

[38] Informações encontradas na Secretaria de Estado de Saúde do Governo do Espírito Santo: SECRETÁRIA DE ESTADO DA SAÚDE. Aedes Aegypti. Disponível em; https://mosquito.saude.es.gov.br/zika-virus. Acesso em 06/10/2021.

das medidas epidemiológicas realçam a notoriedade para importância do estudo e a identificação dos limites atinentes.

Ante a prematuridade da lei em vigência no Brasil, ainda dissonante de uma efetiva experiência de atuação da prevista Autoridade Nacional de Proteção de Dados, do Judiciário e da própria doutrina, na afixação concisa dos limites atinentes a interpretação concessiva do Artigo 11, inciso II e, principalmente da alínea b, bem como do Artigo 7°, inciso III, da Lei 13.709/2018, permeia a indiscutível voga e necessidade da presente pesquisa.

O Artigo 7° da LGPD, apresentado acima, é outro dispositivo legal que promove destaque no compartilhamento de dados entre a administração pública, a viabilizar o desenvolvimento de políticas públicas.

Aponta-se também, nessa senda, que a edição da já citada Lei n° 13.979/2020, que prevê em cunho legal essa via de compartilhamento concilia, em última esfera, a tutela do direito da saúde e da vida. Outrossim, também é responsável pela ratificação do Regulamento Sanitário Internacional de 2005, que assevera o compartilhamento também a nível internacional, perante a Organização Mundial das Nações Unidas e a sistematizar o controle de doença em todo o globo, bem como articular medidas integradas de controle.

Prepondera, assim, a problemática a que impulsiona a presente pesquisa, visto que em que pese seja idôneo o uso de dados em vias da garantia da saúde e da vida com seu tratamento sendo flexibilizado a ser efetuado independente de consentimento para a elaboração das políticas atinentes, deve ter-se sempre em vista um juízo de ponderação, a articular balizas em salvaguardar também outros direitos constitucionais. Emerge ainda mais tal perspectiva, mediante a, conforme já assinalada, decisão do Supremo Tribunal Federal que reconhece o direito à proteção de dados como um direito autônomo fundamental.

De forma peculiar, a Lei Geral de Proteção de Dados entra em vigência no Brasil em um período emergencial em saúde pública, pelos reflexos da pandemia do Covid-19. Exacerba-se assim os aspectos emblemáticos na proteção dos dados sensíveis relativos à saúde, especialmente em que pese ser um contexto caracterizado pela ampla utilização dos mesmos, especificamente no que toca aos dados epidemiológicos.

O compartilhamento de dados epidemiológicos para mapear a dispersão viral e direcionar possíveis frentes e formas de enfrentamento, figurou como uma saída imperiosa a ser tomada.

Nesse cenário, pende ainda mais e coloca em devido prospecto a devida afixação dos limites nessa legalidade e constitucionalidade do tratamento de dados independente do ato de consentir do titular do dado. Apesar de veiculadas e fundamentadas em um interesse público,

cumpre a discussão da preservação do núcleo essencial dos direitos à autodeterminação informativa e à proteção de dados (TRAVINCAS, 2010, p. 129)

A considerar que legislação protecionista quanto à dados ainda figura como inovação e não é ambientada de um experiência prática jurisprudencial concisa e nem de uma carga de experiência na interpretação legal desenvolvida por parte da Autoridade Nacional de Proteção de Dados, cabe o questionamento de como será orquestrado a fixação desses limites e em que estarão pautados.

Há uma válida serventia no compartilhamento de dados sensíveis pessoais, e nos dados epidemiológicos, a que, em momento algum, se denega. É, inclusive, embasado em claros padrões legais (BRASIL, 2018ª Art. 7°, inciso III c/c Art. 11, inciso II, b) e também em constitucionais (BRASIL, 1988, Art.6° e Art.196).

Esse mecanismo serve para uma prestação mais eficaz do direito à saúde, de uma forma preventiva e repressiva e, conforme o recorte da pesquisa aduz, especialmente para o controle epidemiológico e o devido planejamento de ações integradas estatais atinentes.

O que visa-se discutir e afixar claramente são os limites em tal via de compartilhamento, na clara noção de que seu tratamento é validado independente do consentimento do usuário, conforme imprime o parâmetro legal específico incidente.

Mesmo quando impele um tratamento de dados sensíveis referentes à saúde em que há a necessidade *a priori* do consentimento do titular, a que garante vazão em tese ao direito da autodeterminação informativa, ainda assim as fixação de tais balizas é imperiosa pela característica de risco que tal atividade colaciona.

Assim, no que tange a hipótese permissiva em apreço, do Art. 11, inciso II e alínea b da Lei 13.709/2018, os riscos são ainda mais incisivos.

Em tal tangente é que é deveras importante investigar os limites éticos, legais e também constitucionais, na justa medida que os direitos da privacidade, personalidade e até mesmo à autodeterminação informativa, hoje pacificamente reconhecidos, são afetados por esse compartilhamento de dados assinalado e que pelo seu risco inato de tal proceder deve ser objeto de grande precaução.

3.2 A NORMATIZAÇÃO ATINENTE AOS DADOS SENSÍVEIS EM SAÚDE E AOS DADOS EPIDEMIOLÓGICOS SITUADA NA LEI GERAL DE PROTEÇÃO DE DADOS

Conforme já apresentado ao longo deste trabalho, os dados epidemiológicos contém informações referentes a saúde das pessoas, sendo assim considerados como dados pessoais sensíveis, a contar com uma esfera protetiva mais concisa à luz da LGPD.

Quanto aos dados sensíveis houve a destinação da seção II da Lei 13.709/2019, que trata especificamente das operações quanto a tratamento que envolvam tais espécies de dados.

Esta lei evoca a regra do tratamento perante o consentimento do titular, mas assume a possibilidade de exceção para algumas situações previstas na norma (Art.11, inciso II), onde entre elas está na articulação e desenvolvimento de políticas públicas.

O desenvolvimento de políticas públicas em saúde, e precisamente das políticas públicas epidemiológicas, cumpre com o desiderato de criação das diretrizes e ações a que o Poder Público deve atender para a promoção, em última análise, do próprio direito à saúde e do direito à vida. Assim, mostram-se compatíveis com a própria Constituição.

A Constituição Federal indica a importância das ações e serviços em saúde (BRASIL, 1988, Art. 197), a serem realizadas de uma forma descentralizada e a que preze o atendimento universal da população. Ao mesmo tempo indica no próprio caput de seu Art.196 que as políticas públicas são uma forma que o Estado atua para garantir o próprio direito à saúde e que a vigilância epidemiológica e as ações atreladas à ela estão sim no regime de atribuições do SUS (BRASIL, 1988, Art. 200).

A vigilância epidemiológica, enquanto atribuição do Sistema Único de Saúde, na forma da sua caracterização constante no Artigo 6°, §2°, da Lei 8.080, garante uma fonte de contenção ou mesmo de prevenção quanto à saúde dos indivíduos e o campo da saúde pública de todo um Município, Estado ou País. Tem espaço tanto quando a saúde já encontra algum nível de alarme e assim a articular medidas epidemiológicas de contenção ou mesmo para que seja efetuado um controle prévio antes mesmo de atingir de forma grave e expressiva à saúde.

No caso específico da pandemia do Covid-19, para efeitos de exemplo, observa-se que as medidas adotadas tiveram esse dupla fonte de objetivos, agir tanto no controle, quanto em relação a um caráter preventivo.

Tratando eminentemente quanto às políticas públicas em saúde e as epidemiológicas a serem desempenhadas pelo Estado Brasileiro, no cerne do próprio SUS e a promover efetividade a saúde, cumpre também assinalar no que de fato constituem políticas públicas. A

incrementar-se até mesmo a atividade interpretativa em torno do Artigo11, inciso II, b, da Lei 13.709/2018.

O estudo e desenvolvimento quanto à área de políticas públicas vem em um esforço de compreensão das próprias ações governamentais e "como e por que os governos optam por determinadas ações" (SOUZA, 2006, p. 22).

No âmbito dos Estados Unidos, essa disciplina de estudo remete a mais do que apenas o olhar para a instituição formal do Estado, e há uma valorização desse debate após a Guerra Fria e o contexto de cientificidade a apurar e pautar as decisões estatais. Essa cientificidade, seria observada pela adoção de um viés racional que viria orientar as gerências e atuações do Estado[39] (SOUZA, 2006)

De acordo com essas ponderações, sintetiza-se no seguinte sentido,

> As políticas públicas têm sido criadas como respostas do Estado às demandas que emergem da sociedade e do seu próprio interior, sendo expressão do compromisso público de atuação numa determinada área a longo prazo. (CUNHA; CUNHA, 2003, p. 12)

Entre as diversas políticas públicas existem as denominadas políticas sociais, que assumem um relevo ainda maior perante a Carta Magna de 1988. O seu desenvolvimento está pautado na consecução de interesses públicos e voltada a execução de serviços públicos, estabelecidos na própria seara constitucional.

Estas políticas exteriorizam a articulação de uma cartilha de ações de um Estado, que vem, por outra sorte, refletir e orientar sua atuação em uma área específica, como é o caso da área da saúde (CUNHA; CUNHA, 2003, p.12).

Nesse sentido, entendendo a importância das políticas públicas no contexto normativo brasileiro e na estruturação do próprio SUS e de seu regime de competência, é imperioso compartilhar tal disciplina de ações estatais para a consecução da saúde, com os demais princípios e fundamentos que regem esse próprio sistema de saúde.

Como já apresentado, a prestação do serviço de saúde no cerne brasileiro pauta-se em uma gestão competente e descentralizada de forma política-administrativa, a focar em cada esfera de governo, com o desiderato de integralidade de assistência e universalidade nos

[39] Aqui se apresenta a grande influência desenvolvida pelo trabalho da Teoria dos Jogos no ambiente para as decisões quanto a guerra. Esta é desenvolvida e chega a permear até quanto a elaboração de políticas públicas estatais e, dentre elas as sociais. Seja pela confluência da matemática, ciência, informática, quer que seja a área e meio de conhecimento, a orientar o Estado a tomar a melhor decisão possível. (SOUZA, 2006, p. 22)

acessos. Foca então em uma regionalização e hierarquização dos serviços em saúde (Art.7°, inciso IX, alínea b, Lei 8.080/1990).

Como um dos pilares a que assenta esse dever de promoção universal da saúde, enfatizou-se o papel de dever estatal na elaboração da políticas públicas aptas a redução de doenças ou em ofertar um tratamento condizente com as enfermidades constatadas,

> Art. 2º A saúde é um direito fundamental do ser humano, devendo o Estado prover as condições indispensáveis ao seu pleno exercício.
> § 1º 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. (BRASIL, 1990a)

No bojo da própria lei federal quanto ao SUS, em vista ao cumprimento de seus desideratos e fundamentos, reivindica-se a necessidade de estabelecimento de um Sistema Nacional de Informações em Saúde, assim como a necessidade de informatização em tal setor (BRASIL, 1990b, Art.46 e 47).

Quanto ao sistema de informação em saúde, hoje exteriorizado através das tecnologias de informação correspondentes, sempre impele a primordialidade de que seja efetivamente desenvolvida uma interoperabilidade entre os dados que as compõem. Ou seja, que esses dados tenham a interação devida entre si e possam gerar uma gama de informação ao Poder Público, de forma completa e plena, a ser possível mapear o panorama real da saúde no país e desenvolver as ações estatais pertinentes.

A interoperabilidade na saúde revela-se como uma percurso hoje utilizado, e sinalizado desde a promulgação da Constituição de 1988 e da própria Lei 8.080/90 como já muito bem destacado, a fim da promoção tanto de uma maior garantia de acesso à saúde e facilidade no acesso às informações pertinentes para tanto, até mesmo no viés de uma tutela preventiva.

No entanto, esse processo de informatização das informações em saúde enfrenta uma embate central que gira em torno da promoção mais eficaz e afirmativa da prestação da saúde e ao outro lado da proteção mínima da privacidade, autodeterminação informativa e livre desenvolvimento da personalidade de tais titulares de dados.

Os Sistemas de Informação em Saúde (SIS) se utilizados de forma adequada são sim propensos a uma atuação mais assertiva do Estado no campo da promoção da saúde, na medida em que

> Partindo da ideia de que a informação em saúde possui uma dimensão estratégica, o aparto que envolve essas informações necessita estar a serviço de gestores que, por sua vez, precisam possuir pleno conhecimento do SUS, legislação, realidade epistemológica, assistencial, financeira, etc., para acompanhar, avaliar e talvez modificar o sistema de informação e, consequentemente, as principais decisões para melhora de saúde da população pela qual é responsável. Além disso, os SIS contribuem para a construção do saber, pois as informações, quando disseminadas, podem desenvolver o conhecimento, não só acadêmico, mas também popular, a partir do momento que podem sumarizar os dados de saúde da população e resultados de ações e programas de saúde. Assim, evidencia-se a necessidade de desenvolver sistemas disponíveis para acesso e uso ao público, com ferramentas que possam contribuir para otimizar a gestão assistencial prestada pelo Sistema Único de Saúde. (SANTOS; PEREIRA, SILVEIRA, 2017, p. 3)

Um aparato de informações apresentadas à partir de dados em saúde apurados e sistematizados contribui inegavelmente para decisões por parte dos gestores responsáveis, assim como os demais autores competentes, de forma mais acertada. Isso se deve justamente pelos dados aproximarem bem mais a compreensão da realidade tal qual ela é, a fim de que sejam desenvolvidas as políticas correspondentes e em tempo oportuno.

Essas informações são apuradas à partir do processo de coleta desses dados de cidadãos, mas que importantes e correlacionados ao setor da saúde. Posteriormente, os mesmos são tratados para que passem a integrar esses sistemas de informação, se relacionando, inclusive, com outra gama de dados semelhantes e também relevantes.

É valido asseverar precipuamente no que constitui o tratamento de dados, para que se possa perscrutar os limites atinentes a tal ato, quando dos dados sensíveis e, especificamente no caso do trabalho de pesquisa, os epidemiológicos. Assim, define a Lei Geral de Proteção de Dados Brasileira (BRASIL, 2018):

> 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; (BRASIL, 2018)

Portanto, como resta clara na normativa em destaque, até mesmo o mero arquivamento de um dado já resta abrangido na terminologia de tratamento e guarnece uma proteção legal.

Importante ambientar toda essa sistemática protecionista quando do Sistema Único de Saúde e desse desiderato de integralização e informatização de informações, previstos desde a regulamentação do SUS, e posto em prática ao longo dos anos de forma cada vez mais ferrenha.

Esse processo é natural, visto que não há como dissociar-se das relações e fenômenos tão presentes na sociedade. Ademais, apresenta-se como inegável a identificação de aspectos facilitadores no uso de tecnológicas para o cumprimentos de serviços públicos e preceitos tão importantes, como a vida e a saúde.

Quando da pandemia do Covid-19 observou-se de forma muito forte essa integração e informatização de dados e, especialmente, dos dados epidemiológicos na sociedade brasileira. Também quando desse lapso, ainda em vigência, surgiram dispositivos como o Conect SUS, bem como a estruturação de uma Rede Nacional de Dados em Saúde, por meio da Portaria de n° 1.424/2020, como desenvolvimento salutar de ferramentas no sentido da promoção de um sistema integrado de informação em saúde.

Outros mecanismos no âmbito da saúde e para a contenção de doenças como o *contact tracing*, a utilizar-se de meios tecnológicos para rastrear todos os cenários territoriais e possíveis interações que cada indivíduo teve, indicam a fluidez e invasividade que tais aparatos podem representar e a potencialidade de assumirem um condão abusivo no tocante à direitos fundamentais (TOBBIN; CARDIN, 2021, p. 132).

Nessa senda, no campo da saúde por inteiro verifica-se a interface das tecnologias, a produção de dados e, por consequência, a necessidade de incidir também a devida proteção. No campo epidemiológico, como uma das atividades também na consecução de um direito à saúde, também não é diferente.

Para tanto, as ferramentas hoje já existentes e os níveis de coleta e armazenamento de dados já geram a ímpar necessidade de se discutir os desdobramentos e os limites legais e éticos a considerar a lei de proteção de dados como um todo, com seus princípios e objetivos fundantes, para regular o compartilhamento passível de ser efetuado.

Referente a Rede Nacional de Dados em Saúde, assim como o próprio Conect Sus[40], vislumbrou-se que não são ferramentas perecíveis perante o controle do Covid-19, mas em plena manutenção e em expansão de utilização no território brasileiro. Essa Rede Nacional de Dados imprime a utilização de bancos de dados, sofisticado o suficiente para permitir o

[40] Quanto ao *Conect SUS*, foi objeto do Boletim 27, de agosto de 2022, a que objetiva-se sua expansão, com a integração as Unidades Básicas de Saúde, por intermédio do prontuário eletrônico (PEC e-SUS APS). Informação retirada de site oficial do DATASUS, em: https://datasus.saude.gov.br/reunioes-tecnicas-de-expansao-do-conectesus-e-destaque-do-boletim-de-conectesus-27/.

cruzamento de dados que o alimentam e fornecer informações em saúde concisas (MOHR, 2019, p. 67).

Essa Rede Nacional, como bem destaca o Ministério de Saúde, não se trata de um sistema de informação, mas da interface entre inúmeros sistema de informações setoriais, dentro do campo da saúde. A operar justamente na troca e integração de dados- a denominada interoperabilidade- entre esse inúmeros sistemas[41].

Para a consecução deste objetivo, conta com software específico a que garante um sistema duplo de cofre, a que integram seus bancos de dados, um localizado no Rio de Janeiro e outro em Brasília, que são alimentados com os dados atinentes a saúde[42].

Para a elaboração de políticas públicas, na forma da LGPD, esses dados em saúde e os dados epidemiológicos podem ser tratados e operacionalizados independentemente do consentimento de seu titular. Deve-se ter em mente sempre os limites a incidirem e disciplinarem tal permissiva, tendo por norte sempre a intepretação de forma a promover a compreensão sistêmica da Lei 13.709/2018 e a integração com os preceitos constitucionais.

A concessiva do Art. 11, inciso II, alínea b e do próprio Art.7°, inciso III, da Lei 13.709/2018 (BRASIL, 2018), devem ser contextualizadas e interpretadas com os demais dispositivos e com os princípios e objetivos da própria legislação em questão, assim como com a Constituição Federal. Essa ponderação interpretativa e integrativa da LGPD irá atuar na afixação da esfera de possibilidades e legalidade no compartilhamento entre dados sensíveis efetuado pela administração pública.

