CENTRO UNIVERSITÁRIO UNDB
CURSO DE DIREITO

SAMANDA PEREIRA SANTOS

A EFICÁCIA DOS DIREITOS FUNDAMENTAIS NA SOCIEDADE DA INFORMAÇÃO: Uma análise acerca da proteção e promoção de dados em matéria de saúde

São Luís
2020

SAMANDA PEREIRA SANTOS

A EFICÁCIA DOS DIREITOS FUNDAMENTAIS NA SOCIEDADE DA INFORMAÇÃO: Uma análise acerca da proteção e promoção de dados em matéria de saúde

Projeto de Monografia apresentado ao Curso de Graduação em Direito do Centro Universitário UNDB como requisito parcial para obtenção do grau e Bacharela em Direito.

Orientadora: Profa. Dra. Amanda Costa Thomé Travincas

São Luís

2020

Dados Internacionais de Catalogação na Publicação (CIP)
Centro Universitário - UNDB / Biblioteca

Santos, Samanda Pereira

A eficácia dos direitos fundamentais na sociedade da informação: uma análise acerca da proteção e promoção de dados em matéria de saúde. / Samanda Pereira Santos. __ São Luís, 2020.

89 f.

Orientadora: Profª. Dra. Amanda Costa Thomé Travincas.

Monografia (Graduação em Direito) - Curso de Direito – Centro Universitário Unidade de Ensino Superior Dom Bosco – UNDB, 2020.

1. Lei Geral de Proteção de dados. 2. Dados pessoais. 3. Sociedade da informação. 4. Saúde Digital. I. Título.

CDU 340:004.796

SAMANDA PEREIRA SANTOS

A EFICÁCIA DOS DIREITOS FUNDAMENTAIS NA SOCIEDADE DA INFORMAÇÃO: Uma análise acerca da proteção e promoção de dados em matéria de saúde

Projeto de Monografia apresentado ao Curso de Graduação em Direito do Centro Universitário UNDB como requisito parcial para obtenção do grau e Bacharela em Direito.

Aprovada: 11 /12/ 2020.

BANCA EXAMINADORA

_____

Profa. Dra. Amanda Costa Thomé Travincas (Orientadora)
Centro Universitário UNDB

_____

Procurador Federal Daniel Piñeiro Rodriguez
Procuradoria Geral Federal-PGF

_____

Prof. Me. Arnaldo Vieira Sousa
Centro Universitário UNDB

AGRADECIMENTOS

A Deus, por incluir minha vida em seus planos, por seu amor infinito e pela suas bençãos inimagináveis. Agradeço por ter me sustentado até aqui e escutado minhas orações, nunca serei capaz de retribuir tanto amor.

À minha família, que nunca mediu esforços para contribuir na minha formação acadêmica e pessoal. Em especial meu pai Alcino e minha avó Maria José, que em momentos de caos e alegria sempre estiveram ao meu lado, sou grata por terem me proporcionado uma boa educação, para que eu pudesse trilhar os meus próprios caminhos.

Às minhas amigas de faculdade, Marília, Bia, Kaianne e Adriana que, direta ou indiretamente, me ajudaram no percurso acadêmico. Todos os momentos que passamos juntas na UNDB ficarão guardados com muito carinho. Também agradeço a Malysson, um amigo que sem querer querendo encontrei na UNDB, por ter me encorajado e apoiado durante o período de escrita.

Aos Defensores e amigos que conheci no Núcleo da Infância e Juventude da DPE/MA, por todo o aprendizado que obtive durante dois anos como estagiária que foram essenciais para o meu crescimento.

À minha orientadora Amanda Thomé, por ter acreditado em mim como monitora e orientanda. Obrigada por sempre se mostrar atenciosa e disponível desde a primeira reunião. Agradeço o carinho, incentivo e por toda a dedicação e orientação que proporcionaram a concretização dessa pesquisa. Obrigada por ser um exemplo, serei sempre grata por todos os ensinamentos.

A todos que contribuíram no meu percurso e na minha jornada acadêmica, meus sinceros agradecimentos.

Como diria Belchior “presentemente, eu posso até me considerar um sujeito de sorte, porque apesar de muito moço me sinto sã, salvo e forte.”

"La grande trasformazione tecnologica cambia il quadro dei diritti civili e politici, ridisegna il ruolo dei poteri pubblici, muta i rapporti personali e sociali, e incide sull'antropologia stessa delle persone."

(Stefano Rodotá)

RESUMO

Esta monografia se propõe a debater a proteção de dados pessoais em saúde na sociedade da informação. O problema principal a ser enfrentado consiste nos artifícios necessários para que o avanço da sociedade da informação não cause o esvaziamento na garantia do direito fundamental à proteção de dados pessoais sensíveis em matéria de saúde, sendo a principal hipótese a de que o consentimento, a autodeterminação informativa e a adequação da LGPD acabam contribuindo na tutela de dados pessoais. Para isso traz o destaque da sociedade da informação, os seus potenciais riscos aos direitos de personalidade e as principais normativas que trataram sobre a tutela de informações pessoais. Em um segundo momento recebem destaque o direito à privacidade e a necessidade de reconhecer o direito a proteção de dados pessoais como um direito fundamental autônomo, ademais, é elucidado a base principiológica que orienta aplicação da LGPD no tratamento de dados pessoais. Por fim, é apresentado a aplicação da tecnologia no sistema de informação e comunicação (TIC) e os desafios e benefícios da implantação da saúde digital, bem como a tutela especial que é dada pela LGPD aos dados pessoais de saúde. Quanto ao método científico, entende-se que se aplica ao estudo o método dedutivo ao passo que se parte de uma ideia geral e direciona-se a conclusões particulares por meio de um raciocínio lógico e, a técnica de pesquisa é bibliográfica, recorrendo-se, em especial, a dados indiretos.

Palavras-chave: Dados Pessoais. Dados Pessoais Sensíveis. Saúde Digital. Sociedade da Informação.

ABSTRACT

This monograph proposes to discuss the protection of personal data on health in the information society. The main problem to be faced consists in the necessary artifices so that the advancement of the information society does not cause the loss of the guarantee of the fundamental right to the protection of sensitive personal data in health matters, the main hypothesis being that the consent, the informative self-determination and the adequacy of the LGPD end up contributing to the protection of personal data. For this, it brings the prominence of the information society, its potential risks to the rights of personality and the main norms that have dealt with the protection of personal information. The right to privacy and the need to recognize the right to the protection of personal data as an autonomous fundamental right are also highlighted. In addition, the principles that guide the application of LGPD in the treatment of personal data are clarified. Finally, the application of technology in the information and communication system (ICT) and the challenges and benefits of the implementation of digital health are presented, as well as the special protection that is given by LGPD to personal health data. As for the scientific method, it is understood that the deductive method is applied to the study, whereas it starts from a general idea and is directed to particular conclusions through logical reasoning, and the research technique is bibliographic, using, in particular, indirect data.

Keywords: Digital Health. Information Society. Personal Data. Sensitive Personal Data.

LISTA DE ABREVIATURAS E SIMBOLOS

ADIN	Ação Direita de Inconstitucionalidade
ANPD	Autoridade Nacional de Proteção de Dados
CDC	Código de Defesa do Consumidor
LAI	Lei do Acesso à Informação
LGPD	Lei Geral de Proteção de Dados Pessoais
MCI	Marco Civil da Internet
MP	Medida Provisória
OEA	Organização dos Estados Americanos
ONU	Organização das Nações Unidas
PEC	Proposta de Emenda à Constituição
PL	Proposta de Lei
STF	Supremo Tribunal Federal
TIC	Tecnologia de Informação e Comunicação
TISS	Troca de Informação de Saúde Suplementar
§	Parágrafo
§§	Parágrafos

SUMÁRIO

1 INTRODUÇÃO

O presente estudo destina-se a entender os novos paradigmas que estão se formando através do desenvolvimento da sociedade da informação, em especial o direito à proteção de dados pessoais, investigando a necessidade de reconhecimento como direito fundamental autônomo nessa nova conjuntura social, econômica e política, reconhecida pela mitigação da intimidade e da vida privada diante da ampliação dos avanços da tecnologia da informação, buscando tratar de forma mais específica os seus impactos na área da saúde. Exposto isso, o problema que orienta a pesquisa reside na seguinte indagação: quais são os artifícios necessários para que os avanços da sociedade da informação não causem o esvaziamento na garantia do direito fundamental à proteção de dados pessoais sensíveis em matéria de saúde?

A inclusão das tecnologias de informação e comunicação (TIC) no âmbito da saúde vem merecendo um real destaque na atual sociedade da informação. Esse novo modelo de organização social possibilitou que as diversas formas de interações humanas fossem se adequando a era das "Revoluções Tecnológicas", de modo que o amplo uso das modernas tecnologias de informação garantiu o intenso fluxo de utilização de informações e processamento de dados pessoais.

Nada obstante, no Brasil, foi aprovada a lei 13.709/18 sobre a proteção de dados pessoais, conhecida como Lei Geral de Proteção de Dados (LGPD), o texto se tornou um importante meio de proteção aos direitos fundamentais de privacidade, liberdade e o livre desenvolvimento da personalidade, além disso, buscou fomentar o desenvolvimento econômico, tecnológico e a inovação com a imposição de regras para o adequado uso dos dados pessoais. Sucede que, a Lei Geral de Proteção de Dados considerou que dados relacionados à saúde são considerados dados sensíveis, desta forma, a lei buscou intensificar a proteção de dados sensíveis através de fortes mecanismos que não admitem a utilização de dados para atender interesses lucrativos de empresas controladoras de dados pessoais e terceiros.

No entanto, cabe destacar que ao mesmo tempo em que por um lado a sociedade da informação proporciona novos rumos de difusão e aperfeiçoamento da tecnologia às esferas das atividades humanas, por outro, oportuniza o aumento na quantidade de tratamentos de informações pessoais, ou seja, o crescimento na capacidade de armazenamento e comunicação de dados pessoais possibilita as distintas formas que tais dados podem ser apropriados e utilizados de forma indevida ou abusiva. Por isso, reconhece-se a existência de uma sociedade de risco que se mostra uma ameaça a garantia dos direitos personalíssimos.

Em matéria de saúde não é diferente, as possibilidades dos benefícios trazidos pela saúde eletrônica são essenciais para promoção do direito à saúde, mas é preciso observar os riscos a proteção de dados pessoais sensíveis que possam advir de programas que se encarregam de exercer a prestação de serviços de tecnologia no sistema de saúde. Desta forma, o novo cenário da pandemia do Covid-19 apresentou claramente os benéficos e riscos do tratamento de dados pessoais em saúde.

A par disso, é pertinente pontuar que com o avanço da sociedade da informação novos contornos da privacidade precisam ser traçados, já que, mesmo o direito fundamental à privacidade ser amplamente tutelado pela Constituição Federal, há o surgimento de novos direitos que necessitam ser protegidos e garantidos como, por exemplo, o direito a proteção de dados pessoais que apesar de não ser positivado expressamente na Constituição Federal, passou a ser considerado como um direito fundamental autônomo, inclusive na Lei Geral de Proteção de Dados Pessoais. Sendo assim, o tratamento diferenciado dado pela LGPD aos dados sensíveis e o reconhecimento do direito à proteção de dados pessoais como um direito fundamental autônomo, mostram-se, em primeiro momento, importantes mecanismos para tutelar o tratamento de dados pessoais no âmbito da saúde.

Nesta senda, o objetivo geral do presente estudo é analisar as condições de garantia do direito fundamental à proteção de dados pessoais de saúde na sociedade da informação. Para tanto, tem como objetivos específicos, examinar o surgimento da sociedade da informação e seus impactos perante o ordenamento jurídico brasileiro; discutir sobre o direito à privacidade e os seus novos contornos perante a proteção de dados pessoais enquanto direito fundamental e abordar de que forma se dá o uso de dados pessoais no âmbito da saúde eletrônica no Brasil e o tratamento da Lei Geral de Proteção de Dados em matéria de dados de saúde.

Quanto à justificativa, divide-se em acadêmica, importância social e motivação pessoal. Ao que diz respeito à comunidade acadêmica, a atuação do ordenamento jurídico em garantir a tutela e efetivação de proteção de dados pessoais sensíveis é imprescindível para adequação às necessidades públicas das organizações sociais e empresas. Quanto à importância social, a saúde eletrônica se tornou um importante meio de promoção da saúde, proporcionando qualidade e eficiência dos cuidados de saúde, apesar dos proveitos garantindo a sociedade, esta não pode deixar de estar atenta as formas de consentimento e utilização dos seus dados pessoais por empresas controladoras e pelo Estado.

Por fim, a discussão tornou-se básica a presente pesquisadora, pois, diante de um site de notícias UOL, se deparou com a notícia sobre as falhas que ocorreram no sistema de segurança no aplicativo do E-Saúde fornecido pelo Ministério da Saúde em que foram expostos

dados pessoais de milhares de pacientes usuários do Sistema Único de Saúde, durante sete meses, sendo assim, foi possível identificar a vulnerabilidade que os dados pessoais sensíveis possuem no ambiente virtual.

Nesse sentido, a pesquisa fez uso do método dedutivo partindo da análise geral sobre a sociedade informacional e o direito à proteção de dados, para o particular, de modo a observar proteção desse direito na área da saúde. Para isso, tal pesquisa se desenvolve a partir de uma pesquisa bibliográfica desenvolvida com base em material já publicado, constituído principalmente de livros de direito fundamental, proteção de dados pessoais e artigos científicos publicados e disponíveis na internet, conforme a classificação metodológica proposta por Pradanov e Freitas (2013).

Nesse contexto, o primeiro capítulo do trabalho, o qual se refere ao primeiro objetivo específico, possui o intuito de ilustrar as principais características da sociedade da informação, a ser desenvolvido de acordo com o marco teórico da sociedade em rede desenvolvida por Manuel Castells. Assim como, busca demonstrar os riscos que a sociedade informacional pode ocasionar e como o ordenamento jurídico brasileiro está se adequando a essa nova realidade, com o objetivo de promover e tutelar o uso de dados pessoais.

O segundo capítulo, que corresponde ao segundo objetivo específico, ocupa-se em abordar o direito fundamental a privacidade e intimidade e como tais direitos são conceituados e resguardados pela Constituição Federal de 1988. Em seguida, cuida do direito a proteção de dados pessoais como um direito fundamental autônomo a ser tutelado, demonstrando alguns artifícios para a sua defesa.

Por fim, o terceiro capítulo, que se refere ao último objetivo específico, destaca os impactos dos avanços informacionais no âmbito da saúde, buscando entender o motivo que os dados pessoais em saúde são considerados dados sensíveis e por fim, delinear o papel da Lei Geral de Proteção de Dados para regulação dos dados pessoais, em especial os dados sensíveis em matéria de saúde.

2 A SOCIEDADE EM REDE: ENTRE INFORMAÇÃO, RISCO E REGULAÇÃO JURÍDICA

A sociedade da informação se tornou um termo utilizado em substituição ao conceito de “sociedade pós-industrial”, proporcionando a construção de um novo paradigma em que há o destaque pelas novas tecnologias e mudança das relações sociais e econômicas. De acordo com Castells (2009, p. 43), a penetração da tecnologia de informação nas esferas das relações humanas, é o ponto inicial para compreender as facetas e os novos ramos da economia, sociedade e cultura em construção.

Por esse motivo, a afluência entre tecnologia, informação e sociedade forma um trinômio indissociável na cultura digital, sendo cada vez mais perceptível os efeitos colaterais sobre os cidadãos e os impactos aos diversos setores da sociedade. Nesta senda, conforme Coutinho e Lisbôa (2011, p.8) tais características estão intrinsecamente associadas com a democratização do saber, uma vez que, evocam novos espaços para procura e compartilhamento de informações e dados.

No entanto, não se pode negar que há uma outra face da sociedade da informacional que é a sociedade de risco. Já que, o desenvolvimento da sociedade em rede acarreta certos desafios que implicam em preocupações sociais e éticas, que colocam em risco valores caros ao direito que não existem na lógica do âmbito digital, como, por exemplo, a privacidade, intimidade e a proteção de dados (ADOLFO; WINCK, 2012, p. 14).

Indo de acordo com os novos rumos da sociedade em rede, o cenário jurídico brasileiro, buscou amoldar suas legislações a nova realidade, assim, o Código de Defesa do Consumidor, a Lei do Cadastro Positivo, a Lei do Acesso à Informação e o Marco Civil da Internet, são uma das principais regulação jurídicas setoriais que versam sobre a sociedade da informação antes da criação de uma lei geral.

Nesse sentido, o presente capítulo tem por objetivo examinar os aspectos que proporcionaram o surgimento da sociedade da informação, os riscos aos direitos personalíssimos e as suas implicações no ordenamento jurídico brasileiro, tendo como base um dos marcos teóricos adotados no trabalho quanto ao que se convencionou denominar sociedade em rede, desenvolvida por Manuel Castells. Com base nisso, busca-se no próximo capítulo, tratar do direito fundamental à privacidade e a necessidade do reconhecimento da proteção dos dados pessoais, como um direito fundamental autônomo.

2.1 Surgimento e características da sociedade da informação

O uso da expressão sociedade da informação foi dada oficialmente pela primeira vez, em 1993, pela voz do presidente da Comissão Europeia, Jacques Delors, perante o Conselho Europeu, onde inaugurou as ideias das infraestruturas da informação exemplificando os impactos do uso da tecnologia da informação nos diversos setores da sociedade, desde a economia até a prestação de serviços públicos (VIEIRA, 2007, p. 156).

Entende-se que o termo sociedade da informação evoca uma sociedade que possui como centro principal o avanço tecnológico no tratamento da informação, marcada pelo desenvolvimento de bens imateriais, como, por exemplo, o uso de dados, informação e conhecimento. No entanto, é certo que estabelecer um conceito concreto para esse termo é uma tarefa difícil tendo em vista que se trata de uma expressão ampla e que não se reduz apenas aos aspectos tecnológicos, mas também, abrange qualquer forma de transmissão de informação, conhecimento e saber (PAESANI; SIQUEIRA JR., 2013, p. 203).

Nesse sentido, fazendo uma análise histórica da organização social, nota-se que em cada época a existência de um elemento central que representasse o desenvolvimento da sociedade e determinasse importantes marcos históricos. Primeiramente, durante o período da sociedade agrícola, a terra era a principal fonte de riqueza sendo a produção agrícola que fomentava a geração de riquezas e movimentava a economia através de diversas práticas comerciais, tendo como exemplo, o escambo (BIONI, 2019, p. 3).

Já durante a sociedade industrial, o destaque foi dado para o uso das máquinas a vapor e da eletricidade, que desenvolveram uma importante contribuição para o setor da produção fabril e para o crescimento de riquezas e da economia (BIONI, 2019, p. 3). Durante o período da revolução industrial, destaca-se a existência de duas revoluções industriais, em que, a primeira foi calcada na criação de tecnologias como a máquina a vapor e a progressiva substituição das ferramentas manuais pelas máquinas, e a segunda, caracterizou-se pelo destaque da eletricidade, do motor de combustão interna, da fundição de aço e pelo começo do desenvolvimento das tecnologias de comunicação, como o telégrafo e a invenção do telefone (CASTELLS, 2009, p. 71).

Após a Segunda Guerra Mundial, os serviços tiveram um relevante papel na construção da nova ordem socioeconômica. Diante disso, a dita sociedade pós-industrial, remeteu a uma transformação da estrutura ocupacional em que não importava mais pelo o que poderia produzir, mas sim, pelos serviços que poderiam ser ofertados à sociedade e à economia (BIONI, 2019, p. 3). Sendo assim, o ponto distintivo dessa nova ordem social é o desenvolvimento da economia e do trabalho imaterial onde o conhecimento e a inovação se

tornam elementos centrais que se distinguem das forças produtivas que marcaram a sociedade industrial (SANSON, 2009, p. 58).

Nesse contexto, assiste-se à eclosão da sociedade da informação, na qual o seu principal núcleo está pautado na informação que vem estabelecendo novos rumos para a organização social, como também para o desenvolvimento econômico, político e cultural. De acordo com Castells (2009, p.51), nesse novo modelo informacional a principal fonte de produtividade reside na tecnologia de acumulação de conhecimento, geração e processamento de informação e de comunicação de símbolos. A par disso, o informacionalismo contém em si a principal matéria-prima do modelo capitalista, de modo que se tornou um ponto crucial para o avanço socioeconômico por meio do uso intensivo da tecnologia da informação.

Nesta senda, há a presença da revolução da tecnologia da informação que designa um novo paradigma tecnológico que se estrutura através da tecnologia da informação. Compreende tal momento histórico da mesma magnitude de relevância e importância da Revolução Industrial do século XVIII, entretanto, a revolução tecnológica induz a um padrão de descontinuidade material nas bases dos diversos setores da sociedade, desde a economia até a cultura. Sucede assim, que a tecnologia da informação está sendo para o atual momento o que as novas fontes de energia, do motor a vapor até a eletricidade e a energia nuclear, representaram para a Revolução Industrial. No entanto, é certo que a revolução atual possui como núcleo principal a tecnologia da informação, processamento e comunicação, tais características peculiares que a diferencia de qualquer outra revolução que já existiu (CASTELLS, 2009, p. 68).

Outro marco histórico determinante para o progresso, aceleração e formação da tecnologia da informação no atual âmbito social foi o processo de restruturação do modelo capitalista iniciado desde os anos 80, que instaurou um ambiente fértil e propício para o desenvolvimento do sistema econômico/tecnológico que estava em ascensão, iniciando um novo capítulo do capitalismo, podendo caracterizar tal momento como capitalismo informacional (CASTELLS, 2009, p. 55). Posto isto, é notório que o desdobramento da sociedade da informação é fruto de uma transformação histórica que almeja novas fontes produtivas para suprir as necessidades da realidade.

Traçados de modo breve os aspectos históricos que influenciaram no surgimento da sociedade da informação, cabe agora identificar as particularidades que compõe a sua estrutura. Conforme Castells (2009, p.69), a revolução tecnológica estabelece um ciclo de realimentação entre a inserção de novas tecnologias, seu uso e o desenvolvimento em novos domínios, pois, as atuais tecnologias significam não apenas ferramentas a serem utilizadas, mas também,

processos a serem desenvolvidos e redefinidos. A partir disso, há o surgimento de diversos setores voltados para o ramo da informação, como, por exemplo, o avanço da indústria e dos serviços que envolvem pesquisa cientifica, atividades em educação, bancos de dados eletrônicos, biotecnologia, fabricação de equipamentos e sistemas de informação e comunicação. Nisso, nota-se que é cada vez mais evidente que o autor principal da era tecnológica ou da sociedade da informação, é a estrutura, organização e o processamento que é dado a informação (VIEIRA, 2007, p. 158).

O caráter inovador da Revolução Tecnológica se exterioriza no tratamento diferenciado que é dado a informação, deste modo, observa-se a inserção das tecnologias da informação e comunicação atuarem diretamente sobre o processamento informacional influenciando na criação de uma nova ordem baseada na linguagem digital (SANSON, 2009, p. 70). Isto posto, Castells (2009, p.53) denomina esse novo modelo de desenvolvimento informacional, em razão do surgimento de uma nova fase tecnológica assentada na tecnologia da informação.

Assim sendo, a capacidade de processamento de informação é resultado de um processo evolutivo de transição visto que antes era por meio de átomos que se dava o armazenamento e a transmissão da informação, ou seja, era através do método da escrita que se buscava a condensação da informação. No entanto, logo após, com a descoberta do sistema binário de dígitos, os *bits*, foi possível a conjunção da informação em unidades menores. Destarte, os *bits* proporcionaram a desmaterialização da informação permitindo o processamento e o armazenamento da informação nos computadores (BIONI, 2019, p.6).

Aprofundando o exposto acima, o desenvolvimento do sistema binário de dígitos, acarretou a desmaterialização da informação, pois com a ascensão da vida digital toda informação passou a ser a digitalizada, e assim, verifica-se uma implosão na quantidade de informação a ser cada vez mais processada. Além do aumento quantitativo, também houve um progresso qualitativo no processamento da informação, dado que os *bits* garantiram que o uso da informação fosse realizado de forma mais organizada para facilitar o seu próprio acesso. Nesse cenário, vê-se que o progresso quantitativo e qualitativo da informação em conjunto com a criação da internet, foram fatores determinantes para a virtualização do processo informacional (BIONI, 2019, p. 7).

Nesse sentido, outro fator preponderante no processo de avanço tecnológico foi a criação da Internet desenvolvida como consequência da cooperação cientifica, iniciativa tecnologia, inovação contracultural e das estratégias militares. Servindo assim, de base para a ampliação da linguagem digital e para o desenvolvimento das redes de sistemas de comunicação

que propiciaram recursos tecnológicos suficientes para o avanço da comunicação global (CASTELLS, 2009, p. 82). No entanto, cabe destacar que por volta de 1990 o uso da internet ainda era marcado por limitações, como a capacidade de transmissão de gráficos e as dificuldades de receber e identificar informações, diante disso houve a necessidade de difusão da internet por meio da invenção da teia mundial (word wibe web- WWW), que facilitou ao usuário a procura de informações e pesquisas desejadas (CASTELLS, 2009, p. 87-88).

Com isso, o processo comunicativo criado pela Internet contribuiu de maneira significativa para alteração das interações humanas, já que antes as relações eram concebidas apenas no mundo real, mas com a ascensão da internet, as inter-relações passaram a se constituir no mundo virtual (BOFF; DIAS, 2012, p. 336). Conforme Lévy (1999, p. 99), o virtual da informação, ou seja, a transmissão da informação por fontes digitais, é o autor central do ciberespaço, de modo que a capacidade sinérgica da digitalização da informação é um importante meio capaz de tornar o ciberespaço como principal ferramenta de comunicação.

Pierre Lévy define "ciberespaço como o espaço de comunicação aberto pela interconexão mundial dos computadores e das memorias dos computadores" (LÉVY, 1999, p. 92). Sendo assim, a emergência do ciberespaço se deu principalmente por meio do surgimento dos computadores, onde os primeiros computadores surgiram em 1945 na Inglaterra e nos Estados Unidos, mas suas atividades se restringiam ao serviço militar do Estado para cálculos científicos. Já durante os anos 70 foi possível o desenvolvimento de microprocessadores que possibilitaram a eclosão da robótica, das linhas de produção flexíveis, como também dos aparelhos eletrônicos e dos computadores pessoais, dando assim novos rumos ao desenvolvimento tecnológico e econômico e proporcionando um novo mercado de conhecimento e de informação (LÉVY, 1999, p.31).

Nessa linha, de acordo com Paesani (2007, p.20), a difusão da internet e dos computadores ocasionou a transformação da informação em uma mercadoria, de maneira que a tornou em uma nova matéria-prima que faz parte do gênero especial dos bens imateriais, em razão de ser concebida de forma abstrata tendo como o único elemento contínuo a ausência de matéria ou corpo, podendo desta forma, ser submetida a tratamentos, guardada ou manipulada livremente.

Ascensão (2002,p.138), no mesmo sentido, ratifica que na sociedade informacional, a informação, converteu-se em um novo fator de produção, pois, com a manipulação da informação de forma mais precisa e veloz, por meio do uso da internet, de computadores e seus programas, foi possível a expansão do uso da informação pelo homem e assim, a criação de novas possibilidades de armazenamento, transferência e produção desta, de tal modo que, o

homem deixa de ser apenas um receptor passivo de informações e passa a ser protagonista dos atos de comunicação ao se tornar um dialogante universal.

Em outros termos, a sociedade da informação também possui reflexos no ambiente das liberdades de expressão e de informação, pois, com a difusão do acesso à informação novas oportunidades se abrem para o exercício das liberdades públicas, e proporciona um alcance maior à cultura, saúde e educação. Outra característica relevante na sociedade da informação é o uso intensivo da tecnologia no âmbito público e privado, em se tratando do âmbito privado, as empresas manipulam as interações da rede por meio da comunicação e processamento de informação para transformar em prática empresarial, já no âmbito público, o governo busca investir na tecnologia como forma de modernizar o Estado, melhorar a prestação de serviço público e diminuir a burocracia (VIEIRA, 2007, p.162).

Pode-se então entender que "as tecnologias são produtos de uma sociedade e de uma cultura" (LÉVY, 1999, p. 22). No mesmo passo, Castells (2009, p.41) pontua que embora a sociedade não defina o trajeto das transformações tecnológicas e nem as tecnologias determinam o que seja sociedade, não se pode negar que a aptidão de dominação da tecnologia por uma determinada sociedade é sem dúvida, essencial para traçar o seu destino. Desta forma, de acordo com o escólio de Lévy (1999, p.22) as técnicas de utilização da tecnologia são desenvolvidas dentro de uma cultura e a sociedade está condicionada e não determinada por suas técnicas.

