UNIVERSIDADE FEDERAL DE SANTA CATARINA
CENTRO DE CIÊNCIAS JURÍDICAS
PROGRAMA DE PÓS-GRADUAÇÃO EM DIREITO

Camila Kohn de Cristo

Proteção da Privacidade e dados relativos pessoais à saúde após aprovação Lei n. 13.853/2019.

Florianópolis
2021

Camila Kohn de Cristo

Proteção da Privacidade e dados relativos pessoais à saúde após aprovação Lei n. 13.853/2019.

Dissertação submetida ao Programa de Pós-Graduação em Direito da Universidade Federal de Santa Catarina para a obtenção do título de Mestre em Direito.
Orientador: Prof. Mikhail Cancelier

Florianópolis
2021

Ficha de identificação da obra elaborada pelo autor, através do Programa de Geração Automática da Biblioteca Universitária da UFSC

Cristo, Camila
Proteção da Privacidade e dados relativos pessoais à saúde após aprovação Lei n. 13.853/2019 / Camila Cristo ; orientador, Mikhail Cancelier, 2021.
210 p.

Dissertação (mestrado) - Universidade Federal de Santa Catarina, Centro de Ciências Jurídicas, Programa de Pós Graduação em Direito, Florianópolis, 2021.

Inclui referências.

1. Direito. 2. Sociedade da informação. 3. Privacidade. 4. Dados pessoais saúde. 5. Economia de dados. I. Cancelier, Mikhail . II. Universidade Federal de Santa Catarina. Programa de Pós-Graduação em Direito. III. Título.

Camila Kohn de Cristo

Privacidade e dados pessoais de saúde: uma discussão sobre a proteção à privacidade dos dados de saúde após a aprovação da Lei nº 13.853/ 2019

O presente trabalho em nível de mestrado foi avaliado e aprovado por banca examinadora composta pelos seguintes membros:

Profa. Fernanda Schaefer, Dra.
Pontifícia Universidade Católica do Paraná

Profa. Salete Oro Boff, Dra.
Universidade Federal da Fronteira Sul

Profa. Liz Beatriz Sass, Dra.
Universidade Federal de Santa Catarina

Certificamos que esta é a **versão original e final** do trabalho de conclusão que foi julgado adequado para obtenção do título de mestre em Direito pelo Programa de Pós-Graduação em Direito da Universidade Federal de Santa Catarina – PPGD/UFSC.

Documento assinado digitalmente
Norma Sueli Padilha
Data: 09/12/2021 08:25:22-0300
CPF: 050.840.658-71
Verifique as assinaturas em https://v.ufsc.br

Coordenação do Programa de Pós-Graduação

Documento assinado digitalmente
Clarindo Epaminondas de Sa Neto
Data: 02/12/2021 06:41:35-0300
CPF: 006.861.805-00
Verifique as assinaturas em https://v.ufsc.br

Prof. Clarindo Epaminondas de Sá Neto
Presidente da Banca

Florianópolis, 2021

AGRADECIMENTOS

A Universidade Federal de Santa Catarina tem um papel fundamental neste trabalho. Os debates acadêmicos e a intensidade das aulas contribuíram no meu modo de olhar o processo de regulação da privacidade, bem como perceber, de modo crítico, como as mudanças tecnológicas influenciavam em todo o arcabouço social. Agradeço aos meus professores da Universidade Federal de Santa Catarina. Ao CNPq pelo financiamento, o que possibilitou me dedicar à pesquisa e à realização deste trabalho. Aos colegas de estágio da Sinova/UFSC, em especial à Marlise, Paola e Alexandre, e aos servidores da Secretaria do PPGD/UFSC, que sempre ajudaram com o possível em momentos tão atípicos, em especial à Cida. Não posso deixar de mencionar a ajuda e disponibilidade de Jessé nos ajustes deste trabalho.

No entanto, tenho consciência de que nada disso seria possível se não houvesse uma base forte que me sustentou nos dias mais difíceis. À minha família, mas principalmente: meus avós (Roleia e Dorival), mãe (Beatriz), pai (Cristo), madrinha (Denise) e padrinho (Márcio). Sem o incentivo de vocês e a confiança depositada, esta caminhada não teria se concretizado. Minha eterna gratidão. Aos meus melhores amigos, Amanda Batista, Gabriela Mafra, Gabriela Alves, Leonardo Rodrigues, Nicole Silva, Mateus Costa, que nunca soltaram a minha mão, e sempre se colocaram dispostos a ajudar. À minha irmã, Bruna, pela calma e paciência. Ao companheiro da minha vida, Fabio, que tem me apoiado incondicionalmente e por quem tenho uma gigantesca admiração e amor. Estar junto a ti me motiva a ser sempre melhor. Vocês são a razão e força que me levaram até aqui, vocês são minha essência. Essa dissertação é totalmente dedicada a vocês.