Neste ponto asseverado, valorosa pontuação parece oportuna para a compreensão do assunto:

> [...] Ocorre que é perfeitamente possível que haja, ao mesmo tempo, uma intervenção estatal em um direito fundamental e uma fundamentação para essa intervenção. Quando isso ocorre, não se está diante de uma violação a um direito fundamental, mas diante de uma restrição. Essa formalização, ilustra bem, portanto, o caráter não-absoluto dos direitos fundamentais e a centralidade do exame da fundamentação das restrições para a dogmática dos direitos fundamentais acerca de sua constitucionalidade (restrição permitida) ou inconstitucionalidade (violação). (SILVA, 2016, p. 16).

Assim, os dispositivo supracitados da LGPD instrumentalizam uma certa restrição a direitos fundamentais, precipuamente à proteção de dados e autodeterminação informativa. Mas

[41] Informações retiradas do site oficial do Ministério da Saúde, disponibilizadas em: https://www.gov.br/saude/pt-br/assuntos/rnds.

[42] Informação retirada da própria pina oficial do DATASUS e disponibilizada em: https://datasus.saude.gov.br/sobre-o-datasus/.

tal atuação legal funda-se no próprio direito constitucional à proteção de dados, que autoriza uma regulamentação legal, bem como na concepção de que não se trata de um direito absoluto.

A Lei 13.709/2018 revela uma série de princípios que balizam a aplicação de todos os dispositivos que a integram. Quanto aos princípios correspondentes, encontram-se disciplinados no Artigo 6° da referida legislação, e correspondem:

> I - finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;
> II - adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;
> III - necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;
> IV - livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;
> V - qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;
> VI - transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;
> VII - segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;
> VIII - prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;
> IX - não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;
> X - responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas. (BRASIL, 2018)

Dentre os princípios sublinhados acima, para os efeitos da questão quanto à limitação no tratamento independente de consentimento tal qual a permissiva do Artigo 11, inciso II, alínea b, há especial destaque para a finalidade, necessidade, adequação, transparência, segurança e a não discriminação.

Em verdade os princípios todos dialogam entre si e um acaba sendo uma extensão do outro, já que todos se coadunam com os objetivos centrais e os fundamentos[43] que tocam a Lei Geral de Proteção de Dados.

[43] Quanto aos fundamentos atinentes a Lei Geral de Proteção de Dados, estão exteriorizados no bojo de seu artigo 2°: “Art. 2º A disciplina da proteção de dados pessoais tem como fundamentos:

Veicula-se que à fim da promoção de um respeito mínimo à privacidade, ao livre desenvolvimento da personalidade e da autodeterminação informativa (Artigo 2°, incisos I, II e IV) a coleta o manejo de dados pessoais deve ser feito de acordo com o cumprimento estrito de uma finalidade legítima e legal, limitando-se ao mínimo necessário de invasão na esfera íntima das pessoas para perscrutar tal finalidade. Essa atividade deve ser realizada de uma forma transparente e segura, para que não haja o acesso por parte indivíduos não autorizados e não revestidos da devida permissiva.

O Artigo 26 da Lei 13.709/2019 reafirma a imperiosidade de que o compartilhamento de dados seja pautado estritamente na finalidade de execução de políticas públicas e, ademais, que seja vedado conferir acesso dessa base de dados a entidades privadas, salvo em exceções bem específicas (BRASIL, 2018).

Essas balizas que restringem um tratamento arbitrário e fora dos propósitos da legislação dialogam, em última análise, com a cláusula geral de proteção da dignidade humana (Artigo 1°, inciso III, da Constituição Federal de 1988). Portanto, objetivo central em fixar tais limites éticos é justamente na promoção de uma gerência humana quanto à própria vida e as informações que permeiam sua individualidade, para que consiga desenvolver livremente sua personalidade (KONDER, 2019, p. 447).

É necessário que sejam empregados meios e parâmetros técnicos digitais sofisticados e aptos[44] a combater eventuais tentativas não legítimas de acesso aos bancos de dados pessoais que se encontram sob a gerência do estado. Assim, à pautar toda a atividade de tratamento em relação aos dados pessoais, é primordial a consecução de uma segurança digital.

Quanto a este ideário de segurança a legitimar o uso de dados pessoais sensíveis, alerta-se para o processo de ampla informatização do campo da saúde no âmbito do Brasil. Tal qual, inclusive já destacado, no cenário brasileiro já contávamos com um Departamento de Informática do SUS desde o Decreto n°100 a que data de 16 de abril de 1991, no entanto, o

I - o respeito à privacidade; II - a autodeterminação informativa; III - a liberdade de expressão, de informação, de comunicação e de opinião; IV - a inviolabilidade da intimidade, da honra e da imagem; V - o desenvolvimento econômico e tecnológico e a inovação; VI - a livre iniciativa, a livre concorrência e a defesa do consumidor; e VII - os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais." (BRASIL, 2018)

[44] Sobre crises já verificadas quanto a dados em sede no Brasil nos últimos e que revelam uma certa fragilidade na promoção de tal ideário de segurança: "[...] No Brasil, ocorreram aproximadamente de 15 bilhões de ataques cibernéticos apenas nos três primeiros meses de 2020. Há um episódio em que os computadores do Hospital das Clínicas de Barretos sofreram ataques cibernéticos, paralisando temporariamente o funcionamento de alguns atendimentos. Isso, devido à falta de segurança na transmissão das informações, pouco cuidado ou a inexistência de chaves de acesso, permissividades diversas dos sistemas e aplicativos que fragilizam a guarda e troca de informações." (NOGAROLI, 2020, p. 47)

massivo destaque e propósito na digitalização e interoperabilidade dos dados em saúde é exteriorizado à partir do sistema da Rede Nacional de Dados em Saúde (RNDS)[45].

A Rede Nacional de Dados em Saúde entra em voga como uma iniciativa do próprio Departamento de Informática do SUS, através da Portaria de n° 1.434 do ano de 2020. Segundo as próprias informações oficiais do Ministério de Saúde, inicialmente estava sendo desenvolvida de forma paulatina e por meio de um projeto piloto no estado de Alagoas em março de 2020, mas em virtude da pandemia covid-19 essa rede foi implementada a nível nacional à fim de trazer o compartilhamento dos dados relacionados a contenção viral[46].

O questionamento muito suscitado é se essa expansão para âmbito nacional, por ocasião da pandemia situacional, não ocasionou a utilização sem a devida preparação de tal sistema. E ademais, nesse mesmo contexto estava entrando em vigor da Lei Geral de Proteção de Dados brasileira.

A entrada em vigor dessa Rede Nacional de Informação em Saúde, mesmo que em primórdio de forma não tão concisa e mais direcionada à dados epidemiológicos e de vacinações, bem como sua utilização alavancada em nível nacional sem o perpasse pleno pela fase de testes, coadunada com o surgimento de uma nova lei a regular a questão da proteção de dados, mostrou-se um tanto quanto digna de cautelas e das considerações devidas.

Nesse cenário, as notícias de um ataque hacker aos sistemas de informação adstritos ao Ministério da Saúde colocam em suspenso esse ideário principiológico de segurança que deve nortear o tratamento de dados pessoais, segundo a própria Lei Geral de Proteção de Dados. Em dezembro de 2021[47] houve a notificação de um ataque cibernético, já em 17 de maio de 2022 houve anúncio de, agora apenas, tentativa de acesso as plataformas do *Conect* SUS, e-SUS Notifica[48] e SI-PNI[49].

---

[45] Informações consultadas do site oficial do Ministério de Saúde: https://www.gov.br/saude/pt-br/assuntos/rnds.

[46] "A implementação da RNDS se daria a partir de março de 2020, com o projeto piloto, em Alagoas. No entanto, com o Covid-19, o projeto foi redirecionado para receber e compartilhar informações que pudessem dar o devido suporte para cidadãos e profissionais da saúde no combate ao coronavírus. Dessa forma, o Ministério da Saúde, com apoio dos laboratórios públicos e privados, permitirá a recepção e o compartilhamento dos resultados dos exames relacionados ao Covid-19." (FANTONELLI; CELUPPI; OLIVEIRA; BURIGO; DALMARCO; WAZLAWICK, 2020, p. 169)

[47] Informação encontrada no site da CNN, In: https://www.cnnbrasil.com.br/saude/sistemas-do-ministerio-da-saude-estao-fora-do-ar-apos-tentativa-de-invasao/.

[48] O e-SUS notifica trata de um sistema de registro de casos suspeitos de síndrome gripal leve, suspeitos e confirmado do Covid-19, segundo informações do próprio Ministério da Saúde. *In*: https://datasus.saude.gov.br/notifica/

[49] O Ministério da Saúde elenca que o objetivo principal do sistema SI-PNI é o de alertar quanto a possível ocorrência de surtos ou epidemias, à partir do quantitativo de "imunos" aplicados e da população efetivamente vacinada. Informação disponibilização em: http://pni.datasus.gov.br/#

Esses ataques evidenciam uma certa fragilidade de tais sistemas empregados pelo Ministério da Saúde e uma não total adequação aos ditames da Lei Geral de Proteção de Dados. No momento em que a LGPD prevê em seu Artigo 6°, inciso VII, que a segurança é um dos princípios estruturantes e legitimadores de qualquer atividade de tratamento de dados pessoais, esse ideário deve ser efetivado, sob pena de deslegitimação na continuidade de tais operações informatizadas.

No âmbito do site oficial do Ministério da Saúde há um claro destaque para o fato de que a Rede Nacional de Informação em Saúde não se trata de um sistema de informação, mas de um meio, de uma ferramenta para proporcionar a integração entre inúmeros sistemas de informação. Intenta conferir uma interoperabilidade entre os dados em saúde, com a interação entre os dados de diversas localidades e contextos do Brasil, a proporcionar uma melhor resposta Estatal no campo da saúde e no campo da articulação das políticas públicas correspondentes.

O entendimento da interoperabilidade nessa plataforma de Rede Nacional de Dados é exteriorizado por meio da Portaria de n. 1.434/2020, a que apresenta-se a subdivisão da terminologia em duas distintas: interoperabilidade semântica e interoperabilidade prática. No que constaria cada uma delas, o Artigo 232, incisos III e IV da Portaria supracitada informam,

> III - interoperabilidade semântica: a adoção, conforme contexto de uso, de técnicas de modelagem de informação, modelos de informação e uso de vocabulário padronizado, como terminologias, classificações, taxonomias e ontologias, que garantam o entendimento humano de uma estrutura de informações; e
> IV - interoperabilidade sintática: a adoção de modelos e técnicas computacionais que garantam a capacidade de troca de informações padronizadas entre diferentes sistemas, redes e plataformas de informação e comunicação, assegurando o entendimento computacional por todos os envolvidos e a correta conversão para linguagem humana, sem perda ou mudança no significado e contexto da informação. (BRASIL, 2020)

Quantos aos parâmetros nacionais[50] de interoperabilidade é que o texto legal informa que serão divulgados no site oficial do Ministério de Saúde, a que também garante aos Estados

[50] Quanto ao parâmetro utilizado pelo Brasil, a título de informação: "A RNDS, nesse sentido, conforme mencionado optou por utilizar o padrão HL7 FHIR. O Datasus explica que esse padrão é rápido, flexível, gratuito e de ampla adoção mundial. A especificação HL7 FHIR tem como propósito redução dos empecilhos para interoperar em larga escala eliminando os silos de informações geradas pelos sistemas de registro eletrônico em saúde.
Visualizando os desafios para a implementação do padrão HL7 FHIR podemos apontar a questão a adoção como a principal, já que o padrão em si suporta nativamente o Protocolo RESTful que é padronizado em todo o mundo. O padrão, em si, oferece uma série de vantagens, mas na prática a sua implementação é mais complexa por requerer uma adaptação que demandará tempo e necessitará de um suporte substancial às organizações,

e Municípios a possibilidade de utilização de padrões diferenciados, desde que tal proceder não ponha em risco a possibilidade de interoperabilidade nacional (BRASIL, 2020).

Uma conjuntura problemática é o fato de que a própria Rede Nacional de Dados em Saúde ainda não está totalmente implementada. Assim difícil é, *a priori* de sua plena implementação, definir de forma clara os limites éticos e legais, a ser congruente com os ditames da Lei Geral de Proteção de Dados.

Segundo as informações oficiais do governo[51], a expectativa é de que a plena implementação do RNDS apenas se operacionalize em 2028. Portanto, ainda não é possível calcular e precisar todas as demais imbricações desse sistema e os aspectos problemáticos quanto a preservação mínima de um direito à privacidade e autodeterminação informativa.

Ao que já temos hoje em vigor, relacionado a esta Rede Nacional de Dados em Saúde, o Ministério da Saúde publicou cartilha a indicar as operações à conformar tal tecnologia com a Lei Geral de Proteção de Dados (FANTONELLI; CELUPPI; OLIVEIRA; BURIGO; DALMARCO; WAZLAWICK, 2020, p. 169).

Dentre essa cartilha de ações há a previsão de elaboração de Relatório de avaliação de conformidade pelo Núcleo LGPD- este tendo sido criado pela Portaria DATASUS de 22/11/2019-, criação de um subcomitê de governança de dados, assim como estudos periódicos quanto a devida conformidade, bem como o desenvolvimento de um projeto de cooperação internacional entre Brasil e Reino Unido[52].

Na própria cartilha também vem descrevendo a forma de acesso aos dados realizadas pelos sistemas sintetizados na RNDS, a que intenta demonstrar o fidedigno compromisso com a segurança e uma busca autorizada apenas em cumprimento de uma finalidade específica. Tal proceder é bem sintetizado nas linhas abaixo,

> Quanto aos aspectos de segurança da RNDS, ressalta-se que os Dados de Saúde serão coletados, processados e armazenados de acordo com os padrões de confidencialidade e segurança proporcionais à sua sensibilidade.
> [...]
> Todos os acessos aos dados são rastreados, ou seja, a RNDS é capaz de identificar de forma inequívoca que dado foi acessado, por qual profissional e em que estabelecimento de saúde se deu a consulta e quando (data/hora) essa consulta foi realizada. A RNDS também é capaz de rastrear a origem de todo

prejudicando a adoção mundial." (FANTONELLI; CELUPPI; OLIVEIRA; BURIGO; DALMARCO; WAZLAWICK, 2020, p. 170)

[51] Informação constante no site oficial do Ministério de Saúde, In: https://www.gov.br/saude/pt-br/assuntos/rnds.

[52] Informações retiradas da própria cartilha editada pelo Ministério da Saúde, sob o título: "Ações para a adequação da RNDS à Lei Geral de Proteção de Dados". (REDE NACIONAL DE DADOS EM SAÚDE, 2020).

> documento exposto no Portal Conecte SUS[53]. (REDE NACIONAL DE DADOS EM SAÚDE, 2020, p. 3)

Seguindo nessa análise se compatível o tratamento de dados em saúde com o princípio da segurança, observa-se que o acesso dos mesmos pelos gestores, autoridades, pessoas consideradas legítimas por integrarem a articulação da saúde a nível municipal, estadual e federal, deve ser feita por meio de certificado digital. Este certificado é emitido pelo cadastro por tal autoridade e viabilizado pela ferramenta do Gov.Br.

> Como medida de segurança adotada pela RNDS revela-se a instituição da certificação digital para acesso aos dados de saúde. O Certificado Digital é o documento eletrônico que possibilita a troca segura de informações entre duas partes, com a garantia da identidade do emissor e a integridade da mensagem. Para isso, são geradas duas chaves de criptografia: uma pública e outra privada. A chave pública fica em posse do estabelecimento e é utilizada para assinar, enquanto a privada é utilizada para verificar a integridade e autenticar o documento. Essa chave compõe um sistema de criptografia assimétrica, onde os dados só conseguirão ser acessados se o receptor tiver a chave correta para decodificá-los. Essas duas chaves são geradas aleatoriamente por funções matemáticas e trabalham em conjunto. Aderente À LGPD, todo acesso realizado ao RNDS é identificado pelo Certificado Digital e todos os dados enviados ao RNDS é identificado pelo Certificado Digital e todos os dados enviados ao RNDS serão assinados e o cidadão tem a opção de não autorizar o uso desses dados. (FANTONELLI; CELUPPI; OLIVEIRA; BURIGO; DALMARCO; WAZLAWICK, 2020, p. 169)

Sem sombras de dúvidas, por tudo enquanto exposto, há o esforço no desenvolvimento de ações governamentais de forma compatível com consecução dos princípios e objetivos fundantes da LGPD. Mas, ainda constam algumas questões problemáticas que colocam em evidência preocupações reais e relativas ao nível de risco e lesividade que o manejo de dados pessoais pode propiciar.

A ainda não plena implementação dessa Rede Nacional de Dados -que em sua prematuridade já veio a sofrer ataques a colocar em relevo se de fato seus softwares e tecnologias são seguros-, assim como a pendência ainda na fixação dos padrões técnicos nacionais de interoperabilidade de forma mais atualizada, revelam um diagnóstico ainda não totalmente desejável quanto a implementação plena dos preceitos da LGPD.

No tocante aos padrões de interoperabilidade, a Portaria n. 1.434/2020 apenas indicou que seriam apresentados no site oficial do Ministério da Saúde. No site em questão, a busca remete a aplicação da Portaria n.2.073 de 31 de agosto de 2011.

[53] Documento da própria cartilha de ações para a adequação da RNDS à Lei Geral de Proteção de Dados. (REDE NACIONAL DE DADOS EM SAÚDE, 2020).

Ao ter a última disciplina em data anterior a própria Lei Geral de Proteção de Dados e da instituição e sistematização de princípios e normas que devem nortear os padrões atinentes, assim como em recorte temporal bem distante do contexto nacional hodierno de informatização em saúde e do contexto de uma rede nacional de dados.

Esses padrões de interoperabilidade atualizados, diante da ausência da atuação do Ministério da Saúde, pode ser efetuado pela própria Autoridade Nacional de Dados, que detém um papel salutar na defesa desses interesses e a indicar o caminho da própria interpretação e dos limites interpretativos concernentes aos dispositivos que integram a Lei Geral de Proteção de Dados.

Essa Autoridade detém a possibilidade de editar normas complementares justamente nesse sentido de orientar a correta aplicação e interpretação dos ditames da LGPD. Esse seu poder de edição de regulamentos correspondem também na indicação dos meios e parâmetros técnicos mais adequados aos ditames legais.