Castells (2009, p.566), adota a nomenclatura sociedade em rede para determinar essa nova ordem social, uma vez que os processos organizados na era informacional estão a todo tempo se estruturando em torno de redes e a sua extensão é resultado de um novo paradigma da tecnologia da informação que se forma em um espaço de fluxos e tempo intemporal. O liame estabelecido por Manuel Castells com a definição de rede, busca exemplificar uma estrutura social que é instituída em um meio altamente dinâmico passível de inovação tendo reflexos na economia capitalista, no trabalho, cultura e política.

Como se pode perceber são inegáveis os benefícios que a tecnologia em conjunto com a informação impactara as interações sociais, jurídicas e culturais da sociedade, mas por outro lado, o excesso de informação combinado com o seu uso indevido, podem causar riscos a direitos personalíssimos que são inerentes a cada indivíduo.

2.2 Outra face da sociedade informacional: sociedade de risco aos diretos personalíssimos

Pode-se conceituar risco como “é o perigo, é o temor ou o receio de qualquer coisa que nos possa fazer um mal” (SILVA, 2014, p. 1876). Em outros termos, pode compreender risco como um evento futuro, incerto e inesperado que é temido, mas que pode trazer perdas e danos as vítimas, assim como, geram responsabilidade ou encargos para os responsáveis pela causa do risco (SILVA, 2014, p. 1876).

Lado outro, conforme Beck (2010, p.24), os riscos atuais se fundamentam na globalização de seu alcance e de suas causas modernas, visto que, os riscos da modernidade são ocasionados pelo progresso, de modo que o processo de modernização vai se tornando reflexivo, tornando a si mesmo em tema e problema. Nisso, os riscos geram danos definidos, mas irreversíveis e invisíveis, assim como, baseiam-se em interpretações causais que podem ser alterados, aumentados ou diminuídos no âmbito de conhecimento, portanto, Beck (2010, p.025) caracteriza a sociedade de risco como uma sociedade catastrófica, onde o estado de exceção pode se converter em normalidade.

Isto posto, Mendes (2015, não paginado) afirma que Ulrich Beck entendia o risco como um estado intermediário entre a segurança e a destruição possuindo uma dimensão transescalar, pois o desenvolvimento científico e industrial gera um conjunto de riscos que não podem ser controlados espacial e temporariamente. Desta forma, a convergência entre globalização, individualização, desemprego e riscos globais são elementos que determinam a segunda modernidade, já que a primeira foi marcada pelas sociedades do Estado-nação na qual as relações sociais possuíam caráter eminentemente territorial.

Há estudiosos que são menos otimistas com eclosão da sociedade pós-industrial, diante as limitações sociais para o crescimento econômico e o uso de tecnologias, a crise do emprego e de recursos energéticos, assim como o custo social e psicológico de uma rápida evolução faz com que os sacrifícios feitos pela transição sejam perigosos e o futuro não represente um renascimento (MASI, 2003, p. 57). Ainda de acordo com Masi (2003), a ciência e a tecnologia são capazes de transformar as instituições, relações e funções do Estado, cooperando com a transmissão de informações acessíveis aos cidadãos, no entanto, por outro lado também é possível um maior controle externo sobre dados pessoais seja por parte do Estado ou de empresas.

Nessa linha, pode-se observar que a supervalorização da informação fundamentada na massificação do uso da Internet e transmissão da informação digitalizada, acarretou mudanças e impactos na estrutura socio-organizacional, vez que o desenvolvimento da Internet garantiu a eclosão da quantidade de informação repassada através da interconexão da rede de computadores. Contudo, ao mesmo tempo que a informação passou a ser o principal vetor da

dinâmica da sociedade, também houve a necessidade de proteção a sua confidencialidade, tendo em vista que, o uso da prestação de serviços computacionais implica em certas vulnerabilidades que advém de falhas de sistemas ocasionados por ataques cibernéticos. Assim, quanto mais o Estado e a sociedade dependem da conexão de redes para se comunicar, maior é o risco que estão sujeitos a exposição a ataques de hackers e crackers que põe em risco valores personalíssimos (VIEIRA, 2007, p. 163).

Além disso, insta expor que o ambiente digital é um meio fértil para acessos indevidos e abusivos de informações armazenadas dentro de bancos de dados, de sistemas informatizados, a atentado a propriedade intelectual, invasão da privacidade, como também, a possibilidade de estelionatos eletrônicos que tem como consequência a violação da confidencialidade, integridade e autenticidades das informações (VIEIRA, 2007, p. 164).

Bioni (2019, p.36), esclarece a relação que existe entre dados, informação e conhecimento. Dados é o primeiro estado da informação sendo ainda apenas fatos, mas que quando processados e organizados se transformam em informação e a partir do gerenciamento de dados e a modulação em informação é possível extrair algum tipo de conhecimento sobre o titular do dado. Por exemplo, os dados sobre os usuários da Internet quando processados se transformam em informação e nisso, há o gerenciamento de conhecimento, como a divulgação de notícias publicitárias personalizadas.

O armazenamento de banco de dados é capaz de criar dispositivos de troca de informação que servem para controladores e empresas manipularem e descobrirem informações que possam influenciar na tomada de decisões dos titulares dos dados, buscando identificar e traçar o perfil de cada consumidor, assim, essas decisões podem ir desde à escolha de um bem de consumo até a produção de mensagens publicitárias (BIONI, 2019, p.14). No mesmo sentido, para Mendes (2008, p.73) o tratamento de dados pessoais é um processo dinâmico que compreende no conjunto de operações com a finalidade de refinar a informação e torná-la mais valiosa.

Aprofundando o exposto acima, é certo que com o fluxo intenso de informação que assume escala global e enfraquece os limites territoriais e físicos na sociedade informacional, associado com o crescente mercado de produtividade, deu possibilidade para que empresas explorassem de forma excessiva as informações relacionada a intimidade e privacidade de seus clientes com o objetivo de influenciar no modelo comportamental de cada consumidor gerando desta forma ameaça a direitos caros aos bens personalíssimos (VIEIRA, 2007, p. 190).

Nesta senda, conforme Bittar (2015, não paginado), analisando a proteção dos direitos em espécie nos tribunais, trata os direitos da personalidade em esferas que devem ser

divididas em seus aspectos físico, psíquico e moral. No plano dos direitos físicos da personalidade, protege-se a vida, à integridade física, o cadáver, à imagem e a voz. Já no aspecto psíquico, agrupam-se o direito à liberdade, à intimidade, ao segredo e à integridade psíquica. E por fim, no grupo dos direitos morais, abrigam-se os direitos à honra, ao nome e o direito moral do autor (BITTAR, 2015, não paginado.). No entanto, é certo que independentemente de classificação, nota-se que o núcleo essencial dos direitos de personalidade incide sobre a proteção do indivíduo em si.

Emerge, portanto, destacar que por meio da conexão de redes, a Internet é um ambiente virtual propício para o manejo, acúmulo e tratamento de informações pessoais, mas que tal arquitetura também pode pôr em risco direitos fundamentais, como a privacidade e intimidade. O processamento de dados por meio de tecnologias avançadas realizado por agentes públicos e privados, são capazes traçar perfis de cada indivíduo com o objetivo de implemento de práticas comerciais, e com isso cabe ressaltar a existência de determinados dados que possuem um conteúdo discriminatório e se conhecidos ou repassados podem gerar danos a segurança e privacidade de seus titulares (AGUIAR, 2015, p.14).

Desse modo, a partir do momento que o meio virtual vai se tornando um espaço desigual, inseguro e desordenado, invoca-se um ambiente adequado para conflitos e inseguranças que afetam a harmonia do sistema digital. Portanto, os riscos se tornam interessantes e podem contribuir para impedir qualquer tipo de iniciativa inovadora que ofenda os padrões mínimos dos direitos de personalidade (GOULART, 2012, p. 195). Nisso, diante dos riscos na tutela dos bens jurídicos garantidos pelo direito de personalidade, a proteção e relevância da personalidade humana passou a construir importantes pontos do sistema jurídico, pois, o seu principal fundamento está no valor a dignidade da pessoa. Desta forma, os direitos de personalidade devem ser vistos como uma categoria aberta, em que reconhece a proteção integral da personalidade (DE MORAES, 2007, p.5).

Cabe destacar que no ambiente virtual a violação a direitos como, a privacidade e intimidade, se dá de forma mais imperceptível e silenciosa do que no ambiente físico. Posto que, no espaço digital o indivíduo não sabe como e quais as informações que estão sendo capturadas a seu respeito, e nem de que modo é feito o controle dos seus dados pessoais, já no espaço físico, é mais visível os limites da privacidade de maneira que um não interfira no âmbito de proteção de outro (MENDES, 2008, p. 98). Nesse sentido, ressalta-se que quando maior o incentivo do uso de dados por meio de algoritmos para tomadas de decisões, maiores são as consequências dos riscos a eles associados para o indivíduo e, em razão disso, eleva a discussão sobre a discriminação algorítmica tendo em vista que os algoritmos se utilizados de maneira

abusiva ou descuidada podem reforçar resultados discriminatórios (MENDES; MATTIUZZO, 2019, p. 47-48).

Ascensão (1999, p.41), questiona se a sociedade da informação também está relacionada com a sociedade da monopolização da informação, pois ao mesmo tempo que a sociedade se baseia na liberdade informacional sendo a informação livre a qualquer cidadão, também há grandes empresas que utilizam da informação e da comunicação como forma de dominação e de mercadoria.

A propósito, com a hiperconectividade e o volume intenso de dados, conceituado como *Big Data* (grandes dados), criou-se uma grande rede de transmissão de informação onde não há como estabelecer um centro de controle. Sendo assim, por meio da web é possível vigiar e monitorar o comportamento virtual de cada usuário, através do armazenamento de bancos de dados que registram o acesso das pessoas por sistemas informáticos automatizado. Outro ponto de lesão grave à privacidade dos titulares dos dados, ocorre quando empresas utilizam dos dados sem o consentimento de seus titulares, para classificar os internautas em categorias que vão desde produtos e serviços consumidos até classe social ou qualquer tipo de informação que pode ser relevante para setores publicitários (VIEIRA, 2007, p.191). Por isso, que é cada vez mais crescente o número de corporação que estão investindo em tecnologia com o intuito de captação de gerenciamento de dados.

De acordo com Matos (2005, p.8), há diversos meios de coleta de dados pessoais pela Internet. Em primeiro momento há os formulários no qual as pessoas fornecem informações solicitadas pelos sites que vão desde o nome, profissão, idade até dados mais íntimos, sendo que a princípio, pode-se pensar ser informações básicas e inofensivas, mas se comercializadas e repassadas são capazes de identificar características físicas-psíquico de cada titular do dado. Outro meio de coleta de dados é através dos cookies, que são pequenos programas de informações veiculados pelos sites visitados que servem para identificar o navegador utilizado, os horários, quantidade de acessos, áreas de preferência, sistema operacional, bem como, impressão digital para identificação de pessoas, nisso, os cookies tem a capacidade de esmiuçar a vida de seus usuários, quando são utilizados sem o consentimento e conhecimento dos usuários.

Há ainda, os hackers e os crackers, aqueles são indivíduos que possuem alto conhecimento informático e que se dedicam a conhecer e alterar programas e redes de computadores, eles transitam o sistema em busca de falhas e por possuírem conhecimentos especiais, conseguem superar barreiras que são colocadas para impedir o acesso a dados, mas a atuação dos hackers não visa fins prejudiciais. Já os crackers, utilizam seus conhecimentos

para fins ilícitos, ou seja, com o intuito de benefícios particulares ou de causar danos a terceiros (MATOS, 2005, p. 10).

Vieira (2007, p. 194), salienta que cookies são mais uma ameaça à invasão de privacidade e destaca que em 1999, a justiça americana condenou uma empresa em decorrência da utilização de cookies que ameaçava a privacidade dos usuários, através das informações colhidas pelos cookies sem o consentimento de seus usuários, a empresa combinava os perfis dos internautas com as informações de bancos dados retirados de marketing. Nisso, os cookies além de atuarem na formação do perfil dos internautas, também, produzem informações sobre a navegação do indivíduo na Internet.

Na Diretiva Europeia 2002/58/CE, referente ao tratamento de dados pessoais e a proteção da privacidade no setor das comunicações eletrônicas, estabelece a legalidade da utilização do cookie usado como instrumento legítimo e útil, quando tais dispositivos se destinam a fins legítimos e quando houver consenso dos utilizadores da máquina, para que os utilizadores tenham acesso as informações disponibilizada nos cookies (UNIÃO EURÓPEIA,2002, p. 4)

Outro desafio da sociedade da informação é a busca pela verdade. Pois, com o acúmulo e repasse de informações em excesso por diferentes meios de difusão da informação, que vão desde redes sociais até sites na Internet, essa busca se torna cada vez mais difícil. A capacidade que os meios de comunicação possuem de disseminar informações em segundos, por um lado é fascinante, mas por outro pode representar um risco para a sociedade, já que, as informações transitadas nem sempre estão de acordo com a veracidade dos fatos. Nesse sentido, há a prevalência pela relativização da verdade e o surgimento da era da pós-verdade (MANSUR; ANDRADE, 2013, p. 92).

Outrossim, observa-se nas *fakes news* um claro exemplo de como a saturação informacional e a manipulação da informação podem representar grandes ameaças para a sociedade, como, por exemplo, a desinformação, o desconhecimento e a insegurança. O principal impacto das notícias falsas ou *fake news*, está na velocidade de sua propagação e a na dificuldade em identificar a sua ilegitimidade (OLIVEIRA; SOUZA, 2018, p.3). Portanto, há que se reconhecer que um dos maiores desafios de combate às *fake news* está em coibir sua divulgação, sem que afete a liberdade de informação e de expressão na Internet.

A partir dessas constatações, pode-se pensar que a sociedade da informação nasce sob a égide de um novo fator de produção amparado nas tecnologias de informação, mas na base possui uma posição profundamente desequilibrada no que se refere ao domínio e controle sobre a informação. Em suma, diante de tais entraves o ordenamento jurídico brasileiro buscou

estabelecer parâmetros jurídicos que possam regulamentar o uso do meio digital de forma harmônica.

2.3 A regulação da sociedade da informação na ordem jurídica brasileira

Diante do destaque dado ao processamento da informação e o crescimento exponencial do uso de dados pessoais, é sobremodo importante assinalar as principais legislações no âmbito nacional que buscaram regulamentar o uso da informação, da proteção de dados e a privacidade, no âmbito digital. Dentre elas, destaca-se o Código de Defesa do Consumidor, a Lei do Cadastro Positivo, a Lei do Acesso à Informação e o Marco Civil da Internet.

No plano infraconstitucional, a primeira lei que buscou tratar da privacidade e dados pessoais de acordo com as novas tecnologias de processamento de dados foi, o Código de Defesa do Consumidor (Lei 8.078/ 1990). O CDC estabelece uma seção específica para tratar sobre os bancos de dados e cadastros de consumidores, o objetivo do legislador em seu artigo 43 foi abranger todo e qualquer banco de dados pessoais que lesionam o livre desenvolvimento da personalidade do consumidor. Primeiramente, o Código estabelece no artigo 43 §2º que o consumidor deve ser notificado em relação a banco de dados pessoais abertos sem a sua solicitação, sendo assim um dever de comunicação prévia para que o consumidor acompanhe o fluxo de suas informações pessoais. Nesse viés, nota-se que o código do consumidor optou por proporcionar ao consumidor o direito de controlar suas próprias informações, ou seja, de autodeterminação das informações pessoais (BIONI, 2019, p. 127).

O dever de transparência também deve ser garantido no acesso a informações existentes sobre o consumidor, bem como na exatidão dos cadastros e dados dos consumidores que devem ser claros, objetivos, verdadeiros, de fácil compreensão e precisam estar de acordo com o limite temporal de cinco anos para o armazenamento de informações negativas conforme dispõe o artigo 43, §1º do CDC (BRASIL, 1990). Diante disso, em linhas gerais, o CDC, consagrando o direito de acesso, de retificação e cancelamento dos dados e os princípios da qualidade dos dados, transparência e do esquecimento estabelecendo limites temporais de armazenamento, buscou conferir ao consumidor o controle sobre suas informações pessoais (MENDES, 2019, p. 44).

Já a Lei do Cadastro Positivo (lei 12.414/2011) disciplina a formação e consulta a banco de dados de pessoas físicas e jurídicas com informações de adimplemento para formação de histórico de crédito, de modo que a avaliação do crédito teria uma amplitude maior do que

apenas relativo à análise de informações de dívidas inadimplidas. Nesse sentido, a lei trouxe importantes normativas sobre proteção de dados pessoais ao estabelecer ao titular o direito de gerenciá-los, já que, as instituições passam a ser detentoras de um grande volume de dados e, por meio do tratamento desses dados poderão obter informações e conhecimento em relação ao titular dos dados (BIONI, 2019, p. 129).

Portanto, o artigo 3º, §3º incisos I e II, dispõem que ficam proibidas anotações de informações excessivas e sensíveis pertinentes à origem social e étnica, à saúde, à informação genética, à orientação sexual e às convicções políticas, religiosas e filosóficas. Com também, conforme o artigo 5º da referida lei, um dos direitos garantidos ao cadastrado está o de ter os seus dados pessoais utilizados apenas para a finalidade determinada da qual foram coletados (BRASIL, 2011). Nisso, de acordo com a breve análise feita dos artigos, observa-se que a Lei do Castro Positivo inova ao atentar para classe de informações sensíveis, bem como o quadro normativo apresentado pela lei, limita a coleta e as finalidades no tratamento de dado pessoais com objetivo de que o titular dos dados controle as suas informações pessoais (BIONI, 2019, p. 129).

No que se refere ao setor público, a Lei do Acesso à Informação (Lei 12.527/2011), também conhecida como LAI, se mostrou um mecanismo de tutela ao acesso à informação estabelecendo parâmetros razoáveis e, relacionando-os com conceitos de democracia, transparência e gestão compartilhada. Na aplicação da Lei do Acesso à Informação, prevalece o entendimento da máxima divulgação, no qual a sua base fundamental é garantir ao cidadão o amplo acesso a informações pelo Estado. Ademais, é notório que a criação da LAI é resultado de um processo evolutivo cujo marco inicial foi dado pela Constituição Federal de 1988 ao estabelecer como direito fundamental o direito à informação e o direito ao acesso a informações públicas (CLÈVE; FRANZONI, 2013, p. 08).

Com efeito, o direito à informação, no sentido de direito a ser informado, em sua dimensão subjetiva é um direito de defesa, onde o seu titular não pode ser impedido de se informar, como também tem a opção de não se informar. Já do ponto de vista objetivo, observa-se o dever de prestações positivas por parte do Estado com intuito de obter edições de normas de cunho procedimental e organizacional, ou seja, o Estado deve garantir a cada cidadão condições de se informar pincipalmente no que se refere aos assuntos estatais[1]. Nesse contexto,

[1] O ministro Alexandre de Moraes, do Supremo Tribunal Federal, concedeu medida liminar na Ação Direta de Inconstitucionalidade (ADI) 6351 para suspender a eficácia do artigo 6º-B da Lei 13.979/2020, incluído pela Medida Provisória 928/2020, que limitou o acesso às informações prestadas por órgãos públicos durante a emergência de saúde pública decretada por causa da pandemia do novo coronavírus (Covid-19), sob o argumento

que se insere o direito de acesso à informação pública como mecanismo essencial de participação cidadã no âmbito público aprimorando o controle democrático e a transparência da administração pública (SARLET; MOLINARO, 2014, p. 17-21).

A Constituição da República Federativa do Brasil de 1988 dispõe, em seu artigo 5º, inciso XXXIII que é direito de todo cidadão receber dos órgãos públicos informações que lhes dizem respeito, ou de interesse coletivo, ressalvando as hipóteses onde o sigilo é imprescindível para a segurança do Estado e da sociedade (BRASIL, 1988). Mais adiante, o art. 37, §3º, inciso II, esclarece que cabe a lei regulamentar a forma de participação do usuário da administração pública disciplinando "o acesso dos usuários a registros administrativos e a informações sobre atos de governo, observado o disposto no art. 5º, X e XXXIII" (BRASIL, 1988). E ainda, o artigo 216, §2º prevê que a gestão da documentação governamental e as providências para franquear sua consulta, cabe a administração pública (BRASIL, 1988).

Nesse sentido, a Constituição Federal, em linhas gerais, garantiu o acesso gratuito, pleno, imediato as informações que estiverem sobre a custódia do poder público como meio de fomentar a democracia participativa e o controle social. Sendo assim, por meio da LAI, coube ao legislador infraconstitucional regulamentar o direito ao acesso à informação e estabelecer as premissas básicas que norteariam a administração pública (BERNADES, 2015, p.11).

Estão subordinadas as regras da LAI, todos os órgãos e entidades da administração pública direta e indireta, seja no âmbito da União, dos Estados, do Distrito Federal ou dos Munícipios, assim como as entidades privadas sem fins lucrativos que recebam recursos públicos (BRASIL, 2011). Nessa esteira, ressalvadas as hipóteses de sigilo estabelecidas em lei, depreende-se que documentos públicos que estejam sob a guarda do Estado, estão, em regra, disponíveis para consulta por qualquer cidadão (CHAGAS, 2016, p. 39).

Convém observar que, consoante o artigo 3º da LAI, as disposições impostas pela presente lei têm como principal objetivo assegurar o direito fundamental de acesso à informação e possuem algumas diretrizes a serem seguidas, como, por exemplo, respeito da publicidade como regra geral e do sigilo como exceção, desenvolvimento da transparência pública e do controle social da administração pública, bem como da tecnologia de informação como meio de viabilizar a comunicação (BRASIL,2011).

Em consonância com a Constituição Federal e as diretrizes já elencadas, o artigo 5º da LAI, deixa claro que não é suficiente que as informações sejam prestas, mas também é

---

de que o artigo pretende transformar a exceção, que é o sigilo de informações, em regra, afastando a plena incidência dos princípios da publicidade e da transparência (BRASIL, 2020).

necessário que a administração pública zele pela qualidade da informação de modo que ela seja transparente, clara e de fácil compressão (BRASIL, 2011). E em complementação, o artigo 8º trata de um dever de transparência ativa, cabendo ao Estado fornecer informações públicas sem a necessidade de solicitação por parte do cidadão, de modo que estabelece um rol mínimo de dados que devem conter na divulgação das informações (CHAGAS, 2016, p. 49).

Por tais razões, não resta dúvida do papel da LAI na regulamentação do acesso à informação, na garantia da transparência do poder público e da participação democrática. No entanto, se por um lado é imposta ao Estado a ampla divulgação de informações sobre as atividades relacionadas com sua atuação, por outro lado, convém observar os limites dessa divulgação em matéria de dados pessoais de cada cidadão, ou seja, deve haver uma compatibilização entre o dever de transparência com a proteção de informações pessoais (CHAGAS, 2016, p. 73-74).

Sendo assim, o artigo 4º, IV, considera informação pessoal "aquela relacionada à pessoa natural identificada ou identificável" (BRASIL, 2011, não paginado). Em seguida, o artigo 6º ao mesmo tempo que garante o amplo acesso à informação e a transparência da divulgação, também tutela que os procedimentos aplicados pela lei devem levar em consideração a proteção da informação sigilosa e da informação pessoal, observando disponibilidade, autenticidade, integridade e eventual restrição de acesso (BRASIL, 2011).

Ademais, a LAI, destaca que o tratamento de informações pessoais pelos entes públicos deve respeitar à intimidade, vida privada, honra e a imagem das pessoas. De modo que sua divulgação e o acesso a terceiro podem ser autorizados mediante previsão legal ou pelo consentimento expresso da pessoa a qual a informação se referir, sendo certo que todos aqueles que obtiverem acesso as informações pessoais deverão ser responsabilizadas pelo uso indevido delas. Contudo, não será exigido o consentimento quando se tratar de informações explicitadas pela lei, como, por exemplo, nos casos de prevenção e diagnóstico médico; para realização de estatísticas e pesquisas científicas de evidente interesse público ou geral, previstos em lei; ao cumprimento de ordem judicial; à defesa de direitos humanos; ou à proteção do interesse público e geral preponderante (GARRIDO, 2012, p. 66-67).

Convém ainda ressalvar que, a restrição das informações pessoais não podem ser invocadas com o objetivo de prejudicar o processo de apuração de irregularidade em que o titular da informação faça parte, isto é, a lei possibilitou a ponderação dos interesses envolvidos para analisar, no caso concreto, se a informação será ou não divulgada (BERNADES, 2015, p. 107). Por fim, a LAI confirma a responsabilidade civil objetiva do Estado ao responsabilizar no artigo 34 os entes e órgão públicos pelos danos causados em decorrência da divulgação não

autorizada ou utilização indevida de informações sigilosas ou informações pessoais (BRASIL, 2011).

Desta forma, nota-se que a Lei de Acesso à informação elenca como uma de suas principais diretrizes a publicidade da informação e a transparência dos atos, mas também, se preocupa em preconizar limites e regras para o tratamento de informações pessoais. Logo, o estabelecimento de condições e diretrizes para o fornecimento de informações aos cidadãos, compatíveis com a proteção de acesso a informações pessoais são elementos essenciais para efetividade da LAI.

Agora, uma das principais leis em matéria de regulação da informação no âmbito da Internet, foi o Marco Civil da Internet que se concretizou pela lei nº 12.965 de 23 de abril de 2014. Entende-se que tal lei seja uma resposta aos conflitos que surgiram com a disseminação da sociedade da informação e o desenvolvimento da internet, dada pelo legislador (LIMA; JUNIOR, 2016, p. 243). Nisso, assim como a LAI, o Marco Civil da Internet é uma legislação infraconstitucional que deve implementar e regular direitos que já estão dispostos na Constituição Federal.

O amplo uso da internet na sociedade da informação, ao mesmo tempo em que gerou a liberdade de difusão e informação no ambiente digital, também proporcionou alguns riscos aos seus usuários que afetariam de forma direita a garantia de direitos personalíssimos, como, por exemplo, crimes informáticos, manipulação de dados, o uso indiscriminado de bancos de dados e principalmente, a vigilância e invasão da privacidade praticada por um Estado contra outro. Nesse contexto que se instala o Marco Civil da Internet com o objetivo de estabelecer princípios, garantias, direitos e deveres para o uso da internet no Brasil e determinar diretrizes a serem seguidas pelos entes federativos (TOMASEVINICIUS FILHO, 2016, não paginado).

Nessa esteira, o artigo 2º, caput, da lei 12.965/2014 dispõe como fundamento para o uso da internet no Brasil, o respeito a liberdade de expressão. Sendo a internet um meio de comunicação onde os indivíduos se expressam ou emitem conteúdos, tal dispositivo aponta a liberdade de expressão como pressuposto principiológico que marca a dimensão externa da democracia digital (GONÇALVES, 2017, p. 11). Já de acordo com Tomasevinicius Filho (2016), a consagração da liberdade de expressão nos dispositivos do Marco Civil é para afastar críticas de que a lei poderia restaurar a censura no país.

Por seu turno, o artigo 2º em seus incisos ainda disciplina outros fundamentos do uso da rede, nota-se então que o artigo não apenas prestigiou o espaço livre e aberto da internet, mas também garantiu o aspecto promocional do seu uso, como o desenvolvimento da

personalidade e o exercício da cidadania em meios digitais, em conjunto com a livre iniciativa e concorrência e ainda a busca pela finalidade social da rede (GARCIA, 2016, p. 4).

Em relação a tutela de informações pessoais, o artigo 3º trata um rol importante de princípios para proteger usuários, empreendedores e a própria abertura da internet, entretanto, optou-se neste momento pontuar apenas os mais relevantes para à compreensão da proteção de dados pessoais, quais sejam, a garantia da liberdade de expressão, comunicação e manifestação de pensamento; o princípio da proteção da privacidade e dos dados pessoais, contidos nos incisos II e III; princípio da preservação e garantia da neutralidade da rede, contido no inciso IV; e, por fim, o princípio da responsabilidade dos agentes de acordo com as suas atividades, contido no inciso VI (BRASIL, 2014).

A noção de neutralidade de rede possibilita que todos os conteúdos e usuários sejam tratados da mesma forma, sendo assim, não deve existir interferência no conteúdo que é repassado pela rede e nem distinção de origem e destino, pois se fosse possível o controle do acesso à internet, poderia desconfigurar as características essenciais desse meio que é a sua interconectividade e o ambiente aberto da internet (SOUZA, LEMOS, 2016, p. 115-118).

Em outros termos a neutralidade da rede[2] está atrelada em preservar a internet como um ambiente de rede aberta, com liberdade de acesso a seus usuários e sem interferências no destino do tráfego dos dados na rede, nisso, depreende-se que o ponto essencial da neutralidade é a igualdade de tratamento de dados, que não devem ser discriminados sem algum motivo justificável (SOUZA, LEMOS, 2016, p. 115-116). Desta forma, de acordo com Gonçalves (2017, p. 26) a neutralidade da rede está interligada com direitos fundamentais a inclusão digital, igualdade e a privacidade.