“Para todos que tiveram um momento de fraqueza. Não vai doer para sempre, então não deixe isso afetar o que há de melhor em você” (J. A. Redmerski).

RESUMO

O presente trabalho tem como tema privacidade e dados sensíveis de saúde, visando responder ao seguinte problema: A alteração aprovada pelo Congresso Nacional no §4º do art. 11 da LGPD pela Lei 13.853/19 pode ocasionar a violação da privacidade e dos dados relativos à saúde do titular dos dados pessoais tendo em conta a letra original do referido diploma legislativo? A hipótese inicial da pesquisa é que a alteração da redação original do texto da LGPD para permitir o tratamento nas hipóteses relativas à prestação de serviços de saúde, de assistência farmacêutica e de assistência à saúde, incluídos os serviços auxiliares de diagnóstico e terapia, hipóteses que, numa análise preliminar mostram-se muito abertas, possibilitou um universo de interpretações que abarcam inúmeras atividades, que podem violar a privacidade e os dados pessoais da pessoa interessada. O objetivo desta pesquisa é justamente verificar se a alteração do art. 11, §4º pode representar uma violação à privacidade e aos dados relativos à saúde do titular dos dados pessoais. A pesquisa foi estruturada em três capítulos, os quais dizem respeito aos seguintes objetivos específicos: a) contextualizar a Sociedade da Informação, para compreender a Privacidade dentro deste contexto. Apresentar a privacidade; sua origem e seu conceito atual; b) apresentar o conceito de dados pessoais e analisa-los a partir do conceito de economia da informação; e, c) verificar se a alteração legislativa do art. 11, §4º pode representar uma violação à privacidade e à proteção de dados sensíveis de saúde. Para executar o presente trabalho utilizaremos o método de abordagem dedutivo e o método de procedimento monográfico. A técnica de pesquisa será bibliográfica e documental. No primeiro capítulo verificamos que a privacidade protege informações que não gostaríamos de ver caírem no domínio público, é tudo aquilo que não deve ser objeto de informação ou curiosidade da sociedade moderna. A privacidade não se confunde com a proteção de dados que está relacionada com controle informacional. No segundo capítulo buscou-se apresentar o conceito de proteção de dados pessoais e analisa-lo a partir do conceito de economia da informação. Verificou-se que dados pessoais podem ser divididos em diferentes espécies, possuindo uma categoria especial, os dados sensíveis. A criação dessa categoria autônoma de dados pessoais está intimamente ligada aos riscos que o tratamento de certas informações pessoais poderiam causar à personalidade da pessoa humana. Dente os dados sensíveis existe uma subcategoria, os dados de saúde. Para melhor compreender a proteção de dados pessoais, buscamos contextualizar a economia da informação, que possui como matéria-prima as informações. Foi possível concluir o valor dos dados de saúde está relacionado ao grau de sensibilidade. Por fim, o terceiro capítulo tinha como objetivo verificar se a alteração legislativa pode representar uma violação à privacidade e à proteção de dados. Para isso foi analisado a proteção legislativa da privacidade e da proteção de dados pessoais no ordenamento jurídico brasileiro. Como conclusão, o objetivo geral deste trabalho foi atingido e a hipótese foi verificada, uma vez que foi possível constatar que a alteração no art. 11, § 4º, pela Lei n. 13.853/2019, cedeu às pressões do mercado e passou a permitir tratamento de dados de saúde com objetivo de obter vantagem econômica, exceto nas hipóteses relativas à prestação de serviços de saúde, de assistência farmacêutica e de assistência à saúde. A mudança causou sérios riscos à proteção da privacidade dos titulares dos dados de saúde, pois permiti tratamentos de dados de saúde com objetivo de obter vantagem econômica para, praticamente, qualquer atividade.

Palavras-chave: Sociedade da informação. Privacidade. Dados pessoais sensíveis. Dados pessoais de saúde. Economia de dados.