Sua atuação, a que será melhor abordada no capítulo posterior, compreende não só um viés fiscalizatório, como também elucidativo e pedagógico. Este caráter poderia ser exteriorizado, por exemplo, através de uma cooperação técnica com o Ministério da Saúde no próprio desenho e fixação quanto aos parâmetros técnicos atualizados a serem adotados.

4 AS BALIZAS AO TRATAMENTO INDENPENDENTE DE CONSENTIMENTO E A ATUAÇÃO DA ANPD

O Tratamento independente de consentimento de dados pessoais sensíveis é um processo legal e válido reconhecido explicitamente pela Lei Geral de Proteção de Dados (Lei 13.709/2018), especificamente em seu Artigo 11, Inciso II.

A viabilidade de tal previsão pauta-se inicialmente na noção de que o direito à privacidade, à autodeterminação informativa e à proteção de dados não são direitos que detém caráter absoluto. Ante ao reconhecimento de que não tratam-se efetivamente de direitos absolutos, cabe a imposição de eventuais restrições, mediante um juízo de ponderação, e de acordo com os princípios de razoabilidade e proporcionalidade, para que outros direitos também de ordem constitucional tenham a referida tutela.

No campo a que discute-se as restrições à direitos fundamentais e a forma legítima para que tal sistemática possa ser válida e constitucional, cabe algumas sucintas considerações. Primeiro se alerta para o fato de que nem tudo se trata de restrições efetivas à direitos fundamentais, algumas normas apenas apresentam um caráter meramente delineador de tais direitos, se destinando a explicar sua esfera de alcance e em vias a possibilitar sua concretude (SARLET; MARINONI; MITIDIERO, 2020, p. 504).

No entanto é inegável que, por vezes, temos normas, sejam legais ou mesmo constitucionais, que apresentam disposições que tem como consequência uma certa limitação a algum direito fundamental. Aqui se põe em prospecto tal questão, vez que inegável é que a Lei Geral de Proteção de Dados e especialmente o seu Artigo 11 apresenta uma limitação à direitos constitucionais e fundamentais reconhecidos no sistema brasileiro, tal qual à proteção de dados (BRASIL, 1988, Art.5°, LXXIX), à privacidade (BRASIL, 1988, Art.5°, X), autodeterminação informativa e mesmo o livre desenvolvimento da personalidade.

Segundo as pontuações erigidas pela doutrina, há reservas para legitimar limitações à direitos fundamentais. Assim teríamos que,

> No que diz respeito às limitações, registra-se substancial consenso quanto ao fato de que os direitos fundamentais podem ser restringidos tanto por expressa disposição constitucional como por norma legal promulgada com fundamento na Constituição. Da mesma forma, há quem inclua uma terceira alternativa, vinculada à possibilidade de se estabelecerem restrições a direitos por força de colisões entre direitos fundamentais, mesmo inexistindo limitação expressa ou autorização expressa assegurando a possibilidade de restrição pelo legislador. (SARLET; MARINONI, MITIDIERO, 2020, p. 504).

O Artigo 11, inciso II, da Lei Geral de Proteção de Dados nada mais viabiliza do que restrições pontuais aos direitos fundamentais de proteção de dados, privacidade e autodeterminação informativa sem, sobretudo, retirar o seu núcleo essencial. As restrições erigidas são em função de hipóteses que refletem puramente interesses públicos e apenas se tornam viáveis quando o tratamento sem consentimento for indispensável para a consecução de tal interesse.

No caso a que se funda a análise precípua deste trabalho, quer seja o tratamento independente de consentimento para a elaboração de políticas públicas epidemiológicas (BRASIL, 2018, Art. 11, II, b) fica explícito que o interesse público em questão envolve a tutela de um direito à saúde de forma mais eficaz, articulada e direcionada. Há a flexibilização da proteção de dados constitucional, em virtude de uma colisão eventual com a promoção plena do direito à saúde, que se afigura com um dever do estado e um direito fundamental previsto no Artigo 196 da Constituição Federal de 1988.

Este artigo em questão, inclusive, dita que a forma que este direito será alcançado inclui a instituição de políticas públicas e econômicas. Análise reafirmada no contexto do artigo 2° da Lei 8.080/1990, sendo esta legislação a que versa quanto ao Sistema Único de Saúde.

O desenvolvimento de políticas públicas epidemiológicas, que podem vir a utilizar dados pessoais de indivíduos do território brasileiro independente de seu expresso consentimento, tem como objetivo basilar justamente essa redução e controle de doenças nos seus variados graus de dispersão. Destina-se a conjugação de medidas quando as eventuais doenças ainda se verificam em casos pontuais, em endemias, ou mesmo em nível de pandemias, como recentemente o mundo verificou no caso do Covid-19.

A viabilidade e a necessidade da articulação de tais serviços no campo do sistema de saúde se desprendem além do supracitado Artigo 196, também do Artigo 200 da Constituição Federal (BRASIL, 1988) e que disciplina as ações de vigilância epidemiológica e sanitária incluídas entre as atribuições do Sistema Único de Saúde.

Voltando a tratar da possibilidade ou não de restrições à direitos fundamentais, ressalta-se que na própria ponderação acima aduzida (SARLET, MARINONI, MITIDIERO, 2020, p. 504), é indicado que esse processo de limitação seria válido quando também da hipótese de norma legal com fundamentação na própria Constituição. Em outras palavras, seria válido uma norma legal e infraconstitucional, regular e eventualmente trazer alguma restrição à direito fundamental, quando retira da própria Carta Constitucional o fundamento dessa atividade.

Assim, realça-se a disposição contida no Artigo 5°, inciso LXXIX[54] que prevê justamente no texto constitucional a autorização para que lei regulasse, de forma específica e comportando as inúmeras singularidades da matéria, esse direito fundamental à proteção de dados.

Portanto, há uma clara autorização constitucional para a regulação do direito, "nos termos da lei". Sendo assim, se enquadra no considerando que indica a legitimidade de eventuais restrições à direitos fundamentais na forma de lei, quando esta retira seu fundamento de validade da própria Constituição Federal.

A lei em questão se trata da Lei Geral de Proteção de Dados, justamente esta que detém em seu bojo o famigerado Artigo 11 e que veicula uma flexibilização do direito à proteção de dados sensíveis, mas sem se distanciar de um viés legítimo e da preservação de seu núcleo essencial.

À partir de uma análise constitucional não há óbices a uma regulação do direito à proteção de dados com a afixação de limitações em situações específicas. Estas situações, em que pese expressarem a baliza na defesa de outros direitos também constitucionais, autorizam uma flexibilização a ser realizada com a devida cautela e de acordo com os juízos de proporcionalidade e razoabilidade.

> No entanto, não parece contraditório proteger dados sensíveis e, por outro lado, autorizar a sua utilização em situações legítimas diante do valor social da informação. A própria noção contemporânea da privacidade encontra o seu fundamento na inserção da pessoa na sociedade, não mais em uma prerrogativa de isolamento. Em que pese o estabelecimento de um standard protetivo mais rigoroso para os dados sensíveis, a ampla vedação ao seu tratamento se coloca na contramão das diversas utilidades às quais eles podem servir. Restringir desproporcionalmente o tratamento de dados sensíveis, nesta direção, acabaria por inviabilizar várias atividades socialmente relevantes, a exemplo de instituições políticas, religiosas, de saúde, entre outras, que não prescindem do tratamento de dados de natureza sensível. (KORKMAZ, 2019, p. 76).

A restrição à direitos fundamentais é sempre embasada nesse pressuposto de preservação de seu núcleo essencial. Observa-se de pronto a dificuldade de se precisar em termos claros e, à primeira vista, o que constitui o núcleo essencial de cada direito fundamental.

[54] Art. 5°, LXXIX, da CRFB/88: "é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais." (BRASIL, 1988)

Na perspectiva da teoria absoluta[55] o núcleo essencial de um direito não é alterável perante seus desdobramentos práticos, ou seja, perante as inúmeras casuísticas no mundo dos fatos, mas se trata daquilo que legitima a própria existência de tal direito enquanto direito. No tocante a teoria relativa[56], essa definição é mais fluída e delineada perante a aplicação prática de tal direito fundamental, em meio aos dilemas com outros direitos fundamentais na prática concreta.

Ambas as teorias são um esforço nesse desiderato em definir o que consta de fato como o núcleo essencial de direitos e à partir de tal delimitação possibilitar uma demarcação da área a que não caberia uma ingerência e flexibilização[57], sob pena de esvaziar de sentido a existência do próprio direito em questão.

> As duas vertentes ancoram-se sobre uma imagem bipartida dos direitos fundamentais. Projetam-se dois círculos concêntricos, os quais se reportam a um lócus inatingível e um espaço de possível atuação legislativa. [...] ao círculo interior pertencem condutas mínimas, enquanto que o exterior consiste no espaço de deliberação democrática. A área não nuclear é a face principiológica dos direitos fundamentais, enquanto que o centro corresponde a um conteúdo de regra, possuidor de uma eficácia normativa, traduzido por uma proibição de intervenção. (TRAVINCAS, 2010, p. 130).

Sob esse esforço quanto a identificação do centro e polo de não intervenção, nas colocações de Amanda Thomé Travincas (2010), é que há um afastamento entre estas teorizações,

> [...] A diferença está no momento do esboço: enquanto no segmento das teorias absolutas isto se dá em abstrato, para as teorias relativas esta imagem é refeita a cada colisão entre direitos fundamentais. Sempre há um conteúdo atingível e outro não, embora entre uma e outra linha de argumentação penda uma diferença substancial entre a circunstância e a forma de fixa-los. (TRAVINCAS, 2010, p. 130).

---

[55] Para a teoria abstrata segundo a análise de Amanda Thomé em sua Dissertação, o conteúdo essencial de um direito e, portanto, aquele a qual não seria válido uma ingerência e flexibilização, seria: "O essencial de um direito é algo como um consenso sobre um domínio sem o qual a norma desfigura-se, deixa de ser compreendida enquanto tal." (TRAVINCAS, 2010, p. 129)

[56] Quanto a teoria relativa a análise é diametralmente oposta da teoria absoluta e essa definição do núcleo essencial é feita segundo: "[...] a esfera irredutível dos direitos fundamentais só se define concretamente. É a ameaça iminente de desfiguração da norma que especifica o que não pode ceder em face de atos restritivos." (TRAVINCAS, 2010, p. 129)

[57] No tocante ao núcleo essencial de cada direito, segundo Ingo Sarlet (2018, p. 116), esse núcleo é comparado, em analogia, as cláusulas pétreas, justamente por fazer referência a uma área que delimita e impede uma inferência estatal. Ademais, também pontua que o núcleo essencial de cada direito fundamental é diferenciado e concernente as singularidades próprias daquele direito.

Com a filiação em uma teoria relativa, reconhece-se que a área essencial dos direitos fundamentais é viabilizada perante eventuais embates com outros direitos fundamentais e, neste juízo, especial vigor detém a atividade de ponderação e de edição de leis impregnadas de um critério de proporcionalidade e razoabilidade[58]. Ademais, alinha-se com a proteção de tal centralidade quanto ao direito em uma linha subjetiva, visto que o que almeja-se resguardar não é apenas a textualidade da norma, mas os direitos subjetivos que imprimem e são afetos aos indivíduos (TRAVINCAS, 2010, p. 131).

A análise sob a Lei 13.709/218 indica que não há um empreendimento em esvaziamento de direitos, especialmente quando se fala no direito à proteção de dados, à autodeterminação informativa, bem como à privacidade, os quais regulam a legislação em caráter central. Em verdade a legislação indica uma série de objetivos e princípios que caminham no sentido de afirmação de tais direitos fundamentais e ainda os prefixa como seus fundamentos basilares (BRASIL, 2018, Art.2°).

Outrossim, fixa uma série de critérios para viabilizar o tratamento de dados e, ao mesmo tempo, incide um microssistema de proteção amplo, fato este verificado pela notória abertura terminológica do termo tratamento (BRASIL, 2018, Art. 5°, X) a abranger as diversas atividades em interface com os dados pessoais.

Ao vivermos em uma sociedade informacional a que as tecnologias já se encontram impregnadas na vida humana e nas instituições políticas e sociais, assim como o direito à proteção de dados não imprime uma vedação e abstenção total em qualquer tipo de tratamento de dados, há previsão na Lei Geral de Proteção de Dados das diretrizes que irão imperar no desenvolver dessa atividade de tratamento.

A diretriz máxima garante um tratamento perante um prévio consentimento do titular do dado, em vias a asseguração da denominada autodeterminação informativa. Porém em situações bem específicas, prevista no próprio texto da lei e sob um finalidade também bem específica, há a possibilidade do tratamento independente de consentimento, conforme expõe o seu Artigo 11, inciso II.

Essa possibilidade de tratamento independente de consentimento não haveria de induzir a reflexiva de que se estaria minando o núcleo essencial dos direitos fundamentais à proteção de dados, à privacidade e autodeterminação informativa. Tal possibilidade legal não encontra-se desconexa dos demais princípios a que constam na própria Lei 13.709/218 e que remetem a necessidade da consecução de transparência, segurança, finalidade e adequação.

Ademais, não fulmina o conteúdo essencial dos direitos fundamentais em questão, ao tratar de hipóteses taxativas e em vias à afirmação de interesse público e de outros direitos também reconhecidos e garantidos constitucionalmente. O que se exerce é um juízo de ponderação e proporcionalidade a sopesar tais emblemas, de forma a não operacionalizar e instituir legalmente nenhuma agressão total a nenhum direito fundamental e a que reivindica, portanto, a devida constitucionalidade da legislação.

> Tendo seguindo separados, os dois juízos- o de proteção do conteúdo essencial e o de proporcionalidade- encontram-se num ponto tal, a partir do qual seguem sendo a mesma coisa: a lei proporcional sempre respeita a essência dos direitos. Seguindo por essa via, se bem que se considere a proteção do conteúdo essencial como método autônomo, na prática ela invariavelmente converte-se na ponderação que lhe dá suporte. Sua função é, aqui, mais simbólica que substancial, servindo para realçar algo que, ademais, anda necessariamente junto à noção de restrição, a saber, que a atuação estatal não pode resvalar no desaparecimento dos direitos ou num puro "nominalismo dos preceitos constitucionais." (TRAVINCAS, 2010, p. 129-130)

Seguindo essa proposta da proporcionalidade e na afixação de esferas rígidas para o tratamento independente do consentimento, justificadas pelo requisito da finalidade e na defesa de outros direitos também constitucionais, a Lei 13.709/2018 cumpre o propósito constitucional de assegurar o direito à proteção de dados.

O assegurar o direito fundamental é feito de forma constitucional ao reconhecer que, por não se tratar de um direito absoluto, cabe em sua flexibilização a devida ponderação e influência dos princípios da razoabilidade e proporcionalidade.

Assegurado o direito à proteção de dados na forma da lei específica, de acordo com o que o próprio artigo 5°, LXXIX, da CRFB/88 explicita, é importante suscitar o papel da Autoridade Nacional de Proteção de Dados, seu aspecto regulador e como se situa perante as limitações atinentes ao conteúdo e aplicação do Art. 11 da Lei 13.709/2018, especialmente no que toca ao seu inciso II.

4.1 O PAPEL FISCALIZATÓRIO ESTATAL E NO ESTABELECIMENTO DE UMA POLÍTICA PROTETIVA DE DADOS CONCISA

A Autoridade Nacional de Proteção de Dados (ANPD) é instituto disposto na própria Lei Geral de Proteção de Dados sob a forma de uma autarquia de natureza especial, segundo contempla o Artigo 55-A da Lei 13.709/2018. Na própria lei constam diversos dispositivos que

disciplinam suas incumbências nesse sistema protetivo, destaca-se o Artigo 55-J que apresenta sua rede de competências.

Entre a sua extensa lista de atribuições, destaca-se o seu caráter eminentemente fiscalizador da aplicação dos termos da legislação quando a matéria da proteção de dados (Art.55-J, IV), com a elaboração de políticas de conscientização popular (Art.55-J, VI), recebimento de reclamações (Art.55-J, XXIV, V, XXI), celebração de termos de compromisso, em buscas de cessação de eventuais irregularidades na aplicação da lei (Art.55-J, XVII). Assim como a incumbência de aplicação de eventuais sanções (Art.55-J, IV) e a edição de regulamentos e orientações atinentes a uma correta aplicação dos ditames legais (Art.55-J, XIII e XVIII).

A instituição de tal autarquia contempla precipuamente um caráter fiscalizador do cumprimento devido, nas inúmeras operações de dados que circulam em um país com a dimensão do Brasil, e a que os objetivos, princípios e parâmetros da Lei Geral de Proteção de Dados sejam devidamente seguidos[59].

A Agência Nacional de Proteção de Dados exterioriza um papel claro a ser assumido pelo Estado em não tolher as inovações tecnológicas e seu desmembramentos, mas a resguardar o mínimo de ordem e de preservação dos direitos à privacidade e à personalidade dos indivíduos e usuários de tais ferramentas (MOHR, 2019, p. 47).

A interface entre os dados, seu tratamento e a movimentação da economia capitalista hodierna já foram muito bem destacados durante todo este presente trabalho. Nessa seara, conclui-se que não seria compatível ou esperado do Estado Brasileiro assumir uma posição retrógrada e arcaica de tentar frear totalmente o uso de dados e dos meios tecnológicos no seio social.

Mas há que destacar que deve dar o devido realce a atividade de tratamento de dados, enquanto eminentemente de risco e, assim, assumir a postura compatível e cerceadora de possíveis arbitrariedades. Na esteira da busca do livre desenvolvimento econômico, conforme indica o Art.170 da CRFB/88, há que buscar uma compatibilização com os demais dispositivos da mesma Carta Constitucional, a que sinalizam como fundamento da República o princípio da dignidade da pessoa humana (Art. 1°, III, CRFB/88), assim como tem como objetivos a

[59] Sobre o papel de definição e de tornar claro o conteúdo do regime protetivo de dados pela Autoridade Nacional de Proteção de Dados: "[...] A ANPD deve atuar como facilitadora entre empresas, cidadãos e governo, promovendo medidas que difundam a cultura de proteção de dados no Brasil, tornando as previsões da LGPD mais claras, acessíveis e palatáveis, tanto para os titulares de dados quanto para os agentes de tratamento." (PÉRET MOTTA, 2022, p.61-62).

promoção do bem de todos e a construção de uma sociedade livre, justa e igualitária (Art.3°, I e IV, CRFB/88).

Portanto, o desenvolvimento econômico e social devem ser perquiridos, sem olvidar dos outros princípios e direitos fundamentais que integram o catálogo da Constituição da República de 1988 e as próprias raízes fundantes do Estado de Direito[60].