Já em relação a privacidade e o tratamento de dados, o MCI coloca em posição de destaque a privacidade e a proteção de dados possibilitando que o usuário tenha consciência sobre a circulação das informações que lhes dizem respeito, nisso, a lei garante que dados não sejam repassados a terceiros, salvo expresso consentimento ou determinação legal. Com efeito, verifica-se que a lei expressamente menciona a necessidade do consentimento do usuário para a coleta, uso, armazenamento e o tratamento de seus dados pessoais (GARCIA, 2017, p. 4).

O texto da lei ainda deixa claro, que o consentimento deve ser livre, expresso e informado de modo que as informações sobre coleta, uso, armazenamento, tratamento e

[2] Conforme Gonçalves: "A neutralidade de rede visa impedir que, por meio de subterfúgios e artimanhas tecnológicas, possam os provedores de acesso à internet, empresas de telecomunicações e provedores de aplicações de internet terem controle indevido sobre os dados pessoais dos usuários que possam influenciar no seu ir e vir virtual, nas escolhas que faz, nos conteúdos que acessam e nas informações e conhecimento que recebem e produzem" (GONÇALVES, 2017, p.26).

proteção de dados pessoais sejam claras e completas para que o titular possa fazer a escolha de disponibilizar ou não a informação que lhe diz respeito. Nesse mesmo contexto, o MCI dispõe, que o usuário diante de uma aplicação na internet poderá requerer a exclusão de dados pessoais que tiver fornecido, logo após o encerramento da relação entre as partes (BIONI, 2019, p. 132).

Nessa conjuntura, observa-se o olhar atento do MCI em proporcionar que o usuário tenha o controle sobre os seus dados pessoais por meio do consentimento, assegurando assim, a autodeterminação informativa para proteção de dados (BIONI, 2019, p. 132).

Outro aspecto trazido pelo Marco Civil da Internet, foi o combate a ilícitos civis e criminais praticados em afronta ao manto da privacidade na internet, visto que, por muito tempo se imaginou a internet como terra sem lei, em que tudo era permitido pela impossibilidade de descobrir a verdadeira identidade da pessoa, além disso, notou-se dificuldades no âmbito penal no combate a crimes virtuais. Nisso, a legislação tratou da responsabilidade civil dos provedores da Internet por ofensa a direitos personalíssimos, como a honra, imagem e vida privada na tentativa de frear violações a tais direitos por meio de coleta, armazenamento, tratamento de registro e de dados pessoais (TOMASEVICIUS FILHO, 2016, não paginado).

Nesse mesmo sentido, na Câmara dos Deputados, tramita o Projeto de Lei 2.601/2019[3] que atualiza o MCI para que diante de notícias falsas ou *fake news* haja a obrigação de indisponibilização pelos provedores de aplicações de internet. A justificativa apresentada para o projeto de lei é facilitar a remoção de tais notícias sem que seja necessária ordem judicial, já que, em regra, o MCI determina a retirada de uma notícia falsa a uma ordem judicial prévia (BRASIL, 2019). Ante o exposto, não se pode negar a importância do Marco Civil da Internet para disciplinar os direitos e deveres dos usuários da rede, possuindo um significado relevante para a regulação jurídica da internet.

Em suma, diante do arcabouço legislativo, nota-se que no primeiro momento os dados que circulavam no meio digital para formação de informações eram regulados por meio de leis setoriais, já que o Brasil não contava com um marco normativo geral sobre a proteção de dados pessoais, no entanto, é certo a importância dos princípios estruturados por essas leis para a criação da lei geral de proteção de dados. Assim sendo, além do tratamento legislativo, no ambiente da sociedade da informação, observou-se a necessidade de tutelar a proteção de dados pessoais como um direito fundamental autônomo que não está limitado apenas ao direito de privacidade.

[3] Em consulta realizada no dia 07 de setembro de 2020, a PL encontrava-se na Mesa Diretora da Câmara dos Deputados desde o dia 29 de agosto de 2019.

3 NOVOS RUMOS DO DIREITO A PRIVACIDADE E O DIREITO FUNDAMENTAL AUTÔNOMO À PROTEÇÃO DE DADOS PESSOAIS

Traçadas as principais noções sobre a sociedade da informação, cabe agora, a partir dessas reflexões analisar o direito à privacidade sob esse novo paradigma que a sociedade está se formando. Nessa esteira, é certo a importância do uso das tecnologias nas relações entre particulares e com o Estado, no entanto, não é menos importante apontar a necessidade que tais práticas devem ser disciplinadas de acordo com os direitos fundamentais básicos do indivíduo para o desenvolvimento de suas personalidades.

Nesta senda, no presente capítulo, primeiramente irá se analisar o direito fundamental à privacidade, tutelado pela Constituição Federal de 1988 como um direito individual em que cabe ao Estado o dever de abstenção para o livre desenvolvimento da personalidade. Assim como, busca-se demonstrar a sua proteção no âmbito internacional que serviu de base para a construção dos principais conceitos do direito à privacidade.

Ademais, insta apontar o âmbito de proteção do direito à privacidade, que não deve mais ser visto de forma inflexível, e sim, de acordo com a dinâmica da sociedade em rede no ambiente virtual, superando a oposição entre ambiente público e privado. Nesse sentido, faz-se menção a dupla dimensão objetiva e subjetiva dos direitos fundamentais, destacando que além de ser um direito de defesa, também requer do Estado uma prestação positiva para sua efetiva proteção.

Posteriormente, cabe mencionar que o direito a proteção de dados pessoais é resultado do desdobramento do direito à privacidade, já que diante dos novos contornos proporcionados pela sociedade da informação, como demonstrado no capítulo anterior, o direito à privacidade não segue mais o mesmo padrão clamado pelas necessidades da sociedade, pois, com a facilidade de acesso, transmissão e cruzamentos de dados, tornou-se maior a afetação dos direitos fundamentais pessoais, com isso, se reconhece o direito fundamental autônomo a proteção de dados pessoais. E em seguida, convém apresentar a regulamentação dada a proteção de dados pessoais pela Lei Geral de Proteção de Dados Pessoais.

Sendo assim, expostos os caminhos do direito à privacidade diante da sociedade da informação, chega-se ao cerne desta pesquisa para apontar o tratamento de dados pessoais no âmbito da saúde, no próximo capítulo.

3.1 O direito fundamental à privacidade: conceito e dimensões diante da sociedade da informação

Um dos principais marcos doutrinários para a compreensão do direito à privacidade, ocorreu em 1890, nos Estados Unidos, quando os autores Samuel Dennis Warren e Louis Demitz Brandeis, publicaram o artigo *Right to Privacy* criticando a intervenção da impressa americana nos relatos das suas vidas privadas. No texto, os autores defenderam a não prevalência do interesse público em relação a fatos que estão relacionados com a sua vida privada, como também apresentaram a necessidade de reconhecimento pelas Cortes do denominado *"The right to be let alone",* ou simplesmente o direito que o indivíduo tem de estar só, seja com seus pensamentos, emoções ou sentimentos (CANCELIER, 2016, p. 217-218). Tais premissas básicas contribuíram para elaborar os primeiros contornos em face do direito à privacidade.

No âmbito internacional, o direito à privacidade foi reconhecido na Declaração Universal dos Direitos do Homem, aprovada em 10 de dezembro de 1948, que enunciava em seu artigo 12 "ninguém será objeto de ingerências arbitrárias em sua vida privada, sua família, seu domicílio ou sua correspondência, nem de ataques a sua honra ou a sua reputação. Toda pessoa tem direito à proteção da lei contra tais ingerências ou ataques". (ONU, 1948, p. 03). Com redação semelhante, também foi pauta em 1966 pelo Pacto Internacional de Direitos Civis e Políticos, o qual estabeleceu em seu artigo 17, §§1º e 2º, a proteção da vida privada contra ingerências arbitrais e ilegais [4].

E mais a frente, em 1969, o artigo 11 da Convenção Americana sobre Direitos Humanos, no Pacto de São José da Costa Rica, elencou o direito à privacidade com o mesmo texto disposto na Declaração Universal dos Direitos do Homem (OEA, 1969). Diante desse cenário, constata-se o reconhecimento do direito à privacidade no âmbito internacional e logo após, a sua incorporação no ordenamento jurídico interno de cada país.

Sendo assim, no âmbito da legislação infraconstitucional, o Código Civil[5] estabeleceu um capítulo específico para tratar sobre os direitos da personalidade, limitando-se a elencar cinco direitos, quais sejam, direito ao corpo, ao nome, à honra, à imagem e o direito

[4] Artigo 17, do Pacto Internacional de Direitos Civis e Políticos: §1 Ninguém poderá ser objetivo de ingerências arbitrárias ou ilegais em sua vida privada, em sua família, em seu domicílio ou em sua correspondência, nem de ofensas ilegais às suas honra e reputação. §2 Toda pessoa terá direito à proteção da lei contra essas ingerências ou ofensas. (ONU, 1966, não paginado).

[5] Conforme Venosa: "O Código Civil de 2002 introduziu um capítulo dedicado aos direitos da personalidade, categoria que o legislador pátrio se refere, de forma ordenada, pela primeira vez, o que denota a nova feição que assume o direito privado nesta pós-modernidade (VENOSA, 2017, p. 182).

à privacidade. Apesar disso, é sabido que o rol de direitos de personalidade estabelecidos pelo Código Civil não é exaustivo, sendo assim, nada impede que outras manifestações da personalidade sejam protegidas por meio da aplicação direta do artigo 1º, inciso III, da Constituição Federal (SCHREIBER, 2013, p. 15).

Já a Constituição Federal de 1988, consagrou no artigo 5º, inciso X, o direito a inviolabilidade da intimidade, vida privada, honra e imagem que são direitos classificados como direitos individuais, pois privilegiam a autonomia dos particulares e a independência dos indivíduos perante a sociedade e do próprio Estado. Por essa razão, identifica a existência não apenas da autonomia do indivíduo, mas também, da sua liberdade (AFONSO DA SILVA, 2005, p. 191). Nisso, os direitos à vida privada, intimidade, honra e imagem se expressam como limites as interferências ilícitas e abusivas dos meios de comunicações, podendo acarretar, inclusive, a responsabilização por danos morais e materiais causados (BULOS, 2014, p. 571).

Diante dessas premissas introdutórias, cabe agora analisar especificamente o direito à privacidade e a intimidade. A intimidade e a privacidade buscam salvaguardar o direito de estar só, protegendo as esferas inerentes ao ser humano que possam ser suscetíveis a intromissões externas (BULOS, 2014, p. 571). Entretanto, apesar da íntima relação que existe entre tais direitos e o fato de fazerem parte de níveis ou esferas do direito à vida privada, deve-se apontar a distinção no âmbito de proteção que existe entre ambos.

Ao que se refere a intimidade, corresponde a proteção das relações pessoais e mais íntimas do indivíduo, envolvendo suas relações familiares, de amizade e entre outras que fazem parte de sua vida pessoal, nota-se que a intimidade reflete à esfera mais interior do indivíduo, por outro lado, a privacidade, tutela todo tipo de comportamento que envolve os relacionamentos pessoais que o indivíduo deseja preservar do conhecimento público, como, por exemplo, as relações comerciais e profissionais (BULOS, 2014, p. 571). Não obstante tal conceituação, estabelecer uma distinção sólida entre ambos é difícil, em razão da fluidez que permeia as diversas esferas da vida privada. Nesses termos, conforme Moraes (2018, p.142), o direito a intimidade possui menor amplitude e se encontra no âmbito de incidência da privacidade.

Nos Estados Unidos, utiliza-se o termo *privacy* (privacidade) quando se pretende indicar meios jurídicos de respeito a esfera da autonomia pessoal e familiar, englobando o direito de ser deixado em paz (*tort privacy*); à proteção e a inviolabilidade em face do Estado da casa, de objetos e bens pessoais (*fourth amendment privacy*), como impedir a busca e apreensões de modo irrazoável; e o direito de tomar suas próprias decisões de caráter pessoal ou íntimo *(intimate* ou *fundamental decisions privacy*) (SAMPAIO, 2018, p. 558).

Sucede assim, a doutrina constitucional alemã, distingue a intimidade e vida privada por meio da *teoria das esferas* (*Sphärentheorie*) que divide a privacidade em três círculos concêntricos: privacidade, intimidade e o segredo. O círculo de maior amplitude, representa a esfera privada, pois diz respeito a aspectos não sigilosos que podem estar relacionados com a vida familiar, comercial e de trabalho do indivíduo, nisso é possível que haja interferência do interesse público, a título de exemplo, a quebra do sigilo de dados telefônicos pelo poder judiciário (DI FIORE, 2012, p. 3).

Já o segundo círculo, o da intimidade, o acesso é mais restrito, sendo somente permitido as relações pessoais mais intensas. E por último, o segredo, sendo o círculo mais fechado e oculto das esferas já que repousa as informações mais particulares do "eu" que não devem ser compartilhadas ao público e nem sofrer intromissões, sob pena de violação a camada mais profunda da personalidade (DI FIORE, 2012, p. 3).

Arrematando as ideias expostas, nota-se que a Teoria das esferas tem como base principal a informação, alocando-a em maior ou menor grau de relevância em cada uma das esferas. Todavia, a teoria foi largamente criticada em virtude da dificuldade em traçar os limites que cercam os círculos concêntricos, visto que, a noção de círculos não contempla a diversidade de casos que permeia a dinâmica da realidade no mundo pós-moderno (MENDOZA; BRANDÃO, 2016, p. 13-14). Nesse contexto, surge, a teoria do mosaico com o objetivo de construir outra compreensão da privacidade e intimidade.

Na teoria do mosaico, é irrelevante se o conteúdo da informação pertence ao âmbito privado, íntimo ou do segredo, pois, dados que em primeiro momento poderiam ser considerados isoladamente inofensivos, podem em conjunto com outros dados, também insignificantes, servir para violação da privacidade do titular do dado. Com isso, tal teoria defende que independente da esfera em que se alocam as informações pessoais, devem ser protegidas com a mesma intensidade (VIEIRA, 2007, p.31).

Interpretando a teoria do mosaico frente a sociedade da informação, se faz importante ressaltar que com o destaque das novas tecnologias e dos meios de comunicações atuais, a base de estrutura da sociedade da informação, conforme demonstrado no capítulo anterior, está no tratamento que é dado a informação, tendo a internet como o ponto diferencial que possibilita o intenso fluxo das informações. Nisso, determinadas informações que são consideradas irrelevantes quando analisadas isoladamente, como uma simples busca na internet, podem traçar perfis completos de uma pessoa (MENDOZA; BRANDÃO, 2016, p. 14-15).

Assim sendo, de acordo com Vieira (2007, p. 32), é relevante estabelecer uma distinção entre privacidade e intimidade, com o objetivo delimitar a gravidade dos danos causados, pois, quanto mais interior é a violação da vida privada, maior deve ser a atuação do Estado para punir essas condutas. Já, Sarlet (2018, p. 469) aponta que até o momento não há uma definição precisa em que consiste a privacidade e à intimidade e por isso, todo tipo de definição taxativa sobre o âmbito de proteção de tais direitos, deve ser refutada.

Identificando alguns parâmetros de ampla aceitação no ordenamento brasileiro que corroboram para estruturação do direito à privacidade, nota-se que o referido direito foi articulado com base na dicotomia que existe entre o público e o privado, já que sempre houve a necessidade de demarcação entre atividades que deveriam ser realizadas privativamente ou em público (BIONI, 2019, p. 93). No entanto, enquanto direito fundamental e de personalidade, à privacidade, consoante será atestado adiante, supera a dicotomia entre direito público e direito privado.

Dessarte, o direito à privacidade tem por pressuposto lógico à tutela do sujeito contra olhares ou observações de terceiros, bem como de não ter suas informações pessoais expostas ao público em geral (MENDES; BRANCO, 2014, p. 247). Nesse cenário, em uma perspectiva formal, o âmbito de proteção do direito à privacidade é variável de acordo com a visão particular do titular do direito, já no que tange ao ponto de vista material, o âmbito de proteção do direito à privacidade se relaciona com os aspectos da vida pessoal que, de acordo com os ditames sociais, devem ser reservados dos olhos do Estado ou de terceiros para que os indivíduos usufruem a vida com um mínimo de qualidade (SARLET, 2018, p. 471).

Com isso, o bem protegido é a integridade moral do indivíduo, já que o marco principal do seu conteúdo está na possibilidade de constranger terceiros ao respeito e de se defender contra violações ao que lhe é próprio (FERRAZ JUNIOR, 1993, p. 440). Por outro lado, o sujeito está no controle sobre as informações pessoais que deseja repassar, e nesse momento, o direito à privacidade é condição essencial ao livre desenvolvimento da personalidade e da individualidade dos cidadãos, pois fora do âmbito público é o ambiente propício para que o indivíduo desenvolva a sua subjetividade sem ser obrigado a participar de comportamentos socialmente esperados (BIONI, 2019, p. 93).

Nesse viés, os direitos da personalidade nascem e se desenvolvem a partir da percepção de que os atributos essenciais da pessoa humana devem ser protegidos não apenas em face do Estado, mas também no campo das relações privadas, nas interações entre os particulares (SCHREIBER, 2013, p. 13). Já de acordo com Bittar (2001, não paginado), nos direitos de personalidade, a pessoa é, ao mesmo tempo, sujeito e objeto de direitos, tendo a

coletividade como sujeito passivo, ou seja, são direitos oponíveis *erga ommnes* e por isso, devem ser observados e respeitados pelos integrantes da coletividade.

A par disso, cabe ressaltar que enquanto direito fundamental em espécie o direito à privacidade apesenta uma dupla dimensão subjetiva e objetiva. Em se tratando da dimensão objeta, mostram-se como valores a serem perseguidos pelo Estado Democrático de Direito, sendo ao mesmo tempo diretriz e limite para atuação do Estado. Amíude, nessa dimensão, o direito fundamental não é considerado exclusivamente individualista, mas também, o bem protegido é tratado como o valor em si, a ser conservado e promovido (MENDES; BRANCO, 2014, p. 153).

Já em relação à dimensão subjetiva, apresenta-se como o direito que o titular possui de exigir uma pretensão positiva ou negativa de alguém. Pelo caráter negativo, o direito fundamental se põe como um direito de defesa, em que os titulares deste direito esperam um agir negativo do Estado, ou seja, a não intervenção por parte do Estado ou de terceiros no exercício do âmbito de proteção do direito, sendo o direito de autodeterminação do indivíduo de exercer a sua liberdade pessoal (VIEIRA, 2007, p. 83). E o caráter positivo, os titulares do direito à privacidade esperam uma prestação do Estado de modo que este garanta a proteção da privacidade nas relações privadas e crie condições físicas e jurídicas para o exercício do direito. (VIEIRA, 2007, p. 70).

Nesse sentido, diante dos novos parâmetros estabelecidos pela sociedade da informação, o direito à privacidade precisou se readaptar aos novos rumos da sociedade. A virtualização da informação pela internet ensejou um dos principais atrativos e, um dos maiores perigos da rede no que tange ao intenso fluxo de informações que são popularizadas e repassadas no meio virtual, diante disso, é cada ver mais notório a exposição de informações privadas e a invasão da privacidade. Deste modo, o exercício do direito à privacidade deve ser tutelado também na esfera pública, não mais se limitando ao que não é exposto (CANCELIER, 2016, p. 227-228).

Sucede que, no rumo dessas mudanças, encontra-se uma concepção dinâmica para a privacidade, em que, sua definição não está mais apenas atrelada com “ o direito de ser deixado só” e, sim, com a possiblidade de o indivíduo controlar o uso de suas informações pessoais, ou seja, o direito à autodeterminação informativa (MACHADO, 2014, p. 39). Assim sendo, o direito à autodeterminação informativa também se expressa em uma dimensão positiva, visto que, diante da necessidade de regulamentação do uso e coleta de dados pessoais, a autodeterminação informativa impõe limites quanto ao dever de informações e esclarecimentos ao titular dos dados pessoais (VIEIRA, 2007, p.89).

Diante do exposto, observa-se que a Constituição Federal e a doutrina estabeleceram ao direito à privacidade um elevado grau de proteção de forma que limitações ou restrições a esse direito, só se justificam para assegurar a proteção de outros direitos fundamentais relevantes (SARLET, 2018, p. 471). Com efeito, mesmo diante da irrenunciabilidade do direito à privacidade, tal direito, está cada vez mais sofrendo restrições perante a sociedade de vigilância que submete o sujeito ao intenso controle por parte de particulares ou pelo Estado (RUARO, 2015, p. 51).

Em suma, Doneda (2006, p.91) afirma que o crescimento no intenso fluxo de informações, destaca outro ponto do direito à privacidade, qual seja, a sua importância como pré-requisito para o exercício de outras liberdades fundamentais. E assim, por conta dessas novas dimensões, o âmbito de proteção desse direito deve ser encarado de acordo com cada situação em concreto, não se limitando a uma atuação taxativa e rígida. Nesse momento, observa-se, o florescimento de novos direitos, em especial o direito à proteção de dados pessoais que possui suas bases estruturadas no seio do direito à privacidade, mas que tem sido considerado como um direito fundamental autônomo.

3.2 A proteção de dados pessoais como um direito fundamental autônomo

Em meio a sociedade informacional em que a informação constitui elemento central do controle social e da geração de riquezas, a proteção dos dados pessoais sofre dois vetores de pressão. O primeiro, advém do Estado para aumentar a quantidade e qualidade de informações sobre as pessoas com o fundamento de garantir a segurança e a saúde, e o segundo, está relacionado com a pressão do mercado, no que tange ao valor econômico que os dados dos consumidores possuem (GEDIEL; CORRÊA, 2008, p. 145).

Nesse contexto, o Estado com o argumento de garantia da segurança pública, busca através de tecnologias controlar o acesso e saída de cidadãos em determinados locais, do mesmo modo, com a justificativa de valorização da saúde, os sistemas de saúde exigem um amplo acesso ao tratamento de dados de saúde com o fim de garantir o controle de epidemias, por exemplo. Já no âmbito do mercado, o acesso a dados pessoais possui um valor essencial, principalmente para concorrência entre empresas. No entanto, apesar dos benefícios, o acesso e uso de dados pessoais precisa ser protegido em todas as suas nuances e lacunas (GEDIEL; CORRÊA, 2008, p. 146).

A luz do exposto, reconhece-se que a sociedade da informação permitiu uma nova dinâmica na infraestrutura informacional e novos obstáculos precisaram ser superados para a

proteção no tratamento de dados pessoais. A monetização de tais dados é capaz de identificar e formar perfis completos de um indivíduo que podem ser usados e manipulados para finalidades diversas afetando de forma direta os direitos fundamentais das pessoas e, por esse motivo, reclama-se a necessidade de uma normatização específica que ampare a autonomia do direito a proteção de dados pessoais (BIONI, 2019, p. 100-101).

O art. 2º da Diretiva Européia 95/46/CE, de 24 de outubro de 1995, a qual já está revogada, prevê que dados pessoais são "qualquer informação relativa a uma pessoa singular identificado ou identificável" (UNIÃO EUROPÉIA, 1995, não paginado) e dado identificável é "todo aquele que possa ser identificado, directa ou indirectamente, nomeadamente por referência a um número de identificação ou a um ou mais elementos específicos da sua identidade física, fisiológica, psíquica, económica, cultural ou social" (UNIÃO EUROPÉIA, 1995, não paginado). Tomando como base o conceito estabelecido pela diretiva, considera-se pessoal todo dado que diz respeito a um determinado indivíduo identificável ou identificado, seja uma identificação direta ou indireta (VIEIRA, 2007, p. 227).

À vista disso, independente dos dados pessoais estarem ou não diretamente vinculados a um sujeito, eles devem ser protegidos, pois com o fluxo de informações incrementado pela Internet, se tornou mais fácil o cruzamento de dados que podem pôr em riscos direitos personalíssimos (VIEIRA, 2007, p. 228). Neste ponto, importa esclarecer que a informação em sua dimensão reduzida pode ser representada por dado, já o entendimento de dados pessoais, pode-se incluir, o nome, endereço, telefone, números dos documentos de identificação, mas também dados de saúde, biométricos, hábitos de consumo e endereço eletrônico (GEDIEL; CORRÊA, 2008, p. 146).

Conforme Doneda (2011, p.94), existe uma equação básica recíproca entre informação pessoal e privacidade, na qual, correlaciona-se a maior propagação de informações pessoais a um menor grau de proteção da privacidade. No entanto, apesar de tal associação não abarcar a complexidade que permeia o manuseio de informações pessoais pelo meio tecnológico, ela serve como fundamento para demonstrar que a tutela de informações e dados pessoais é resultado do desdobramento do direito à privacidade.

Nesse sentido, diante das diferentes formas de controle e manipulação de dados pessoais, determinadas garantias que estariam atreladas à privacidade devem ser interpretadas de forma abrangente indo de acordo com esses novos interesses (DONEDA, 2011, p. 95). E a partir desse contexto, percebe-se que viver em uma sociedade democrática no meio da eclosão do ambiente virtual possui outro sentido, já que se almeja a preocupação estatal na efetiva

proteção no tratamento de registro, distorções, divulgações e utilização de dados pessoais (RUARO; RODRIGUEZ, 2010, p. 184).

Desse modo, tendo a privacidade o seu eixo de cunho individualista calcado no "direito de ser deixado só", em que espera do seu titular a determinação de quais fatos referentes a sua vida devem ser excluídos do ambiente público, entende-se ser um direito estático e permeado pela liberdade negativa, já que determinava aos outros apenas um dever de abstenção, de não fazer. Em contrapartida, a parte do direito à privacidade que compreenderia o direito à proteção de dados pessoais, abrange uma concepção mais dinâmica atrelada a liberdade positiva e ao controle sobre as informações pessoais (BIONI, 2019, p. 97).

Aprofundando o exposto acima, a proteção de dados pessoais enquanto direito fundamental, deve ser encarado como a possibilidade de cada indivíduo poder governar a circulação das informações que lhes dizem respeito, sendo um elemento central para o exercício da liberdade do cidadão. No entanto, os poderes conferidos aos titulares dos dados pessoais, não está apenas no controle sobre o acesso, mas também, no que tange ao tratamento, circulação e utilização de dados pessoais. Assim, pode-se afirmar que o direito a proteção de dados pessoais é um elemento básico a ser desenvolvido e tutelado na sociedade informacional (RODOTÁ, 2003, p.17).

À par disso, apesar da íntima relação que existe entre o direito à privacidade e a proteção de dados pessoais, não se pode afirmar que o direito à proteção de dados pessoais deva somente ser uma mera evolução do direito à privacidade, de sorte que, o direito a proteção de dados pessoais, sendo reconhecido como um novo direito da personalidade, não há a necessidade de ficar vinculado a uma categoria específica do direito à privacidade (BIONI, 2019, p. 98).

É possível estabelecer um âmbito de proteção do direito à proteção de dados pessoais, de modo que não haja lacunas nas esferas que envolvem a manipulação, coleta e o armazenamento de dados pessoais, como, por exemplo, o direito do não reconhecimento de dados pessoais pelo Estado ou por terceiro, ou seja, o direito ao sigilo dos dados pessoais, assim como, o direito de conhecer os responsáveis pelo manuseio dos dados pessoais e também, o direito de saber a destinação ou finalidade do uso dos dados. No entanto, delimitar de forma taxativa a incidência do âmbito de proteção do direito a proteção de dados pessoais não se trata de uma tarefa fácil, tendo em vista que as inúmeras possibilidades de utilização de dados podem causar ao mesmo tempo violação a outros direitos. (SARLET, 2018, p. 496).

Por outro lado, o direito à proteção de dados pessoais apesar de não ter previsão expressa no texto da Constituição Federal, pode ser associado ao direito à privacidade e ao

direito ao livre desenvolvimento da personalidade, no que tange ao direito de dispor livremente sobre os seus respectivos dados pessoais, isto é, o direito à autodeterminação informativa (SARLET, 2018, p. 495).

O direito à autodeterminação informativa teve suas primeiras premissas elencadas no tribunal constitucional alemão, que reconheceu a capacidade dos indivíduos de autodeterminar os seus dados pessoais, como sendo um exercício do livre desenvolvimento da personalidade (BIONI, 2019, p. 103). A lei do censo de 1983, determinou o recenseamento da população por meio do uso dos dados pessoais dos cidadãos que seriam utilizados nas estatísticas de distribuição geográfica da população, mas ao mesmo tempo, ela estabelecia a possibilidade que os dados coletados fossem comparados com os registros públicos existentes, como também que os dados tornados anônimos pudessem ser usados para outras finalidades de repartições públicas (MARTINS, 2005, p. 234).

Assim sendo, em decisão sobre a constitucionalidade da Lei Censo de 1983, o tribunal alemão declarou a inconstitucionalidade parcial da referida lei, pois, o tribunal argumentou que o uso e compartilhamento dos dados pessoais coletados da população, apenas deveriam ser utilizados para a realização do recenseamento e com isso, confirmou a constitucionalidade da lei em geral, mas julgou nulos os artigos que tratavam sobre a comparação e transmissão de dados para repartições públicas. Por tais razões, o tribunal reconheceu o direito à autodeterminação informativa[6] como um direito de cada titular proteger e controlar o uso de seus dados pessoais (MARTINS, 2005, p. 234 -237).