ABSTRACT

The present work has as its theme privacy and sensitive health data, aiming to respond to the following problem: The amendment approved by the National Congress in §4 of art. 11 of the LGPD by Law 13.853/19 can cause the violation of privacy and data relating to the health of the holder of personal data, taking into account the original letter of the aforementioned legislative diploma? The initial hypothesis of the research is that the alteration of the original wording of the LGPD text that enables treatment in the hypotheses related to the provision of health services, pharmaceutical assistance and health care, including auxiliary diagnostic and therapy services, hypotheses that, in a preliminary analysis, they are very open, allowing a universe of interpretations that encompass numerous activities, which may violate the privacy and personal data of the interested person. The purpose of this research is to verify whether the amendment to art. 11, §4 may represent a violation of privacy and data relating to the health of the holder of personal data. The research was structured in three chapters, which are related to the following specific objectives: a) contextualize the Information Society, in order to understand Privacy within this context. Present privacy; its origin and its current concept; b) present the concept of personal data and analyze them from the concept of information economy; and, c) verify whether the legislative amendment to art. 11, §4 may represent a violation of privacy and the protection of sensitive health data. To carry out this work, we will use the ductive approach method and the monographic procedure method. The research technique will be bibliographical and documentary. In the first chapter we verified that privacy protects information that we would not like to see fall into the public domain, it is everything that should not be the object of information or curiosity in modern society. Privacy is not to be confused with data protection that is related to informational control. The second chapter sought to present the concept of personal data protection and analyze it from the concept of information economy. It was found that personal data can be divided into different species, having a special category, sensitive data. The creation of this autonomous category of personal data is closely linked to the risks that the processing of certain personal information could pose to the human person's personality. Tooth sensitive data there is a subcategory, health data. To better understand the protection of personal data, we seek to contextualize the economy of information, which has information as its raw material. It was possible to conclude the value of health data is related to the degree of sensitivity. Finally, the third chapter aimed to verify whether the legislative change could represent a violation of privacy and data protection. For this, the legislative protection of privacy and the protection of personal data in the Brazilian legal system was analyzed. As conclusion, the general objective of this work was reached and the hypothesis was verified, since it was possible to verify that the alteration in art. 11, § 4, by Law n. 13,853/2019, gave in to market pressures and started to allow the processing of health data with the objective of obtaining economic advantage, except in the cases related to the provision of health services, pharmaceutical assistance and health assistance. The change caused serious risks to the protection of the privacy of the holders of health data, as it allowed treatment of health data in order to obtain an economic advantage for practically any activity.

Keywords: Information Society. Privacy. Sensitive Personal Data. Personal Health Data. Data Economy.

SUMÁRIO

1 INTRODUÇÃO

O valor de algumas coisas na vida só é plenamente compreendido após a sua perda: o amor de alguém, a saúde, a companhia de um animal de estimação, a resistência de um chuveiro em uma manhã de inverno e também a privacidade. Em relação a este último item, Edward Snowden, ex-administrador de sistemas da CIA, que tornou públicos detalhes de diversos programas de vigilância global dos Estados Unidos, diz que a "privacidade não é sobre ter algo a esconder". É sobre ter algo para proteger. E esse algo é quem você é. É algo em que você acredita. É quem você quer se tornar. Engloba a sua essência. Privacidade é o direito de si mesmo. É o que lhe permite compartilhar com o mundo quem você é nos seus próprios termos.

Com o avanço da tecnologia e a informatização da sociedade, o uso da internet praticamente deixou de ser opcional. Está cada vez mais insólito pensar que em um passado não muito distante usávamos mapas impressos para nos nortearmos, enfrentávamos filas de banco para saber quanto de dinheiro nos restava em nossas contas bancárias, íamos até os correios enviar cartas, bem como tantas outras atividades que, aos olhos dos que nasceram em um mundo pós-internet, são difíceis de imaginar.

Após a digitalização e informatização dos sistemas que movem o mundo, bem como das relações interpessoais, o assunto privacidade e proteção de dados assumiu um lugar de destaque. Com o avanço da tecnologia, uma infinidade de dados sobre nós é gerada diariamente. Nossos hábitos, percursos, preferências, histórico de compras, histórico médico e até mesmo de sinais vitais são coletados e armazenados. Essa quantidade imensa de informação, de dados, chamada de big data, é o que alimenta os algoritmos de inteligência artificial responsáveis por nos analisar, nos entender e até mesmo prever ações e nos manipular.