O compartilhamento e tratamento de dados tendo reflexos na economia é algo inegável. Porém, cabe assinalar que no tocante ao tratamento de dados pessoais em saúde há uma série de restrições, instrumentalizadas pelas normas do Artigo 11, §§ 4° e 5°, justamente em virtude da sensibilidade dos mesmos.

> § 4º É vedada a comunicação ou o uso compartilhado entre controladores de dados pessoais sensíveis referentes à saúde com objetivo de obter vantagem econômica, exceto nas hipóteses relativas a prestação de serviços de saúde, de assistência farmacêutica e de assistência à saúde, desde que observado o § 5º deste artigo, incluídos os serviços auxiliares de diagnose e terapia, em benefício dos interesses dos titulares de dados, e para permitir:
> I - a portabilidade de dados quando solicitada pelo titular; ou
> II - as transações financeiras e administrativas resultantes do uso e da prestação dos serviços de que trata este parágrafo
> § 5º É vedado às operadoras de planos privados de assistência à saúde o tratamento de dados de saúde para a prática de seleção de riscos na contratação de qualquer modalidade, assim como na contratação e exclusão de beneficiários (BRASIL, 2018)

A prescrição do parágrafo 3° do Artigo 11 da lei em questão já direciona que o compartilhamento de dados sensíveis com a finalidade econômica pode ser objeto de regulamentação e vedação por parte da própria ANPD. Quanto a este parágrafos subsequentes, explicitados acima, consubstancia no próprio texto da lei vedações concisas ao campo de compartilhamento de dados em saúde a incompatibilizar com uma acepção monetária, a não ser apenas em casos bem pontuais e específicos.

Nesse sentido, quando tratar-se de serviços de assistência de saúde e farmacêutica, a englobar diagnoses e terapias é que seria legítimo esse compartilhamento, desde que observada a finalidade precípua de ser o melhor interesse à saúde e ao bem do titular do dado. Esse compartilhamento só seria possível, no estrito cumprimento da finalística de quando da

[60] "O papel do Estado na proteção de dados não se resume a visão protecionista da liberdade, da privacidade e o livre desenvolvimento da personalidade da pessoa natural, senão tem o condão de estabelecer uma política sólida de regulamentação, aliando a tutela pretendida ao desenvolvimento econômico e o progresso tecnológico." (MOHR, 2019, p. 52)

portabilidade de dados solicitada pelo próprio titular do dado ou quando referente a transações financeiras e administrativas referentes a estes serviços em saúde citados[61].

Não seria legal o fim eminentemente monetário no acesso e manejo de dados em saúde, especialmente no que toca aos planos de saúde e as discriminações oportunas as contratações dos planos de assistência, conforme adiciona o parágrafo 5° do Artigo 11.

Quanto aos compartilhamentos de dados em saúde que não tenham por desiderato esse sentido monetário, a lei faz a permissiva que a administração pública realize tal empreendimento quando visto a necessidade para o desenvolvimento adequado de políticas públicas (BRASIL, 2018, Art.7°, inciso III) e atenta a escrutínio de um interesse público, com a vedação em regra do compartilhamento com terceiros particulares (Art.23 da lei em questão).

Revelam muito da estrutura desse sistema protetivo e do papel salutar que essa autoridade nacional vem desempenhar, quando nessa perspectiva de compartilhamento de dados sensíveis no cerne da LGPD há um notório papel de destaque a ser efetuado pela ANPD (Art.11, §3°). Papel esse que aduz não apenas uma fiscalização quanto às operações de tratamento de dados, como até mesmo um caráter normativo complementar à orientar e elucidar o claro entendimento e implementação dos termos da lei.

No âmbito do papel fiscalizador, instrumentaliza uma incumbência estatal através da autarquia de proteção de dados, visto que não seria oportuno e administrável que todos as transgressões em matéria de dados pessoais só fossem tratadas no campo repressivo e em uma via judicial.

Apenas a análise judicial levaria a uma inegável insegurança quanto à devida interpretação e aplicabilidade dos termos da normativa referentes a matéria, à considerar também que ainda recente no país a legislação protetiva e desconhecida a inúmeros setores da sociedade. Outrossim, iria despender um abarrotamento do judiciário e uma ineficiência prática no devido cumprimento da lei, bem como na não celeridade de resolução de eventuais arbitrariedades perpetradas.

Para tanto é que chega-se na conclusiva desse papel fiscalizador e repreendedor de abusos que a ANPD desenvolve, a fim de conter irregularidades. Atua de uma forma repressiva,

[61] Os parágrafos 4° e 5° do Artigo 11 da LGPD foram objeto de mudança, por intermédio da Lei 13.853/2019, a que se defende que foi visando justamente a que esse compartilhamento fosse realizado em hipóteses estritas e necessárias, vejamos: "Na redação original da LGPD não existia a previsão do §5°, e o §4° restringia a possibilidade da comunicação ou uso compartilhado dos dados referentes à saúde para fins econômicos aos casos de portabilidade ou na hipótese do consentimento da pessoa à qual os dados se referem (..), a redação original do §4° acabaria por inviabilizar as atividades de hospitais, clínicas, laboratórios diagnóstico e operadoras de planos de saúde, que necessitam do uso compartilhado de dados pessoais para diversas operações de prestação do serviço de saúde, embora seja relevante frisar a importância do princípio da finalidade neste tocante." (KORKMAZ, 2019, p. 94)

tendo o poder de aplicação de sanções correspondentes no casos devidos, como também em um viés preventivo e pedagógico, a direcionar o fiel cumprimento da lei e indicar as inadequações com potenciais lesivos aos preceitos normativos legais.

> [...] a tutela estatal na proteção de dados não pode se resumir à função reparativa, de responsabilizar no âmbito civil ou criminal o uso indevido de dados pessoais. Compete-lhe, senão, atuar mediante política pública de prevenção, fiscalização e regulação, a evitar o uso indevido e a consecução de lesões concretas e irreparáveis, assim como o de estabelecer políticas públicas a fomentar o desenvolvimento criativo. (MOHR, 2019, p. 54)

Remete-se assim a essa autoridade nacional não apenas um papel de meramente integrante desse sistema protetivo de dados no Brasil, mas eminentemente um papel basilar e fundamental para sua sustentação (DONEDA; MENDES, 2019, p. 319).

> Uma análise de mais de 40 hipóteses do texto legal em que a Autoridade é chamada para atuar demonstra que a sua competência vai desde a solicitação e análise de relatórios de impacto de privacidade, determinação de medidas para reverter efeitos de vazamentos de dados, disposição sobre padrões técnicos de segurança da informação até a autorização da transferência internacional de dados pessoais. Isso demonstra que o órgão não é um mero coadjuvante do sistema de proteção de dados: ao contrário, é o seu pilar de sustentação, sem o qual todo o arcabouço normativo e principiológico não está apto a funcionar de forma adequada. (DONEDA; MENDES, 2019, p. 319)

Perante a quantidade intensa de operações com dados em todo o país, revela-se a complexidade do tema. Para tanto é que salienta o eminente questionamento de como a recém criada e implementada ANPD seria capaz de satisfazer ao anseio fiscalizatório, sancionador e direcionador interpretativo no que diz respeito à toda atividade de tratamento de dados realizada no Brasil.

A coresponsabilização quanto a segurança na internet[62] e nos meios digitais análogos reivindica uma participação ativa e voluntária de todos os diversos atores envolvidos no processo de tratamento de dados. Desde o titular do dado, provedores de internet, as grandes empresas que fazem interface também com os dados, como a própria ANPD, devem ter um papel ativo e colaborativo em promover esse ambiente seguro, a implicar o respeito aos direitos fundamentais de privacidade, proteção de dados, personalidade.

Não olvida-se que o papel predominante no sentido da interpretação da LGPD, bem como da afixação de suas diretrizes e regulamentos destinados a sua plena implementação deve

[62] Sobre o papel comunitário na segurança da internet: "[...] a segurança da internet é responsabilidade de todos, e cada um tem a responsabilidade de entender qual é o seu papel e quais responsabilidades perante à sociedade estão associadas a cada papel em particular." (ÀLVAREZ, 2018, p. 413).

ser desempenhado pela Autoridade Nacional de Proteção de Dados. Esse papel salutar e preponderante é disposto no próprio Artigo 55-K e seu parágrafo único da Lei 13.709/2018.

Não obstante esse seu papel de destaque, conforme já apontado, a multiplicidade e a complexidade do fenômeno envolve uma coparticipação nesse contexto de governança na internet[63].

Sobre esse estilo de governança que leva em conta a participação dos variados atores envolvidos, geraria ao mesmo tempo a existência de regulamentos de ordem pública, privada e também os de natureza técnica e algorítmica

> À luz desta consideração, é importante destacar que os diferentes instrumentos de regulação da Internet podem ser de origem pública, tais como convenções internacionais, leis, regulamentos e decisões tomadas por tribunais e agências nacionais, mas podem ter também natureza privada. Neste último caso, a regulação privada pode ser de natureza contratual, como os termos e condições que definem as regras para o uso de plataformas web, aplicativos móveis e redes de acesso à internet, ou podem ser de natureza técnica, como algoritmos, padrões e os protocolos que definem a arquitetura de software e hardware que determinam o que os usuários podem ou não fazer no ambiente digital. (ÀLVAREZ, 2018, p. 49).

Esses regulamentos privados como resultado de uma elaboração pelos próprios provedores de internet, devem estar compatíveis com os ditames da Lei Geral de Proteção de Dados, assim como aos regulamentos complementares que indicam a interpretação adequada as normas conferidos pela própria ANPD. Parece bem claro que no desenho desse sistema protetivo, apesar de ser possível e desejável uma colaboração de esforços da sociedade, há o dever de cumprimento dos preceitos legais e normas complementares editados pela autarquia especial competente.

O artigo 50 da lei específica[64] indica muito bem esse desiderato de envolvimento de todos os atores quando do tratamento de dados e possibilita um caminho de políticas de boas

---

[63] Quanto ao que conceitua-se como governança na internet, utiliza-se das considerações seguintes: "[...] a governança da internet pode ser considerada como o conjunto de processos que devem estimular a comparação de ideias e, idealmente, promover a formação colaborativa de novos "regimes internacionais" que permitam o bom funcionamento da Internet." (ÀLVAREZ, 2018, p. 48)
Utiliza-se também da definição empregada na Agenda de Tunis, parágrafo 34 (COMITÊ GESTOR DA INTERNET NO BRASIL, 2005, p. 88) "Uma definição de trabalho da governança da Internet é o desenvolvimento e a aplicação por parte dos governos, do setor privado e da sociedade civil, em seus respectivos papéis, de princípios, normas, regras, procedimentos decisórios e programas compartilhados que dão forma à evolução e uso da Internet."

[64] Na íntegra o artigo em questão da Lei 13.709/2018: "Art. 50. Os controladores e operadores, no âmbito de suas competências, pelo tratamento de dados pessoais, individualmente ou por meio de associações, poderão formular regras de boas práticas e de governança que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os

práticas e governança. Porém, com a devida parcimônia de destaque sempre desse aspecto de análise pela autarquia especial (ANPD), a conferir e sugestionar os padrões técnicos que estejam mais próximos da promoção da autodeterminação informativa dos usuários.

Com o destinatário claro da dicção do Artigo 55-K da LGPD afeto aos demais órgãos e entidades da administração pública, verifica-se que estes quanto tenham competência que toquem a questão da proteção de dados, há uma sobrevalia da competência da ANPD. A leitura e interpretação deste dispositivo reforça justamente esse papel central nesse microssistema protetivo desempenhado por tal autarquia.

Por fim, mas não distante de tudo enquanto ponderado, a aplicação das sanções previstas na Lei Geral de Proteção de Dados é de competência exclusiva da ANPD. Não há um compartilhamento nem mesmo nos casos que tocam a interface de outros órgãos públicos, nessas situações o que será verificado é um papel articulador da ANPD, sem afastar uma certa centralidade, conforme verificada até mesmo pelo garante de tal exclusividade sancionatória e por sua especialidade na área da proteção de dados.

Quanto a essa integração com serviços de outros órgãos e entidades públicas na defesa do interesse da proteção de dados[65] já observou-se de forma, inclusive, prática, apesar de ainda prematura a autoridade nacional em tela[66]. Nesse sentido é que cita-se a recomendação elaborada pelo Ministério Público Federal (MPF), Conselho Administrativo de Defesa Econômica (CADE), Secretaria Nacional do Consumidor (SENACON) e pela própria ANPD, quanto a nova política de privacidade do aplicativo de mensagens *WhatsApp* e a preocupação com a adequação ou não a LGPD[67].

Nota-se esse papel de destaque conferido e desempenhado pela ANPD quando a própria recomendação em questão justifica a propositura em conjunto, pelos diversos órgãos e

---

mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais.

§ 1º Ao estabelecer regras de boas práticas, o controlador e o operador levarão em consideração, em relação ao tratamento e aos dados, a natureza, o escopo, a finalidade e a probabilidade e a gravidade dos riscos e dos benefícios decorrentes de tratamento de dados do titular."

[65] Sobre esta interação e articulação também é palpável ser observada através de acordos de cooperação técnica entre a ANPD e o Conselho Administrativo de Defesa Econômica (GARCIA, 2021, p. 90), a que implica a troca de informações, experiências e ações educativas. Sobre tal acordo encontra-se noticiado em: https://www.lgpdbrasil.com.br/anpd-e-cade-assinam-acordo-de-cooperacao-tecnica/.

[66] Outro acordo de cooperação técnica também foi firmado entre a ANPD e a Secretaria Nacional de Defesa do Consumidor (SENACON), a que multiplica-se os esforços inclusive no direcionamento e nas providência quanto as reclamações recebida pelos consumidores, a gerar uma linha de resposta mais assertiva, célere e uniforme. A notícia sobre o fato pode ser extraída de matéria disponível em: https://agenciabrasil.ebc.com.br/justica/noticia/2021-03/senacon-e-anpd-assinam-acordo-visando-protecao-de-dados.

[67] A notícia em questão pode ser extraída da pina: https://www.mpf.mp.br/pgr/noticias-pgr/mpf-cade-anpd-e-senacon-recomendam-que-whatsapp-adie-entrada-em-vigor-da-nova-politica-de-privacidade.

entidades públicas, justamente por essa possibilidade de ação articulada e coordenada por parte da autoridade nacional[68]. Assim como ilustra que a recomendação apenas é endereçada após a instauração de um Processo Administrativo[69] e de análise por parte da Coordenação-Geral de Fiscalização da ANPD.

Em síntese esse demais órgãos atuaram de forma conjunta e complementar para garantir o melhor interesse dos titulares de dados e potenciais agressões verificadas, mas há que se atentar nesse papel de centralidade a todo tempo exercido pela ANPD, tendo em vista a especialidade da matéria e que é outorgado a ele o dever de apresentar a interpretação adequada quanto as terminologias envoltas e aos dispositivos que integram a Lei Geral de Proteção de Dados. (GARCIA, 2021, p. 93)

Essa percepção vem a indicar em linhas claras que,

> Em última análise, o que se verifica é que os demais órgãos da administração pública, dentre os quais se encontram as agências reguladoras, poderão regular e fiscalizar questões setoriais referentes ao tratamento de dados pessoais de forma complementar à ANPD. No entanto, pela leitura da LGPD, essa regulação não poderá, a princípio, ir contra diretrizes e interpretações técnicas já conferidas pela ANPD, justamente, em razão de sua especificidade para o tema, sob pena de implicar eventual violação à segurança jurídica tanto aos agentes de tratamento como aos titulares de dados pessoais. (GARCIA, 2021, p. 94)

Sem dúvidas o sistema protetivo de dados no Brasil, segundo o desenho da legislação específica, esboça-se em uma atuação tanto a nível administrativo, quanto judicial. A integrar de forma concisa a coibição de irregularidades e abusos no campo da privacidade e dos dados pessoais dos usuários.

À partir da própria tendência já operante no direito pátrio, e a fins de uma melhor resposta no campo preventivo e repressivo, é que é imperioso observar a proteção de dados não apenas em um âmbito individual, como também, nos casos que assim cabem, em uma perspectiva coletiva (GARCIA, 2021, p. 92-93).

---

[68] Sob o reconhecimento da articulação de atividades da ANPD com outros órgãos estatais: "[...] a possibilidade de atuação da ANPD de forma coordenada com outros órgãos e entidades públicas responsáveis pela regulação de setores específicos, nos termos do art. 55-J, XXIII e §§3° a 5° da LGPD, que visa conferir maior eficiência estatal, além dos reflexos que as questões relativas à proteção de dados também têm em relação ao consumidor." Retirado da íntegra da reclamação em questão e disponibilizado em: https://www.mpf.mp.br/pgr/documentos/Recomendao_WhatsAppAssinada.pdf.

[69] Processo Administrativo de n. eletrônico 00261.00012/2021-04 e a Nota Técnica que indica a análise da Coordenação- Geral de Fiscalização da ANPD é a de n. 02/2021/CGTP/ANPD de 22/03/2021. Informações retiradas do relatório, disponível em: https://www.mpf.mp.br/pgr/documentos/Recomendao_WhatsAppAssinada.pdf.

No campo administrativo isso pode ser viabilizado justamente por meio da atuação coordenadora da ANPD com órgãos de atuação setoriais em matérias que transitam em torno da proteção de dados pessoais. Pode ser feita uma sistematização com órgãos e entes públicos, como o PROCON, a já citada SEDEN, dentre outros mecanismos especializados para que chegue as informações em tempo célere de potenciais agressões, bem como as respostas em promover a cessação das irregularidades seja feita de uma forma mais orgânica e viável (ZANATTA, 2019, p. 22).

O múnus de fiscalização a nível nacional de um problema tão complexo e tão extenso, com a dispersão e difusão cada vez maior da produção e operações de dados, necessita de mecanismos e da articulação de uma fronte de identificação e combate a possíveis arbitrariedades, em prol da proteção dos dados e da privacidade dos usuários.

Quanto à possibilidade também de judicialização de potenciais agressões no campo dos dados pessoais é importante assinalar que não há um cerceamento pela legislação. Ao revés, o Artigo 42 da LGPD revela muito bem tal possibilidade, no entanto nos ditames de tal texto legal é perfeitamente possível e perquirido a convivência entre esses dois ambientes protetivos, tanto o administrativo, como o judicial.

Na verdade uma multiplicidade protetiva beneficia puramente o usuário e titular do dado que se vê na maioria das vezes em situação de fragilidade perante os grandes controladores e provedores da internet. Torna-se, por oportuno, mais ágil e mais simplificado as reclamações quando do cometimento de irregularidades e ilegalidades.