Nesse sentido, a autodeterminação informativa realça o direito a proteção de dados pessoais como um direito autônomo que assume novas técnicas de proteção desconectada da separação entre público e privado. Sucede que, embora o direito a proteção de dados pessoais não proceda de uma leitura literal do texto constitucional, diante dos riscos proporcionados pela sociedade da informação no tratamento automatizado de dados, avoca- se o direito fundamental a proteção de dados pessoais a partir das garantias constitucionais de igualdade, liberdade, dignidade da pessoa humana, com também a proteção da intimidade e da vida privada (DONEDA, MONTEIRO, 2015, p. 164).

Partindo desse entendimento, a omissão no texto constitucional não é fundamento para negar a proteção de dados pessoais como um direito fundamental autônomo, tendo em

[6] "(...) o Tribunal Constitucional não recorre ao discurso do que é público ou privado para criar o direito à autodeterminação informacional. Ao revés, a sua fundamentação acaba por transpor tal dicotomia, na medida em que estabelece que o uso das informações pessoais não deve afetar o desenvolvimento da personalidade das pessoas. Para tanto, o controle exercido pelo cidadão sobre seus dados seria de fundamental importância, bem como a prevenção de práticas de discriminação social." (BIONI, 2019, p. 103)

vista que, o artigo 5º, §2º, da Constituição Federal dispõe sobre a cláusula de abertura[7] que possibilita a outros direitos status constitucionais de direito fundamental, em virtude de seu conteúdo, isto é, além dos direitos taxativamente positivados na Constituição, há direitos que por seu conteúdo ou significado integram o sistema de direitos fundamentais da constituição (SARLET, 2018, p. 1014).

Entende-se que a Constituição Federal adotou um sistema aberto de direitos fundamentais, no qual não se limita aos direitos fundamentais estabelecidos no Título II da Constituição (MENDES; BRANCO, 2017, p.156). Nisso, o direito à proteção de dados pessoais possui status de direitos fundamentais, sendo um direito materialmente fundamental, visto que o seu conteúdo está relacionado com os direito da intimidade, privacidade, entre outros que compõe a estrutura básica do Estado democrático brasileiro, bem como com o princípio da dignidade da pessoa humana. Servindo, desta forma, como meio para concretizar direitos já catalogados, tais como os acima elencados.

Já no âmbito internacional a proteção de dados pessoais não se trata de um tema novo, vale aqui um destaque especial para os países europeus que se tornaram referência no que toca a regulamentação da proteção de dados pessoais. Na Europa, o grande marco normativo sobre a proteção de dados pessoais ocorreu em 1981 na *Convenção 108*, aprovada pelo Conselho Europeu, sendo denominada "Convenção para Proteção das Pessoas relativamente ao Tratamento Automatizado de Dados de Caráter Pessoal" que além de estabelecer princípios para o tratamento de dados pessoais, tinha como objetivo principal garantir a toda pessoa, o respeito aos direitos e liberdades fundamentais estabelecendo um mínimo de proteção aos dados pessoais automatizados (VIEIRA, 2007, p. 236).

Posteriormente, em 1995, foi aprovada a Diretiva 95/46/CE tendo como principal propósito harmonização de toda a legislação que existia na Europa sobre proteção de dados pessoais, com o intuito de reforçar as medidas de segurança no tratamento de dados para facilitar o fluxo de informações internacionais no mercado interno (VIEIRA, 2007, p. 240). Um ponto importante apresentado por essa diretiva, foi a criação de autoridades centrais de proteção de dados, que seriam responsáveis pela fiscalização, legislação e arbitragem de demandas envolvendo a proteção de dados pessoais (POLIDO, 2018, p. 6).

Há também, a Diretiva 97/66/CE que teve como objetivo a proteção da intimidade no setor da telecomunicação e a Diretiva 2002/53/CE que regulamentou o tratamento de dados

[7] "O art. 5º, § 2º, da CF, representa, portanto, uma cláusula que consagra a abertura material do sistema constitucional de direitos fundamentais como sendo um sistema inclusivo e amigo dos direitos fundamentais." (SARLET, 2018, p. 1014).

pessoais no âmbito das comunicações eletrônicas (VIEIRA, 2007, p. 240). Tais diretivas são orientações de como os estados-membros da União Europeia deveriam criar suas leis nacionais (MENDES, BIONI, 2019, p.163).

Diante desse percurso, o direito a proteção de dados pessoais foi incluindo como um direito fundamental na Carta de Direitos Fundamentais da União Europeia que após a vigência das diretivas, observou-se a necessidade de um olhar mais consistente e uniforme sobre a proteção de dados pessoais no bloco europeu e assim, foi criado o Regulamento Europeu de Proteção de Dados Pessoais sendo o ponto de chegada de toda uma jornada europeia de proteção de dados (MENDES, BIONI, 2019, p.163). Portanto, é certo que a ampla discussão e relevância dada a proteção de dados pessoais no âmbito internacional, acabaram por incentivar que no tratamento nacional de dados pessoais fossem criados mecanismo de regulamentação na proteção de dados pessoais.

Impende dispor ainda que, apesar do fundamento materialmente constitucional e do elevado tratamento internacional dado a tal direito, em 2019, o plenário do Senado propôs a Proposta de Emenda à Constituição 17/2019[8], que inclui expressamente o direito à proteção de dados pessoais, inclusive os incluídos nos meios digitais, no rol de direitos fundamentais da constituição federal. A justificativa apresentada para a propositura da PEC 17/2019 foi a autonomia valorativa em torno da proteção de dados pessoais que possui peculiaridades que a diferencia da privacidade, tal como destacaram que o Brasil precisa mais do que uma lei ordinária que disponha sobre o tema e por isso, há a necessidade de mudança na Constituição Federal (BRASIL, 2020). Sendo assim, o direito a proteção de dados pessoais teria fundamento constitucional formal e material.

Já em recente decisão do Supremo Tribunal Federal sobre o compartilhamento de dados de usuários de telefonia, pôde-se afirmar que a Corte reconheceu, pela primeira vez, a existência de um direito fundamental a proteção de dados pessoais. A Medida Provisória 954/2020 previa a liberação do compartilhamento de dados de usuários de telecomunicações com o Instituto Brasileiro de Geografia e Estatística (IBGE) para produção de estatística durante o período de pandemia do novo coronavírus.

No entanto, a medida provisória ensejou o ajuizamento de cinco Ações Diretas de Inconstitucionalidade (ADI 6387, ADI 6388, ADI 6389, ADI 6390, ADI 6393) que questionavam a constitucionalidade e pediam a suspensão da MP 954/2020, tendo em vista que a referida MP apresentava dispositivos que violavam a intimidade, vida privada, honra, imagem

[8] Em consulta realizada no dia 10 de agosto de 2020, a PEC encontrava-se sujeita à Apreciação do Plenário desde o dia 11 de fevereiro de 2020.

e o sigilo de dados. Dessa forma, em decisão liminar na ADI 6387, a relatora, ministra Rosa Weber, decidiu por suspender a MP 954/2020, baseada nos argumentos de que o art. 2 da MP ao impor as empresas prestadoras de serviços telefônico o compartilhamento com o IBGE de nomes, números de telefone, endereços de seus consumidores, sejam eles pessoais físicas ou jurídicas, exorbitou os limites da constituição ao dispor sobre a disponibilização de dados pessoais dos consumidores (BRASIL, 2020).

A ministra ainda relatou que a MP não delimita de forma clara o objeto da estatística a ser produzida, a finalidade e amplitude específica da utilização dos dados e, nem esclarece como os dados serão efetivamente utilizados. Outro ponto destacado por Rosa Weber foi que a MP 954/2020 não apresenta mecanismos técnicos para proteger os dados pessoais, em possível casos de acessos não autorizados, vazamento ou utilização indevida. Desse espectro, ao não prever nenhum tipo de exigência que possa assegurar o sigilo, a higidez e o anonimato de dados pessoais, a relatora entendeu que a MP não cumpre com as expectativas do texto constitucional no que tange a proteção dos direitos fundamentais (BRASIL, 2020). Em julgamento posterior, o Plenário do STF referendou a medida cautelar e suspendeu a MP 954/2020.

De modo claro, a decisão do Suprema Corte é um marco histórico, pois, tornou expressa a proteção de dados pessoais como um direito fundamental. De acordo com Mendes (2020, não paginado), o julgamento pela corte foi importante para entender que no tratamento de dados pessoais, não existe mais dados insignificantes, de modo que todos os dados devem ser protegidos e não apenas aqueles considerados íntimos, uma vez que qualquer dado pode ser utilizado para identificação de pessoas e usados para formação de perfis informacionais.

Ainda importa destacar que o reconhecimento de dados pessoais como um direito fundamental autônomo, enseja uma dimensão subjetiva de defesa do indivíduo em que cada cidadão em sua esfera individual, espera um agir negativo do estado de não intervenção, mas também, possibilita uma dimensão objetiva de dever de proteção estatal para garantir a efetividade desse direito nas relações privadas (MENDES, 2020, não paginado).

Na mesma linha Sarlet (2018, p. 496), pontua que cabe ao Estado um dever de proteção a ser efetivado por meio de prestações normativas e fáticas que asseguram a concretização do direito a proteção de dados pessoais. Do exposto, percebe-se que, hoje, a tutela e reconhecimento do direito fundamental a proteção de dados pessoais é um elemento imprescindível para que o cidadão tenha consciência de que forma estão sendo utilizado seus dados e desenvolva a sua liberdade de forma plena, para tal propósito a Lei geral de Proteção de Dados Pessoais se torna um importante mecanismo de regulação e proteção de dados

pessoais, de modo que objetiva estabelecer princípios, fundamentos e sanções que deverão ser aplicados nas relações jurídicas públicas e privadas.

3.3 A Lei Geral de Proteção de Dados Pessoais como marco a proteção jurídica de dados

O núcleo principal da tutela de dados pessoais não está na proteção dos dados por si só, e sim, na pessoa que é titular desses dados. Nisso, a legislação que trata sobre proteção de dados é um marco regulatório para tutela do indivíduo em face do manuseio de dados ou informações pessoais por terceiros, seja pessoa física ou jurídica. Antes de 2018, os dados pessoais no ordenamento jurídico brasileiro não se estruturavam em um complexo normativo único e eram tratados por lei setoriais, como, por exemplo, o Marco Civil da Internet, a Lei de Acesso à Informação Pública, o Código de Defesa do Consumidor e a Lei do Cadastro Positivo, entretanto, tai leis ainda se mostravam frágeis no que tange a proteção do titular de dados pessoais (MENDES, 2019, p. 44).

Assim sendo, perante o aumento de casos de vazamentos de dados e do uso indevido deles afetando de modo direto os seus titulares, em conjunto com o cenário internacional dado pelo Regulamento Geral sobre a Proteção de Dados[9] na Europa, de 2018, e os fatos a respeito do uso de dados do Facebook para analisar e influenciar os eleitores na campanha eleitoral estadunidense de 2016, pela empresa *Cambridge Analytica*, em afronta às normas de proteção de dados, contribuíram para o processo de regulamentação pelo legislador da LGPD, lei nº 13.709 de 14 de agosto de 2018 (MENDES, 2019, p. 2).

Tendo em vista que qualquer manuseio de dados pode afetar a personalidade e violar direitos fundamentais dos titulares dos dados, a LGPD estabeleceu um novo paradigma ao regime de proteção de dados, ao normatizar a concepção de que não existem mais dados irrelevantes diante do seu tratamento automatizado na sociedade da informação (MENDES, 2019, p. 45).

Nessa celeuma, é sobremodo importante, agora, analisar os principais fundamentos e princípios que regem a Lei Geral de Proteção de Dados Pessoais. A princípio, a LGPD, trata no artigo 1º que o objetivo de sua regulamentação é proteger os direitos fundamentais de liberdade, privacidade e o livre desenvolvimento da pessoa natural e, ainda menciona, o âmbito de aplicação da lei que abrange o tratamento de dados pessoais por pessoa natural ou jurídica,

[9]"(...) constitui um marco fundamental na regulação do tratamento dos dados pessoais, tendo como escopo responder aos novos desafios na área de proteção de dados pessoais gerados pela evolução das novas tecnologias e pela globalização dos mercados. Este regulamento faz parte do pacote da União Europeia relativo à reforma da proteção de dados (...)" (MAGALHÃES; PEREIRA, 2018, p. 17).

seja no âmbito físico ou digital (BRASIL, 2018). Nesse sentido, Mendes (2019, p. 46) aponta que essas primeiras características trazidas pela LGPD permitem que os direitos dos cidadãos sejam assegurados independentemente da modalidade de tratamento de dados e quem os utiliza.

Mais adiante, o artigo 2º aponta os fundamentos que estruturam a proteção de dados pessoais, destaca-se, a privacidade; a autodeterminação informativa; a liberdade de expressão, de informação, de comunicação e de opinião, a inviolabilidade da intimidade, da honra e da imagem; o desenvolvimento econômico e tecnológico e a inovação; a livre iniciativa, a livre concorrência e a defesa do consumidor, como também, os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais (BRASIL, 2018).

No rol dos fundamentos, depreende-se que a privacidade possui a mesma hierarquia com os preceitos de desenvolvimento econômico e tecnológico, inovação, livre iniciativa e livre concorrência, pois a sistemática proposta pela LGPD busca proteger a privacidade dos dados pessoais, sem, contudo, impossibilitar o uso de dados para o desenvolvimento tecnológico e da inovação, elementos essenciais da sociedade da informação (CABRAL, 2019, p. 62). De outro lado, nota-se que os fundamentos trazidos pela LGPD têm uma correspondência clara, explícita ou implícita com a Constituição Federal.

Todo tratamento de dados pessoais, seja o realizado pelo setor público ou privado, a princípio está submetido a LGPD. Entretanto, o artigo 4º dispõe de algumas exceções a sua aplicação, assim, a LGPD não se aplica ao tratamento de dados pessoais realizado por pessoas naturais para fins exclusivamente particulares e não econômicos, como também para fins exclusivamente jornalísticos, artísticos, acadêmicos, de segurança pública, de defesa nacional, de segurança do Estado ou de atividades de investigação e repressão de infrações penais (BRASIL, 2018).

Por serem operações cotidianas, como, por exemplo, compartilhamento e armazenamento de contatos e e-mails, a inaplicabilidade da LGPD aos dados pessoais utilizados por pessoais naturais para fins exclusivamente particulares, explica-se pelo fato de que não há assimetria de informações nas interações entre relações pessoais sem finalidade econômica, ou seja, ainda que possa haver violação da privacidade, nesse caso, não se observa uma vulnerabilidade especifica do titular em face do uso de seus dados pessoais. Em se tratando dos fins exclusivamente jornalísticos, essa hipótese busca garantir a liberdade de impressa e o acesso à informação tendo em vista que a intervenção prévia do Estado na atividade jornalística poderia pôr em cheque o exercício pleno desta atividade, entretanto, se a atuação jornalística for exercida por uma empresa que integra grupo econômico e vier, por exemplo, a criar bancos

de dados sem uma finalidade clara, as informações que foram coletadas estão sujeitas as regras da LGPD (MENEZES; COLAÇO, 2019, p. 80-82).

No que se refere aos fins exclusivamente artísticos, prioriza-se a liberdade de expressão e de informação, mas estão sujeitas a uma reparação a posteriori em caso de lesão ou ameaça a direitos personalíssimos. Da mesma, a restrição da aplicação da lei para fins acadêmicos, por exemplo, para fins de pesquisa científica, se justifica pelo fato do controle e fiscalização da pesquisa serem feitos pelos próprios comitês de éticas. E por fim, em relação a não incidência da LGPD para fins exclusivos de segurança pública, defesa nacional, segurança do Estado ou de atividades de investigação e repressão das infrações penais, tende a garantir os interesses públicos e o combate às infrações penais, fraude digital e crime organizado, por exemplo (MENEZES; COLAÇO, 2019, p. 84-85).

Cabe ainda destacar que a referida lei não se aplica ao tratamento de dados pessoais advindos de fora do território nacional e que não tenham sido objeto de comunicação ou uso compartilhado com agentes de tratamento brasileiros ou, ainda, objeto de transferência internacional de dados com outro país que não o de proveniência, desde que o país de proveniência proporcione grau de proteção de dados pessoais adequado ao previsto nesta Lei. (BRASIL, 2018). Ou seja, a exceção do artigo 4º, inciso IV, deve ser interpretada de forma restritivamente, já que a regra, é que se o tratamento de dados ocorrer em território nacional, deve-se aplicar a LGPD mesmo que os dados tenham origem no exterior (MENEZES; COLAÇO, 2019, p. 84-85).

Em se tratando dos princípios que regem a Lei Geral de Proteção de Dados Pessoais, o artigo 6º elenca a boa-fé e determinados princípios que devem ser seguidos nas atividades de tratamento de dados pessoais, os quais são: finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação, responsabilização e prestação de contas (BRASIL, 2018). A boa-fé objetiva, apresenta-se como uma forma de ressaltar que o tratamento de dados pessoais seja disciplinado pela ética e por padrões objetivos de lealdade apurados em cada caso concreto (MENDES, 2019, p.49).

O princípio da transparência, do livre acesso, da qualidade dos dados, são princípios que garantem ao titular dos dados informações claras, adequadas e completas sobre o tratamento de dados que lhe diz respeito, assim como, a facilidade de acesso de seus dados para fins de correção ou atualização (BIONI, 2019, p. 134). Os princípios da prevenção, da segurança e da responsabilidade também estão relacionados, uma vez que o primeiro objetiva evitar danos ao titular pelo uso inadequado dos dados pessoais, já o segundo pretende impedir situações ilícitas e acessos não autorizados, nisso, observa-se que o ilícito e o dano são conceitos

relacionados com a responsabilidade civil. Não obstante o princípio da responsabilização e prestação de contas dispõe sobre a necessidade de adoção de medidas que sejam capazes de fazer valer o cumprimento das normas de proteção de dados pessoais (OLIVEIRA; LOPES, 2019, p. 77).

Já o princípio da finalidade, destaca-se pela vinculação que deve existir entre o tratamento do dado pessoal e o fim que gerou ou motivou a sua coleta, tal vínculo visa impedir que os dados sejam manuseados com finalidades diferentes daquela que permitiu a sua primeira coleta, no entanto para a sua realização, é preciso que haja prévia informação e consentimento do titular dos dados (MENDES, 2019, p. 3). Ao longo do texto da LGPD, é possível notar vários artigos que fazem referência ao princípio da finalidade e a necessidade do consentimento, principalmente quando se trata da mudança de finalidade no tratamento de dados sensíveis, como, por exemplo, o artigo 7º, I, o artigo 7º, §3º, artigo 8º, §4º, artigo 9º, §2º, e o artigo 10º.

Ao que se refere a adequação e necessidade são princípios em que o uso dos dados deve estar de acordo com as expectativas esperadas pelo seu titular e, isso deve ser feito de acordo com o contexto da coleta e a finalidade especificada para o tratamento dos dados. Contudo, apenas os dados mínimos relacionados ou necessários à atividade devem ser tratados, buscando assegurar que eles sejam pertinentes, proporcionais e não excessivos (BIONI, 2019, p. 135). Desta forma, nota-se a relação e a pertinência que existe entre os princípios da finalidade, adequação e necessidade, que corroboram com a ideia de controle de informações pessoais pelo titular dos dados.

A não discriminação é o princípio que veda o tratamento de dados pessoais para fins discriminatórios ilícitos e abusivos, deste modo, no uso de dados pessoais, sejam sensíveis ou não, tal princípio deve ser levado em consideração para que não gere nenhum tipo de desvalor ou indução na utilização desses dados (MULHOLLAND, 2018, p. 174). Sendo assim, aqui que se identifica a base de sustentação no tratamento diferenciado que é dado a categoria dos dados sensíveis. A Lei Geral de Proteção de Dados tutela e identifica de forma diferenciada os dados pessoais e os dados pessoais sensíveis, conforme o artigo 5º, I, dado pessoal é toda "informação relacionada a pessoa natural identificada ou identificável" (BRASIL, 2018, não paginado) e o inciso II do mesmo artigo elenca que dado pessoal sensível se refere a "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, não paginado).

Aprofundando o exposto acima, os dados pessoais sensíveis englobam informações que se conhecidas ou repassadas, apresentariam um elevado potencial discriminatório ou lesivo

aos seus titulares (DONEDA, 2010, p. 26). Como acentua Rodotá (2003, p.21), há uma perfeita correlação entre o tratamento de dados pessoais sensíveis e as normas constitucionais de igualdade, de modo que a tutela dos dados sensíveis não é para estimar o segredo em si mesmo, mas sim, para tornar a igualdade efetiva e evitar possíveis discriminações.

Nessa vertente, a discriminação resultado do uso de informações sensíveis, por tratarem de grupos historicamente discriminados, torna mais difícil a esse agrupamento superar determinada situação prejudicial, como, por exemplo, a exposição de dados de saúde de um indivíduo, que pode influenciar em uma não contratação no setor trabalhista, ou também, pode impossibilitar a concessão de um contrato de seguro (MENDES; MARTTIUZZO, 2019, p.54). Notadamente, percebe-se que ao estabelecer a natureza sensível a um determinado dado, a LGPD buscou garantir um regime jurídico mais protetivo tendo em vista os riscos que englobam o tratamento de tais dados.

Diante do intenso fluxo de informações que pode ser agregado e utilizado para criar um perfil básico de hábitos de um determinado consumidor, é cada vez mais perceptível o caráter volátil dos dados pessoais. Nisso, o titular dos dados deve ter consciência a respeito dos atores que gerenciam suas informações pessoais, ou seja, deve haver o consentimento do titular (BIONI, 2019, p. 146). Com esse intuito, a LGPD ainda aborda de forma extensiva as condições de legitimidade para o tratamento de dados pessoais, pontuando como característica principal o consentimento do próprio titular do dado que deve ser válido, livre, informado, inequívoco e de acordo com uma finalidade determinada, conforme exposto acima (MENDES, 2019, p. 3).

No entanto, apesar da lei estabelecer hipóteses de dispensa de consentimento pelo titular no artigo 7º, §4º para dados tornados manifestamente públicos pelo titular, por outro lado, ela garante no artigo 7, §6º que mesmo nesses casos, o agente de tratamento de dados deve seguir as demais obrigações impostas pela lei, como também deve observar os direitos e princípios da LGPD (BRASIL, 2018). Mais uma vez, o titular dos dados pessoais possui papel de protagonista da Lei Geral de Proteção de Dados.

Outro ponto básico que ainda deve ser destacado é o tratamento de dados pessoais no setor público, já que tal setor vale do uso de informações pessoais dos cidadãos não apenas para execução de políticas públicas, mas também, para elaboração e oferecimento de outros serviços que fazem uso de dados pessoais. Sendo assim, apesar da transparência ser um princípio central regulamentado pela Lei do Acesso à Informação, tem como um dos seus limites a vedação do fornecimento de dados pessoais pelo setor público, conforme já destacado no capítulo anterior. Nisso, coube à LGPD disciplinar o tratamento de dados pessoais pelo poder público com o intuito de estabelecer um equilíbrio entre o acesso à informação a administração

pública e a proteção de dados pessoais dos cidadãos (INSTITUTO DE TECNOLOGIA E SOCIEDADE, 2019, p. 3-4).

Nesse viés, o tratamento de dados pessoais pelo âmbito público deve ser realizado em atendimento à finalidade e o interesse público para executar e cumprir atribuições do serviço público, de modo que seja fornecido informações sobre a finalidade, procedimento e práticas utilizadas para execução das atividades. Ademais, o uso compartilhado de dados pessoais pelo ente público deve estar de acordo com as finalidades específicas para a execução de políticas públicas, bem como é preciso respeitar os princípios de proteção de dados pessoais dispostos no artigo 6º da LGPD (BRASIL, 2018).

Para Mendes (2019, p. 46), a aplicação da LGPD deve ser observada em três níveis. O primeiro, está relacionado com as condições de legitimidade que devem ser atendidas para qualquer tipo de tratamento de dados pessoais, nesta senda, as bases legais previstas no artigo 7º ou no artigo 23º da LGPD e, os princípios elencados no artigo 6º, precisam ser considerados para que o tratamento de dados pessoais sejam legítimos. Logo após de observada as condições de legitimidade, o tratamento de dados pessoais deve obedecer determinados procedimentos para garantir a proteção dos dados, que se encontram na forma de direitos dos titulares dos dados e nas obrigações dos agentes de tratamento de dados pessoais.

Assim, no artigo 18º da LGPD, estão dispostos os principais direitos do titular dos dados pessoais e, em linhas gerais, o artigo elenca que o titular tenha livre acesso aos seus dados, que os dados equivocados ou desatualizados possam ser corrigidos, como também tem o poder de cancelar dados que foram armazenados indevidamente ou que o consentimento tenha sido cancelado pelo titular dos dados. Nessa fase, além de atentar para os direitos dos titulares é preciso também estabelecer as obrigações de todos que realizam o tratamento de dados, como, por exemplo, em seu artigo 46º, a LGPD estabelece obrigações primordiais que devem ser seguidas pelos agentes de tratamentos na aplicação adequada de medidas de segurança para proteger os dados pessoais de acessos (MENDES, 2019, p. 50-51).

Superado o primeiro e segundo nível, chega-se ao terceiro nível do modelo de aplicação da LGPD, tal fase consiste na aplicação de sanções administrativas, arroladas no artigo 52º da LGPD e civis, pontuadas nos artigos 42º a 45º da mesma lei, no caso de violação dos direitos elencados acima. Logo, o intuito dessa etapa é atribuir efetividade as normas previstas na LGPD, ou seja, conferir eficácia as etapas anteriores (MENDES, 2019, p. 52-23).

Diante de todo o exposto, por meio dos princípios e demais artigos arrolados acima, observou-se que a LGPD elencou através do controle dos dados pessoais, o consentimento como um dos principais protagonistas da proteção de dados pessoais. Todavia, a complexidade

do fluxo informacional em conjunto com as limitações cognitivas do indivíduo para uma tomada racional de decisão sobre os seus dados pessoais, acaba impedido que os titulares dos dados sejam capazes de controlar as suas informações pessoais de modo racional (BIONI, 2019, p. 159).

Assim sendo, a ação de uma Autoridade Nacional de Proteção de Dados (ANPD) se justifica pelo fato de que com o desenvolvimento tecnológico e a fluidez das informações pessoais, o tratamento de dados e os seus possíveis efeitos são dificilmente de serem controlados de forma eficiente pelo cidadão. Portanto, a atuação de uma autoridade de garantia de direitos fundamentais, mostra a sua relevância na promoção de um equilíbrio dinâmico entre os valores que se referem a pessoa (DONEDA, 2019, p. 319).

Sem a menor pretensão de abordar todos os artigos da LGPD, cabe destacar a importância deste ente criado para atuar zelando pela proteção dos dados pessoais, na edição de normas e procedimentos, deliberação de interpretação sobre a lei e aplicação de sanções a empresas que não cumprirem com a LGPD. A ANPD, possui amplas prerrogativas elencadas previstas no artigo 55-j da Lei Geral de Proteção de Dados, nisso, a criação de uma Autoridade Nacional de Proteção de Dados e seus órgãos integrantes, se tornou de extrema necessidade para elaboração de diretrizes de aplicação da lei (ASSAF; DOMINGUES; 2020, p. 147).

A LGPD prevê um amplo rol de artigos que dependem de posterior regulamentação por parte da ANPD e por isso, a ela cabe realizar as necessárias adequações para que a lei tenha sua eficácia garantida de modo pleno. Desta forma, a ANPD, apresenta-se como um importante órgão de orientação geral que irá ser responsável pela adequação e aplicação da Lei Geral de Proteção de Dados (PINHEIRO, 2020, não paginado). No entanto, para que sua atuação seja exitosa, é preciso garantir a independência dessa autoridade que não deve ser subordinada hierarquicamente a outros órgãos (DONEDA, 2019, p. 315).

A independência da ANPD, manifesta-se importante para a proteção do cidadão e para estruturação do sistema normativo de proteção de dados, que inclui a regulação do fluxo de dados pessoais. Portanto, se faz pertinente destacar dois pontos da necessidade de independência da autoridade, o primeiro, é o seu papel na imposição de medidas regulatórias de caráter preventivo como advertências ou aconselhamentos, até que se chegue ao regime de sanção próprio. E o segundo, é para obstar os riscos de fragmentação na interpretação da lei perante tribunais e órgãos administrativos (DONEDA, 2019, p. 315).

Assim sendo, no dia 26 de agosto de 2020, o governo federal criou o Decreto nº 10.474/2020 que estrutura a Autoridade Nacional de Proteção de Dados e pontua em seu artigo 1º que a ANPD é o órgão integrante da Presidência da República, dotada de autonomia técnica

e decisória e tem como objetivo de proteger os direitos fundamentais de liberdade e privacidade e o livre desenvolvimento da personalidade da pessoa natural, orientada pela Lei Geral de Proteção de Dados (BRASIL, 2020).