O desenvolvimento da tecnologia, em especial o avanço da capacidade de armazenamento de dados, permitiu o surgimento de uma quantidade de informação gigantesca. Para se ter uma ideia, o volume de dados gerados nos últimos dois anos é maior do que a quantidade de informação produzida pela humanidade desde os seus primórdios. No entanto, toda tecnologia tem dois lados. A pólvora usada para explodir rochedos e permitir a construção de estradas é a mesma usada no cartucho para permitir o disparo de um projétil. Da mesma forma que a imensa quantidade de dados coletados ao se navegar pela internet,

fazer compras, usar aplicativos e usar *wearables* pode ser usada para prever epidemias, também pode ser usada para vigilância governamental e marginalização de grupos de pessoas.

Dentro desse contexto, torna-se imprescindível pensar na proteção da personalidade humana e na sensibilidade inerente a algumas categorias de dados pessoais. Os dados de saúde, pela proximidade com a privacidade e a potencialidade discriminatória, causam especial preocupação dentro desse mundo conectado.

Dados pessoais de saúde são gerados a todo instante, quando um médico preenche um prontuário eletrônico, quando um paciente compra um remédio na farmácia, quando um atleta usa um *wearable* para monitorar dados vitais durante uma atividade física, entre diversas outras atividades. Esses dados podem ser utilizados em diversas situações, por exemplo, alimentar algoritmos de inteligência artificial que permitem a construção de sistemas de apoio à decisão clínica, ou seja, interpretam padrões a partir de uma quantidade colossal de informação e ajudam o médico na tomada de decisão. Mas também podem ser utilizados pelos planos de saúde para ajudar na identificação de clientes potencialmente onerosos, pacientes que estatisticamente consomem do serviço mais do que contribuem, o que pode fazer com que os planos de saúde parem de aceitar pacientes com esse perfil ou então aumentem as suas mensalidades, visando ao lucro máximo.

Dessa forma, faz-se necessária a intervenção do poder público, por meio da criação de leis, para ponderar e normatizar o uso desses dados. Em uma sociedade caracterizada pela informação, dados podem ser valiosos a diferentes setores da economia, podendo ser utilizados em prol do bem coletivo ou em benefício de poucos.

Contudo, será que apenas os textos legislativos, tais como a recente Lei Geral de Proteção de Dados, são suficientes para garantir o uso ético dos dados sensíveis de saúde?

Existem muito interesses envolvidos quando o assunto envolve dados pessoais, muitos deles obscuros. Nesse sentido, a recente alteração na novíssima legislação de dados brasileira nos faz refletir sobre o quão protegidos e seguros os dados sensíveis de saúde e a privacidade realmente se encontram, e é nesse tópico que nos aprofundamos.

Assim, diante do tema privacidade e dados sensíveis de saúde, o presente trabalho se propõe a responder ao seguinte problema: A alteração aprovada pelo Congresso Nacional no § 4º do art. 11 da LGPD pela Lei 13.853/19 pode ocasionar a violação da privacidade e dos dados relativos à saúde do titular dos dados pessoais tendo em conta a letra original do referido diploma legislativo?

A hipótese apresentada é que, muito embora a versão original da Lei Geral de Proteção de Dados (Lei n. 13.709/2018), aprovada em 14 de agosto de 2018, previsse uma vedação ao tratamento de dados pessoais de saúde com objetivo de obter vantagem econômica, trazendo apenas uma exceção – nos casos de portabilidade de dados quando consentida pelo titular –, o texto mais protetivo foi alterado para permitir o tratamento nas hipóteses relativas à prestação de serviços de saúde, de assistência farmacêutica e de assistência à saúde, incluídos os serviços auxiliares de diagnóstico e terapia, hipóteses que, numa análise preliminar, mostram-se muito abertas, possibilitando um universo de interpretações que abarca inúmeras atividades que podem violar a privacidade e os dados pessoais da pessoa interessada.

À vista disso, o objetivo desta pesquisa é justamente verificar se a alteração do art. 11, § 4º pode representar uma violação à privacidade e aos dados relativos à saúde do titular dos dados pessoais.

Da mesma forma, os objetivos específicos são:

1. Contextualizar a Sociedade da Informação, para compreender a privacidade dentro deste contexto. Apresentar a privacidade, sua origem e seu conceito atual.
2. Apresentar o conceito de dados pessoais e analisá-los a partir do conceito de economia da informação.
3. Verificar se a alteração legislativa do art. 11, § 4º pode representar uma violação à privacidade e à proteção de dados sensíveis de saúde.