No campo judicial esse olhar também coletivo para o campo da tutela do direito à proteção de dados é perfeitamente possível. A tutela dos direitos a ser feita em juízo de forma individual ou coletiva tem amparo legal no Artigo 22 da Lei 13.709, e assim

> [...]a LGPD absorveu parte da tradição de tutela coletiva no Brasil, abrindo espaço para que a proteção dos direitos assegurados na legislação seja feita de forma coletiva, ao lado das múltiplas normas de proteção individual dos direitos. (ZANATTA, 2019, p. 2)

A previsão de uma Autoridade Nacional de Proteção de Dados no sistema brasileiro é feita de uma forma a garantir uma papel preponderante e essencial. Sua existência é considerada a força motriz (DONEDA; MENDES, 2019) para a plena implementação e seguimento, nos diversos níveis da sociedade brasileira, dos dispositivos que integram o sistema legal protetivo de dados.

Sua atuação, em que pese no campo administrativo poder assumir contornos tanto preventivos, como repressivos- como é o caso da aplicação de multas correspondentes-, não

cerceia a também possibilidade de acionamento da justiça, quando cabível. Inclusive, acionar a justiça pode ser por parte de informação e impulso da própria autoridade nacional[70], como forma de cumprimento pleno de seu desiderato fiscalizador de defensor da privacidade.

Essa atuação salutar e articuladora da autoridade é um caminho no garante para que efetivamente seja possível criar uma política protetiva de dados concisa no Brasil, à partir de uma fiscalização possível e palpável. Ao se tratar do campo de dados da saúde, e dos dados epidemiológicos, como em qualquer outra vertente setorial a que circule o tratamento de dados, é importante ter um autarquia fortificada e não apenas prevista legalmente, mas dotada de mecanismos que possibilitem seu exercício prático.

4.2 A ANPD E SEU PROCESSO DE IMPLEMENTAÇÃO À LUZ DA LEI GERAL DE PROTEÇÃO DE DADOS

Conforme já abordado ao longo deste trabalho, com a criação de um sistema legal específico atinente a proteção de dados também houve a previsão da implementação de um Autoridade Nacional de Proteção de Dados, a ANPD.

Apesar de ter sido indicada e prevista desde a própria Lei Geral de Proteção de Dados (BRASIL, 2018), aponta-se que sua plena implementação apenas data à partir da existência do Decreto n° 10.474 de 26 de agosto de 2020 que promoveu sua estruturação (GARCIA, 2021, p. 80).

A existência de uma autoridade nacional a firmar um papel basilar e central nesse sistema protetivo é inquestionável e já foi extensamente abordado ao longo do tópico anterior. Para além da implementação dessa autoridade nacional também é deveras importante considerar a forma a que será estruturada e, à partir disso, se será fidedigna no cumprimento dos desideratos máximos que a LGPD retrata.

É válido compreender os pormenores de tramitação da legislação que garantem a criação da ANPD e as alterações sedimentadas, conforme os reflexos que são vislumbrados nessa sistemática protetiva.

[70] Esse aspecto pode ser desprendido claramente da dicção do Artigo 55-J, inciso XXI e XXII, a que impõe o dever de comunicação pela ANPD no tocante as irregularidades que tomar conhecimento, inclusive, para aplicação das sanções penais correspondentes.

O projeto legal (PL 5.276/16), a que foi declarado prejudicado em virtude de subemenda substitutiva[71] , acabou por ser apensado ao Projeto de Lei de n. 4.060/2012. Este projeto de lei em questão, tem por numeração no Senado Federal a de 53/2018.

O índice de destaque de tal projeto legal, a que desencadeia na Lei 13.709/2018, é de que houve veto parcial de seu texto originário. Incialmente contava-se com a criação de uma ANPD nos seguintes termos do então Artigo 55, caput: "É criada a Autoridade Nacional de Proteção de Dados (ANPD), integrante da administração pública federal indireta, submetida a regime autárquico especial e vinculada ao Ministério da Justiça."[72]

Mediante veto parcial (Veto n. 33/2018) os dispositivos que tratavam da criação de tal estrutura fiscalizatória foram retirados, com a justificativa de inconstitucionalidade formal. Decorrente de tal extirpação do texto original é que ficou-se a pendência em sua efetiva instituição.

A Medida Provisória de n. 869/2018[73] é editada em vias a alterar a LGPD e efetivamente retornar a dispor quanto a criação de tal instituto. Não obstante, seu texto indicou uma instituição sob a forma de órgão da administração pública federal e integrante da Presidência da República.

Em clara síntese, inicialmente (PL 5.276/16) previa-se que a ANPD contaria com autonomia e independência em relação ao executivo federal, partindo do pressuposto claro de conferir a estrutura adequada para o exercício da função que lhe foi conferida. No entanto, à partir de veto presidencial, por suposta inconstitucionalidade formal, desencadeou a alteração de tal forma que passou a ser vinculada à Presidência da República (MP 869/2018), minando duramente uma autonomia em seus trabalhos.

A alteração desencadeada pela medida provisória em prospecto retratou-se como um claro retrocesso na justa medida que uma independência funcional mínima é indissociável da própria existência da autoridade nacional compromissada com à proteção de dados no país e a englobar a fiscalização de todos os segmentos da sociedade, inclusive os públicos governamentais.

> Não apenas constatação de que a constituição da autoridade é fundamental, mas também a discussão sobre o próprio modelo a ser adotado é fundamental.

[71] Informação de tramitação do PL 5.276/16 retirada do próprio site oficial da Câmara dos Deputados. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2084378.

[72] Texto retirado do próprio site do Congresso Nacional, disponível em: https://www.congressonacional.leg.br/materias/vetos/-/veto/detalhe/12024.

[73] Dispositivo originário pode ser encontrado no site do planalto que contém a Lei 13.709/2018, com as devidas assinalações de que houve alteração e não está, portanto, mais em voga. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm.

> Como se verá adiante, é fundamental que a autoridade esteja amparada no seguinte tripé: independência, poder sancionatório e expertise. (MENDES, 2018a, p. 578)

Sobre a independência como atributo que lhe deve ser inerente, também concorda Danilo Doneda (2020, p. 306)

> 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, como também para a estruturação de todo o sistema normativo de proteção de dados, que compreende aspectos da regulação do próprio fluxo de dados.

Reconhecendo e sopesando tais críticas numerosas por parte da doutrina, através da Medida Provisória de n. 1.124 de 2022 houve novamente alteração em relação a autoridade, trazendo agora a seguinte dicção ao artigo 55-A da Lei 13.709/2018:

> Art. 55-A. Fica criada a Autoridade Nacional de Proteção de Dados - ANPD, autarquia de natureza especial, dotada de autonomia técnica e decisória, com patrimônio próprio e com sede e foro no Distrito Federal. (Redação dada pela Medida Provisória nº 1.124, de 2022) (BRASIL, 2018)

Fica instituída uma estrutura compatível com independência no campo do desenvolvimento de suas legítimas atividades. Independência esta possibilitada por uma autonomia financeira, vez que dotada de patrimônio próprio, técnica e também decisória.

Quanto a autonomia técnica, é primoroso um perfil técnico a constituir e orientar o desempenho das atividades pela autarquia especial. Remete-se as próprias funções desempenhadas por esta, a que cabe os ditames da interpretação adequada da LGPD, bem como até mesmo na edição de normas complementares no garante de sua efetivação.

Devido ao arraigado tecnicismo que imprime a própria matéria de dados, que traz em si mesmo um vernáculo próprio da tecnologia da informação e muitas vezes distantes dos diversos setores da sociedade, é importante a constituição de uma autoridade que prime pela tecnicidade e especialidade que a matéria vem exigir.

> Outras características devem estar igualmente presentes em uma Autoridade, como a necessária presença de pessoal técnico capacitado- tanto em assuntos jurídicos e regulatórios como nos aspectos técnicos do tratamento de dados pessoais- para que as diversas atividades da Autoridade que não são de cunho repressivo, como as de caráter educativo, de orientação, o estabelecimento de parâmetros e outras, possam ser implementadas. A Autoridade é um elemento indispensável para garantir a adaptação da lei, ao elaborar normas e

> regulamentos sobre temas específicos como segurança da informação e outras situações, sem que haja necessidade de alteração da lei. Ela pode ainda estabelecer parâmetros para a aplicação da lei conforme características de cada setor ou mercado, objetivando ações que sejam mais eficazes para a proteção de direitos do cidadão [...]. Para tanto, contar com pessoal técnico especializado é um elemento de primeira importância. (DONEDA, 2020, p. 307)

Conforme já abordado, a forma de estruturação regimental e quadro demonstrativo dos cargos em comissão e de função de confiança quanto a esta autoridade ocorreu por ocasião do Decreto n. 10.474. À partir do seu próprio artigo 6° há o indicativo claro de que só haveria a entrada em vigor de tal decreto e do plano estrutural em si quando da data de publicação da nomeação do Diretor Presidente da ANPD.

Segundo as informações da nomeação, que apenas se deu em 06 de novembro de 2020, é que pode-se precisar a data da implementação da ANPD no Brasil, com seu devido "funcionamento" (PARENTONI, 2021, p. 167)

Referente as questões da sua estrutura organizacional, é composta por

> Art. 55-C. A ANPD é composta de:
> I - Conselho Diretor, órgão máximo de direção;
> II - Conselho Nacional de Proteção de Dados Pessoais e da Privacidade;
> III - Corregedoria;
> IV - Ouvidoria;
> V - Procuradoria; e
> VI - unidades administrativas e unidades especializadas necessárias à aplicação do disposto nesta Lei. (BRASIL, 2018)

O Conselho Diretor nessa orgânica figura-se como o órgão máximo. Para tais trabalhos, conta com além de uma Diretor-Presidente, também com outros 4 diretores (BRASIL, 2018, Art. 55-D).

Importante assinalar perante a máxima deste órgão e sua hierarquia estrutural dentro da própria ANPD, que a escolha de seus membros[74] será feita na forma de cargo em comissão e perante a escolha presidencial. A certa autonomia configura-se na medida em que é necessário, para a devida nomeação, uma aprovação do Senado Federal.

[74] Esses membros podem ser selecionados entre brasileiros que preencham os seguintes requisitos: I)brasileiros; II) com nível superior de educação; III) elevada especialidade para tal material. Nesse rigor, parece evidente o conceito da tecnicidade da composição e na própria razão de ser da ANPD.
Há que se destacar que essa especialidade pode incluir para além de conhecimentos no campo das tecnologias da informação, outros conteúdos a que são também indispensáveis e congruentes com as funções a serem desempenhadas pela autoridade. Assim, há a possibilidade de um especialidade jurídica ou administrativa-coordenatória, por exemplo.

Aprofundando ao regimento desta autarquia especial, que conforme já assinalado foi disciplinado pelo Presidente da República na forma do Decreto n. 10.474/2020, aponta-se que o Conselho Nacional de Proteção de Dados e da Privacidade é um órgão consultivo, assim como a Secretaria-Geral e a Coordenação-Geral de Relações Institucionais e Internacionais e que promovem assistência direta ao Conselho Diretor (Art. 3° do Decreto).

Há a previsão de uma Procuradoria-Geral Especializada, bem como de uma Coordenação Geral de Administração e outra Coordenação distinta para tratar da Tecnologia de Informação. São órgão seccionais a integrarem tal regimento e são válidos a serem pontuados, visto a magnitude do trabalho e do múnus a que se espera de tal autoridade, sendo assim, bem avança em ter a previsão de órgãos especializados em promover auxílio de algumas de suas competências.

Entre as inúmeras incumbências afetas ao Conselho Diretor veicula-se seu poder de regulamentação quanto o uso compartilhado de dados sensíveis e até mesmo ao formato que tais dados irão ser apresentados. Ademais, podem realizar diligência na verificação de como essas atividades de tratamento estão sendo desenvolvidas, solicitar relatório de impacto à proteção de dados, entre outras tantas a que estão extensamente dispostas no Artigo 4°, Anexo 1 do Decreto 10.474/2020.

Levando em consideração que o presente tópico dedica-se a abordagem quanto a implementação da Autoridade Nacional de Proteção de Dados no Brasil, é importante apresentar essa estrutura regimental e a esfera de competência de cada um do órgãos que a integram. No entanto, em virtude do desiderato máximo da presente pesquisa, a que discute o tratamento de dados independente de consentimento para o desenvolvimento de políticas públicas em saúde, dá-se uma ênfase maior nas atribuições que tocam especificamente esta matéria.

Sendo assim, destaca-se que entre as atribuições do Conselho Diretor existe a de solicitar as autoridades públicas a publicação periódica de relatórios de impacto quanto à proteção de dados, bem como a sugestão e direcionamento de práticas técnicas informatizadas e operativas e dos padrões de interoperabilidade (Art. 4°, I, d e III, c, Decreto 10.474, Anexo 1) que melhor compactuem com os termos da LGPD.

A sua destreza na disposição dos padrões técnicos de segurança a serem adotados e especificamente dos padrões de interoperabilidade também tem impacto firme quanto a definição, no campo da prática e dos limites, da aplicação do Artigo 11, inciso II, alínea b, da Lei 13.709/2018.

Assinala-se que todas as demais competência pormenorizadas, e por demais extensas, atribuídas ao Conselho Diretor, bem como a própria ANPD de forma geral, resvalam um compromisso na assunção de um papel ativo regulatório e fiscalizatório. Nesse sentido, atua delineando os padrões técnicos mínimos a serem adotados pelos diversos seguimentos sociais, como pelo próprio Estado, realiza auditorias e diligências para verificar se os termos da Lei e das recomendações estão sendo observados, assim como aplica sanções e determina término de tratamento de dados em caso de arbitrariedades e ilegalidades.

Observa-se que a atuação de tal autarquia é complexa, vez que atua desde a proposição de diretrizes estratégicas, com a veiculação dos padrões técnicos mínimos, apresentados à luz das normas e princípios que regem a LGPD. Assim como também atua de uma forma colaborativa, pedagógica e elucidativa à toda a sociedade e aos próprios órgãos e entidades públicas, tal qual ao próprio Ministério na Saúde.

Para efeitos de uma pequena comparação e também informação, a dinâmica da existência de uma autoridade que detém o desiderato fiscalizatório quanto à atividade de tratamento de dados é a realidade da maioria dos países que detém uma legislação específica quanto a tal temática[75]. Para além, mesmo os países que não contam com leis gerais quanto a matéria há organizações que desempenham papel similar (DONEDA, 2020, p. 302-303), como é o caso dos Estados Unidos com a "Federal Trade Comission"[76]

Apesar de no caso dos EUA[77] ser vinculada a questão comercial e das relações que ali se operam, inegável o viés protetivo que desempenha nessa área setorial. (DONEDA, 2020, p. 302)

Quanto ao regime europeu, aponta-se que desde a Lei de Hesse de 1970 na Alemanha, indicada já neste trabalho como legislação pioneira quanto a questão dos dados, haveria o esboço de um estrutura similar do que viria a ser conhecida como tais autoridades de proteção de dados. Naquele momento era denominada de Comissário e atuava justamente nesse sentido de conferir vazão aos parâmetros e ditames legais (DONEDA, 2020, p. 302)

Nos dias de hoje, a Europa conta com a existência de tal modelo (PARENTONI, 2021, p. 169), a que a todo tempo destaca-se as características que esta autoridade deve possuir. Nesta medida, é que o Tratado sobre o Funcionamento da União Europeia quanto toca a questão indica

[75] Assim aponta Danilo Doneda (2020, p. 302) a que cita que há a existência de uma organização similar, mesmo que com algumas distinções presentes, na grande maioria dos países a que contam como leis tocante a matéria protetiva dos dados.

[76] Que com a tradução livre, seria: "Comissão Federal de Comércio".

[77] Danilo Doneda (2020, p.302) aponta que no contexto americano a existência de uma autoridade nacional é um tanto quanto dispensável, visto a concentração de tutela judicial quanto a matéria. A situação, no entanto, é diametralmente oposta quanto toca o cerne europeu.

que “a observância dessas normas fica sujeita ao controle de autoridades independentes.” (TRATADO..., 2016, p. 55)

A Carta dos Direitos Fundamentais da União Europeia, assim como o próprio Regulamento Europeu em matéria de proteção de dados, ambos documentos já citados no corpo do presente trabalho, indicam que as normas serão implementadas e aplicadas através do auxílio de uma autoridade no campo de cada país (UNIÃO EUROPEIA, 2012).

No entanto, como bem destaca Leonardo Parentoni (2021, p. 168-169), não há a exigência de um modelo estrutural, regimental ou mesmo de rol de competências a serem implantados pelos países europeus quando da instituição dessa autoridade. O que parece ser o denominador comum é justamente a garantia de uma plena autonomia a legitimar a sua própria existência e seu papel de controle, a que o Tratado de Funcionamento da União Europeia bem destaca.

Na experiência brasileira, durante todo esse hiatos da plena instituição da ANPD diversas atecnias no seu processo de instituição foram verificadas e já expurgadas, como é o caso da MP 869/2018, a que andou próximo de desvirtuar o real sentido desse mecanismo. No entanto, grande salto deu quando não só passou-se a garantir sua estruturação autônoma financeira, técnica e estrutural administrativa, vem a estabelece-la enquanto autarquia especial (MP 1. 124/2022).

4.3 A DEFINIÇÃO DOS LIMITES ÉTICOS E LEGAIS QUE TANGENCIAM O ARTIGO 11, INCISO II, ALÍNEA B, DA LEI 13.709/2018

Conforme já extensamente retratado, o regime de proteção de dados exteriorizado precipuamente na Lei 13.709/2018 veicula como regra um tratamento a que seja precedido pelo consentimento do titular daquele dado.

Nesse sistema protetivo o consentimento vem revelar a efetivação, ou ao menos uma busca em efetivação, do direito à autodeterminação informativa (AZEVEDO, 2021, p. 90) daquele usuário sob o qual o dado versa. Tutela assim que os indivíduos apenas disponibilizem e tenham tratados dados e informações sobre sua pessoa, com os quais consinta.

Em um caráter mais amplo, a exigência de um consentimento aponta também o garante de um direito à proteção de dados. Ressalta-se que para ser válido este consentimento deve ser operacionalizado na forma da LGPD (Art.5°, inciso XII), sendo uma manifestação inequívoca de vontade e de forma informada.