Contudo, diante do contexto da pandemia do SARS-Cov-2 (Covid-19) foi proposta a MP 959/2020 que prorrogou a *vacation legis* da LGPD para 2021, o argumento apresentado pelo Ministro da Economia para o adiamento da entrada em vigor dos dispositivos da referida lei foi que há uma incapacidade de parcela da sociedade em se adequar a LGPD tendo em vista os impactos econômicos e sociais provocados pela pandemia, bem como para que sua aplicação não gere insegurança jurídica (SANTOS, 2020, p. 1).

Entretanto, em plenário de votação da MP 959/2020 sobre sua conversão em lei, a Câmara dos Deputados, no dia 25 de agosto de 2020, entendeu em determinar o adiamento da lei até 31 de dezembro de 2020, mas no dia 26 de agosto de 2020, o Senado constatou por prejudicado o artigo da MP que determinava o adiamento da vigência da lei para 2021, logo, a lei geral de proteção de dados deve entrar em vigor logo após que o projeto de lei de conversão da MP for sancionado pelo Presidente da República (SANTOS, 2020, p. 2). Nisso, diante da sanção presidência da lei 14.058/20, a LGPD entrou em vigor no dia 18 de setembro de 2020.

Apesar da entrada em vigor da LGPD, discute-se a urgência e necessidade de implantação da ANPD que está estruturada apenas no papel por meio do decreto 10.474/2020, visto que a falta de criação do órgão além de comprometer a própria atuação da ANPD, dificulta a eficácia e adequação das normas da LGPD, o que pode gerar um excesso de casos questionando pela lei via judicial aspectos relacionados da lei (CERIONI, 2020, não paginado). Desta forma, a ANPD deve ser um elemento central para garantir a uniformidade e segurança jurídica na aplicação da LGPD, como também os direitos dos cidadãos (DONEDA, 2019, p. 315).

Com isso, nota-se que a LGPD já é uma realidade para a sociedade e para empresas públicas e privadas que precisam se adequar a sua regulamentação, tendo em vista que é um importante marco legislativo para a proteção dados pessoais de forma completa e estruturada, como também possibilita a tutela de outros direitos fundamentais, como, por exemplo, privacidade, intimidade, honra, imagem, liberdade de expressão, de informação e do livre desenvolvimento da personalidade. Para isso, observa-se a importância da criação de uma autoridade nacional de proteção de dados para garantir de modo pleno a proteção dos dados pessoais.

4 O TRATAMENTO DE DADOS PESSOAIS EM MATERIA DE SAÚDE E A TUTELA DA LEI GERAL DE PROTEÇÃO DE DADOS.

Os avanços tecnológicos combinados com a interoperabilidade de bancos de dados na saúde são capazes de identificar cada cidadão, e em razão disso, aumentam o potencial de ameaças a proteção de dados e a privacidade das informações fornecidas pelo cidadão aos profissionais da saúde ou estabelecimento de saúde. Nisso, as iniciativas como o Prontuário Eletrônico do Paciente, e-Saúde, Telemedicina e Telessaúde, são ações que contribuem para melhoria da qualidade de acesso ao sistema de saúde, mas ao mesmo tempo, provocam preocupações e uma delas está relacionada com o risco de invasão da privacidade, confidencialidade e proteção de dados.

É nesse contexto, de uma sociedade cada vez uma informatizada que se precisa tutelar aspectos da personalidade garantindo que os indivíduos tenham o direito de controlar as suas próprias informações pessoais e de mantê-las protegidas. Nesse viés, o baluarte de tais direitos advém da proteção dos direitos fundamentais a saúde, privacidade, intimidade e dos dados pessoais, bem como do dever de confiança e do princípio da dignidade da pessoa humana.

Não obstante, a doença da Covid-19 que foi declarada como pandemia em 11 de março de 2020 pela OMS e no Brasil o primeiro caso se deu em 16 de fevereiro de 2020, fortaleceu o desenvolvimento de tecnologias de informação e comunicação ligadas a saúde com o objetivo de proporcionar segurança e qualidade no atendimento dado a população. Assim, em meio a pandemia o Estado precisou regulamentar e desenvolver mecanismos para a redução da propagação do vírus, como, por exemplo, as técnicas da Telessaúde e da Telemedicina. Além disso, o Brasil adotou medidas de monitoramento e vigilância de infectados por meio do uso de aplicativos celulares, no entanto, para a sustentação dessas atividades se fez necessário o uso e controle do compartilhamento de dados pessoais sensíveis.

Sendo assim, o presente capítulo, no primeiro momento se ocupará em analisar de que forma a tecnologia da informação e comunicação está sendo utilizada no Brasil para proporcionar a garantia do acesso e qualidade do sistema de saúde, destacando a importância e regulamentação do sistema de e-saúde no desenvolvimento do Prontuário Eletrônico do Paciente, Telemedicina, Telessaúde e aplicativos de saúde. Posteriormente, no segundo momento, busca entender a necessidade de preservação dos dados pessoais referentes a saúde e, em consequência, os desafios a serem superados com a sua utilização indevida, bem como, compreender os motivos do tratamento diferenciado na tutela dada pela Lei Geral de Proteção de Dados Pessoais os dados pessoais sensíveis.

4.1 E-saúde e o uso da tecnologia no âmbito da saúde eletrônica no Brasil

A introdução da inovação tecnológica nas atividades humanas tem determinado novas formas de organizações sociais, de sorte que os impactos da sociedade da informação também proporcionaram novos moldes no ramo da saúde, visto que, o uso das tecnologias podem auxiliar a resolver problemas relacionados com o sistema de saúde brasileiro, como, por exemplo, déficit na infraestrutura das ações de saúde e a falta de acesso aos serviços na área desse setor (SARLET; KEINERT, 2015, p. 133). Em suma, o propósito da inovação no âmbito da saúde é possibilitar a transformação do processo de trabalho e dos modelos econômicos essenciais para o desenvolvimento de um melhor atendimento às necessidades da população (MARIN; FERREIRA, 2017, p. 49).

Nesse sentido, apesar dos desafios[10] a serem superados para garantir o exponencial desenvolvimento do uso da tecnologia na saúde, a utilização das tecnologias de informação e comunicação (TIC) geraram alguns benefícios, como o aumento da qualidade dos tratamentos e eficiência dos serviços de saúde, tanto no setor privado quanto público. De tal modo que o manejo e utilização da cultura digital nesse setor, serviu para administrações de unidades de saúde, gestão de recursos na saúde pública e, assegurou a criação de aplicativos que garantiriam um mais seguro e melhor atendimento de saúde dos pacientes (VIEIRA, 2015, p. 33).

Sendo assim, todo o processo de informatização que é aplicado no âmbito da saúde, leva o nome de e-Saúde (em inglês, *eHealth*). Para efeitos da aplicação da e-saúde, considera-se as tecnologias empregadas diretamente aos profissionais de saúde, as dirigidas ao diagnóstico e tratamento, como também as que tratam de coletar, armazenar e analisar de forma eficiente a informação emitida no cuidado dos pacientes (HIDALGO; CARRION et al, 2016, p. 32). Já na Política Nacional de Informação e Informática em Saúde (PNIIS) que orienta as ações de tecnologia da informação e comunicação de todo o sistema brasileiro de saúde, definiu o termo e-saúde das seguintes formas:

> 1.Fortalecimento da área de informação e informática em saúde, com apoio à organização, ao desenvolvimento e integração à atenção à saúde nas três esferas de governo; 2. Estabelecimento e manutenção atualizada de um repositório nacional de

[10] "A maior dificuldade para a consolidação da e-Saúde não reside no desenvolvimento tecnológico, que evidentemente terá de ser avaliado à medida que vão sendo incorporadas na atenção em saúde as novas tecnologias, mas na necessidade de uma organização que suporte adequadamente as mudanças que a introdução da saúde digital inevitavelmente requer, para garantir sua eficiência. A implementação da tecnologia que viabiliza a e-Saúde se produz seguindo processos dinâmicos, nos quais intervêm diversos atores, que tomam decisões de acordo com estímulos e critérios diferentes, aspectos que são necessários considerar e que vão além dos estritamente técnicos. Nesse sentido, é preciso avançar em conhecimento em relação aos processos, aos fatores críticos e às estratégias de integração das TIC nos sistemas de saúde, identificando especificamente quais transformações são geradas mediante as interações entre a organização e a tecnologia introduzida." (HIDALGO; CARRION, 2016, p. 32).

> software em saúde que inclua componentes e aplicações de acesso público e irrestrito, em conformidade com padrões e protocolos de funcionalidade, interoperabilidade e segurança; 3. Promoção de estratégias e mecanismos para a redução ou simplificação dos sistemas de informação em saúde e para a qualificação da produção e gestão da informação em saúde; 4. Promoção da disseminação e publicização de dados e informação em saúde de forma a atender tanto às necessidades de usuários, de profissionais, de gestores, de prestadores de serviços e do controle social, quanto às necessidades de intercâmbio com instituições de ensino e pesquisa (MINISTÉRIO DA SAÚDE, 2016).

À vista do exposto, nota-se que os objetivos oportunizados pela saúde digital são múltiplos, pois permite o aumento na qualidade da atenção e atendimento dados ao paciente, à ampliação do acesso à saúde de modo a beneficiar o fluxo assistencial de trocas de informações entre equipes de saúde e entre médico e paciente. No entanto, para obter tais vantagens associadas ao e-Saúde, é preciso que haja profundas mudanças nas próprias habilidades digitais dos profissionais da saúde para que as tecnologias sejam utilizadas de forma adequada e eficiente pelos profissionais e organizações (HIDALGO; CARRION et al, 2015, p. 33).

Há, pois, um complexo sistema que abrange a aplicação de tecnologias de informação e comunicação no setor da saúde, incluindo, entre outros, os aplicativos de saúde, os registros médicos eletrônicos, os serviços de telemedicina e Telessaúde que visam contribuir na melhoria da infraestrutura em saúde atuando no âmbito da prevenção, tratamento e diagnóstico (FERNÁNDEZ; CARRASCO, 2016, p. 39).

Tendo em vista, a tecnologia da informação em saúde se tornou também um diferencial no mercado competitivo das empresas, a Apple e Google já se apresentaram como investidoras desse novo mercado. A título de exemplo, a Apple como o intuito de facilitar o acesso do paciente aos registros médicos, vem desenvolvendo o aplicativo *Health Records*. Do mesmo modo, a Google tem investido na criação de *startups* com o foco na saúde, fazendo o uso de, por exemplo, algoritmos para detecção de doenças (DE NEGRI, 2018, p.32).

Nisso, em se tratando dos registros médicos eletrônicos, tendo como um importante marco regulatório a Resolução do CFM nº 1821/2007, há a figura do prontuário eletrônico do paciente (PEP) que é um modelo de prontuário médico digital, sendo utilizado no armazenamento, registro e controle digital das informações dos pacientes, de tal modo que tais informações possam ser compartilhadas automaticamente com outras instituições e médicos que estão no cuidado do paciente proporcionado uma assistência integral à saúde. No entanto, é preciso que seja garantidos modelos de segurança para assegurar a confidencialidade, autenticidade e integridade das informações em saúde (CONSELHO FEDERAL DE MEDICINA, 2012, p. 4).

Nesse sentido, a atuação do PEP na assistência integral de saúde é vista ao possibilitar a integração entre a informação do paciente originada do prontuário eletrônico com as informações baseadas no conhecimento científico, que são capazes de gerar sugestões de diagnósticos ou tratamentos terapêuticos por meio da informatização clínica, com isso, mostra-se como um importante meio para a qualidade assistencial e na prevenção de erros (FERNÁNDEZ; CARRASCO, 2016, p. 41).

Os prontuários físicos escritos à mão pelos profissionais de saúde apresentam algumas limitações e desvantagens em relação ao prontuário eletrônico, uma vez que as informações no papel possuem baixa mobilidade ao ficarem disponível apenas a um profissional, do mesmo modo, o arquivamento em pastas gera um grande volume de dados que dificulta o acesso e a pesquisa coletiva. Assim, nota-se que os prontuários físicos estão sucessivamente sendo adaptados por sistemas eletrônicos com arquivos digitais, entretanto, o seu uso para que tenha validade jurídica, deve ser feito com a utilização do sistema de certificação digital com intuito de garantir uma comunicação segura entre dois sistemas, por exemplo (CONSELHO FEDERAL DE MEDICINA, 2012, p. 7).

Realça-se ainda que no final do ano de 2016, o Ministério da Saúde instituiu o prontuário eletrônico do cidadão (PEC) como parte do sistema de aplicativo e-SUS Atenção Básica. A utilização do prontuário eletrônico nas Unidades Básicas de Saúde busca otimizar o fluxo de informações no atendimento do cidadão pelos profissionais de saúde, já que o acesso facilitado de informações clínicas no que tange a condição de saúde ou a evolução de uma determinada doença do paciente, possibilita efetividade no cuidado e no trabalho dos profissionais da saúde (MINISTÉRIO DA SAÚDE, 2017).

Sucede assim, de acordo com a pesquisa TIC Saúde 2019 divulgada pelo Comitê Gestor da Internet do Brasil, por meio do Centro Regional de Estudos para o Desenvolvimento da Sociedade da Informação do Núcleo de Informação e Coordenação do Ponto BR, mostrou que houve diminuição nos indicadores de estabelecimentos de saúde que possuíam informações clínicas e cadastrais nos prontuários dos pacientes armazenadas apenas em formato de papel, pois, em 2018, a pesquisa apontou o percentual de 27% para as informações clínicas em prontuários utilizadas em papel, entretanto, se comparado com o ano de 2019, tal porcentagem reduziu para 18%. Por outro lado, observou-se um aumento nos indicadores das Unidades Básicas de Saúde (UBS) que registram as informações dos pacientes apenas em formato eletrônico, já que em 2018, as UBS apresentaram 12% de informações dos pacientes disponíveis no meio eletrônico, mas em 2019, o percentual aumentou para 15% demonstrando um avanço na informatização das UBS (CETIC.BR, 2019).

Outro ponto a ser destacado como manifestação do uso das tecnologias de informação e comunicação no âmbito da saúde, é a telessaúde. Tal termo se caracteriza pelo uso de tecnologia para o exercício de atividades a distância relacionadas a saúde[11], nisso, a atuação dos serviços da telessaúde proporcionam o aumento das ações como as teleconsultas e os telediagnósticos que intensificam o oferecimento de atividades no âmbito da saúde, sendo um apoio na prestabilidade de diagnóstico e terapêutico (BRASIL, 2012, p. 16).

A Portaria nº 2.546/2011 instituiu o Programa Nacional Telessaúde Brasil Redes que tem como propósito auxiliar a consolidação das Redes de Atenção Básica de Saúde no âmbito do Sistema Único de Saúde (SUS). Desta forma, a rede de Telessaúde Brasil fornecerá os serviços de teleconsultoria, telediagnóstico, segunda opinião formativa e tele-educação para integração do Sistema Único de Saúde (BRASIL, 2011). Já a Portaria nº 2.554/2011, instaurou no âmbito do Programa de Requalificação das Unidades Básicas de Saúde (UBS), o Componente de Informatização e Telessaúde Brasil Redes na Atenção Básica, com a finalidade de estimular o uso das tecnologias de informação e comunicação para a realização de atividades à distância relacionadas à saúde (BRASIL, 2011).

Aprofundando o exposto acima, cabe ressaltar o incentivo do Programa Telessaúde Brasil Redes na Atenção Primária à Saúde (APS) consolidando uma ampla rede de acesso e comunicação entre os serviços do Sistema Único de Saúde, já que a atenção primária à saúde é o primeiro nível de acesso ao sistema de saúde e, por isso, o programa busca criar estratégias de apoio assistencial que garantam a integração entre os serviços de saúde de modo a aprimorar a sua resolubilidade (MINISTÉRIO DA SAÚDE, 2012, p. 22).

No Brasil, em razão de sua grande extensão territorial, há diversos locais isolados e de difícil acesso, nos quais se nota uma distribuição desigual de recursos e médicos de qualidade que dificultam a efetivação do direito à saúde de forma integral, universal e equânime. Além do mais, tendo em vista que os grandes problemas enfrentados pelo sistema de saúde estão relacionados com acesso, qualidade, equidade e custo, a telemedicina, apresenta-se como um importante mecanismo para o enfrentamento dos desafios no âmbito da saúde (MALDONADO; CRUZ et al, 2016, p. 52). Importa ressaltar que em se tratando de saúde o fator custo sempre estará relacionado com qualquer tipo de prestação de serviço, assim, embora a diminuição do custo possa ocorrer com a telemedicina, o seu principal objetivo é aprimorar

[11] No Maranhão, por exemplo, há o núcleo de Telessaúde do Hospital Universitário da Universidade Federal do Maranhão, que desenvolve os serviços de teleconsultoria, tele-educação, e telediagnóstico, criou uma ferramenta na modalidade de assistente virtual, SOFIA Bot, que calcula o risco de covid-19 a partir das informações dos sintomas dos pacientes, assim, ao fazer a classificação de risco orienta se o paciente deve ficar em casa ou procurar uma UBS ou UPA mais próxima de seu domicílio (NÚCLEO DE TELESSAÚDE DO MARANÃO, 2020).

os recursos que contribuirão com um acesso facilitado aos serviços de saúde (BARBOSA; PEREIRA et al, 2020, p.19).

Neste cenário, destaca-se o desenvolvimento e expansão da telemedicina que de acordo com a Resolução do Conselho Federal de Medicina nº 1.643/2002 é o "exercício da medicina através da utilização de metodologias interativas de comunicação áudio -visual e de dados, com o objetivo de assistência, educação e pesquisa em Saúde." (CONSELHO FEDERAL DE MEDICINA, 2002, p.2). Assim, as atividades no ramo da telemedicina podem ser subdividas, por exemplo, em teleconsulta, teleconsultoria, telediagnóstico, telemonitoramento e telecirurgia, sendo que o principal ponto proporcionado por esse ramo é a interação e integração, seja entre profissionais de saúde, entre estes e pacientes ou entre gestores e profissionais de saúde (HARZHEIM; SIQUEIRA et al, 2015, p. 94).

A partir disso, a tecnologia de informação e comunicação, ao permitir a interação entre as diferentes partes que compõe o processo de assistência a distância, é capaz de ofertar acesso e serviços com maior qualidade e, como consequência reduzir custos em saúde, pois, ao ampliar a cobertura em lugares remotos onde os serviços não requerem a presença de um profissional da saúde, observa-se a diminuição no tempo de espera, facilitando o diagnóstico e a capacidade resolutiva no atendimento primário, aproximando assim, a população dos serviços de saúde (HARZHEIM; SIQUEIRA et al, 2015, p. 94).

Cabe salientar, no entanto, que em razão do Brasil ser um país com elevado nível de distribuição regional desigual no que tange a disponibilidade de banca larga, a falta de infraestrutura em rede de bancos de dados com banca larga é um dos principais problemas restritivos da expansão da telemedicina no interior do país, assim, observa-se que caso o acesso não seja universal, já que, as pessoas que não possuem recursos tecnológicos para acessar os serviços de telemedicina ficam impedidas a essa modalidade de assistência, há a violação do direito social de assistência integral à saúde (BARBOSA; PEREIRA et al, 2019, p. 13).

Além do mais, outro ponto digno de destaque é que embora os valores da Telemedicina sejam claros para o setor da saúde, no Brasil, ainda não foi esclarecido por meio de pesquisas cientificas o custo-benefício do seu uso, uma vez que apesar das políticas públicas e do programas de desenvolvimento da telemedicina, conforme já demonstrado, há carência em estudos que demonstram se de fato o uso da assistência digital é efetiva e vantajosa se comparada com os modelos tradicionais (BARBOSA; PEREIRA et al, 2019, p. 13).

Com isso, de acordo com a estratégia e-saúde para o Brasil, entre os benefícios da telemedicina, espera-se a facilitação do acesso às informações de saúde, troca de informação entre os serviços de saúde, suporte à assistência em serviço, superação de dificuldade de acesso,

promoção de educação permanente e, também, a permissão de pesquisas multicêntricas. (MINISTÉRIO DA SAÚDE, 2017, p. 57). Assim sendo, os desafios apresentados não retiram de imediato os possíveis benefícios e vantagens que a utilização da Telemedicina pode causa.

Portanto, o uso da telemedicina precisa estar de acordo com os dispositivos legais que versam sobre o seu manuseio. Assim sendo, Código de Ética Médica prevê em seu artigo 37 que é vedado ao médico prescrever procedimentos ou tratamentos sem o exame direito do paciente, salvo no caso de urgência e emergência, de tal modo que o exercício da telemedicina ou qualquer tipo de atendimento a distância deve ser regulamentado pelo Conselho Federal de Medicina (CFM) (CONSELHO FEDERAL DE MEDICINA, 2019, p. 28). Em outros termos, o Código de Ética Médica não veta, portanto, o exercício da telemedicina, mas estabelece a necessidade de regulamentação da matéria[12] por meio do CFM.

Nesta senda, por meio da Resolução 1.643/2002, instituída pelo CFM, a telemedicina compreende como o exercício da medicina mediado por meio de metodologias interativas na relação entre médico e paciente. No entanto, para isso, a prestação dos serviços de telemedicina deve estar de acordo com uma infraestrutura de tecnologia adequada que obedeçam às normas técnicas do CFM atreladas a guarda, manuseio, transmissão de dados, confidencialidade, privacidade e garantia do sigilo profissional. Assim como, em caso de emergência, a resolução permitiu ao médico que emitir o laudo a distância, a prestar também o devido suporte diagnóstico e terapêutico (CONSELHO FEDERAL DE MEDICINA, 2020, p.2).

No Parecer 14/2017, o CFM autorizou o uso do Whatsaap e plataformas similares, para comunicação entre médico e paciente, como também entre médico e médico, em caráter privado, para o envio de dados ou dúvida. O parecer considerou que a expansão das mídias sociais possui mais aspectos benéficos do que maléficos se aplicados dentro de específicos critérios de controle. Portanto, é assegurado a troca de informações entre pacientes e médicos, quando se tratar de pessoas que já estão recebendo assistência, com o intuito de esclarecer dúvidas, tratar de pontos evolutivos e repassar orientações ou intervenções de caráter emergencial (CONSELHO FEDERAL DE MEDICINA, 2017).

[12] Além da telemedicina, outros setores da saúde apresentam recomendações sobre o uso de tecnologias em suas atividades, como, por exemplo, o Conselho Federal de Enfermagem na Resolução nº 0487/2015, permite a execução de prescrição médica à distância somente em casos de urgência ou emergência (CONSELHO FEDERAL DE ENFERMAGEM, 2020). O Conselho Federal de Fonoaudiologia, dispõe sobre a regulamentação da Telessaúde em Fonoaudiologia e dá outras providências por meio da Resolução nº 427 de 01/03/2013 (CONSELHO FEDERAL DE FONOAUDIOLOGIA, 2013) e o Conselho Federal de Psicologia que regulamentou e detalhou várias modalidades de serviços psicológicos à distância, tanto em caráter clínico quanto de pesquisa por meio da Resolução nº 011/2012 (CONSELHO FEDERAL DE PSICOLOGIA, 2012).

Nessa perspectiva, tendo em vista os avanços tecnológicos, a expansão da Internet, o desenvolvimento da inteligência artificial e de equipamentos modernos no ramo da saúde, o Conselho Federal de Medicina, editou a Resolução 2.227/2018 que define a telemedicina como o "exercício da medicina mediado por tecnologias para fins de assistência, educação, pesquisa, prevenção de doenças e lesões e promoção de saúde." (CONSELHO FEDERAL DE MEDICINA, 2018, p.2). Ao contrário da Resolução 1.643/2002, a presente ampliou a regulamentação da telemedicina ao versar sobre, por exemplo, teleconsulta, teleinterconsulta, telediagnóstico, telecirurgia, teletriagem e o telemonitoramento ou televigilância. De modo breve, em se tratando da teleconsulta, em uma consulta médico e paciente em diferentes espaços geográficos, deve ter o consentimento pelo paciente e como premissa a obrigatoriedade de uma relação prévia presencial entre médico e paciente.

A teleinterconsulta possibilita que médicos troquem informações com o objetivo de auxiliar em diagnósticos e cirurgias. Atrelado a este, para emissão de laudos ou pareceres por um médico a distância, há o telediagnóstico. Mais à frente, o CFM em seu artigo 8º, estabeleceu que a telecirurgia, por meio de interação tecnológica, é possível a cirurgia remota, com um médico executor e um equipamento robótico em espaços diferentes, no entanto, além da indispensabilidade do consentimento pelo paciente, a resolução pondera a necessidade que seja feita em infraestrutura adequada, segura e com garantia de funcionamento de equipamentos e de internet (CONSELHO FEDERAL DE MEDICINA, 2018).

Já a teletriagem médica, o médico realiza uma avaliação prévia dos sintomas, a distância, com o intuito de encaminhar o paciente ao tipo adequado de assistência ou especialista, não se tratando, porém, de um diagnóstico médico. Além disso, a resolução também disciplinou o telemonitoramento para monitoramento a distância do estado de saúde ou doença, sob supervisão médica e com auxílio de imagens, sinais e dados de equipamentos e/ou dispositivos agregados ou implantáveis nos pacientes (CONSELHO FEDERAL DE MEDICINA, 2018). Assim sendo, a Resolução 2.227/2018 avançou trazendo uma abordagem mais completa e importantes pontos técnicos que permeiam a telemedicina com a introdução de novas tecnologias.

Apesar disso, após manifestação de médicos e entidades representativas da classe, o Conselho Federal de Medicina revogou a Resolução 2.227/2018, uma das críticas apresentadas, por exemplo, foi a falta de clareza sobre a responsabilidade do médico que atende a distância e, em consequência, a ausência de segurança jurídica. Contudo, a revogação não anula e nem proíbe a Telemedicina, tendo em vista que a Resolução nº 2. 228/2019, restabeleceu

a Resolução 1.643/2002 que versa sobre a Telemedicina (CONSELHO FEDERAL DE MEDICINA, 2019).

Ocorre que diante de uma outra realidade proporcionada pelo avanço da Covid-19, tem suscitado a busca de novas soluções para coibir o desenvolvimento da doença, assim, a telemedicina se mostrou como um método eficiente para auxiliar no combate a pandemia. Com origem em Wuhan, na China, a Organização Mundial de Saúde (OMS) em 31 de dezembro de 2019, mencionou o primeiro caso da Covid-19 doença que é causada pelo novo Coronavírus (variante do SARS- CoV-2) e no dia 11 de março de 2020, a OMS classificou a doença como uma pandemia (ORGANIZAÇÃO MUNDIAL DE SAÚDE, 2020).

No Brasil, de acordo com o Ministério da Saúde (2020), o primeiro caso de Covid-19 foi identificado no dia 26 de fevereiro de 2020, em São Paulo. Nisso, a Covid-19 se tornou uma emergência de saúde global, já que o alto contágio e a facilidade de disseminação do vírus, necessitou que fossem tomadas medidas de isolamento social e quarentena domiciliar com o intuito de evitar a proliferação e a sobrecarga no sistema de saúde. Nesse cenário, o emprego da tecnologia no sistema de saúde[13], em especial a telemedicina, apresentou-se como uma oportunidade de garantir o cuidado em saúde por meio do distanciamento social (SIMÕES; OLIVEIRA et al, 2020, p. 105-106).

O uso da telemedicina durante a pandemia, possui determinados benefícios, como, por exemplo, evitar idas aos serviços de emergência em hospitais e clínicas uma vez que possibilita a triagem de pacientes com suspeita de Covid-19, assim como garante que a relação médico e pacientes infectados seja feita por meio de monitoramento remoto e, também, diminui o risco de exposição dos profissionais de saúde a contaminação do vírus (SIMÕES; OLIVEIRA et al, 2020, p. 106). Portanto, diante do aumento exponencial de infectados da doença, o governo brasileiro decretou o Estado de Calamidade Pública e por meio da lei 13. 979/2020 impões medidas para enfrentamento da emergência de saúde pública de importância internacional decorrente do coronavírus responsável pelo surto de 2019.

Considerando a decretação do Estado de Calamidade Pública no Brasil, a propagação descontrolada da Covid-19 e com o intuito de proteger a saúde de médicos e pacientes, o Conselho Federal de Medicina emitiu o Ofício CFM 1.756/2020- COJUR para o Ministério da Saúde, reconhecendo a utilização da telemedicina em caráter excepcional e

[13] De acordo com a Pesquisa sobre o uso da Internet realizada pelo Centro Regional de Estudos para o Desenvolvimento da Sociedade da Informação, no Brasil durante a pandemia do novo coronavírus, entre os usuários de internet que realizaram consulta médica ou com outro profissional de saúde pela Internet, 63% efetuaram o atendimento pela rede pública (SUS) e 50% utilizaram rede privada (plano de saúde) (CETIC.BR, 2020)

enquanto durar o contágio da Covid-19, mas apenas, na modalidade de teleorientação[14], telemonitoramento[15], teleinterconsulta[16]. Em termos claros, o referido documento apesar de não autorizar o uso da Telemedicina de modo irrestrito, busca estabelecer condições mínimas legais para o atendimento médico a distância sem a necessidade de prévio atendimento presencial. (JUNIOR; NOGAROLI et al, 2020, p. 8).