Para tanto, esta dissertação dividiu o trabalho em três partes. O primeiro capítulo apresentará a Sociedade da Informação, conceito desenvolvido por Castells, para entender a sociedade atual e como está arquitetada. Após discutirmos a sociedade atual, passaremos a analisar como as pessoas compreendem o conceito de privacidade dentro dessa nova organização social. Objetiva-se com essa discussão entender o valor da privacidade, pois as mudanças sociais e tecnológicas têm impacto naquilo que deve ser objeto ou não de proteção. Por isso, torna-se necessário analisar o cenário atual.

Por sua vez, o segundo capítulo visará a conceituar dados pessoais e analisá-los a partir do conceito de economia da informação. Abordaremos de forma mais minuciosa alguns conceitos-chave, como dados pessoais (informações relacionadas à pessoa) e mais especificamente dados sensíveis de saúde (informações de saúde relacionadas a uma pessoa com potencial de causar graves danos a seus titulares no caso de se tornar pública). Ainda nesse item, discutiremos como a maioria dos modelos de negócio da atualidade depende dos

dados pessoais, e com base nesse mapeamento buscaremos apresentar o mercado de saúde e a dependência existente em dados de saúde. Por fim, temos o intuito de avaliar os dados de saúde e entender o funcionamento desse nicho específico do mercado de dados pessoais.

O terceiro e último capítulo cuidará da análise da legislação brasileira referente à proteção da privacidade e dos dados pessoais. Será verificado o caminho para a aprovação da LGPD, a Lei Geral de Proteção de Dados brasileira. Essa breve digressão histórica possibilitará entender como surgiu o texto da lei, e também como os vários atores, com seus interesses diversos, influenciaram na formulação e, posteriormente, alteração do texto legislativo objeto deste estudo. Para, ao fim, analisar especificamente se a alteração no § 4º do artigo 11 da Lei Geral de Proteção de Dados pode representar uma violação à privacidade e à proteção de dados sensíveis de saúde.

Para executar o presente trabalho, utilizaremos o método de abordagem dedutivo e o método de procedimento monográfico. A técnica de pesquisa será bibliográfica e documental, de modo que o estudo será embasado no levantamento da bibliografia especializada, livros, artigos, teses e dissertações nacionais e internacionais.

2 PRIVACIDADE E DADOS PESSOAIS EM CONTEXTO

A ciência jurídica não está isolada da realidade ao seu entorno (CORRÊA, 2016, p. 12), muito pelo contrário, ela apenas existe vinculada a uma realidade histórico-cultural (REALE, 1998, p. 31), sendo inseparável do meio social. Logo, o Direito precisa ser "inserido e correlacionado com o momento e a realidade que o cerca". Não há como desassociar o Direito da realidade histórica, dos fenômenos econômicos e das mudanças tecnológicas e sociais (AZEVEDO, 1997, p. 32). A ciência jurídica precisa ser estudada juntamente com outras disciplinas, pois não há como entender o significado de uma norma jurídica sem adentrar nos aspectos sociais, políticos, econômicos e culturais (CORRÊA, 2016, p. 12).

Neste sentido, para compreender o direito de hoje, é necessário adentrar no contexto da sociedade, visualizar os caminhos percorridos por essa ciência e o contexto em que esse direito se desenvolveu. Faz-se necessário analisar quais foram as ordens de realidade que se alteraram e, igualmente, foram alterando outros fatores da vida, bem como as normas jurídicas.

Assim, perceber as origens e o desenvolvimento de um conceito jurídico, juntamente com o contexto social, permite entendê-lo com mais nitidez (AZEVEDO, 1997, p. 33). Até porque não há como compreender o direito positivado sem suas razões antes de se transformar em uma norma, sendo imperioso para o jurista assimilar a sociedade em que estão inseridas as normas, bem como a cultura, a política e a economia dessa sociedade. Para conhecer de modo completo o direito positivo, então, faz-se necessário entender o aspecto histórico-social para melhor contextualização jurídica (DONEDA, 2006, p. 114).