Porém, na mesma legislação que profere tanto realce ao consentimento no propósito de assegurar os princípios e objetivos que a norteiam, há também a flexibilização de hipóteses que autorizam o tratamento de dados independente do consentimento.

Sabe-se que a Lei Geral de Dados no Brasil e a própria tendência mundial quanto a matéria não conferem uma dispensabilidade de valor a qualquer dado pessoal que o seja, todos devem ser protegidos por serem projeções da própria personalidade do sujeito[78]. Essa proteção, no entanto, se verifica como ainda mais rígida ao tratar-se de dados pessoais entendidos como sensíveis.

Já tendo sido explicitado neste trabalho o que efetivamente constituem-se como dados sensíveis, nos termos da legislação geral (Art. 5°, inciso II), sua discussão enquanto a este tópico especificamente é justamente apresentar que mesmo na hipótese de dados pessoais sensíveis a lei também abre a possibilidade no tratamento independente do consentimento.

Não podendo ser diferente, claro que a disposição normativa atinente não faz uma flexibilização ao consentimento de forma vasta e leviana, mas apenas em situações específicas e com a previsão explícita em lei a viabilizar e legitimar.

O artigo 11, em seu inciso II é quem veicula essa possibilidade de independência ao consentimento na ambiência dos dados sensíveis. O enfoque da análise será firmado na permissiva de tratamento independente do ato de consentir do usuário na hipótese precípua ao desenvolvimento de políticas públicas em saúde epidemiológicas.

Não obstante, os dados que versam sobre informações quanto à saúde são definidos enquanto dados sensíveis. Essa sensibilidade atine ao próprio potencial lesivo que pode ser gerado no âmbito da privacidade e personalidade com o manejo de tais fontes de informações.

Apesar deste potencial ofensivo, já até mesmo discorrido ao longo do trabalho, cumpre trazer algumas considerações sobre a razão de ser desta hipótese autorizativa do Artigo 11, inciso II, alínea b, assim como sobre as definições dos limites na sua aplicação.

A própria previsão de uma possibilidade de tratamento independente do consentimento já imprime e reafirma o contexto de que, apesar de tão caros ao ordenamento jurídico brasileiro, sendo elevado até mesmo a categoria de direito fundamental, o direito à proteção de dados e à autodeterminação informativa não são direitos absolutos (MENDES, 2018b, p. 212).

Pelo simples fato de não serem direitos absolutos cabe, em algumas situações e em determinados conflitos com a asseguração de outros direitos fundamentais, um juízo de

[78] "[...] Os dados pessoais são projeções diretas da personalidade e como tais devem ser considerados. Assim, qualquer tratamento de dados, por influenciar na representação da pessoa na sociedade, pode afetar a sua personalidade e, portanto, tem o potencial de violar os seus direitos fundamentais." (MENDES, 2018a, p. 577)

ponderação. Este juízo pode gerar uma certa flexibilização do direito fundamental, a uma certa medida e com a devida proporcionalidade e razoabilidade, de forma a não suprimir seu núcleo essencial.

E, assim sendo, viabiliza-se uma certa flexibilização até mesmo quando tratam-se de dados sensíveis, aqui inclusos os dados quanto a saúde, por entender que seu tratamento e utilização das informações a que carrega podem e são úteis a toda uma coletividade (KORKMAZ, 2019, p. 75).

Essa utilidade por parte de toda uma coletividade é o que de fato referenda a utilização nestes casos, justamente a perscrutar um interesse público. Outrossim, não apenas o acesso a tais dados é viabilizado, como também há a permissiva no compartilhamento efetuado no âmbito da administração pública.

Esse compartilhamento é primoroso para a próprio desenvolvimento das políticas públicas concernentes, como mui bem ilustra o Artigo 7°, inciso III, da LGPD. Assim, quanto ao âmbito do SUS e da vigilância epidemiológica, é precípuo uma gestão descentralizada, a englobar todos os níveis de uma assistência em saúde e a uma descentralização político e administrativa em cada esfera do governo (Artigo 7°, incisos II e IX, da Lei 8.080/1990).

O compartilhamento nesse cerne dos dados pessoais sensíveis é limitado pela própria LGPD, a que em seu Artigo 23, caput reafirma a necessidade do cumprimento do princípio da finalidade. Por oportuno, é que só pode ser efetuado em vias de asseguração do interesse público e no desenvolvimento da competência quanto a execução de serviço público.

Em via de regra principal, garante-se também que esse compartilhamento seja feito apenas no bojo da própria administração pública e não haja interface com os setores particulares, vistos as novas potencialidades de riscos e monetarização que seriam geradas.

Dessa forma, uma eventual restrição, ou melhor dizendo ponderação, quanto ao interesse exclusivamente privado do indivíduo/ cidadão justificar-se-ia em prol do benefício de toda uma região, localidade, município, estado ou mesmo do país de uma forma geral. Em última análise, como o potencial usuário é destinatário também desses serviços públicos, esse indivíduo sob o qual o dado versa também poderia estar sendo classificado como tendo seus interesses privilegiado, mesmo que não seja o interesse tão direto e imediato.

Nessa mesma análise também pende o regime europeu de proteção de dados, a autorizar a consecução do interesse público em certas situações em detrimento do interesse individualista de um usuário. Para tanto é que o Artigo 9° do Regulamento Europeu prevê a necessidade do consentimento como modelo de regra e proíbe a utilização de dados pessoais sensíveis sem esse

ato de consentir do titular, salvo em algumas exceções pontuais que estão dispostas em seus incisos:

> g) Se o tratamento for necessário por motivos de interesse público importante, com base no direito da União ou de um Estado-Membro, que deve ser proporcional ao objetivo visado, respeitar a essência do direito à proteção dos dados pessoais e prever medidas adequadas e específicas que salvaguardem os direitos fundamentais e os interesses do titular dos dados;[...]
> i) Se o tratamento for necessário por motivos de interesse público no domínio da saúde pública, tais como a proteção contra ameaças transfronteiriças graves para a saúde ou para assegurar um elevado nível de qualidade e de segurança dos cuidados de saúde e dos medicamentos ou dispositivos médicos, com base no direito da União ou dos Estados-Membros que preveja medidas adequadas e específicas que salvaguardem os direitos e liberdades do titular dos dados, em particular o sigilo profissional. (EUROPIAN UNION LAW, 2016)

Sob a análise congregada destas duas alíneas previstas no Artigo 9° do Regulamento, verifica-se a possibilidade no tratamento livre de consentimento para o alcance de interesse público. Nessa busca do interesse público indica de forma mais pormenorizada ainda, quando da tutela de um direito à saúde na salvaguarda de uma prestação do serviço estatal de saúde em nível mais elevado de qualidade.

Assim impele o próprio reconhecimento pela legislação europeia que as tecnologias podem ser utilizadas sim para modernizar, promover uma maior dinâmica e agilidade entre as informações e a gerar respostas mais assertivas na promoção da saúde (NUNES, 2019, p. 46). Essas respostas não são restritas apenas ao diagnóstico e a prescrição do tratamento e regime de intervenção adequado, como até mesmo, em um grau amplo, sistematizar as políticas públicas de saúde.

Por entender de tal forma, é que o próprio Plano de Estratégia de Saúde Digital para o Brasil dos anos de 2020 à 2028[79] apresentado pelo Ministério da Saúde, impele as estratégias de enriquecimento da tecnologias de informação no âmbito da saúde, com a consecução de uma integração da interoperabilidade em ampla esfera dos dados em saúde, inclusive com os viabilizados pela saúde privada.

No tocante a essa informatização em saúde, com um empreendimento de melhoria da prestação do serviço e do dever estatal à saúde (Artigo 196 da CRFB/88) ser viável, cumpre que o rigor do sistema de proteção de dados não seja olvidado, assim como que os padrões

[79] Tal plano encontra-se disponível em: https://bvsms.saude.gov.br/bvs/publicacoes/estrategia_saude_digital_Brasil.pdf. Vem a promover uma visão estratégica de saúde digital para o Brasil, revelando as diretrizes do Ministério da Saúde para sua implementação.

técnicos empregados sejam os melhores, a fim de um mínimo de segurança, adequação e transparência em tal manejo.

Esse tratamento de dados a ser desenvolvido pela administração pública, para a elaboração de políticas públicas (BRASIL, 2018, Artigo 7°, inciso III), a ser dissociado do consentimento (Artigo 11, inciso II, b) não se dissocia da necessidade de cumprimento dos princípios da LGPD e dos padrões técnicos que, por sua vez, o instrumentalizem.

O tratamento de dados em geral, e aqueles que refletem informações quanto a saúde, devem atentar para os desideratos da finalidade, adequação, segurança, transparência, prevenção, não descriminação, assim como os demais princípios indicados no artigo 6° da LGPD- como a própria boa-fé, a que está contido em seu *caput*, a diferença dos demais que estão divididos entre seus incisos.

Importante assinalar o ideal de não descriminação, justamente pela potencialidade de risco nesse sentido que a sensibilidade dos dados em saúde se mal manejados/ utilizados podem concatenar. Uma busca pela não descriminação é, inclusive, um das bases utilizadas para classificar alguns dados enquanto sensíveis[80] e, portanto, detentores de um sistema mais rígido de proteção.

Dessa forma é que defende-se que é inviável a prescrição de um rol taxativo dos dados entendidos como sensíveis (KONDER, 2019, p. 455), justamente porque essa afixação rígida enrijeceria o sistema e poderia afetar a um novo nível de potencial ofensivo, invasivo e discriminatório quanto a demais dados que se desdobram e revelam-se posteriormente enquanto sensíveis. Não é por outra razão a que a legislação indica que os dados considerados inicialmente apenas como pessoais e que, durante o percurso de seu tratamento, revelem-se como sensíveis, cabe o mesmo rigor das normas atinentes a proteção de dados sensíveis (Art. 11, §1° da LGPD).

Para a empreitada de promover concretude aos princípios legais assinalados na Lei Geral de Proteção de Dados, impele um papel basilar a ser desempenhado pela Autoridade Nacional de Proteção de Dados. Esta que se constitui enquanto autarquia prevista pela própria lei e já implementada no Brasil, apesar da experiência nessa implementação ainda ser prematura.

---

[80] Sobre a potencialidade de descriminação como critério de classificação de dados, enquanto sensíveis: "[...] os dados sensíveis são dados pessoais especialmente suscetíveis de utilização para fins discriminatórios, como estigmatização, exclusão ou segregação, de modo que seu tratamento atinja a dignidade de seu titular, lesionando sua identidade pessoal ou privacidade. O próprio anteprojeto da legislação identifica que o fim precípuo do tratamento diferenciado dos dados sensíveis é impedir a descriminação da pessoa humana com base nas suas informações. Por essa razão somente podem ser sensíveis os dados referentes à pessoa humana, em virtude do valor intrínseco da sua dignidade." (KONDER, 2019, p. 455)

Sobre a elementaridade dessa autoridade nacional nesse múnus de definição de parâmetros claros a viabilizar a aplicação da LGPD, com a edição de normativas complementares para que a lei seja de fato aplicada e compreendida pela sociedade e pelo cidadão comum,

> Ainda, em uma área tão dinâmica e influenciada pelo desenvolvimento tecnológico como a proteção de dados pessoais, é natural que a legislação deva se ater a um determinado nível de generalidade para que não caia rapidamente na obsolescência nem suscite "pontos cegos" quanto à sua aplicabilidade. Ao mesmo tempo, os efeitos cada vez mais intensos do tratamento de dados pessoais na vida dos cidadãos implicam a necessidade de proporcionar garantia rápida a direitos cujos contornos podem ser bastante fluídos. (MENDES, 2018, p. 24)

Imperioso que a legislação, para sua própria permanência no tempo, esteja sedimentada em preceitos mais gerais, como é próprio da maior parte das normas nos dias atuais, especialmente aquelas afetas a matérias tão dinâmicas como é o caso das tecnologias, dados e interfaces com os indivíduos e a sociedade em geral. Assim sendo, o papel máximo de interpretação dos dispositivos normativos, a promover seu entendimento claro e sua concretude, é desempenhado por essa autoridade nacional (Artigo 55-J da LGPD e Artigo 4°, VIII do Decreto 10.474).

Nessa mesma concludente apresenta a consideração de Danilo Doneda, quanto ao caráter interpretativo e integrativo da LGPD desempenhado pela ANPD, perante a fluidez e capacidade de mudança constante pertinente a matéria,

> A cuidadosa escolha dos instrumentos de tutela adequados à natureza dos interesses em questão é necessária em uma realidade moldada pela tecnologia que, ao mesmo tempo que requer clareza e precisão, está sujeita a radicais mudanças de rumo- requerendo a adaptação de todo um instrumental jurídico. (DONEDA, 2020, p. 309)

Dessa feita, considera-se que,

> Uma Autoridade, nesse contexto, é elemento indispensável para garantir a adaptação da lei a novas circunstâncias sem que se abra mão da segurança jurídica, ao proporcionar orientação sobre a interpretação e aplicação da lei, ao elaborar normas e regulamentos sobre temas específicos como segurança da informação ou outras situações, sem que haja necessidade de alteração da lei. Ela pode ainda estabelecer parâmetros para a aplicação da lei conforme as características de cada setor ou mercado, objetivando ações que sejam mais eficazes para a proteção de direitos do cidadão e garantindo proporcionalidade na sua aplicação [...] (MENDES, 2018, p. 24)

Esta Autoridade atua na definição dos parâmetros a serem executados, inclusive pela própria administração pública no tratamento de dados em saúde-especialmente no tocante aos dados epidemiológicos. A definição destes parâmetros coaduna com seu regime de competência, conforme extensamente apresentado no tópico anterior, e permite uma coordenação de esforços no sentido de consecução aos princípios da legislação protetiva.

Chega-se as concludentes iniciais de que: I) O tratamento independente de consentimento para o desenvolvimento de políticas públicas em saúde, como é o caso das políticas epidemiológicas, é totalmente possível e constitucional, visto que os direitos fundamentais à proteção de dados e à autodeterminação informativa não são absolutos; II) Os limites nesse tratamento independente de consentimento são desprendidos da própria legislação, à partir de sua interpretação integrada e harmônica e à partir da própria definição dos princípios e fundamentos que irão reger o tratamento de dados pessoais no Brasil; III) Como a legislação geral de proteção de dados sedimenta suas normas em um certo viés geral, próprio da matéria e da opção a que não fique defasada e sem utilidade em tempo recorde, cabe um papel basilar a ser desempenhado pela Autoridade Nacional de Proteção de Dados na interpretação não só do Artigo 11, inciso II, alínea b, mas deste em relação a LGPD como um todo e em relação a própria Constituição Federal, na afixação dos parâmetros e dos limites atinentes ao tratamento independente de consentimento para o desempenho de políticas públicas epidemiológicas.

A Autoridade Nacional cabe não apenas afixar os parâmetros técnicos de implementação plena da Lei 13.709/2018, como atuar nessa interpretação legal de uma forma sistêmica e integrativa. Ademais, compete a ela até mesmo editar eventuais normas complementares a legislação.

Como resultado desse seu múnus interpretativo dos dispositivos normativos, pode vir a editar normas complementares que indiquem a interpretação e aplicação adequada dos desideratos da lei. Nesse sentido, inclusive, no campo da definição dos limites na aplicação do Artigo 11, inciso II, b pode vir a instrumentalizar regulamentos a dissolverem eventuais controvérsias e clarearem as zonas escuras que, porventura, abram margens a possíveis arbitrariedades nas operações pelo setor público.

Esses limites a serem testificados pela ANPD devem revelar a compreensão da interpretação sistemática da legislação, conforme já abordado, assim como em relação a própria Constituição e demais normativas atinentes a matéria. A nível de desenvolvimento de políticas

públicas, integra-se as legislações desse esforço de efetivação do direito à saúde, as que cuidam das especificidades do campo da saúde, como a que concerne ao próprio SUS (Lei 8.080/90).

Os limites éticos pertinentes, a que também são almejados nessa análise, são os que exprimem, perante esta ponderação pela própria autoridade, a utilidade e necessidade do tratamento daquele dado sensível epidemiológico. Em outras palavras, não faz adentrar questões íntimas do usuário se houver outro meio menos invasivo ou se não for estritamente necessário.

Necessidade essa que deve estar definitivamente atrelada a uma finalidade específica e quando ocorrer seu devido esgotamento não há legitimidade para perpetuar o tratamento e operação quanto aquele dado sensível em saúde. Essa finalidade, como se pode ver e já mui bem destacada e reiterada no corpo do trabalho, imprime, no caso em prospecto, desenvolvimento exímio de uma política pública epidemiológica e na defesa do que pode ser definido como interesse público.

Desenvolvimento de política pública este a revelar o desempenho de um serviço estatal, como é o caso do serviço a saúde e em especial da vigilância epidemiológica, e a proporcionar o "conhecimento, detectação ou prevenção" de fatores que promovem uma modificação no campo da saúde coletiva dos cidadãos, a viabilizar e articular ações de controle e/ou prevenção de forma mais eficaz, condizente com a real situação social e em tempo oportuno, como bem indica o Artigo 6°, §2° da Lei 8.080/90.

Os limites éticos indicam, com a definição platônica (AMORIM, 2018, p.92-93) de ética sob uma finalísticas racional, de uma ação a pender entre o bem ou mal, ao lado adequado ou inadequado e, em última esfera, ao ético ou antiético. É ímpar considerar que o que pode pender ao lado ético ou não vem depender de uma variada gama de considerações, a que devem ser observadas na baliza e consolidação do que se entenderia enquanto tais espécies de limites.

Neste juízo, e na forma de tratamento de dados independente de consentimento para a consecução de políticas públicas epidemiológicas, inclusive com o compartilhamento destes dados entre a administração pública, com a formação dos bancos de dados públicos- como a própria Rede Nacional de Dados em Saúde revela-, as limitações devem ser feitas com a devida parcimônia e de forma a garantir o núcleo essencial dos direitos constitucionais em evidência, sem o sacrifício total de nenhum deles.

Nessa esfera em que há em relevo, de um lado, à autodeterminação informativa, proteção de dados, privacidade e amplo desenvolvimento da personalidade e, por outro, a defesa da saúde, da vida, há que ponderar os direitos em jogo na busca de adoção de limites e

parâmetros próprios. Os parâmetros interpretativos, como bem já visto, quanto a LGPD são desempenhados de forma central pela própria autoridade nacional.

Esses parâmetros levam à baila a efetivação dos princípios constantes na legislação e seus próprios fundamentos. Assim, os limites atinentes a interpretação do Artigo 11, inciso II a serem desempenhados pela ANPD exprimem um compromisso com a promoção máxima da autodeterminação informativa dos usuários, levando as operações sem consentimento a serem efetivadas em esferas bem restritas e necessárias.