Logo após, o Ministério da Saúde, com o fundamento de operacionalizar e regulamentar as medidas de enfretamento ao Covid-19 previstas no artigo 3º da lei 13. 979/2020, baixou a Portaria 467/2020 que dispõe em caráter excepcional e temporário, sobre as ações de Telemedicina, legitimando todas as suas modalidades e, ampliando as ações de telemedicina para abranger o atendimento "pré-clínico, de suporte assistencial, de consulta, monitoramento e diagnóstico, por meio de tecnologia da informação e comunicação, no âmbito do SUS, bem como na saúde suplementar e privada" (BRASIL, 2020, não paginado). Além disso, a portaria é clara ao dispor que todo o procedimento de utilização da tecnologia da informação, deve garantir a integridade, segurança e sigilo das informações (BRASIL, 2020).

De acordo com Junior e Nagaroli et al (2020, p.15), a referida portaria, além de possibilitar o uso da teleconsulta e do telediagnóstico, pontos que foram omitidos no ofício CFM 1.756/2020, proporciona maior segurança jurídica para a execução da Telemedicina no Brasil, tendo em vista que o seu uso se tornou indispensável e necessário no contexto da pandemia, especialmente para limitar a circulação de pessoas de modo desnecessário.

Nesse mesmo ímpeto, com o objetivo proporcionar segurança jurídica e dá maior efetividade a Telemedicina no Brasil, foi publicada a lei 13.989/2020 que autoriza o uso da telemedicina durante a pandemia, em qualquer atividade da área da saúde. Em contraposição a Resolução 1.643/2002, a lei da telemedicina apesar de possuir caráter emergencial e temporário, ampliou o conceito de telemedicina para abarcar o exercício da medicina mediado por tecnologias para fins prevenção de doenças e lesões e promoção de saúde. A justificativa apresentada para o projeto de lei foi que em razão do caráter emergencial ocasionada pelo coronavírus, deve ser dispensável todo requisito burocrático que dificulte o exercício da

[14] Ofício do Conselho Federal de Medicina 1756/2020: "Teleorientação: para que profissionais da medicina realizem à distância a orientação e o encaminhamento de pacientes em isolamento" (BRASIL, 2020)

[15] Ofício do Conselho Federal de Medicina 1756/2020: "Telemonitoramento: ato realizado sob orientação e supervisão médica para monitoramento ou vigência à distância de parâmetros de saúde e/ou doença" (BRASIL, 2020).

[16]Ofício do Conselho Federal de Medicina 1756/2020: "Teleinterconsulta: exclusivamente para troca de informações e opiniões entre médicos, para auxílio diagnóstico ou terapêutico" (BRASIL, 2020).

telemedicina, para que possa ser assegurado à população a continuidade dos atendimentos em saúde (BRASIL, 2020).

Diante de todo esse percurso, nota-se que a telemedicina se tornou uma peça fundamental no combate da pandemia, bem como possibilitou a abrangência dos serviços de saúde ao pluralizar a capacidade de enfrentamento a Covid-19. Dessa forma, é certo que após a pandemia, a telemedicina, precisa ser regulamentada de modo a atualizar a prática de suas atividades conforme a nova realidade do uso das tecnologias no ramo da saúde.

Além disso, o Ministério da Saúde, apresentou um plano de consultas virtuais aos pacientes do Sistema Único de Saúde (SUS) nos postos de saúde da atenção primária a partir do mês de maio com foco nos pacientes crônicos. Por meio de uma plataforma on-line, os profissionais da saúde poderão realizar teleconsultas médicas, de enfermagem e multiprofissionais no âmbito da Atenção Primária. Além disso, a população pode ter acesso ao TeleSus que realiza atendimento pré-clínico por telefone, chat on-line e de aplicativo para o monitoramento de casos de Covid-19. Nisso, o consultório virtual, trata-se de uma estratégia para evitar a propagação do coronavírus (MINISTÉRIO DA SAÚDE, 2020).

Com isso, ressalta-se que a implementação processo de informatização no âmbito da saúde por meio do emprego de tecnologias de informação e comunicação é um importante componente de garantia e proteção do direito à saúde, o que ficou evidente durante a crise na saúde global provocada pela Covid-19. No entanto, diante do excesso de dados pessoais coletados para uso na saúde, principalmente durante o período de pandemia, casos de vazamento de dados de saúde e a sua coleta indevida se tornaram cada vez mais recorrente.

4.2 Os dados de saúde como dados sensíveis e a problemática em face de sua informatização

O processamento de informações, por meio do e-saúde, envolve desde a simples comunicação entre pacientes e médicos até o compartilhamento mais complexo de dados entre instituições de saúde. Desta forma, ao mesmo tempo em que se deve proporcionar o emprego da tecnologia no âmbito da saúde, é preciso garantir a proteção de dados pessoais e da privacidade dos usuários dos serviços de saúde (KAMEDA; PAZELLO, 2015, p.52-53). Nesse sentido, o direito a saúde, enquanto direito fundamental autônomo, aparece como um sistema de direitos individuais e coletivos que também dão sustentação a outros bens fundamentais indissociáveis, fato que reforça a interdependência e convergência de todos os direitos fundamentais (SARLET; KEINERT, 2015, p. 133).

Conforme já demonstrado, a Telessaúde, se tornou um meio complementar de assistência e garantia do direito à saúde. Contudo, a introdução de tecnologias traz a ideia de que informações referentes à saúde poderão ser transmitidas ou armazenadas e, por isso, tendo em vista que essas informações são de propriedade do paciente, deve ser assegurado que elas permaneçam em sigilo. Desta forma, o sigilo vai além do respeito a autonomia do paciente, pois outros atores são obrigados a certificar a confidencialidade, privacidade e o consentimento (REZENDE; TAVARES et al, 2013, p. 368-369).

Um dos principais desafios com a quebra da privacidade ou o vazamento de informações pessoais em saúde, é o seu potencial discriminatório, principalmente doenças que ainda são estigmatizadas, como, por exemplo, Aids, doenças mentais ou relacionadas à genética humana (SARLET; KEINERT, 2015, p.130). Em 2017, exemplificando, em virtude do uso indevido de informações obtidas por meio de um login válido, dados pessoais de usuários do cartão nacional de saúde SUS, como nome, endereço, CPF e datas de nascimento, foram expostos na internet, violando o direito à privacidade, intimidade e proteção dos dados pessoais.

Entretanto, os dados pessoais em saúde cumprem outra função além da proteção da privacidade, visto que há consequências positivas para a sociedade com o compartilhamento de dados de saúde, como o controle de epidemias[17]. Por tais razões, a dinâmica de dados pessoais, privacidade e informações de saúde, requer que se articule mecanismos para que esse conjunto esteja em equilíbrio e em compasso com as necessidades comuns e as possibilidades tecnologias (ARAGÃO; SCHIOCCHET, 2020, p. 700).

Nesse ínterim, a importância dos dados pessoais como um direito fundamental dos cidadãos, deve ser observada não apenas pelo espectro de proteção das escolhas individuais sobre a exposição de sua personalidade em público, mas também, com o intuito de garantir a liberdade de um indivíduo para que não seja discriminado ou estigmatizado com o tratamento abusivo de seus dados, realidade esta que é mais visível quando o tratamento dos dados estão relacionados à saúde de um cidadão (DONEDA; MONTEIRO, 2015, p. 149). Desse ponto de vista, os dados de saúde, por exemplo, devem gozar de especial proteção, em virtude de que atingem os pontos mais íntimos da personalidade e compelem o indivíduo a encarar com sua própria individualidade (RIVABEM, 2010, p.41).

[17] Não por outra razão, tendo em vista a necessidade de conhecimento de dados para entender a evolução da doença, no meio da pandemia do Covid-19, diante a omissão de dados de casos de Covid-19 pelo Governo Federal, os Estados e os meios de comunicação, resolveram paralelamente contabilizar os novos casos de Covid-19 para entender de que forma o doença estava se espalhando pelo país (AGENCIA ESTADO, 2020).

Assim sendo, o direito fundamental à proteção de dados pessoais dada aos dados de saúde, atenta para o fato de que o manuseio de informações de saúde do cidadão em diferentes bases de dados pode favorecer o acesso indevido a informações sensíveis (DONEDA; MONTEIRO, 2015, p. 149). E em razão dos dados pessoais sensíveis de saúde circularem em diversas redes informatizadas entre instituições, tornam mais vulnerável a garantia da proteção dos dados pessoais e da privacidade, com isso, tais práticas precisam ser protegidas por meio de normatizações (SARLET; KEINERT, 2015, p.135).

A Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018), estabeleceu que dados referentes a saúde são dados sensíveis, assim como os dados pessoais sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural (BRASIL, 2018). A Lei .709/2018 estendeu o alcance em relação ao artigo 3, §3, inciso II da Lei de Cadastro Positivo que, vedou a anotação em bancos de dados de "informações sensíveis, assim consideradas aquelas pertinentes à origem social e étnica, à saúde, à informação genética, à orientação sexual e às convicções políticas, religiosas e filosóficas" (BRASIL, 2011, não paginado).

Aprofundando o exposto acima, os dados sensíveis podem ser considerados como uma espécie de dados pessoais, que possuem um tratamento diferenciado por conta do seu conteúdo apresentar uma especial vulnerabilidade de discriminação, ou seja, há uma preocupação em tais dados estabelecerem uma distinção ou diferenciação de uma pessoa por conta de características da sua personalidade. Com isso, a tutela especial garantida aos dados sensíveis pela lei de proteção de dados, possui o intuito que o indivíduo desenvolva livremente sua personalidade e ao mesmo tempo, é uma forma de evitar práticas discriminatórios que o vazamento desses dados pode causar (BIONI, 2019, p. 85-86).

Os dados médicos, por exemplo, compõem-se de dois elementos, quais sejam o elemento material e imaterial. O primeiro abarca todo suporte físico da informação, como exames e amostras biológicas, já o segundo abrange o conjunto de informações obtidos da história clínica do paciente ou de documentos médicos diversos. Dessarte, tais elementos são considerados bens da personalidade, posto que observadas as suas singularidades, integram-se como parte do indivíduo, no entanto, para que sejam classificados como dados pessoais sensíveis, é preciso que os dados médicos se refiram a uma pessoa determinada ou determinável em que sejam capazes de identificar aspectos objetivos dos indivíduos (RIVABEM, 2010, p.40).

Nesta senda, para o tratamento de dados pessoais sensíveis, a LGPD estabeleceu determinadas exigências. Primeiramente, é necessário que as formas de consentimento do titular sejam para uma finalidade destacada e específica. Em segundo lugar, é possível o uso de dados sensíveis sem o consentimento do titular no caso de obrigação legal; para a formulação de políticas públicas; realização de estudos por órgãos de pesquisa; exercício regular de direitos em contratos e processos; proteção da vida ou da incolumidade física; tutela da saúde por profissionais ou serviço de saúde; garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos. Entretanto, nessa última hipótese, o tratamento de dados sensíveis deve ocorrer apenas em situações indispensáveis, cabendo ao controlador provar a indispensabilidade (BRASIL, 2019).

Através do consentimento, nota-se que a LGPD privilegia a participação ativa do titular do dado sensível, sendo que o consentimento deve advir de uma manifestação livre, informada e inequívoca com uma finalidade determinada. É livre, pois o titular deve consentir sem coação física, moral, mental ou outro meio que o induza, por outro lado, tem que ser informado e inequívoco, uma vez que o uso e compartilhamento dos dados devem ser comunicados ao titular de modo clara e de fácil compreensão. Já a finalidade determinada, apresenta-se como um princípio que rege a atuação da LGPD, logo é necessário a demonstração específica sobre quais serão as aplicações do tratamento das informações (ARAGÃO; SCHIOCCHET, 2020, p. 700).

Conforme Sarlet e Caldeira (2019, 14), o consentimento é uma das principais garantias que orientam o contato entre pacientes e profissionais da saúde, de tal forma que o ato de consentir implica em assegurar a transparência na coleta, armazenamento, finalidade, tratamento e transmissão de dados pessoais, assim, o paciente é livre para deliberar sobre seus dados, como também para revisar e retirar a sua anuência a qualquer tempo sem resultar prejuízos.

Nessa esteira, não basta apenas o consentimento do titular sobre se seus dados poderão ou não ser coletado, mas de acordo com a LGPD é preciso que as informações dispostas ao titular sejam previamente apresentadas de forma transparente, clara e inequívoca, bem como, o controlador deve informar ao titular caso haja mudança na finalidade para o tratamento de dado sensíveis no consentimento original, a fim de que ele possa concordar ou revogar o seu consentimento. Dessa maneira, destaca-se que é nítida a primazia do consentimento ao enfatizar o direito a portabilidade consagrando o direito à informação e de esclarecimento sobre a utilização de dados (SARLET; CALDEIRA, 2019, p. 22).

Além do consentimento como meio de proteção dos dados sensíveis, a LGPD elencou em seu artigo 12 que os dados anonimizados não seriam dados pessoais, mas em seu §4º estabeleceu que poderão ser considerados como dados pessoais, aqueles dados anonimizados utilizados para formação de perfil comportamental de determinada pessoa natural se identificada (BRASIL, 2018). Nesse contexto, que se encaixa o perfilamento discriminatório causado a partir da discriminação algorítmica[18] pelo uso de informações sensíveis, que tende atacar grupos discriminados historicamente por conta de um conteúdo específico da sua individualidade (MENDES; MATTIUZZO, 2019, p. 52).

Pode-se inferir, portanto, que os dados anônimos que se tornam dados pessoais, quando utilizados para formação de perfis, por ser objeto de tutela da LGPD, atraem a incidência dos princípios impostos pela lei geral que, rejeitam toda forma de discriminação oriunda do tratamento de dados pessoais, em especial no caso dos dados sensíveis. Assim, observa-se que a LGPD expandiu a proteção nas atividades de tratamento de dados que poderiam lesionar o livre desenvolvimento da personalidade (BIONI, 2019, p. 81).

Tendo em vista os riscos que envolve a transferência de dados pessoais sensíveis em saúde sem o consentimento do titular, ou a utilização de tais dados para fins diversos dos quais foram legitimados a sua coleta, dos princípios propostos pela LGPD, de acordo com Mulholland (2018, p. 163) dois devem ser visto com especial atenção no tratamento de dados sensíveis, quais sejam, o princípio da finalidade e da não-discriminação, pois, na coleta desses tipos de dados, os controladores devem restringir a coleta apenas a finalidade designada inicialmente e, caso seja necessário qualquer modificação o paciente deve ser comunicado para evitar desvios ou uso indevido com fins discriminatório. Com isso, ainda se destaca o papel da Autoridade Nacional em dispor sobre padrões, técnicas e parâmetros de segurança utilizados no processo de anonimização de dados pessoais de acordo com o artigo 12, §3º da LGPD (BRASIL, 2018).

Entretanto, de acordo com Bioni (2019, p. 144), diante da sociedade informacional, cada vez mais a participação social depende do trânsito informacional, no entanto, em decorrência da assimetria informacional, técnica e econômica, entre o cidadão e o controlador

[18] “ Os algoritmos estão hoje sendo programados para a extração de padrões e inferências a partir dos quais serão tomadas, de forma automatizada, decisões sobre questões objetivas, mas que estão atreladas a importantes dados sensíveis, assim como decisões sobre questões subjetivas e que envolvem complexos juízos de valor, tais como (i) avaliar as características, a personalidade, as inclinações e as propensões de uma pessoa, inclusive no que diz respeito à sua orientação sexual; (ii) analisar o estado de ânimo ou de atenção de uma pessoa; (iii) identificar estados emocionais, pensamentos, intenções e mesmo mentiras; (iv) detectar a capacidade e a habilidade para determinados empregos ou funções; (v) analisar a propensão à criminalidade; (vi) antever sinais de doenças, inclusive depressão, episódios de mania e outros distúrbios, mesmo antes da manifestação de qualquer sintoma”(FRAZÃO, 2019, p. 12).

de dados pessoais, nota-se que o cidadão deve ser identificado como um sujeito vulnerável. Assim sendo, é preciso que disposições normativas interfiram no fluxo informacional facilitando a tomada de decisão do sujeito, não deixando, o protagonismo do consentimento ficar a cargo apenas do titular dos dados.[19]

Dado isso, diante dos riscos envolvidos, é necessário que além da LGPD, outras regulações setoriais sejam feitas com o intuito de garantir o ato do consentimento. Por seu turno, na área da saúde, para garantir a confidencialidade de informações prestadas, é essencial o uso do termo de consentimento livre e esclarecido[20] (TCLE) para garantir a autonomia do paciente a partir de uma decisão voluntária. Em se tratando do uso da telessaúde, o paciente deve ser informado sobre as limitações e inovações empregadas no atendimento, respeitando a vontade do usuário e vinculando o profissional da saúde a responsabilidade de seus atos (REZENDE; TAVARES et al, 2013, p. 370). Como exemplo, destaca-se a Resolução 2.227/2018, que disciplinava o uso da telemedicina ampliando as suas modalidades de cabimento, apesar de sua revogação, a resolução foi clara ao estabelecer que no teleatendimento, na telecirurgia robótica e na transmissão de imagens e dados, a necessidade de consentimento informado do paciente.

Outro ponto que cabe destacar, é que o emprego da implantação do e-saúde para o Brasil, enseja um maior acesso às informações clínicas do paciente e, com isso, a combinação de dados de saúde com outros tipos de dados pode resultar em usos indevidos e não autorizados ao compartilhamento pelo paciente. Assim, os serviços voltados para definir e implantar uma arquitetura para a e-saúde devem estar pautados em políticas e mecanismos de controle de acesso, permissões e gestão do fluxo das informações (MINISTÉRIO DA SAÚDE, 2017, p. 61).

De modo semelhante, observa-se com o desenvolvimento e uso do Prontuário Eletrônico do Paciente (PEP), pois, o compartilhamento em rede dos dados pessoais do paciente possibilita o armazenamento de diversos dados sensíveis, de modo que o uso inadequado e o acesso indevido podem pôr em xeque a privacidade, proteção dos dados pessoais e a confidencialidade (SARLET; KEINERT, 2015, p. 135). De acordo com Lima (2017, p. 16),

[19] "Em relações de assimetria e cuja causa regulatória é a proteção de um vulnerável, necessário se faz uma *pitada de paternalismo* para que efetivamente seja alcançada uma autonomia por parte do elo mais fraco no processo de tomada de decisão e, complementar e subsidiariamente, tomadas mais intervencionistas para a sua proteção." (BIONI, 2019, p. 168-169).

[20] "No termo de consentimento livre e esclarecido para a prática da telemedicina, deverão constar informações sobre os benefícios esperados e os possíveis riscos associados à utilização da tecnologia. Acima de tudo, o médico precisa expor claramente ao paciente quais as diferenças na prestação do serviço médico a distância em relação ao atendimento presencial, para aquele paciente e caso específicos. Após repassadas todas as informações necessárias, ainda é imprescindível um diálogo entre o médico e o paciente, no intuito de que aquele se certifique que este compreendeu tudo que lhe foi transmitido." (DANTAS; NOGAROLI, 2020, p. 164).

pode ocorrer de dois modos o manejo inadequado de dados do prontuário eletrônico, o primeiro reside no compartilhamento de dados entre profissionais da saúde ou entre estes e instituições sem o consentimento ou conhecimento do paciente e, o segundo, decorre das mudanças na finalidade da coleta dos dados sem o consentimento ou conhecimento do usuário. Nesse ponto, cabe apontar que a Resolução do CFM nº 1821/2007 ao versa sobre o prontuário eletrônico, é omissa em ressaltar e disciplinar a necessidade de consentimento do titular do dado em caso de compartilhamento.

Nesse cenário, em virtude da falta de padronização nos procedimentos para o tratamento e obtenção de dados em saúde e entre outras lacunas, o Ministério da Saúde criou a Política Nacional de Informação e Informática em Saúde (PNIIS), com o intuito de orientar o sistema de saúde brasileiro diante da implementação das novas tecnologias para formular um Sistema Nacional de Informação em Saúde (SNIS), sendo assim, entre os princípios que norteiam o PNIIS, está o princípio da confidencialidade, sigilo e privacidade da informação de saúde pessoal como direito de todo indivíduo que possui ligação direta com a proteção de dados pessoais (MINISTÉRIO DA SAÚDE, 2016, p. 7- 13).

No mesmo sentido, em se tratando de tecnologia no âmbito da saúde, a Agência Nacional de Saúde Suplementar (ANS)[21] estabeleceu um Padrão para Troca de Informação de Saúde Suplementar (TISS) que estabelece um padrão obrigatório para as trocas eletrônicas de dados dos beneficiários de planos, entre os agentes da saúde suplementar. O Padrão TISS, atualizado em outubro de 2020 é organizado em cinco componentes, quais sejam: organizacional, conteúdo e estrutura, representação de conceitos em saúde, segurança e privacidade e comunicação (AGÊNCIA NACIONAL DE SAÚDE SUPLEMENTAR, 2012).

A medida regulatória do Padrão TISS foi inicialmente estabelecida pela Resolução Normativa nº305 de 2012 que regulamentou o padrão obrigatório para Troca de Informações na Saúde Suplementar - Padrão TISS dos dados de atenção à saúde dos beneficiários de plano privado de assistência à saúde. A resolução buscou identificar as finalidades e obrigações do Padrão TISS, como também estabeleceu penalidades administrativas. Nisso, o artigo 14 da presente resolução traz que o componente de segurança e privacidade abrange proteção dos dados de atenção à saúde e visam assegurar o direito individual ao sigilo, à privacidade e à

[21] Artigo 2º do Decreto nº 3.327, de 5 de janeiro de 2020: "A ANS terá por finalidade institucional promover a defesa do interesse público na assistência suplementar à saúde, regulando as operadoras setoriais, inclusive quanto à suas relações com prestadores e consumidores, contribuindo para o desenvolvimento das ações de saúde no País." (BRASIL, 2020).

confidencialidade dos dados de atenção à saúde (AGÊNCIA NACIONAL DE SAÚDE SUPLEMENTAR, 2012).

Superada essa primeira análise sobre a proteção de dados pessoais em saúde, a partir de agora, cabe entender os desafios que estão sendo enfrentados com o uso de dados pessoais sensíveis durante a Covid-19. O atual contexto da Covid-19, exigiu que os governos adotassem medidas de combate a proliferação do vírus, em prol da sociedade e da promoção saúde. Dentre as medidas adotadas, destaca-se o uso da tecnologia para possibilitar o rastreamento de sintomas, contatos e deslocamento de acompanhamento e avaliação na vigilância de contágios[22], todavia, indaga-se a quantidade e tipos de dados pessoais, em especial sensíveis, usados, coletados e compartilhados em nome saúde pública sem o devido respeito à privacidade, aos dados pessoais sensíveis e a confidencialidade.

Nesse panorama, o Brasil investiu do desenvolvimento de aplicativos que tem como objetivo contribuir para a vigilância epidemiologia, difusão de informações e monitoramento do quadro clínico dos indivíduos. Entre esses aplicativos, avaliando a política de privacidade, destaca-se o Coronavírus SUS, antes de sua atualização, o aplicativo não apresentava nenhum tipo de documento ao usuário em relação ao consentimento expresso do uso dos dados pessoais, após sua atualização, o aplicativo deixou de utilizar dados de geolocalização dos usuários para fazer o rastreamento de contato e passou a adotar um modelo descentralizado de armazenamento de dados baseado nas trocas de informações via bluetooth protegidas por criptografia (FAVARO; ZANATTA, 2020).

Todavia, ainda se questiona a efetividade no rastreamento de contato digital, pois, além de não existir estudo científicos que comprove a eficácia do uso do rastreamento digital no Brasil, depende do ato voluntário de cada indivíduo de usar e comunicar que testou positivo e seguir o isolamento, além do mais no modelo descentralizado o Estado não tem como monitorar o cumprimento do isolamento. Nesse sentido, ainda que a plataforma tenha sido atualizada mostrando uma preocupação com a proteção dos dados pessoais, a falta de acessibilidade e confiança da população mais o baixo nível de testagem comprometem a plena eficácia desse sistema de rastreamento (FAVARO; ZANATTA, 2020).

[22] "A Coreia do Sul está rastreando telefones de indivíduos e criando um mapa publicamente disponível para permitir que outros cidadãos verifiquem se podem ter cruzado com pacientes contaminados pelo coronavírus. Os dados de rastreamento que entram no mapa não se limitam aos dados de telefones celulares; registros de cartão de crédito e até mesmo entrevistas pessoais com pacientes estão sendo usados para criar um mapa retroativo de onde eles estiveram. Não apenas o mapa está lá para os cidadãos verificarem, mas o governo sul-coreano está usando-o para enviar proativamente mensagens de texto regionais, alertando as pessoas de que podem ter entrado em contato com alguém portador do vírus." (MOURA; FERRAZ, 2020, p. 1-2).

Além do uso de aplicativos, a empresa de telefonia TIM e a prefeitura do Rio de Janeiro, fecharam uma parceria para a construção, a partir de uma base dados, de um mapa de deslocamento durante a pandemia com o intuito de auxiliar no controle do vírus e nas medidas a serem tomadas pelos órgão governamentais. A empresa afirma que as informações coletas serão anônimas e estarão de acordo com a confidencialidade e segurança dos dados pessoais, no entanto, os serviços de telecomunicação detém dados cadastrais e de identificação civil de milhões de pessoais e, por isso, o esforço para a anonimização de dados pode se tornar reativo e não proativo, pois é possível o cruzamento de dados pessoais com as informações que a empresa já detém. Assim, é preciso que os governos, antes de adotarem tecnologias de monitoramento, assegurem um elevado padrão de proteção dos dados pessoais (MOURA; FERRAZ, 2020, p. 6).

A lei 13.979 de 6 de fevereiro de 2020 que dispõe sobre as medidas de enfrentamento da emergência de saúde pública de importância internacional decorrente do coronavírus responsável pelo surto de 2019, elenca em seu artigo 6º que entre os órgãos e entidades da administração pública é obrigatório o compartilhamento de dados para identificação de pessoas infectadas ou com suspeita de infecção pelo coronavírus, com a finalidade exclusiva de evitar a sua propagação (BRASIL, 2020). No primeiro momento, observa-se que não há violação ao direito dos titulares, pois a própria LGPD em seu artigo 11, II, a, garante a possibilidade do uso de dados sensíveis para o cumprimento de obrigação legal. Entretanto, a lei é omissa em relação de como será a tomada de decisões sobre as informações de dados pessoais, além disso, apesar da importância da LGPD para guiar o uso de tratamento de dados pessoais, ela só entrou em vigor no dia 18 de setembro de 2020, o que gerou uma insegurança jurídica no manuseio de dados ao combate ao coronavírus (OLIVEIRA, 2020, p. 27).

Ainda nesse contexto, Oliveira (2020, p. 28) aponta que o artigo 6º da lei 13.979/2020 possui quatros problemas, já que retira de modo arbitrário, a possibilidade do titular dos dados de controlar seus próprios dados, não estabelece quais dados poderão ser compartilhados, bem como não apresenta nenhuma política interna no tratamento de dados pessoais e de transparência. Diante disso, o fluxo informacional ocasionado pela administração pública no compartilhamento de dados pessoais sem o processamento adequado sob o argumento de evitar a propagação do vírus, pode ocasionar a discriminação de dados pessoais.

Para tanto, conforme já mencionado no primeiro capítulo, a LAI visa que o poder público informe e seja transparente quanto aos seus atos perante a população, para isso adota os princípios da publicidade e transparente, entretanto, tais princípios devem ser observados

com cautela quando se tratada de dados pessoais nas mãos da administração pública, já que os princípios da intimidade, confidencialidade e privacidade das informações devem ser levados em conta. Nesse sentido, tendo em vista assimetria entre a administração pública e os titulares dos dados, a coleta de dados sensíveis no âmbito do poder público confere grande responsabilidade ao controlador dos dados e, por isso, o artigo 23 da LGPD, impõe, como regra, para utilização de informação pessoais, o dever de atender uma finalidade determinada com base no interesse público e com o objetivo de executar competências e atribuições legais do serviço público (FLORÊS; SILVA, 2020, p. 23-24).

Não por outra razão, o relatório "Privacidade e pandemia: recomendações para o uso legítimo de dados no combate à COVID-19" do Data Privacy Brasil, apresentou os princípios e recomendações para formulação de políticas públicas de compartilhamento de dados pessoais, pela administração pública e entre o setor privado. Sendo assim, o primeiro passo a ser seguido é avaliar a necessidade da elaboração de políticas de saúde centrada e orientadas por dados, essa necessidade, entretanto, deve ser demonstrada por meio de uma motivação fundamentada, para impedir o exercício arbitrário do Estado, em evidencias técnicas e científicas ou expondo as razões da eficiência do uso dos dados, além do mais, a obrigatoriedade de compartilhamento de dados por parte do setor privado para o setor público deve está amparada por lei formal e, por fim, é necessário a formulação de um termo contratual (BIONI; ZANATTA et al, 2020, p.14-16).