Destarte, se as mudanças sociais e tecnológicas têm impacto direto no direito vigente, torna-se necessário analisar o contexto atual, reconhecer a complexidade atinente à privacidade e à proteção de dados. Nesse mister, se faz necessário analisar a trajetória desse conceito na sociedade atual, não deixando de lado os aspectos econômicos e as mudanças sociotécnicas que acabaram por trazer "novas necessidades e possibilidades para a reivindicação de direitos e para a percepção de novos problemas nas esferas que compõem o agregado social" (SILVEIRA, 2017, p. 218). O real possui influência sobre o Direito, que vai redesenhando e reivindicando novos tipos de proteção para novos impasses que surgem nas esferas que compõem o agregado social, pois "a ordem jurídica está aberta à contraprova da realidade" (CORRÊA, 2016, p. 14).

A privacidade e a proteção de dados são noções culturais que se transformam no curso do tempo por condicionantes de ordem fática que vão sendo alterados conforme "as tecnologias de intrusão" que invadem os espaços pessoais, transformando-os (SILVEIRA, 2017, p. 218). Para o presente estudo, é fundamental traçar esboço da esfera privada do ser humano, mas esse conceito esbarra diretamente em uma série de tensões que expressam diferentes "visões de mundo, práticas discursivas, ideologias e também interesses econômicos" (SILVEIRA, 2017, p. 218). Neste sentido, temos como proposta nesse primeiro capítulo contextualizar as mudanças ocorridas no mundo contemporâneo e seus impactos diretos sobre a concepção dos valores atinentes à privacidade e à proteção de dados que influem diretamente na norma jurídica atual.

2.1 A SOCIEDADE DA INFORMAÇÃO

Conforme exposto, existe a imprescindibilidade de obter fundamentos sociológicos para melhor compreender o direito posto "diante do novo cenário mundial que se instalou, caracterizado pelo extraordinário avanço na tecnologia[1] da informação e pela supervalorização da informação" (VIEIRA, 2007, p. 155). Neste sentido, faz-se necessário analisar sob o viés da sociologia os contornos da sociedade da informação, definir seus conceitos e principais características.

Ademais, quando existe o propósito de entender o direito à privacidade, Peres-Neto (2018, p. 1) relata a necessidade de envolver saberes de diversas áreas, pois a privacidade possui um conceito de natureza multiforme, demandando adentrar em campos aparentemente tão diferentes como os da computação, sociologia, filosofia, comunicação, psicologia, direito, entre outros.

Assim, começamos a discussão sobre a percepção da importância da informação para aperfeiçoar a produção de riqueza e controle social. Essa visão não é um fenômeno novo[2]. No

1 Por tecnologia, compactuamos com a visão de Lyon (1994, p. 44), que escreve: "A tecnologia pode ser entendida tanto na dimensão técnica de que as tarefas podem ser realizadas usando este ou aquele artefato ou sistema, quanto na dimensão das origens e consequências sociais. Além disso, se a tecnologia é uma atividade humana, ela também se relaciona com propósitos políticos, preferências pessoais e até mesmo compromissos religiosos. Em suma, a tecnologia também deve ser vista normativamente se quiser ser entendida de maneira adequada".

2 Podemos citar como exemplo a administração científica desenvolvida pelo engenheiro norte-americano Frederick Taylor, conhecida como taylorismo, que passou a estudar o seu processo de produção, e com os

entanto, a partir dos anos de 1960, houve uma ruptura do paradigma da era industrial para um novo paradigma na era pós-industrial, que abalou o modo como as informações são coletadas, armazenadas e recuperadas. Marineli (2017, p. 10), analisando a obra de Alvin Toffler, define esse novo paradigma como sendo a "Era da Informação", que veio substituir o paradigma industrial. Essas novas condições foram possíveis graças ao desenvolvimento tecnológico sem precedentes na história da humanidade, seja em extensão, seja em velocidade. Neste sentido, podemos dizer que essas alterações estão ligadas a uma categoria própria de "[...] tecnologias que se inter-relacionam e, mais recentemente, se encontram em posição de convergência: as denominadas Tecnologias da Comunicação e Informação, ou TCIs" (MARINELI, 2017, p. 6).

Hodiernamente, a sociedade está inserida em uma nova configuração organizacional em que a informação transformou-se no elemento nuclear para o "desenvolvimento da economia, substituindo os recursos que outrora estruturaram as sociedades agrícola, industrial e pós-industrial" (BIONI, 2020, p. 4). Essa nova forma de organização social, que deu origem ao paradigma da Tecnologia da Informação, é proveniente da chamada Revolução da Tecnologia da Informação iniciada nos Estados Unidos, mais especificamente no Vale do Silício, condado de Santa Clara, 48 km ao sul de San Francisco, entre Stanford e San Jose, no norte da Califórnia (CASTELLS, 2020, p. 116).