Outrossim, quanto ao compartilhamento e operações quanto a esses dados impele que seja feita segundo um ideário de segurança, adequação, não discriminação, prevenção. Bem como o ideário de responsabilização e prestação de contas, que imprime que a administração pública demonstre que vem cumprindo tais normas protetivas e, quando não o faça, seja devidamente responsabilizada.

Esta prevenção limitadora é reivindicada com a adoção dos melhores sistemas informatizados possíveis a estes ideais assinalados, a destaque quanto à segurança. Ademais, como competência da própria ANPD e em virtude das notícias já apresentadas, quanto a hackers no sistemas informatizados de saúde- especificamente na plataforma do *Conect* SUS-, é dever fiscalizar os softwares implementados pelo Ministério da Saúde e apresentar os parâmetros técnicos de segurança a serem seguidos, se não compatíveis com os adequados à luz do princípio da segurança.

Tais esferas de atuação compatibilizam-se com as competências do Conselho Diretor, enquanto órgão máximo da ANPD, contida nos incisos do Artigo 4°, retirado do Anexo 1, do Decreto 10.474/2020. Entre estas competências cabe definir, inclusive os padrões de interoperabilidade de dados, a que cumpre revisar os adotados hoje pelo Ministério da Saúde, vez que seguem os ditames de uma Portaria (2.073) que data de 2011.

Como já realizado com outros órgãos e entes da administração pública, já indicados ao longo do trabalho, também é válida uma atuação elucidativa destes limites. Para tanto é que seria oportuno realizar um acordo de cooperação técnica com o Ministério da Saúde ou demais estruturas públicas diretamente responsáveis por essas operações com os dados pessoais sensíveis em saúde (BRASIL, 2018, Art.55-J, §4°).

Destaca-se que essa atuação na definição de limites interpretativos tem um denodo central pela própria ANPD, a que não impede asseverações por parte do Judiciário e do próprio Supremo Tribunal Federal, a cumprir e complementar tal mister. Essa demarcação de limites não deve ser firmada apenas quando do cometimento de atrocidades e irregularidades no tocante

aos direitos mínimos dos usuários, em verdade o ideal e desejado é que seja feita em um nível primário.

Essa primariedade imprime uma atuação ainda na esfera preventiva e anterior aos desvios éticos e legais. Portanto, é de grande valia que a autoridade nacional enfrente tal questão com a afixação dos parâmetros técnicos desejáveis e interpretativos legais.

Esse cunho interpretativo e elucidativo, por oportuno, deve ser feito não só nos dias atuais, mas em contínua permanência. A deter uma atenção aos desdobramentos que o fenômeno da informatização e os novos aparatos tecnológicos em surgimento e em contínua sofisticação imprimem enquanto novos riscos e novos potenciais ofensivos à direitos mínimos de usuários, cabe sempre atualizar e proceder na análise da interpretação adequada e desejável.

Desenvolver essa elucidação interpretativa também aduz um caráter pedagógico, de indicar a interpretação e os parâmetros adequados aos ditames da Lei Geral de Proteção de Dados. Esse viés pedagógico tem como destinatário não só os operadores e controladores dos dados, mas inclusive o próprio titular do dado.

Apresentar os limites e as balizas no tratamento de dados sinaliza os comportamentos irregulares e arbitrários e permite uma maior eficiência da lei, ao tornar a própria sociedade e os cidadãos comuns fiscalizadores e denunciantes aptos. Assim o caráter pedagógico envolve não apenas administração pública, mas a toda sociedade no que tange ao tratamento com dados sensíveis e com os dados epidemiológicos.

5 CONSIDERAÇÕES FINAIS

A identificação da viabilidade no tratamento de dados sensíveis em saúde no Brasil independente de consentimento constituiu-se como ponto primário do desenvolvimento da presente pesquisa. Partindo de tal permissiva legal, instrumentalizada na forma do Artigo 11, inciso II, e especificamente sua alínea b, da Lei 13.709/2018, o cerne desta produção esteve focado justamente na identificação dos limites atinentes a tal normativa e sua aplicação prática na esfera brasileira.

A temática em voga é de suprema importância, tanto pela contemporaneidade e prematuridade da entrada em vigor da Lei Geral de Proteção de Dados Brasileira (LGPD) e da própria implementação efetiva da Autoridade Nacional de Proteção de Dados (ANPD). Para tanto, a destarte de uma não experiência prática tão concisa, o debate propulsionou-se justamente quanto ao questionamento referente quais são os limites interpretativos atinentes a permissiva legal supramencionada e de forma subsidiária, qual seria o papel desempenhado pela ANPD no que toca essa afixação de balizas interpretativas.

Por oportuno, as hipóteses levantadas no início da atividade de investigação foram confirmadas, apesar de serem melhor desenvolvidas e delineadas neste momento de considerações finais. Quanto à primeira hipótese, ademais dos limites estarem esculpidos nos preceitos interpretativos legais, também estão fundamentos de acordo com uma análise constitucional e ética.

Referente à segunda hipótese, a ANPD além de concernir um papel na efetivação prática e fiscalizatória das balizas interpretativas apresentadas, tem, sobretudo, uma atuação salutar quando do desenvolvimento e fixação desses limites.

Quanto ao primeiro problema suscitado e a concludente alcançada, identificou-se que os limites a balizarem a interpretação do Art. 11, inciso II, alínea b, constituem-se enquanto limites éticos, legais e constitucionais. Os limites legais traduzem-se à partir da própria interpretação integrativa e axiológica da LGPD, assim devem traduzir os princípios e fundamentos que sustentam a legislação especifica, como a segurança, a finalidade, a adequação, utilidade, não discriminação, responsabilidade, boa-fé e outros dos que constam no Art. 6° da legislação.

Os limites éticos refletem e pautam que no processo de aplicação dos preceitos normativos legais, a interpretação apta é a congruente com uma utilidade e adequação que promova menos lesividade e invasão aos direitos fundamentais dos usuários. No âmbito dos limites constitucionais, é primordial que perante conflito entre direitos fundamentais,

justamente nesse esforço de promoção de menor lesividade possível, preserve-se o núcleo essencial destes direitos.

O processo de interpretação de uma lei protetiva firmada em preceitos normativos de aspectos generalistas, incumbe uma atividade ponderadora perante as casuísticas, que garanta a preservação máxima de direitos. Esse juízo de ponderação envolve, de um lado, o direito à proteção de dados e autodeterminação informativa e, por outro, à saúde e à vida, e devem estar alinhados também com os ideários axiológicos norteares da Lei 13.709/2018.

A problemática subsidiária traçada na pesquisa aponta o papel basilar que a ANPD exerce no desenvolvimento dessa atividade interpretativa e elucidativa quanto aos dispositivos normativos atinentes à Lei Geral de Dados. Dessa forma, tem inclusive a competência de editar normas complementares (Art.30), de emitir parecer técnicos (Art.29) e de indicar os padrões técnicos para que os limites referentes ao Art.11 sejam sinalizados e cumpridos de fato.

Destaca-se para essa autoridade além de um papel repressivo, com a imposição de sanções, um papel também preventivo, pedagógico e elucidativo, a direcionar os caminhos interpretativos de forma a guardar mais congruência com os objetivos e direitos fundamentais resguardados na lei.

Os objetivos específicos traçados foram desenvolvidos em três capítulos, em que cada um deles alcançou os desideratos principais levantados. Quanto ao primeiro capítulo tem-se por consideração, a existência consagrada de um direito autônomo à proteção de dados, enquanto histórico e socialmente desenvolvido, à partir da elasticidade conferida ao conceito tradicional de privacidade.

Nesse ponto, primoroso asseverar que o direito à proteção de dados não se confunde com o direito à privacidade e nem se trata de um mero salto evolutivo deste último, houve em verdade o incremento e desenvolvimento de um outro aspecto quanto ao direito clássico de privacidade, de forma a ser condizente aos desdobramentos sociais e jurídicos por ocasião do fenômeno da informatização.

Por oportuno, não pode ser reduzido ou confundido, uma vez que trata-se de um direito autônomo que surge como corolário de outros direitos, como é o caso da privacidade e personalidade, já consagrados na ordem constitucional. Assim é que caminha em igual sentido e propósito máximo, em promover a proteção plena da personalidade humana de acordo com os multicontornos possíveis de serem assumidos.

Quanto ao sistema protetivo brasileiro foi observado que antes da LGPD o Brasil trazia a resolução concernente a questão de dados pessoais aplicando, por analogia, outras legislações esparsas e setoriais. Nesse sentido, a Lei Geral implicou em grande avanço, a promover unidade

e sistematicidade quanto à matéria, apresentando princípios e fundamentos com vistas a nortearem tal temática.

Ao cunho do segundo capítulo avençou-se quanto a importância e necessidade das políticas públicas dentro do Sistema de Saúde, como forma de viabilizar a efetivação do próprio direito constitucional à saúde (Art.196, CRFB/88). A saúde enquanto dever do Estado, depende de uma efetivação prática por meio de uma série de ações estatais e, dessa forma, as políticas públicas assumem um caráter essencial, como é o caso das que coadunam estratégias referentes à vigilância epidemiológica.

Enquanto estas políticas detém relevância primordial firma-se um papel salutar das tecnologias como facilitadoras em seu desenvolvimento e, mais do que isso, na formulação de políticas mais adequadas, eficazes e condizentes com a realidade brasileira. Ao efetuar um mapeamento do precípuo estado situacional brasileiro em um tempo ágil, oportuno e não somente coletar dados, mas estrutura-los de maneira a gerar informações valiosas quanto à saúde, estas tecnologias atuam no nível de capacitação orientando e articulando políticas epidemiológicas mais eficazes e acertadas.

No último capítulo ao analisar a ANPD, sua implementação, seu papel e os limites para o tratamento independente de consentimento, indicou-se o grande avanço da previsão de uma autoridade dotada de autonomia e sob a forma de autarquia especial, tendo sido vislumbrada enquanto fidedigna ao múnus que lhe é incumbido.

A autoridade nacional enquanto própria força motriz de sustentação do sistema protetivo de dados no Brasil, é desenhada no cerne da própria legislação, lhe sendo conferida um amplo regime de competências.

Em um tema tão complexo, cujo cenário aponta para o surgimento de novas tecnologias ou ainda para a sofisticação das existentes, os potenciais riscos à direitos fundamentais mínimos dos usuários são cada vez mais alavancados. Acerta a lei quando está firmada em preceitos gerais, a não promover uma defasagem tão rápida quanto aos possíveis desdobramentos tecnológicos e sociais atinentes ao fenômeno.

Nessa perspectiva, a implementação de uma Autoridade Nacional de Proteção de Dados fortificada e com um papel de centralidade demarcado, é imperiosa para higidez e segurança do próprio sistema protetivo. Para tanto, bem mais do que sua previsão legal e regimental nesses parâmetros, há que perscrutar sua atividade prática, se condizente com o cargo tão importante que lhe foi conferido e se há efetivamente a proteção de dados pessoais.

Esta autarquia desenvolve um extenso rol de competências e, perante a tal complexidade e extensão geográfica brasileira, é relevante o desenvolvimento de uma política de governança

pautada em um ideário de corresponsabilização dos atores envolvidos no campo da internet e das tecnologias atinentes. Quanto a esta corresponsabilidade, o destaque e a articulação incumbe à própria autoridade nacional, que, para além, ainda prefixa os parâmetros técnicos e interpretativos compatíveis com a plena aplicação da lei.

No exercício de tal atividade é também importante uma articulação com os demais órgãos e entes públicos por parte da ANPD. Tal ação integrada compactua no auxílio do enfrentamento da matéria, visando agigantar seu poder de fiscalização e monitoramento sem, contudo, retirar a centralidade que sua especialidade e prerrogativa legal lhe conferem.

O impacto e a contribuição da presente pesquisa é evidenciado, não só pela análise interpretativa e investigativa no campo das diretrizes normativas e constitucionais referentes ao contexto da proteção de dados. Há um claro papel social também em precisar a importância da Autoridade Nacional de Proteção de Dados e seu papel no envolvimento e estímulo a um compromisso de toda a sociedade para a preservação do núcleo essencial protetivo nas operações de dados em território nacional.

Este impacto social também é representado ao pensar-se que a atividade de definição de limites interpretativos atinentes a Lei 13.709/2018 tem como destinatários, além de todos os segmentos da sociedade, precipuamente os gestores em saúde. Para tanto, à partir da fixação das balizas interpretativas, há que se refletir em um compromisso desses atores no seguimento dos preceitos, agora claros e inequívocos, da legislação.

Munidos não apenas da normativa generalista e abstrata que a Lei Geral de Proteção de Dados pode representar, mas também das devidas nuances interpretativas complementares, bem como dos parâmetros técnicos adequados elucidados pela ANPD, é muito mais viável um sistema hígido e com enfoque em uma perspectiva preventiva e pedagógica no campo da proteção de dados pessoais no Brasil.

REFERÊNCIAS

ALMEIDA, Gustavo Palheiro Mendes de. **Proteção de dados no contrato de plano de saúde**: aspectos jurídicos da LGPD na experiência do consumidor. 2020. 231 f. Dissertação (Mestrado em Direito) - Programa de Pós-Graduação da Pontifícia Universidade Católica de São Paulo, Pontifícia Universidade de São Paulo, São Paulo, 2020.

ÀLVAREZ, Carlos. Quem é responsável pela segurança na internet?. *In*: BELLI, Luca; CAVALLI, Olga (org.). **Governança e Regulações da internet na América Latina**. Rio de Janeiro: Escola de Direito do Rio de Janeiro da Fundação Getúlio Vargas, 2019.

ARAGÃO, Suéllyn Mattos de; SCHIOCCHET, Taysa. Lei Geral de Proteção de Dados: desafio do Sistema Único de Saúde. **Revista Eletrônica de Comunicação, Informação & Inovação em Saúde**, [*s. l.*], jul./set. 2020.

AZEVEDO, Daniel Sampaio de. **Base do Legítimo Interesse**: dinâmica normativa e o direito à proteção de dados pessoais. 2021. Dissertação (Mestrado em Ciências Jurídicas) - Programa de Pós- Graduação em Ciências Jurídicas, Universidade Federal da Paraíba, João Pessoa, 2021.

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

BITTAR, Carlos A. **Os Direitos da Personalidade. 8; ed.** São Paulo: Saraiva, 2015.

BRASIL. [Constituição (1988)]. **Constituição da República Federativa do Brasil**. Brasília, DF: Presidência da República, 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm. Acesso em: 15 set. 2022.

BRASIL. **Lei nº 10.406, de 10 de janeiro de 2002**. Institui o Código Civil. Brasília, DF: Presidência da República, 2002. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/2002/l10406compilada.htm. Acesso em: 1 jun. 2022.

BRASIL. **Lei nº 12.037, de 1 de outubro de 2009**. Dispõe sobre a identificação criminal do civilmente identificado, regulamentando o art. 5º, inciso LVIII, da Constituição Federal. Brasília, DF: Presidência da República, 2009. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2007-2010/2009/lei/l12037.htm. Acesso em: 1 jun. 2022.

BRASIL. **Lei nº 12.414, de 9 de junho de 2011**. Disciplina a formação e consulta a bancos de dados com informações de adimplemento, de pessoas naturais ou de pessoas jurídicas, para formação de histórico de crédito. Brasília, DF: Presidência da República, 2011a. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12414.htm. Acesso em: 1 jun. 2022.

BRASIL. **Lei nº 12.527, de 18 de novembro de 2011**. Regula o acesso a informações previsto no inciso XXXIII do art. 5º , no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá

outras providências. Brasília, DF: Presidência da República, 2011b. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm. Acesso em 01 de jun. 2022.

BRASIL. **Lei nº 12.965, de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília, DF: Presidência da República, 2014. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 2 jun. 2022.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 10 jun. 2022.

BRASIL. **Lei nº 4.117, de 27 de agosto de 1962**. Institui o Código Brasileiro de Telecomunicações. Brasília, DF: Presidência da República, 1962. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l4117compilada.htm. Acesso em: 3 jun. 2022.

BRASIL. **Lei nº 8.078, de 11 de setembro de 1990**. Dispõe sobre a proteção do consumidor e dá outras providências. Brasília, DF: Presidência da República, 1990a. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm. Acesso em: 1 jun. 2022.

BRASIL. **Lei nº 8.080, de 19 de setembro de 1990**. Dispõe sobre as condições para a promoção, proteção e recuperação da saúde, a organização e o funcionamento dos serviços correspondentes e dá outras providências. Brasília, DF: Presidência da República, 1990b. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8080.htm. Acesso em: 27 out. 2022.

BRASIL. Supremo Tribunal Federal**. Medida Cautelar em Ação Direta de Inconstitucionalidade nº 6389**. Voto Conjunto ADIs 6.389, 6.390, 6.391, 6.393, 6.388 e 6.387- Ministro Gilmar Mendes. Relator: Ministra Rosa Weber. Brasília, DF: STF, 2020. Disponível em: https://www.conjur.com.br/dl/pandemia-reforca-necessidade-protecao.pdf. Acesso em: 29 set. 2021.

CACHAPUZ, Maria Claúdia; JOBIM, Maria Luiza Kurban. Da proteção de dados a uma política pública de privacidade. *In*: CALDEIRA, Cristina Maria de Gouveia; PINHEIRO, Alexandre Sousa (org.). Privacy and Data Protection Magazine. **Revista Científica na Área Jurídica**, [*s. l.*], n. 1, 2021.

CANCELIER, Mikhail Vieira de Lorenzi. O direito à privacidade hoje: perspectiva histórica e o cenário brasileiro. **Revista Sequência**, Florianópolis, n. 76, p. 213-240, ago. 2017.

CARVALHO, Marcelo Sávio Revoredo Mendes de. **A trajetória da internet no Brasil**: do surgimento das redes de computadores à instituição dos mecanismos de governança. 2006. 260 f. Dissertação (Mestrado em Engenharia da Computação) - Programa de Pós-Graduação de Engenharia da Universidade Federal do Rio de Janeiro, Universidade Federal do Rio de Janeiro, Rio de Janeiro, 2006.

COLOMBO, Cristiano; FACCHINI NETO, Eugênio. Mineração de dados e análise preditiva: reflexões sobre possíveis violações ao direito de privacidade na sociedade da informação e critérios para sua adequada implementação à luz do ordenamento brasileiro. **Revista de Direito, Governança e Novas Tecnologias**, [*s. l.*], v. 3, n. 2, p. 59-80, jul./dez. 2017.