O segundo passo, é a definição expressa da finalidade e necessidade do tratamento em coerência com o artigo 6º, I e III da LGPD. Nisso, qualquer tratamento de dados para o combate da covid-19 deve ser motivado com uma finalidade determinada indicando a medida de combate em específico cogitada para mitigar os riscos que os dados sejam usados para fins discriminatórios ou abusivos com finalidades posteriores que não estão relacionadas exclusivamente com o enfretamento da Covid-19. Nesse sentido, é vedado o uso de dados pessoais com finalidade lucrativas e discriminatória na utilização de informações em saúde que são dados pessoais sensíveis, conforme dispõe o artigo 11, §4º da LGPD. Outro ponto que deve ser observado para concretização do segundo passo, é a utilização do mínimo necessário para a coleta de dados com o fim de atingir a finalidade pretendida no combate a pandemia (BIONI; ZANATTA et al, 2020, p.16-18).

Após definido a finalidade e necessidade do uso e coleta dos dados pessoais, chega-se ao terceiro passo em que o gestor público deve formular o ciclo de vidas do dados pessoais prevendo início, meio e fim dos dados coletados, da mesma maneira que deve garantir a qualidade dos dados segundo o artigo 6º, V da LGPD assegurando a exatidão, clareza,

relevância e atualização dos dados dos titulares. Já o quarto passo, busca salvaguarda os direitos fundamentais a partir do processo de pseudo - anonimização como forma de garantir baixos riscos de reidentificação de pessoas. Assim, tendo em vista que a alta probabilidade de reindentificação de dados de celulares de localização, principalmente os supostamente anonimizados por meio de estatística, as políticas públicas devem sempre garantir o maior nível possível de pseudo - anonimização, nesse viés, deve ser evitado a propagação de divulgações da identidade de recuperados, infectados ou suspeitos a Covid-19 e adotado medidas de segurança da informação (BIONI; ZANATTA et al, 2020, p. 18-22).

A título de ilustração sobre o disposto acima de vazamentos de dados pessoais sensíveis no período de Covid-19, cabe relatar que em Arapongas, município do Paraná, foi divulgado na Internet uma lista de pessoas infectadas com o novo coronavírus. Dentre os nomes do paciente, a lista apresentava o telefone, endereço, o dia que receberam o resultado, assim como o posto de saúde que foram atendidos. Nota-se assim, os malefícios do perfilamento (profiling), com uso de dados pessoais que geram tratamento discriminatório, pois, o vazamento de dados pessoais sensíveis pode se tornar um produto lucrativo, por exemplo, para empresas de saúde que utilizam do cruzamento de informações, sem a autorização do paciente, para produção de medicamentos e tratamentos ou com o fim de investigação da vida pregressa do paciente (SILVA, 2020, p. 66).

Por fim, o quinto passo, recomenda a adoção de medidas de transparência, conforme o artigo 6, VI da LGPD, para que o poder público e entidades privadas prestem informações claras, precisas e acessíveis sobre o tratamento dos dados e os respectivos controladores. Assim sendo, todo esse percurso precisa ser traçado com o objetivo de que o uso de dados pessoais, em especial os sensíveis, seja utilizado de maneira legítima para formulação de políticas públicas e iniciativas privadas em combate ao Covid-19, como também, o papel da LGPD deve ser encarado como referência para proteção de direitos e liberdade fundamentais e não como um obstáculo ao uso de dados pessoais (BIONI; ZANATTA et al, 2020, p. 12).

Além da observância de recomendações, o papel da ANPD, apresenta-se de grande relevância para a tutela dos dados pessoais, em especial os sensíveis, diante do manejo e controle de dados por empresas e pelo Estado. Em suas competências elencadas no art. 55-J da LGPD, destaca o dever de zelar pela proteção de dados pessoais, fiscalizar e aplicar sanções, como também pode requisitar, às entidades do poder público que realizem operações de tratamento de dados pessoais informe a finalidade específica sobre os dados e os demais detalhes do tratamento realizado (BRASIL, 2019). Aqui, mais uma vez se observa a dimensão

objetiva do dever de prestação estatal do direito a proteção de dados pessoais, já que a ANPD é a exata manifestação do Estado tentando criar meios para que o direito seja protegido.

Nesta senda, é preciso reconhecer que, no âmbito da sociedade da informação, a defesa da privacidade e dos dados pessoais estabelecem os limites entre os interesses públicos e privados, visto que na esfera pública, o Estado tem o dever de garantir a saúde universal e o interesse da coletividade o que requer o desenvolvimento de mecanismos de comunicação e tecnologia em saúde para proporcionar um melhor atendimento, já na dimensão privada, o cidadão espera que tenha sua privacidade e confidencialidade preservada sobre seus dados de saúde e, nisso, cabe ao Estado o dever de garantir por meio de investimento em políticas de privacidade, proteção de dados pessoais sensíveis, assim como de respeito a cidadania de cada ser humano (MORAES, 2015, p. 11).

5 CONSIDERAÇÕES FINAIS

Com a presente monografia, objetivou-se analisar, á luz da sociedade da informação, a proteção e promoção dos dados pessoais em saúde no ambiente virtual. Sendo assim, o estudo foi dividido em três capítulos.

O primeiro capítulo tratou do surgimento da sociedade da informação, suas nuances e os marcos normativos. Inicialmente, abordou-se o surgimento e características da sociedade da informação que impactou nos diversos ramos da estrutura organizacional da sociedade, tendo como novo destaque a informação. Com informatização da informação e a sua capacidade de processamento no meio virtual, observou-se a revolução da tecnologia da informação que contribui para o avanço tecnológico e, em consequência, a possibilidade no cruzamento de dados pessoais.

Destarte, na sequência, foi destacado que, por outro lado, a troca de informações intensificada pelo uso das redes digitais trouxe um conjunto de riscos aos direitos personalizadíssimos, já que o uso inadequado ou abusivo de dados pessoais por meio de empresas ou pelo Estado, acabou pondo em cheque a garantia dos direitos de privacidade, intimidade e proteção de dados pessoais, como também a capacidade do indivíduo de controlar seus dados pessoais.

Assim, observou-se que em conjunto com a sociedade da informação eclodiu a sociedade de risco que tornou o ambiente digital um lugar propício para que controladores e operadores se beneficiassem do excesso de dados pessoais disponíveis com o objetivo de utilizá-los para fins econômicos, sem o consentimento do titular. E por isso, é certo que diante da assimetria informacional, o indivíduo está em uma situação de vulnerabilidade.

Com isso, se fez necessário as primeiras regulamentações que trataram sobre o manuseio de bancos de dados pessoais, destacou- se o Código de Defesa do Consumidor, a Lei do Cadastro Positivo, a Lei do Acesso a Informação e o Marco Civil da Internet. O CDC e a Lei do Cadastro Positivo regulamentaram os bancos de dados dos consumidores na concessão de crédito, já a LAI buscou garantir que o manuseio das informações pessoais pelo setor público respeite à intimidade, vida privada, honra e a imagem das pessoas. E o Marco Civil da Internet elencou princípios fundamentais que tutelam o uso da Internet. Nisso, pôde-se interferir que tais leis setoriais contribuíram para formação de uma Lei Geral de Proteção de Dados Pessoais.

No segundo capítulo deste trabalho, desenvolveu-se o estudo do direito a privacidade e o percurso traçado para a garantia do direito a proteção de dados pessoais como um direito fundamental autônomo. Pode-se interpretar que o livre desenvolvimento da personalidade estabelece uma íntima relação entre a privacidade e a proteção de dados pessoais, nisso, foi possível constatar que diante da sociedade da informação, o direito a proteção dos dados pessoais não deveria ser entendido apenas como uma mera evolução do direito à privacidade e sim, como um direito fundamental autônomo.

Portanto, analisou-se que a proteção de dados pessoais deve ser reconhecida como um direito fundamental autônomo que, apesar de não está previsto expressamente na Constituição Federal, pode ser reconhecido como um direito materialmente fundamental por conta da cláusula de abertura do artigo 5º, §2º da Constituição Federal, além do mais, por meio da ADI 6387 o Supremo Tribunal Federal reconheceu o direito a proteção dos dados pessoais como um direito fundamental autônomo.

Nesse sentido, observou-se a proteção de dados pessoais como um novo direito de personalidade e, com isso, o alcance normativo da LGPD é essencial para garantir o direito a proteção dos dados pessoais, personalidade, intimidade e privacidade do titular do dado, sem, contudo, impossibilitar o desenvolvimento tecnológico. A LGPD trouxe um rol de princípios que guiarão a coleta e o tratamento de dados pessoais tanto no setor público quando no privado, de tal forma que a proteção dados pessoais seja tutelada por uma lei geral completa e estruturada.

Por fim, no terceiro capítulo, analisa-se os impactos da sociedade da informação na saúde por meio no uso da tecnologia de informação e comunicação na saúde digital, destacando que apesar de determinados desafios que devem ser superados, o e-saúde é um componente importante na promoção do direito a saúde, seja por meio dos prontuários eletrônicos, da telessaúde ou da telemedicina. Visualizou-se que em meio a pandemia do Covid-19 e os problemas de saúde enfrentados globalmente, a telemedicina se destacou como elemento integrador da portabilidade do direito à saúde.

Diante disso, notou-se que o intenso uso e transmissão de informações pessoais no âmbito da saúde digital, avoca que o sigilo, a confidencialidade e o consentimento sejam garantidos, já que a LGPD trata dos dados de saúde como dados sensíveis que merecem uma tutela especial em razão do conteúdo discriminatório que carregam. E por isso, qualquer tentativa de violação desses dados devem rechaçadas.

Assim, o terceiro capítulo encerra demonstrando que a LGPD estabeleceu a qualquer tratamento de dados pessoais sensíveis o consentimento do titular, de modo a tutelar

a autodeterminação informativa do titular dos dados no controle das informações que lhe diz respeito. Bem como, observou-se com a pandemia da Covid-19 como o uso de dados pessoais sensíveis de saúde, podem ser usados para o benefício da sociedade ou para a violação de direitos fundamentais personalíssimos.

Ao final desta monografia, conclui-se que a proteção dos dados pessoais assume cada vez mais espaço no contexto da sociedade informacional, tendo em vista os diversos riscos que podem originar no tratamento indevido e abusivo de dados pessoais, principalmente em relação aos dados sensíveis. Desta forma, ao garantir o direito fundamental a proteção de dados pessoais como um direito autônomo, outros direitos fundamentais necessários para o desenvolvimento da livre personalidade serão efetivados e protegidos. Deste modo, tendo em vista o teor dos dados sensíveis de saúde, observou-se a necessidade do tratamento diferenciado a esses dados, pois, ao mesmo tempo em que seu uso serve para a criação de tecnologias na saúde digital, também pode ser utilizado para fins discriminatórios e abusivos. Nesse sentido, a aplicação e adequação da LGPD é um importante mecanismo de garantir a efetivação desse direito de modo pleno.

REFERÊNCIAS

AFONSO DA SILVA, José. **Curso de Direito Constitucional Positivo**. 25. Ed. São Paulo: Malheiros Editores, 2005.

AGÊNCIA ESTADO. Após Omissão de dados pelo governo pelo governo federal, estados e sociedade fazem contagem paralela de casos de Covid-19**. Dom Total**.2020. Disponível em: https://domtotal.com/noticia/1451257/2020/06/apos-omissao-de-dados-pelo-governo-federal-estados-e-sociedade-fazem-contagem-paralela-de-casos-de-covid-19/ Acesso em 20 nov. 2020

AGÊNCIA NACIONAL DE SAÚDE SUPLEMENTAR. **Resolução Normativa RN no 305, de 9 de outubro de 2012**. Esta Resolução estabelece o padrão obrigatório para Troca de Informações na Saúde Suplementar – Padrão TISS dos dados de atenção à saúde dos beneficiários de Plano Privado de Assistência à Saúde; revoga a Resolução Normativa – RN no 153, de 28 de maio de 2007 e os artigos 6º e 9o da RN no 190, de 30 de abril de 2009. Diário Oficial da União 2012; 10 out.

AGUIAR, Rodrigo Goulart et al. **Sociedade em rede e internet: direitos fundamentais em diálogo.** 2015. Disponível em: http://tede2.pucrs.br/tede2/bitstream/tede/6116/2/470206%20%20Texto%20Parcial.pdfAcesso em 15 set. 2019

ARAGÃO, Suéllyn Matos de; SCHIOCCHET, Taysa. Lei Geral de Proteção de Dados: desafio do Sistema Único de Saúde. **Rev Eletron Comun Inf Inov Saúde**. 2020 jul.-set.; Disponível em https://www.arca.fiocruz.br/bitstream/icict/43716/2/14.pdf Acesso 18 nov. 2020.

ASCENÇÃO, José de Oliveira. O direito do autor no ciberespaço**. Direito**, 1999. Disponível em: http://www.egov.ufsc.br/portal/sites/default/files/o_direito_do_autor_ni_ciberespaco.pdf Acesso 1 nov. 2019

ASCENÇÃO, José de Oliveira. Direito Intelectual, exclusivo e liberdade. **Revista Esmafe**: Escola de Magistratura Federal da 5ª Região, n. 3, mar. 2002.

ASSAF, Maria Inês Costa; DOMINGUES, Fabio Henrique Assaf. **Da Autoridade Nacional de Proteção de Dados (ANPD) e do Conselho Nacional de Proteção de Dados Pessoais e da Privacidade**. In: Comentários à Lei Geral de Proteção de Dados. 2020. Jan. 2020.

BARBOSA, Denis Borges. **O Direito Constitucional da Inovação**. 2006. Disponível em: http://denisbarbosa.addr.com/inovaconst.pdf Acesso em 15 abr. 2019.

BARBOSA, Paulo Henrique Ferreira de Araujo; PEREIRA, Thiago Vidal et al. Telemedicina. In: LEITE, Cicília Raquel Maia; REIS, Célia Aparecida dos; BINSFELD, Pedro Canisio; ROSA, Suélia de Siqueira Rodrigues Fleury (org.). **Novas tecnologias aplicadas à saúde:** desenvolvimento de sistemas dinâmicos: conceitos, aplicações e utilização de técnicas inteligentes e regulação. Mossoró - RN: EDUERN, 2019. E-book (608 p.). Disponível em: https://ppgcc.ufersa.edu.br/wpcontent/uploads/sites/42/2019/07/novas-tecnologias-vol2-final3.pdf. Acesso em: 01 nov. 2020.

BECK, Ulrich. **Sociedade de risco: rumo a uma outra modernidade**. São Paulo: Ed. 34, 2010.

BERNARDES, Camila Fernandes Santos. **O Direito Fundamental de Acesso à Informação: Uma Análise sob a Ótica do Princípio da Transparência.** 2015. 175 f. Dissertação (Mestrado em Direitos e Garantias Fundamentais) – Universidade Federal de Uberlândia, Uberlândia, 2015.

BIONI, Bruno Ricardo**. Proteção de dados pessoais: a função e os limites do consentimento.** Rio de Janeiro: Forense, 2019.

BIONI, Bruno; ZANATTA, Rafael et al. **Privacidade e pandemia: recomendações para o uso legítimo de dados no combate à COVID-19**. Conciliando o combate à COVID-19 com o uso legítimo de dados pessoais e o respeito aos direitos fundamentais. São Paulo: Data Privacy Brasil, 2020. Disponível em https://www.dataprivacybr.org/wp-content/uploads/2020/04/relatorio_privacidade_e_pandemia_final.pdf Acesso em 19 nov. 2020.

BITTAR, Carlos Alberto. **Os direitos da personalidade**. 8.ed., ver. aum. e mod. por Eduardo C. B. Bittar. São Paulo: Saraiva, 2015.

BOFF, Salete Oro; DIAS, Felipe da Veiga. O acesso à informação no campo digital: uma análise entre a sociedade da informação e sociedade de risco. **Revista de Estudos Jurídicos UNESP**, v. 16, n. 23, 2012. Disponível em: https://ojs.franca.unesp.br/index.php/estudosjuridicosunesp/article/view/482/654 Acesso em: 15 abr. 2019

BRASIL. **Constituição da República Federativa do Brasil de 1988**. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em 05 maio. 2020

BRASIL. **Decreto nº 3.327/2000**. Aprova o Regulamento da Agência Nacional de Saúde Suplementar- ANS, e dá outras providencias. Diário Oficial da União, Brasília, DF, 5 jan. 2000. Disponível em: https://www2.camara.leg.br/legin/fed/decret/2000/decreto-3327-5-janeiro-2000-370758-publicacaooriginal-1-pe.html Acesso em 12 nov. 2020

BRASIL. **Lei n. 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais. Dispõe sobre a proteção de dados pessoais e altera a Lei N. 12.965, de 23 de abril de 2014 (Marco Civil da Internet). Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em 15 ago. 2020

BRASIL. Lei nº 13.853, de 8 de julho de 2019. Altera a Lei nº 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados; e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2019/Lei/L13853.htm#art1 Acesso 25 nov. 2020

BRASIL. **Lei nº 13.989/2020, de 15 de abril de 2020.** Dispõe sobre o uso da telemedicina durante a crise causada ao coronavírus (SARS-COV-2). Diário Oficial da União. Disponível

em: https://www.in.gov.br/en/web/dou/-/lei-n-13.989-de-15-de-abril-de-2020-252726328 Acesso em 16 nov. 2020

BRASIL. **Lei nº. 8.078, de 11 de setembro de 1990**. Código de Defesa do Consumidor. Dispõe sobre a proteção do consumidor e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/Leis/L8078.htm Acesso em: 01 nov. 2019.

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. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011- 2014/2011/lei/l12414.htm - Acesso em 01 nov. 2019.

BRASIL. **Lei nº 13.979, de 6 de fevereiro de 2020.** Dispõe sobre as medidas para enfrentamento da emergência de saúde pública de importância internacional decorrente do coronavírus responsável pelo surto de 2019. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/lei/l13979.htm Acesso em 18 nov. 2020

BRASIL. Presidência da República. **Lei n. 12.527, de 18 de novembro de 2011**. Regula o acesso à informação inciso II do § 3odo art. 37 e no § 2o do art. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm. Acesso em: 01 nov. 2019.

BRASIL. **Lei n. 12.965, de 23 de abril de 2014**. Marco civil da internet. Lei n. 12.965, de 23 de abril de 2014, que estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil. 2. ed. Brasília: Câmara dos Deputados, Edições Câmara, 2015. (Série legislação; n. 164).

BRASIL. Câmara dos deputados. **Projeto de Lei nº 2.601,** de 05 de maio de 2019. Altera a lei nº12. 965/2014, para criar obrigação de indisponibilização de notícias falsas por provedores de aplicações de internet e dá outras providencias**.** Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2199770 Acesso em 07 set. 2020

BRASIL. **Decreto nº 10.474, de 26 de agosto de 2020**. Aprova a Estrutura Regimental e o Quadro demonstrativo dos Cargos em Comissão e das Funções de Confiança da Autoridade Nacional de Proteção de Dados e remaneja e transforma cargos em comissão e função de confiança. Disponível em: https://www.in.gov.br/en/web/dou/-/decreto-n-10.474-de-26-de-agosto-de-2020-274389226 Acesso em 15 ago. 2020

BRASIL. **Portaria 467/2020 do Ministério da Saúde**. Diário Oficial da União. 23 de março de 2020. Disponível em: https://www.in.gov.br/en/web/dou/-/portaria-n-467-de-13-de-agosto-de-2020-272047946 Acesso em 15 nov. 2020

BRASIL. **Portaria nº 2.546, de 27 de outubro de 2011**. Redefine e amplia o Programa Telessaúde Brasil, que passa a ser denominado Programa Nacional Telessaúde Brasil Redes (Telessaúde Brasil Redes). Disponível em: https://bvsms.saude.gov.br/bvs/saudelegis/gm/2011/prt2546_27_10_2011.html Acesso em 24 out. 2020

BRASIL. **Portaria nº 2.554, de 28 de outubro de 2011**. Institui, no Programa de Requalificação de Unidades Básicas de Saúde, o Componente de Informatização e Telessaúde Brasil Redes na Atenção Básica, integrado ao Programa Nacional Telessaúde Brasil Redes. Disponível em: http://bvsms.saude.gov.br/bvs/saudelegis/gm/2011/prt2554_28_10_2011.html Acesso em 24 out. 2020

BRASIL. Senado Federal. **Proposta de Emenda à Constituição 17/2019**. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/135594 Acesso 10 ago. 2020

BRASIL.SUPREMO TRIBUNAL FEDERAL**. Suspensa norma que restringe acesso à informação públicas**. Min. Alexandre de Moraes, 26 de março de 2020. Disponível em: http://www.stf.jus.br/portal/cms/verNoticiaDetalhe.asp?idConteudo=440207#:~:text=O%20ministro%20Alexandre%20de%20Moraes,por%20%C3%B3rg%C3%A3os%20p%C3%BAblicos%20durante%20a Acesso em 26 ago. 2020.

BRASIL. SUPREMO TRIBUNAL FEDERAL. **MEDIDA CAUTELAR NA AÇÃO DIRETA DE INCONSTITUCIONALIDADE 6.387 DISTRITO FEDERAL**. Relatora: Min. Rosa Webber, 24 de abril de 2020. Disponível em http://www.stf.jus.br/arquivo/cms/noticiaNoticiaStf/anexo/ADI6357MC.pdf Acesso 15 ago. 2020

BULOS, Uadi Lammêgo. **Curso de direito constitucional** I .8. cd. rcv. e atrn.11. de acordo com a Emenda Constitucional n. 76/2013 - Seio Paulo: Saraiva, 2014.

CABRAL, Felipe Fonteles. **O Relatório de Impacto à Proteção de Dados Pessoais como um instrumento para o gerenciamento de riscos na Lei Geral de Proteção a Dados Pessoais – Lei n.o 13.709/18. 2019**. 152 p. Dissertação (Mestrado). Universidade do Estado do Rio de Janeiro. 2019. Disponível em: https://sucupira.capes.gov.br/sucupira/public/consultas/coleta/trabalhoConclusao/viewTrabalhoConclusao.jsf?popup=true&id_trabalho=7679364 Acesso 05 set. 2020

CALLE, Guillermo Antonio Dávila; SILVA, EL da. Inovação no contexto da sociedade do conhecimento. **Revista TEXTOS de la CiberSociedad**, v. 8, p. 1-20, 2008. Disponível em: http://www.ngs.ufsc.br/wp-content/uploads/2010/05/DAVILA-CALLE_SILVA_2008.pdf Acesso em: 12 set. 2019

CANCELIER, Mikhail Vieira de Lorenzi. O Direito à Privacidade hoje: perspectiva histórica e o cenário brasileiro. Universidade Federal de Santa Catarina, Florianópolis – SC, Brasil. **Revista Sequência (Florianópolis),** n. 76, p. 213-240, ago. 2017. Disponível em: Acesso em: 05 jun. 2020

CASTELLS, Manuel. **A Sociedade em rede**. São Paulo: Paz e Terra. 2009.

CERIONI, CLARA. Com a ANPD só no papel, como fica a aplicação da LGPD no Brasil?.Lei que altera a proteção dos dados de todos os brasileiros entrou em vigor sem que houvesse orientação da Autoridade. **JOTA**. 2020. Disponível em: https://www.jota.info/justica/anpd-aplicacao-lgpd-brasil-24092020 Acesso em 20 ago. 2020

CETIC.BR. Pesquisa sobre o uso das tecnologias de informação e comunicação nos estabelecimentos de saúde brasileiros: **TIC Saúde 2019 [livro eletrônico**]. Núcleo de Informação e Coordenação do Ponto BR. 1. ed. São Paulo: Comitê Gestor da Internet no Brasil, 2020. Disponível em: https://cetic.br/media/docs/publicacoes/2/20201123084414/tic_saude_2019_livro_eletronico.pdf Acesso em 24 out. 2020

CETIC.BR. Usuários de Internet que realizaram consulta médica ou com outro profissional de saúde pela internet, por rede de atendimento. Pesquisa sobre o uso da Internet no Brasil durante a pandemia do novo coronavírus. **Painel TIC COVID-19**. 2020. Disponível em: https://cetic.br/pt/tics/tic-covid-19/painel-covid-19/2-edicao/S2W/ Acesso em 24 out. 2020

CHAGAS, Claudia Maria de Freitas. **Acesso à informação e intimidade: um dilema do Estado Democrático de Direito**. 2016. 141 f. Dissertação (Mestrado em Direito) - Universidade de Brasília, Brasília, 2016. Disponível em : https://repositorio.unb.br/handle/10482/20745 Acesso em: 01 nov.2019.

CLÈVE, Clèmerson Merlin; FRANZONI, Julia Ávila. Administração Pública e a nova Lei de Acesso à Informação. **Interesse Público — IP**, Belo Horizonte, ano 15, n. 79, maio/jun. 2013. Disponível em: https://www.editoraforum.com.br/wp-content/uploads/2013/10/Direito-Publico-Administracao-Publica-e-a-nova-Lei-de-Acesso-a-Informacao.pdf Acesso em 07 set. 2020

CONSELHO FEDERAL DE ENFERMAGEM. O Conselho Federal de Enfermagem atualizou nº225/2000 e nº 281/2003, sobre o cumprimento da prescrição medicamentos/terapêutica à distância e sobre a repetição/cumprimento da prescrição medicamentosa por profissional da saúde. **Resolução nº 0487/2015.** Disponível em http://www.cofen.gov.br/resolucao-cofen-no-4872015_33939.html Acesso em 24 ago. 2019

CONSELHO FEDERAL DE FONOAUDIOLOGIA. Dispõe sobre a regulamentação da telessaúde em fonoaudiologia e dá outras providencias**. Resolução CFF a Nº 427 DE 01/03/2013.** Disponível em: https://www.legisweb.com.br/legislacao/?id=251914. Acesso em 24 de ago. 2019

CONSELHO FEDERAL DE MEDICINA. **Cartilha sobre prontuário eletrônico: a certificação de sistemas de registro eletrônico de saúde**¸ fev. 2012. Disponível em: https://portal.cfm.org.br/crmdigital/Cartilha_SBIS_CFM_Prontuario_Eletronico_fev_2012.pdf Acesso em: 18 de out. 2020

CONSELHO FEDERAL DE MEDICINA**. Código de Ética Médica. Resolução CFM n° 2.217, de 27 de setembro de 2018, modificada pelas Resoluções CFM nº 2.222/2018 e 2.226/2019**. Brasília: Conselho Federal de Medicina, 2019. Disponível em : https://portal.cfm.org.br/images/PDF/cem2019.pdf Acesso em: 24 de ago. 2019

CONSELHO FEDERAL DE MEDICINA. **Conselheiros do CFM Revogam a Resolução n º 2.227/2018, que trata da telemedicina.2019**. Disponível em https://portal.cfm.org.br/index.php?option=com_content&view=article&id=28096:2019-02-22-15-13-20&catid=3 Acesso em 24 ago. 2019

CONSELHO FEDERAL DE MEDICINA. Define e disciplina a telemedicina como forma de prestação de serviços médicos mediados por tecnologias. **RESOLUÇÃO CFM Nº 2.227/2018. 2018**. Disponível em : < https://sistemas.cfm.org.br/normas/visualizar/resolucoes/BR/2018/2227> Acesso em 18 abr. 2019.

CONSELHO FEDERAL DE MEDICINA. **Ofício CFM nº 1.756/2020- COJUR**. Disponível em: https://portal.cfm.org.br/images/PDF/2020_oficio_telemedicina.pdf Acesso 12 nov. 2020

CONSELHO FEDERAL DE MEDICINA. **Resolução CFM nº 1.643/2002**. Diário Oficial da União. 26 de agosto 2002. Disponível em: https://sistemas.cfm.org.br/normas/visualizar/resolucoes/BR/2002/1643 Acesso em 25 out. 2020

CONSELHO FEDERAL DE MEDICINA. Uso do Whatsapp em ambiente hospitalar. PROCESSO- **CONSULTA CFM nº 50/2016- PARECER CFM nº 14/2017**. Disponível em : https://sistemas.cfm.org.br/normas/visualizar/pareceres/BR/2017/14 24 de ago. 2019

CONSELHO FERAL DE PSICOLOGIA. Regulamenta os serviços psicológicos realizados por meios tecnológicos de comunicação a distância, o atendimento psicoterapêutico em caráter experimental e revoga a Resolução CFP N.º 12/2005. **RESOLUÇÃO CFP N° 011/ 2012**. Disponível em: https://site.cfp.org.br/wp-content/uploads/2012/07/Resoluxo_CFP_nx_011-12.pdf Acesso em 24 ago. 2019.