Segundo Castells (2020, p. 122), as principais características do paradigma da Tecnologia da Informação representam a base material da sociedade atual. A primeira característica: a informação não está apenas para agir sobre a tecnologia, mas a informação é matéria-prima, ou seja, "são tecnologias para agir sobre a informação". A segunda característica é que a informação é uma "parte integral de toda a atividade humana", os novos meios tecnológicos penetraram completamente em todos os aspectos da existência das pessoas, tanto individualmente como coletivamente. A terceira característica diz respeito à "lógica de redes em qualquer sistema ou conjunto de relações", por intermédio das novas tecnologias da informação, para "estruturar o não estruturado, porém preservando a flexibilidade, pois o não estruturado é a força motriz da inovação na atividade humana". A quarta característica é que o novo paradigma está baseado na flexibilidade, possuindo uma capacidade de reconfiguração – um aspecto importante, em uma sociedade marcada por constantes alterações e fluidez organizacional. Por fim, a quinta característica é a integração

resultados obtidos treinou seus funcionários com o intuito de alcançar maior produtividade. Logo, a sociedade industrial já valorizava a informação (BIONI, 2020, p. 9).

das novas tecnologias nos sistemas de informação, não sendo possível distingui-las e separá-las (CASTELLS, 2020, p. 124-125).

Estamos diante de uma nova estrutura social, diretamente ligada a um novo modelo de desenvolvimento, o informacionalismo, fruto da reestruturação do modo de produção capitalista do final do século XX (CASTELLS, 2020, p. 72). Essa nova estrutura, denominada Sociedade da Informação, possui como elemento basilar a informação. A informação foi responsável pela (re)organização da sociedade, "tal como o fizeram a terra, as máquinas a vapor e a eletricidade, bem como os serviços, respectivamente, nas sociedades agrícola, industrial e pós-industrial" (BIONI, 2020, p. 5).

Neste sentido, a Sociedade da Informação pode ser apontada como uma configuração distintiva de organização social na qual "a geração, o processamento e a transmissão de informação se convertem nas fontes fundamentais da produtividade e do poder por conta das novas condições tecnológicas surgidas neste período histórico" (BOFF, 2018, p. 9). Percebe-se, então, que a sociedade da informação criou um novo paradigma: "a informação como recurso estruturante da sociedade e que possui relevante valor político e econômico que se sobrepõe aos demais meios de geração de riqueza" (SCHAEFER, 2010, p. 132).

Para Vieira (2007, p. 156), que analisa a obra de Castells, a sociedade da informação é um novo modelo de organização social, político e econômico que se utiliza intensamente "da tecnologia da informação para coleta, produção, processamento, transmissão e armazenamento de informações". Assim, a "facilidade em estocar e recuperar informações a partir do monitoramento cotidiano das ações dos indivíduos é uma característica mais ampla das sociedades informacionais e vem se intensificando velozmente nas últimas décadas" (BRUNO, 2013, p. 145).

Conforme mencionado acima, uma das características da sociedade da informação encontra-se no fato de ela estar organizada em redes[3]. O objeto que cria o fluxo da rede não é

3 Segundo Castells (2020, p. 554) "rede é um conjunto de nós interconectados. Nó é o ponto no qual uma curva se entrecorta. Concretamente, o que um nó é depende do tipo de redes concretas de que falamos. [...] A inclusão/exclusão em redes e a arquitetura das relações entre redes, possibilitadas por tecnologias da informação que operam à velocidade da luz, configuram os processos e funções predominantes em nossas sociedades. Redes são estruturas abertas capazes de expandir de forma ilimitada, integrando novos nós desde que consigam comunicar-se dentro da rede, ou seja, desde que compartilhem os mesmos códigos de comunicação (por exemplo, valores ou objetivos de desempenho). Uma estrutura social com base em redes é um sistema aberto altamente dinâmico suscetível de inovação sem ameaças ao seu equilíbrio. Redes são instrumentos apropriados para a economia capitalista baseada na inovação, globalização e concentração descentralizada; para o trabalho, trabalhadores e empresas voltadas para a flexibilidade e adaptabilidade; para

importante, mas sim o mecanismo de conexão entre os nós e entre as pontas daquela rede. Os instrumentos de poder nessa sociedade são nós que possibilitam as conexões. Os conectores são os detentores do poder, ou seja, "o poder dos fluxos é mais importante que os fluxos do poder". Neste sentido, redes "constituem a nova morfologia social de nossas sociedades e a difusão da lógica de redes modifica de forma substancial a operação e os resultados dos processos produtivos e de experiência, poder e cultura" (CASTELLS, 2020, p. 553).