COMITÊ GESTOR DA INTERNET NO BRASIL. **Documentos da Cúpula Mundial sobre a Sociedade da Informação**- Genebra 2003 e Túnis 2005. Cadernos Cgi.br, 2014. Disponível em: https://www.cgi.br/media/docs/publicacoes/1/CadernosCGIbr_DocumentosCMSI.pdf. Acesso em: 15 ago. 2022.

CONSENTINO, Leonardo A. M. Aspectos evolutivos da interação homem máquina: Tecnologia, computador e evolução humana. *In*: PRADO, Oliver Zancul; FORTIM, Ivelise; CONSENTINO, Leonardo (org.). **Psicologia & Informática**: produções do III psicoinfo e II jornada do NPPI. São Paulo: Conselho Regional de Psicologia de São Paulo, 2006.

COSTA, Ramon Silva; OLIVEIRA, Samuel Rodrigues de. Os direitos da personalidade frente à sociedade de vigilância: privacidade, proteção de dados pessoais e consentimento nas redes sociais. **Revista Brasileira de Direito Civil em Perspectiva**, [*s. l.*], v. 5, n. 2, p. 22-41, jul./dez. 2019.

CUNHA, Anita Spies da. A autodeterminação informativa na jurisprudência alemã além da volkszailungsurteil: da tradicional dimensão subjetiva ao reconhecimento da dimensão objetiva. *In*: SARLET, Ingo Wolfgang; MARTINS, Amanda Donadello (org.). **Constituição e Direitos Fundamentais:** jurisprudência nacional, estrangeira e internacional comentada. Porto Alegre: Fundação Fênix, 2022.

CUNHA; Edite de Penha; CUNHA, Eleonora Schettini M. Políticas públicas sociais. *In*: CARVALHO, Alysson; SALLES, Fátima; GUIMARÃES, Marília; UDE, Walter (org.). **Políticas Públicas**. Belo Horizonte: UFMG, 2003.

DANIEL, Vanessa Marques; PEREIRA, Gabriela Viale; MACADAR, Marie Anne. Perspectiva Institucional dos Sistemas de Informação em Saúde em dois estados brasileiros**.** **Revista de Administração Contemporânea**, [*s. l.*], v. 18, n. 5, p. 650-669, set./out. 2014.

DONEDA, Danilo. A proteção dos dados pessoais como um direito fundamental. Revista Espaço Jurídico. **Revista Espaço Jurídico**, Joçaba, v. 12, n. 2, p. 91-108, jul/dez. 2011.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. 2. ed. São Paulo: Thompson Reuters Brasil, 2020.

DONEDA, Danilo. Panorama Histórico da proteção de Dados Pessoais. *In*: BIONI, Bruno Ricardo (coord.). **Tratado de Proteção de Dados Pessoais**. Rio de Janeiro: Forense, 2021.

DONEDA, Danilo; MENDES, Laura Schertel. Um perfil da nova Lei Geral de Proteção de Dados brasileira. *In*: BELLI, Luca; CAVALLI, Olga (org.). **Governança e Regulações da internet na América Latina**. Rio de Janeiro: Escola de Direito do Rio de Janeiro da Fundação Getúlio Vargas, 2019.

EUROPEAN UNION LAW. **Directiva 95/46/CE do Parlamento Europeu e Conselho**. Relativa à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. Luxemburgo: Parlamento Europeu, 1995. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A31995L0046. Acesso em: 20 set. 2021.

EUROPEAN UNION LAW. **Regulation (EU) 2016/679 of 27 April 2016**. Luxemburgo: Parlamento Europeu, 2016. Disponível em: https://eur-lex.europa.eu/legal-content/EN-PT-ES/TXT/?from=EN&uri=CELEX%3A02016R0679-20160504. Acesso em 13 de set. 2021.

FANTONELLI, Miliane; CELUPPI, Ianka Cristina; OLIVEIRA, Fernanda Maia de; BURIGO, Fernando; DALMARCO, Eduardo Monguilhott; WAZLAWICK, Raul Sidnei. Lei geral de proteção de dados e a interoperabilidade na saúde pública. ***Journal of Health Informatics***, [*s. l.*], n. especial, dez. 2020.

FORNAZIN, Marcelo. **A informatização da saúde no Brasil**: uma análise multi-paper inspirada na teoria ator-rede. 2015. 164 f. Tese (Doutorado em Administração) - Programa de Doutorado em Administração da Escola Brasileira de Administração Pública e de Empresas da Fundação Getúlio Vargas, Fundação Getúlio Vargas, Rio de Janeiro, 2015.

FOUCALT, Michel. **Microfísica do poder**. 13. ed. Rio de Janeiro: Graal, 1979.

GARCIA, Rafael Silveira. **O papel da autoridade nacional de proteção de dados e os co-legitimados na defesa dos titulares de dados pessoais**. 2021. 116 f. Dissertação (Mestrado em Direito) - Programa de Mestrado Profissional em Direito, Instituto Brasileiro de Ensino, Pesquisa e Desenvolvimento, Brasília, 2021.

GNOATTON, Letícia Mulinari. **A conformidade da Autoridade Nacional de Proteção de Dados aos critérios exigidos pela União Europeia para a concessão da decisão de adequação ao Brasil nos termos do Regulamento Geral de Proteção de Dados**. 2021. 183 f. Dissertação (Mestrado em Direito) - Programa de Pós-Graduação de Direito da Universidade Federal de Santa Catarina, Universidade Federal de Santa Catarina, Florianópolis, 2021.

GODOY, Claudio Luiz Bueno de. Desafios atuais dos direitos da personalidade. *In*: CORREIA, Atalá; CAPUCHO, Fábio Jun. **Direitos da personalidade:** a contribuição de Silmara J. A. Chinellato. São Paulo: Manole, 2019.

GONÇALVES, Vinicius Aquini. A proteção de dados relativos à saúde na prestação de serviços de computação em nuvem. **Lex Medicinae - Revista Portuguesa de Direito da Saúde**, Coimbra, ano 17, n. 33, 2020.

KONDER, Carlos Nelson. O tratamento de dados sensíveis à luz da Lei 13.709/2018. *In*: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (coord.). **Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro**. São Paulo: Thomson Reuters Brasil, 2019.

KORKMAZ, Maria Regina Detoni Cavalcanti Rigolon. **Dados sensíveis na lei geral de proteção de dados pessoais**: mecanismos de tutela para o livre desenvolvimento da personalidade. 2019. 119 f. Dissertação de Mestrado (Mestrado em Direito) - Programa de Pós-Graduação da Faculdade de Direito, Universidade Federal de Juiz de Fora, Juiz de Fora, 2019.

LEME, Renata Salgado; BLANK, Marcelo. Jurisprudência e legislação sanitária comentadas Lei Geral de Proteção de Dados e segurança da informação na área da saúde. **Cadernos Iberoamericanos de Direito Sanitário**, [*s. l.*], v. 9, n. 3, jul./set. 2021.

LIMA, Cíntia Rosa Pereira de. Agentes de Tratamento de Dados Pessoais. *In*: LIMA, Cíntia Rosa Pereira de (coord.). **Comentários à Lei Geral de Proteção de Dados**. Portugal: Grupo Almedina, 2020.

LIVRE Desenvolvimento da Personalidade - BVERFGE 65, 1 (Volkszahlung). *In*: MARTINS, Leonardo (org.). **Cinquenta anos de jurisprudência do Tribunal Constitucional Federal Alemão**. Uruguai: Konrad Adenauer Stiftung, 2005.

MENDES, Laura Ferreira Schertel. Comentário à nova Lei de Proteção de Dados (Lei 13.709/2018): o novo paradigma da proteção de dados no Brasil. **Revista de Direito do Consumidor**, [*s. l.*], v. 120, p. 555-587, nov./dez. 2018a.

MENDES, Laura Ferreira Schertel. Habeas Data e Autodeterminação Informativa: os dois lados da mesma moeda. **Revista Direitos Fundamentais & Justiça**, Belo Horizonte, v. 12, n. 39, p. 185-216, jul./dez. 2018b.

MENDES, Laura Ferreira Schertel. **Privacidade, proteção de dados e defesa do consumidor**: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014. (Série IDP - Linha de pesquisa acadêmica).

MENDES, Laura Ferreira Schertel; FONSECA, Gabriel Campos Soares da. STF reconhece direito fundamental à proteção de dados. **Revista de Direito do Consumidor**, [*s. l.*], v. 130, p. 471-478, jul./ago. 2020.

MENDES, Laura Schertel Ferreira. Autodeterminação Informativa: a história de um conceito. **Revista de Ciências Jurídicas Pensar**, [*s. l.*], v. 25, n. 4, p.1-18, out./dez. 2020.

MENEZES NETO, Elias Jacob de. **Surveillance, Democracia e Direitos Humanos**: os limites do Estado na era do Big Data. 2016. 291 f. Tese (Doutorado em Direito) - Programa de Pós-Graduação em Direito da Universidade do Vale do Rio dos Sinos, Universidade do Vale do Rio dos Sinos, São Leopoldo, 2016.

MOHR, Tatiana. **Aspectos jurídicos da proteção de dados pessoais sob a perspectiva do Estado**. 2019. 97 f. Dissertação de Mestrado (Mestrado em Direito) - Programa de Mestrado em Direito da Universidade de Marília, Universidade de Marília, Marília, 2019.

NUNES, Gonçalo Alexandre Ferreira. **O tratamento de dados pessoais de saúde à luz do regulamento geral europeu de proteção de dados pessoais**. 2019. 80 f. Dissertação de Mestrado (Mestrado em Gestão e Economia da Saúde) - Faculdade de Economia, Universidade de Coimbra, Coimbra, 2019.

PARENTONI, Leonardo Netto. Por que confiar na Autoridade Nacional de Proteção de Dados?. **Revista da Faculdade de Direito da UFMG**, Belo Horizonte, n. 79, p. 163-192, jul./dez. 2021.

PÉRET MOTTA, Clara Amédée. Evolução legislativa do direito digital: a influência europeia na Lei geral de proteção de dados e na criação da autoridade nacional de proteção de dados. **Revista controle**, [*s. l.*], v. 20, n. 1, p. 50-69, jan./jun. 2022.

REDE NACIONAL DE DADOS EM SAÚDE. **Ações para a adequação da RNDS à Lei Geral de Proteção de Dados**. Brasília, DF: jun. 2020. Disponível em: https://www.gov.br/saude/pt-br/assuntos/saude-digital/material-de-apoio/AesparaaAdequaodaRNDSLGPD24.06.2020.pdf. Acesso em: 27 out. 2022.

RODOTÀ, Stefano. **A vida na sociedade da vigilância**: a privacidade hoje. São Paulo: Renovar, 2008.

RUARO, Regina Linden. Algumas reflexões em torno do RGPD, em especial quanto ao consentimento, com alusões à LGPD (um exercício interpretativo). **Revista Direitos Fundamentais & Justiça**, Belo Horizonte, v.14, n. 42, p. 219-249, jan./jun. 2020.

RUARO, Regina Linden; MOLINARO, Carlos Alberto. Conflito real ou aparente de interesses entre o direito fundamental à proteção de dados pessoais e o livre mercado. *In*: RUARO, Regina Linden; PIÑAR MAÑAS, José Luis; MOLINARO, Carlos Alberto (org.). **Privacidade e proteção de dados pessoais na sociedade digital.** Porto Alegre: Fi, 2017.

RUARO, Regina Linden; RODRIGUEZ, Daniel Piñeiro. O direito à proteção de dados pessoais e a privacidade. **Revista da Faculdade de Direito- UFPR**, Curitiba, n. 53, p. 45-66, 2011.

RUARO, Regina Linden; RODRIGUEZ, Daniel Piñeiro. O direito à proteção dos dados pessoais: uma leitura do sistema europeu e a necessária tutela dos dados sensíveis como paradigma para um sistema jurídico brasileiro. **Revista Direitos Fundamentais & Justiça**, [*s. l.*], n. 11, abr./jun. 2010.

RUARO, Regine Linden; SILVA, Cecília Alberton Coutinho. Proteção de Dados e o Acordo de Livre Comércio Mercosul-União Europeia: Notas sobre a Adequação da Autoridade Nacional de Proteção de Dados no Brasil. **Revista de Direito Público**, [*s. l.*], v. 18, n. 98, p. 909-944, mar./abr. 2021.

SALES, Gabrielle Bezerra; MOLINARO, Carlos Alberto. Impactos da computação pervasiva na esfera da privacidade e da ética. **Revista de Estudos e Pesquisas Avançadas do Terceiro Setor**, [*s. l.*], v. 4, n. 2, p. 328-351, jul./dez. 2017.

SANTOS, Tamyres Oliveira dos; PEREIRA, Letícia Passos; SIVEIRA, Denise Tolfo. Implantação de sistemas informatizados na saúde: uma revisão sistemática. **Revista Eletrônica de Comunicação, Informação & Inovação em Saúde**, [*s. l.*], p. 1-11, jul./set. 2017.

SARLET, Gabrielle Bezerra Sales; CALDEIRA, Cristina. O consentimento informado e a proteção de dados pessoais de saúde na internet: uma análise das experiências legislativas de Portugal e do Brasil para a proteção integral da pessoa humana. **Revista Civilistica.com**, [*s. l.*], v. 8, n. 1, 2019.

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

SARLET, Gabrielle Bezerra Sales; RUARO, Regina Linden. A proteção de Dados sensíveis no sistema normativo brasileiro sob o enfoque da Lei Geral de Proteção de Dados (LGPD)- L 13.709/2018. **Revista Direitos Fundamentais e Democracia**, [*s. l.*], v. 26, n. 2, p. 81-106, maio/ago. 2021.

SARLET, Ingo Wolfgang. **Eficácia dos Direitos Fundamentais**: uma teoria geral dos direitos fundamentais na perspectiva constitucional. 13. ed. Porto Alegre: Livraria do Advogado, 2018.

SARLET, Ingo Wolfgang. O direito fundamental à proteção de dados pessoais na Constituição Federal Brasileira de 1988. *In*: CALDEIRA, Cristina Maria de Gouveia; PINHEIRO, Alexandre Sousa (org.). Privacy and Data Protection Magazine. **Revista Científica na Área Jurídica**, [*s. l.*], n. 1, 2021.

SARLET, Ingo Wolfgang; MARINONI, Luiz Guilherme; MITIDIERO, Daniel. **Curso de Direito Constitucional**. 9. ed. São Paulo: Saraiva Educação, 2020.

SCHEREIBER, Anderson. **Direitos da Personalidade**. 3. ed. São Paulo: Atlas, 2014.

SILVA, José Afonso da. **Curso de Direito Constitucional Positivo**. 39. ed. São Paulo: Malheiros, 2016.

SOUZA, Celina. Políticas Públicas: uma revisão de literatura. **Revista de Sociologias**, Porto Alegre, v. 8, n. 16, p. 20-45, jul./dez. 2006.

SZINVELSKI, Mártin Marks; ARCENO, Taynara Silva; FRANCISCO, Lucas Baratieri. Perspectivas jurídicas da relação entre big data e proteção de dados. **Revista Perspectivas em Ciência de Informação**, [*s. l.*], v. 24, n. 4, p. 132-144, out./dez. 2019.

TOBBIN, Raíssa Arantes; CARDIN, Valéria Silva Galdino. Perfis informacionais e publicidade comportamental: direito à autodeterminação informativa e a proteção de dados pessoais no ambiente virtual. *In:* CONGRESSO BRASILEIRO DE PROFESSO COLETIVO E CIDADANIA, 8., 2020. **Anais** [...]. [*S. l.: s. n.*], out. 2020. p. 1260-1276.

TOBBIN, Raíssa Arantes; CARDIN, Valéria Silva Galdino. Tecnologias vestíveis e capitalismo de vigilância: do compartilhamento de dados sobre saúde e a proteção dos direitos da personalidade. **Revista de Direito, Governança e Novas Tecnologias**, [*s. l.*], v. 7, n. 1, p. 126-147, jan./jul. 2021.

TRATADO sobre o Funcionamento da União Europeia (Versão Consolidada). 2016. Jornal Oficial da União Europeia, 7 jun. 2016. Disponível em: https://eur-lex.europa.eu/resource.html?uri=cellar:9e8d52e1-2c70-11e6-b497-01aa75ed71a1.0019.01/DOC_3&format=PDF. Acesso em: 10 ago. 2022.

TRAVINCAS, Amanda Costa Thomé**. Restrições aos Direitos Fundamentais não expressamente autorizadas pela Constituição Brasileira**: Estrutura, Fundamentos e Metodologias de Controle. 2010. 185 f. Dissertação (Mestrado em Direito) - Programa de Pós- Graduação em Direito pela Pontifícia Universidade Católica do Rio Grande do Sul, Pontifícia Universidade Católica do Rio Grande do Sul, Porto Alegre, 2010.

UNIÃO EUROPEIA. Carta dos Direitos Fundamentais da União Europeia. **Jornal Oficial da Comunidade Europeia,** [*s. l.*], 26 out. 2012. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:12012P/TXT&from=CS. Acesso em: 29 set. 2021.

VENTURA, Miriam; COELI, Claúdia Medina. Para além da privacidade: direito à informação na saúde, proteção de dados pessoais e governança. **Cadernos de Saúde Pública**, [*s. l.*], v. 34, n. 7, 2018.

VIOLA, Mario; TEFFÊ, Chiara Spadaccini de. Tratamento de dados pessoais na LGPD: estudo sobre as bases legais dos artigos 7° e 11. *In*: BIONI, Bruno (coord.). **Tratado de Proteção de Dados Pessoais**. Rio de Janeiro: Grupo Editorial Nacional, 2020.

WARREN, Samuel D.; BRANDEIS, Louis D. The right of privacy. **Havard Law Review**, [*s. l.*], v. 4, n. 5, p. 193-220, Dec. 1890. Disponível em: https://www.jstor.org/stable/1321160?seq=1#metadata_info_tab_contents. Acesso em: 15 set. 2021.

ZANATTA, Rafael A. F.; SOUZA, Michel R. O. A tutela coletiva na proteção de dados pessoais: tendências e desafios. *In*: LUCCA, Newton de; ROSA, Cíntia. **Direito & Internet IV: Proteção de Dados Pessoais**. São Paulo: Quartier Latin, 2019.

ZUBOFF, Shoshana. **A era do capitalismo de vigilância**. Tradução de George Schlesinger. Rio de Janeiro: Intrínseca, 2019.