COUTINHO, Clara Pereira; LISBÔA, Eliana Santana. Sociedade da informação, do conhecimento e da aprendizagem: desafios para educação no século XXI. **Revista de Educação**, v. 18, n. 1, p. 5-22, 2011. Disponível em: https://repositorium.sdum.uminho.pt/bitstream/1822/14854/1/Revista_Educa%C3%A7%C3%A3o%2cVolXVIII%2cn%C2%BA1_5-22.pdf Acesso em 15 abr. 2019

DANTAS, Eduardo; NOGAROLI, Rafaella. O Consentimento Informado do Paciente Frente às novas tecnologias da saúde: telemedicina, cirurgia robótica e inteligência artificial. **Revista de Direito médico e da saúde: doutrina, legislação, jurisprudência**. Brasília: VEM MAIS EDITORAÇÃO, n. 21. jul. 2020. 164p.:

DE NEGRI, Fernanda. As tecnologias da informação podem revolucionar o cuidado com a saúde? **Instituto de Pesquisa Economica Aplicada (Ipea**). 2018. Disponível em: http://repositorio.ipea.gov.br/handle/11058/8614 Acesso em 29 nov. 20020

DE MORAES, Melina Ferracini. Inovação Tecnológica como Instrumento para o Desenvolvimento no Brasil. **Revista de Direito, Inovação, Propriedade Intelectual e Concorrência**, v. 2, n. 1, p. 77-93, 2016.

DE MORAES, Maria Celina Bodin. Ampliando os direitos de personalidade. **Revista de Saúde Pública**, v. 41, n.5, 2007. Disponível em: https://www.researchgate.net/publication/288490662_Ampliando_os_direitos_da_personalidade Acesso em 27 nov. 2020

DI FIORE, Bruno Henrique. **Teoria dos Círculos Concêntricos da Vida Privada e suas Repercussões na Praxe Jurídica**. Disponível em

http://www.flaviotartuce.adv.br/index2.php?sec=artigosc&totalPage=2 Acesso em 30 maio 2020

DONEDA, Danilo. A proteção de dados pessoais nas relações de consumo: para além da informação creditícia. **Escola Nacional de Defesa do Consumidor**; Brasília: SDE/DPDC, 2010, p. 26.

DONEDA, Danilo. **A proteção dos dados pessoais como um direito fundamental**. Espaço Jurídico. Joaçaba, v. 12, n. 2, p. 91-108, jul./dez. 2011

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais.** Rio de Janeiro: Renovar, 2006. 448 p.

DONEDA, Danilo. **O papel das autoridades independentes na proteção de dados pessoais** (Capítulo 4 - Ponto 4.3). In: Da privacidade à proteção de dados pessoais. 2ed. São Paulo: Thomson Reuters Brasil, 2019. p.307 - 323.

DONEDA, Danilo; MONTEIRO, Marilia de Aguiar. **Proteção de dados pessoais enquanto direito fundamental e o direito fundamental à saúde** – privacidade e e-Health. In: KEINERT, Tania Margarete Mezzomo et al (Org.). Proteção à privacidade e acesso às informações em saúde: tecnologias, direitos e ética. São Paulo: Instituto de Saúde, 2015.

FAVARO, Iasmine; ZANATTA, Rafael. **App Coronavirus SUS: dá pra confiar**? Data Privacy BR. ago. 2020. Disponível em https://observatorioprivacidade.com.br/2020/08/28/app-coronavirus-sus-da-pra-confiar/. Acesso 06 nov. 2020

FLORÊS, Mariana Rocha de; SILVA, Rosane Leal. Desafios e perspectivas da proteção de dados pessoais sensíveis em poder da administração pública: entre o dever público de informar e o direito do cidadão de ser tutelado. **Revista de direito**. Viçosa.v. 12. N. 02. 2020 Disponível em: https://periodicos.ufv.br/revistadir/article/view/10327/5807 Acesso em 16 nov. 2020

FERNÁNDEZ, Andrés; CARRASCO, Ignacio. Modelo conceitual para avaliar impactos de investimentos em saúde digital. In: BARBOSA, Alexandre F. (Org.). **TIC SAÚDE 2015** - pesquisa sobre o uso das tecnologias de informação e comunicação nos estabelecimentos de saúde brasileiros. 2. ed. rev. São Paulo: Comitê Gestor da Internet no Brasil, 2016, p. 39

FERRAZ JUNIOR, Tércio Sampaio. Sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do Estado. **Revista da Faculdade de Direito**, Universidade de São Paulo, v. 88, p. 439-459, 1993

FRAZÃO, Ana. **Fundamentos da proteção dos dados pessoais. Noções introdutórias para a compreensão da importância da Lei Geral de Proteção de Dados**. In: TEPEDINO, Gustavo. FRAZÃO, Ana. OLIVA, Milena Donato (Orgs). Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro. Thomson Reuters, Revista dos Tribunais, 2019, p. 80-85

GARCIA, Rebeca. Marco Civil da Internet no Brasil: Repercussões e Perspectivas. Revista dos Tribunais. vol. 964. São Paulo: Ed. RT, 2016.

GARRIDO, Elena Pacita Lois. Lei de Acesso às informações públicas. **Revista Jurídica CNM**. Brasília: CNM. 2012. 160 p.

GEDIEL, José Antônio Peres; CORRÊA, Adriana Espíndola. PROTEÇÃO JURÍDICA DE DADOS PESSOAIS: A INTIMIDADE SITIADA ENTRE O ESTADO E O MERCADO. **Revista da Faculdade de Direito**- UFPR, Curitiba, n.47, p. 141-153, 2008.

GONÇALVES, Victor Hugo Pereira. **Marco civil da internet comentado**. 1. ed. São Paulo: Atlas, 2017

GOULART, Guilherme Damásio. **Segurança da informação e a proteção contra a violação de dados pessoais: a confidencialidade no direito do consumidor**. Dissertação.2012. Disponível em: https://www.lume.ufrgs.br/handle/10183/194427 Acesso em 25 de out. 2019

HARZHEIM, Erno; SIQUEIRA, Ana Célia da Silva. **Telemedicina como motor da coordenação assistencial: muito além da tecnologia**. In: BARBOSA, Alexandre F. (Org.). TIC SAÚDE 2013 - pesquisa sobre o uso das tecnologias de informação e comunicação nos estabelecimentos de saúde brasileiros. 2. ed. rev. São Paulo: Comitê Gestor da Internet no Brasil, 2015, p. 33-46.

HIDALGO, Julio Villalobos; CARRION, Carme et al. Saúde digital: a necessária reengenharia da atenção em saúde. In: BARBOSA, Alexandre F. (Org.). **TIC SAÚDE 2015** - pesquisa sobre o uso das tecnologias de informação e comunicação nos estabelecimentos de saúde brasileiros. 2. ed. rev. São Paulo: Comitê Gestor da Internet no Brasil, 2016, p. 32

INSTITUTO DE TECNOLOGIA E SOCIEDADE. **Lei Geral de Proteção de Dados no Setor Público: Um guia da lei 13.709/2018, voltado para os órgãos e entidades públicas**. 2019. Disponível em: https://itsrio.org/wp-content/uploads/2019/05/LGPD-vf-1.pdf Acesso em 07 ago. 2020

JUNIOR, José Luiz de Moura Faleiros; NAGAROLI, Rafaella et al. TELEMEDICINA E PROTEÇÃO DE DADOS: REFLEXÕES SOBRE A PANDEMIA DA COVID-19 E OS IMPACTOS JURÍDICOS DA TECNOLOGIA APLICADA Á SAUDE. **Revista dos Tribunais.** Vol. 1016/2020. Jun. 2020

KAMEDA, Koichi; PAZELLO, Magaly. **E-saúde e desafios à proteção da privacidade no Brasil**. In: KEINERT, Tania Margarete Mezzomo et al (Org.). Proteção à privacidade e acesso às informações em saúde: tecnologias, direitos e ética. São Paulo: Instituto de Saúde, 2015.

LÉVY, Pierre. **Cibercultura**. São Paulo. Ed. 34. 1999.

LIMA, Manuela Ithamar. Do direito à proteção de dados em matéria de saúde na sociedade da informação. **Arquivo Jurídico**. Teresina-PI. v. 4 .n. 1 p. 1-24. Jan./Jul. de 2017. Disponível em https://www.ojs.ufpi.br/index.php/raj/article/view/7416/4303 Acesso em 16 nov. 2020

LIMA, Marco Antonio; BARRETO JUNIOR, Irineu Francisco. Marco civil da internet: limites da previsão legal de consentimento expresso e inequívoco como proteção jurídica dos dados pessoais na internet. **Revista de Direito, Governança e Novas Tecnologias**. Brasília,

vol. 1, n. 2, p. 241-260, jan/jun. 2016. Disponível em: https://indexlaw.org/index.php/revistadgnt/article/view/831 Acesso em 05 maio 2020.

MACHADO, Joana de Moraes Souza. **CAMINHOS PARA A TUTELA DA PRIVACIDADE NA SOCIEDADE DA INFORMAÇÃO: a proteção da pessoa em face da coleta e tratamento de dados pessoais por agentes privados no Brasil**. 2014. 186 p. Tese (Doutorado)- Fundação Edson de Queiroz, Universidade de Fortaleza, Centro de Ciencias Jurídicas, Programa de Pós-Graduação em direito constitucional, 2014. Disponível em: https://uol.unifor.br/oul/conteudosite/F86027120141111150021922278/Tese.pdf Acesso 10 jun. 2020

MAGALHÃES, Felipa Matias; PEREIRA, Maria Leitão. Regulamento Geral de Proteção de Dados. **Manual Prático. VidaEcononomia, Porto, PT**, 2018

MALDONADO, Jose Manuel Santos de Varge; MARQUES, Alexandre Barbosa et al. Telemedicina: desafios à sua difusão no Brasil. **Cadernos de Saúde Pública**, Rio de Janeiro, v. 32,p. 1-12, 2016 Disponível em: https://www.scielosp.org/article/ssm/content/raw/?resource_ssm_path=/media/assets/csp/v32s2/pt_1678-4464-csp-32-s2-e00155615.pdf Acesso em 26 out. 2020

MANSUR, Monica Tereza; ANDRADE, Ronaldo Alves de. Verdade, mentira e imprensa na sociedade da informação. **O direito na sociedade da Informação III**. Liliana Minardi Paesani (coordenadora), São Paulo: Atlas, 2013.

MARIN, Heimar de Fátima; FERREIRA, Cesar Biselli. INOVAÇÃO EM TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO EM SAÚDE. In: Núcleo de Informação e Coordenação do Ponto BR (Org.). **TIC SAÚDE 2016** - Núcleo de Informação e Coordenação do Ponto BR [editor] – São Paulo: Comitê Gestor da Internet no Brasil, 2017. 3.700 Kb; PDF

MARTINS, Leonardo**. Indrodução á jurisprudencia do Tribunal Constitucional Federal Alemão. Cinquenta anos de jurisprudencia do Tribunal Constitucional Federal Alemão**. Organização e Indrodução: Leonardo Martins. Préfacio: Jan Woischnik. Trad. Beatriz Henning et al. Mentevidéu: Fundação Konrand Adenauer, 2005, p. 223-234.

MASI, Domenico de. **A sociedade pós-indutrial**. 4.ed. São Paulo. Ed: Senasc São Paulo, 2003.

MATOS, Tiago Farina. Comércio de dados pessoais, privacidade e Internet. **Revista de Doutrina da 4ª Região**, v. 18, n. 7, 2005.

MENDES, Gilmar Ferreira; BRANCO, Paulo Gustavo Gonet. Curso de direito constitucional .12. ed. rev. e atual. – São Paulo: Saraiva, 2017.

MENDES, José Manuel. **Ulrich Beck: a imanência do social e a sociedade do risco**. Análise Social, n. 214, p. 211-215, 2015.

MENDES, Laura Schertel. Privacidade e dados pessoais. Proteção de dados pessoais: fundamento, conceitos, e modelo de aplicação. **Panorama Setorial da Internet**. nº 2. Junho, 2019, Ano 11. Disponível em https://nic.br/media/docs/publicacoes/6/15122520190717-panorama_setorial_ano-xi_n_2_privacidade_e_dados_pessoais.pdf Acesso em 05 set. 2020

MENDES, Laura Schertel; MARTTIUZZO, Marcela. **Discriminação Algorítmica: Conceito, Fundamento Legal e Tipologia. Proteção de Dados e Inteligência Artificial: Perspectivas Éticas e Regulatórias**. RDU, Porto Alegre, Volume 16, n. 90, 2019, 39-64, nov-dez 2019

MENDES, Laura Schetel. A lei geral de proteção de dados pessoais: um modelo de aplicação em três níveis. In: **A LEI GERAL DE PROTEÇÃO DE DADOS**. Revista dos Tribunais: Edição Especial LGPD 2019. p. 35-56

MENDES, Laura Schertel. **Transparência e privacidade: violação e proteção da informação pessoal na sociedade de consumo**. 2008. 156 f. Dissertação (Mestrado em Direito) -Universidade de Brasília, Brasília, 2008. Disponível em https://repositorio.unb.br/handle/10482/4782. Acesso em 19 fev. 2020

MENDES, LAURA SCHERTEL. Decisão histórica do STF reconhece direito fundamental à proteção de dados pessoais. **JOTA**. 2020. Disponível em https://www.jota.info/opiniao-e-analise/artigos/decisao-historica-do-stf-reconhece-direito-fundamental-a-protecao-de-dados-pessoais-10052020 Acesso 15 ago. 2020

MENDES, Laura Schertel; BIONI, Bruno R. O Regulamento Europeu de Proteção de Dados Pessoais e a Lei Geral de Proteção de Dados Brasileira: mapeando convergências na direção de um nível de equivalência. **Revista de Direito do Consumidor**. vol. 124. ano 28. p. 157-180. São Paulo: Ed. RT, jul.-ago. 2019.

MENDOZA, Melanie Claire Fonseca; BRANDÃO, Luiz Mathias Rocha. Do direito à privacidade à proteção de dados: Das Teorias de Suporte e a Exigência da Contextualização. **Revista de Direito, Governança e Novas tecnologias**, v.2, n.1, p. 1-22.2016. Disponível em : http://conpedi.danilolr.info/publicacoes/y0ii48h0/k778x2oo/l56YZ81vr6hQj17b.pdf Acesso em 01 jun. 2020

MENEZES, Joyceane Bezerra de; GOLAÇO, Hian Silva. **Quando a Lei Geral de Proteção de Dados não se aplica?.** In: TEPEDINO, Gustavo. FRAZÃO, Ana. OLIVA, Milena Donato (Orgs). Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro. Thomson Reuters, Revista dos Tribunais, 2019, p. 80-85.

MINISTÉRIO DA SAÚDE. **Estratégia e-saúde para Brasil. Ministério da Saúde. Comitê Gestor da Estratégia e-saúde.** Brasília. 2017. Disponível em https://portalarquivos.saude.gov.br/images/pdf/2017/julho/12/Estrategia-e-saude-para-o-Brasil.pdf Acesso em 11 nov. 2020

MINISTÉRIO DA SAÚDE. Manual de Telessaúde: para Atenção Básica/Atenção Primária à Saúde. Brasília: **Ministério da Saúde**, 2012. Disponível em: http://bvsms.saude.gov.br/bvs/publicacoes/manual_telessaude_atencao_basica.pdf Acesso em: 20 out. 2020

MINISTÉRIO DA SAÚDE. **O que é Prontuário Eletrônico do Cidadão**? 2017. Disponível em: http://aps.saude.gov.br/noticia/2300#:~:text=De%20forma%20direta%2C%20o%20Prontu%

C3%A1rio,de%20atendimento%20do%20cidad%C3%A3o%20realizado Acesso em 27 out. 2020

MINISTÉRIO DA SAÚDE. Política Nacional de Informação e Informática em Saúde. Brasília: **Ministério da Saúde**, 2016. Disponível em: http://bvsms.saude.gov.br/bvs/publicacoes/politica_nacional_infor_informatica_saude_2016.pdf Acesso em: 17 de out. 2020

MINISTERIO DE SAÚDE. **Postos de saúde do SUS terão consulta virtual**. Disponível em https://www.gov.br/saude/pt-br/assuntos/noticias/postos-de-saude-do-sus-terao-consulta-virtual Acesso em 16 nov. 2020

MINSTÉRIO DA SAÚDE. **Resposta Nacional e Interacional de Enfrentamento ao novo coronavírus.** Linha do Tempo. Fev. 2020. Disponível em: https://coronavirus.saude.gov.br/linha-do-tempo/ Acesso em 11 nov. 2020.

MORAES, Alexandre de. **Direito constitucional**. 34. ed. - São Paulo: Atlas, 2018.

MORAES, Ilara Hämmerli Sozzi de**. Prefácio**. In: KEINERT, Tania Margarete Mezzomo et al (Org.). Proteção à privacidade e acesso às informações em saúde: tecnologias, direitos e ética. São Paulo: Instituto de Saúde, 2015.

MOURA, Raíssa; FERRAZ, Lara. **Meios de Controle à Pandemia da COVID-19 e a Inviolabilidade da Privacidade**. Disponível em: https://content.inloco.com.br/hubfs/Estudos%20-%20Conte%C3%BAdo/Coronavirus/Meios%20de%20controle%20a%CC%80%20pandemia%20da%20COVID-19%20e%20a%20inviolabilidade%20da%20privacidade.pdf?hsCtaTracking=ad1577ba-e5bc-4ff3-afdd-54a896891088%7C07ab4d6b-53d3-4a06-9f43-fb43621df88f&hsLang=pt Acesso em 18 nov.. 2020.

MULHOLLAND, Caitlin Sampaio. Dados pessoais sensíveis e a tutela de Direitos Fundamentais: uma análise à luz da Lei Geral de Proteção de Dados (Lei 13.709/18). **Estado de Direito e Tecnologia,** edição temática, Vitória, FDV publicações, v. 19, set./dez. 2018.

NÚCLEO DE TELESSAÚDE. **Telessaúde Maranhão Huufma**. 2020. Disponível em: http://telessaude.huufma.br/ Acesso em 24 out. 2020

OEA. **Pacto de San Jose da Costa Rica**. Convenção Americana sobre Direitos Humanos. 22 de novembro de 1969. Disponível em: https://www.cidh.oas.org/basicos/portugues/c.convencao_americana.htm Acesso em 22 maio 2020

OLIVEIRA, Luís Fernando Costa Oliveira. **A interpretação do artigo 6° da lei n. 13.979/2020 – ofensa à autodeterminação informativa e ausência de accountability por parte da administração pública.** In: Os dados e o vírus: pandemia, proteção de dados e democracia [livro eletrônico]. São Paulo: Reticências Creative Design Studio, 2020. xxp; 21x29,7cm | 1 Mb ; PDF. Disponível em: https://www.dataprivacybr.org/wp-content/uploads/2020/09/eBook_selecoes_osdados_eo_virus.pdf Acesso em 19 nov. 2020

OLIVEIRA, Marco Aurélio Bellizze; LOPES, Isabela Maria Pereira. **Os princípios norteadores da proteção de dados no Brasil e sua otimização pela lei 13.709/2018**. In: TEPEDINO, Gustavo. FRAZÃO, Ana. OLIVA, Milena Donato (Orgs). Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro. Thomson Reuters, Revista dos Tribunais, 2019, p. 77.

OLIVEIRA, Maria Lívia Pacheco; SOUZA, Edivanio Duarte. A competência crítica em informação no contexto das fake news: os desafios do sujeito informacional no ciberespaço. In**: XIX ENCONTRO NACIONAL DE PESQUISA EM CIÊNCIA DA INFORMAÇÃO (XIX ENANCIB**). 2018. Disponível em: http://hdl.handle.net/20.500.11959/brapci/102566 Acesso 19 de fev. 2020

ORGANIZAÇÃO MUNDIAL DE SAÚDE. **A OMS Caracteriza COVID-19 como uma pandemia**. Disponível em: https://www.who.int/emergencies/diseases/novel-coronavirus-2019/events-as-they-happen Acesso em 11 nov. 2020

ONU. Declaração Universal dos Direitos do Homem. **Resolução n. 217 A (III)** da Assembleia Geral das Nações Unidas. 10 de dezembro de 1948. Disponível em: https://www.scielo.br/scielo.php?script=sci_arttext&pid=S0103-56652008000200015 Acesso em 10 jun. 2020

ONU. Pacto Internacional de Direitos Civis e Políticos. Adoptado e aberto à assinatura, ratificação e adesão pela **Resolução 2200-A (XXI)** da Assembleia Geral das Nações Unidas, de 16 de dezembro de 1966. Disponível em: < http://www.cne.pt/sites/default/files/dl/2_pacto_direitos_civis_politicos.pdf> Acesso em: 22 maio 2020.

PAESANI, Liliana Minardi. **Direito de informática: comercialização e desenvolvimento internacional do *software***. 6.ed. São Paulo: Atlas, 2017

PAESANI, Liliana Minardi; SIQUEIRA JR, Paulo Hamilton. **O direito na sociedade da Informação III**. São Paulo: Atlas, 2013.

PINHEIRO, Patrícia Beck**. Proteção de dados pessoais: comentários à lei n.13.709/2018 (LGPD)**. 2.ed. São Paulo: Saraiva Educação, 2020. 152 p.

POLIDO, Fabrício B. Pasquot et al. **GDPR e suas Repercussões no direito brasileiro:** Primeiras impressões de análise comparativa. Instituto de Referência em Internet e Sociedade. 2018.

PRODANOV, Cleber Cristiano; FREITAS, Ernani Cesar de. **Metodologia do trabalho científico [recurso eletrônico]**: métodos e técnicas da pesquisa e do trabalho acadêmico.2. ed. Novo Hamburgo: Feevale, 2013.

REZENDE, Edson José Carpintero et al. Telessaúde: confidencialidade e consentimento informado. **Revista Médica de Minas Gerais, Belo Horizonte**, v. 23.3, p. 367-373, jul./set. 2013. Disponivel em: http://www.rmmg.org/artigo/detalhes/223 Acesso em 11 nov. 2020

RIVABEM, Fernanda Schaefer. Telemática em saúde e sigilo profissional: A busca pelo equilíbrio entre privacidade interesse social. Tese (Doutorado)- Universidade Federal do

Paraná. Disponível em: https://acervodigital.ufpr.br/bitstream/handle/1884/23014/RIVABEM;jsessionid=7BB3AE26FC2999F0F98EF843EDA98FBC?sequence=1 Acesso em 16 nov. 2020

RODOTÁ, Stefano. **Democracia y protección de datos**. Cuadernos de Derecho Público, núms. 19-20 (mayo-diciciembre 2003).

RUARO, Regina Linden. Privacidade e autodeterminação informativa obstáculos ao estado de vigilância**? /** Privacy and informational self-determination obstacles to the vigilant state? (p.41)**. Revista Jurídica Eletrônica da UFPI,** v.2, n.01, 2015. Disponível em: https://revistas.ufpi.br/index.php/raj/article/view/4505 Acesso em 31 jun. 2020

RUARO, Regina Linden; RODRIGUES, Daniel Piñeiro. O direito à proteção de dados pessoais na sociedade de informação. **Revista Direito, Estado e Sociedade, Rio de Janeiro**, n. 36, p. 178-199, jan./jun. 2010.

SAMPAIO, José Ardércio Leite. Comentário ao artigo 5º, XI E XII. In: CANOTILHO, J.J. Gomes; MENDES, Gilmar F.; SARLET, Ingo W.; STRECK, Lenio L. (Coords.). **Comentários à Constituição do Brasil**. 2.ed. São Paulo: Saraiva Educação,2018, p. 558

SANSON, Cesar. Trabalho e Subjetividade: da sociedade industrial à sociedade pós-industrial. **Cadernos IHU**, p. 1-63, 2009.
SANTOS, Mario Filipe Cavalcanti de Souza. LGPDP: O INÍCIO DA VIGÊNCIA DO QUE JÁ VIGIA. Disponível em https://www.conjur.com.br/dl/artigo-mario-cavalcanti.pdf Acesso 16 ago. 2020

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.** Civilistica.com. Rio de Janeiro, a. 8, n. 1, 2019. Disponível em: https://run.unl.pt/bitstream/10362/94969/1/O_consentimento_informado_e_a_prote_o_de_dados_.pdf Acesso em: 09 nov. 2020

SARLET, Ingo Wolfgang. **Direitos Fundamentais em Espécie**. In: SARLET, Ingo Wolfgang; MARINONI, Luiz Guilherme; MITIDIERO, Daniel. Curso de Direito Constitucional. 5. ed. rev. e atual. São Paulo: Saraiva,2018, p. 400-735.

SARLET, Ingo Wolfgang; MOLINARO, Carlos Alberto. O direito à informação na ordem constitucional brasileira: breves apontamentos. In: **Acesso à informação como direito fundamental e dever estatal**. Livraria do Advogado, 2016. p.11-26.

SARLET, Ingo Wolfgang. Comentário ao artigo 5º, §2º In: CANOTILHO, J.J. Gomes; MENDES, Gilmar F.; SARLET, Ingo W.; STRECK, Lenio L. (Coords.). **Comentários à Constituição do Brasil**. 2.ed. São Paulo: Saraiva Educação,2018, p. 1014

SARLET, Ingo Wolfgang; KEINERT, Tania Margarete Mezzomo. **O direito fundamental à privacidade e as informações em saúde: alguns desafios**. In: KEINERT, Tania Margarete Mezzomo et al (Org.). Proteção à privacidade e acesso às informações em saúde: tecnologias, direitos e ética. São Paulo: Instituto de Saúde, 2015.

SCHREIBER, Anderson. **Direitos da personalidade.** 2. ed. São Paulo: Atlas, 2013.

SILVA, De Plácido e. **Vocabulário Jurídico**. 31. ed. – Rio de Janeiro: Forense, 2014.

SILVA, Tiago Vinícius Soares. **O tratamento de dados pessoais sensíveis nas empresas do setor de saúde, segundo a lei geral de proteção de dados (LGPD).** Dissertação (Mestrado). Universidade do Vale do Rio SINOS- UNISINOS. Programa de Pós- graduação em direito. 2020. p. 130. Disponível em: http://repositorio.jesuita.org.br/bitstream/handle/UNISINOS/9364/Tiago%20Vin%c3%adcius%20Soares%20Silva_.pdf?sequence=1&isAllowed=y Acesso em 19 nov. 2020

SIMÕES, Silva Magalhaes; OLIVEIRA, Adicinéia et al. Telemedicina na Covid-19. Revista Interdisciplinar de Pesquisa e Inovação, v. 7, n.2, p. 104-109. 2020 Disponível em: https://www.revista.ufs.br/index.php/revipi/article/view/14220 Acesso em 01 nov. 2020
SOUZA, Carlos Affonso; LEMOS, Ronaldo. **Marco civil da internet: construção e aplicação**. Juiz de Fora: Editar Editora Associada Ltda, 2016.

TOMASEVICIUS FILHO, Eduardo. **Marco Civil da Internet: uma lei sem conteúdo normativo**. Estudos Avançados, v. 30, n. 86, p. 269-285, 2016.

UNIÃO EUROPÉIA. Directiva 2002/58/CE do Parlamento Europeu e do Conselho da Europa, de 12 de julho de 2002, relativa ao tratamento de dados pessoais e à proteção da privacidade no sector das comunicações electrónicas (Directiva relativa à privacidade e ás comunicações electrónicas). **Jornal Oficial das Comunidades Europeias**. Portugal, 31 jul. 2002. Nº L 201, pp. 37-47. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32002L0058 Acesso em 10 ago. 2020.

UNIÃO EUROPÉIA. DIRECTIVA 95/46 CE do Parlamento Europeu e do Conselho da Europa, 24 de outubro de 1995. Relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. **Jornal Oficial das Comunidades Europeias**. Portugal, 23 de nov. 1995. nº L 281, pp. 31-50

VENOSA, Sílvio de Salvo **Direito civil: parte geral**.17. ed. São Paulo: Atlas, 2017

VIEIRA, Augusto Cesar Gadelha. O projeto cartão nacional de saúde e a construção de esaúde para o Brasil. In: BARBOSA, Alexandre F. (Org.). **TIC SAÚDE 2013** - pesquisa sobre o uso das tecnologias de informação e comunicação nos estabelecimentos de saúde brasileiros. 2. ed. rev. São Paulo: Comitê Gestor da Internet no Brasil, 2015, p. 33-46

VIEIRA, Tatiana Malta. **O direito à privacidade na sociedade da informação: efetividade desse direito fundamental diante dos avanços da tecnologia da informação**. 2007. 297 f. Dissertação (Mestrado em Direito) - Universidade de Brasília, Brasília, 2007. Disponível em: http://repositorio.unb.br/handle/10482/3358 Acesso em: 16 fev.2019.

WINCK, Fernando Pritsch. **Direitos fundamentais na sociedade da informação**. In: Luiz Gonzaga Silva Adolfo (Org.). Florianópolis: UFSC/GEDAI, 2012. 228p. Disponível em: https://biblioteca.unilasalle.edu.br/docs_online/livros/direitos_fundamentais_sociedade_informacao.pdf Acesso em 17 abr. 2019.