A arquitetura em redes, criada pelas novas tecnologias de informação, alterou a essência da sociedade, em qualquer setor: governo, economia, universidade, sociedade civil. Para Lemos (2014, p. 8) a arquitetura em rede da Sociedade da Informação, transformou a sociedade que passou a ser mais interativa e plural, pois as pessoas passaram a estar conectadas por redes globais de comunicação e informação. Ademais, a sociedade tornou-se mais dinâmica, pois envolta em um emaranhado de informações que se conectam e desconectam a todo instante, as pessoas e as organizações passaram a ser "organismos informativos, cuja identidade e integridade também são moldadas pelas próprias informações disponibilizadas e tratadas" dentro dessa grande rede global (LIMA, 2018, p. 136).

Durante os anos de 1970 e início dos anos 1980, as novas condições sociais e as novas tecnologias foram recebidas com muito entusiasmo. Era o começo da Sociedade da Informação e com ela vinha a promessa de prosperidade, novas oportunidades democráticas e educacionais. As distâncias espaciais foram encurtadas com a tecnologia, o mundo virava uma "aldeia global" – tal encurtamento está muito relacionado com o advento da internet, que será melhor trabalhado em seguida.

É inegável que houve inúmeras vantagens com o desenvolvimento tecnológico. Contudo, as inovações também trouxeram novas formas de interferências, não tão boas, na vida das pessoas. Conforme já mencionado, a revolução da Tecnologia da Informação foi iniciada em território norte-americano, mais especificamente no Vale do Silício, onde surgiram "o circuito integrado, o microprocessador e o microcomputador, entre outras tecnologias importantes", e tal região é reconhecida como "o coração das inovações eletrônicas" pulsando por mais de quarenta anos (CASTELLS, 2020, p. 116). Tendo em vista os impactos[4] que essas inovações tecnológicas tiveram para a sociedade contemporânea, se

uma cultura de desconstrução e reconstrução contínuas; para uma política destinada ao processamento instantâneo de novos valores e humores públicos.

4 A emergência de novas tecnologias é sempre produzida "dentro de uma cultura, e uma sociedade encontra-se condicionada por suas técnicas. E digo condicionada, não determinada. [...] Não há uma 'causa' identificável para um estado de fato social ou cultural, mas sim um conjunto infinitamente complexo e parcialmente

faz necessário passar um panorama geral sobre essa revolução iniciada da década de 1970 com a microeletrônica, passando pelos computadores até chegar às telecomunicações (CASTELLS, 2020, p. 95).

Apesar do surgimento dos primeiros computadores em 1945 na Inglaterra e nos Estados Unidos, que nada se assemelham com os modelos que temos hoje em dia. Segundo Lévy (2010, p. 31) eram espécies de calculadoras programáveis reservadas para usos militares para cálculos de cunho científico, bem como para a formulação de estatísticas do Estado e de algumas poucas grandes empresas que os utilizavam para tarefas pesadas de gerenciamento[5].

Os computadores apesar começaram a ser disseminados para uso civil durante os anos 60, conforme será mais bem explanado (LÉVY, 2010, p. 31). No entanto, podemos adiantar que a virada fundamental data dos anos 70, e, apesar de origem norte-americana, a revolução da Tecnologia da Informação, pela sua importância e relevância, difundiu-se entre diferentes nações, culturas e organizações, visando a inúmeros fins. As novas tecnologias da informação foram utilizadas para os mais diversos tipos de aplicações e usos, que, por sua vez, "produziram [mais] inovação tecnológica, acelerando a velocidade e ampliando o escopo das transformações tecnológicas, bem como diversificando as suas fontes" (CASTELLS, 2020, p. 65).

As expansões da tecnologia e das relações técnicas de produção adentraram e difundiram-se "por todo o conjunto de relações e estruturas sociais, penetrando no poder e na experiência e modificando-os". As inovações tecnológicas possuem o condão de alterar e moldar "toda a esfera de comportamento social, inclusive a comunicação simbólica" (CASTELLS, 2020, p. 74-75). Assim, os modos de desenvolvimento estão inseridos em uma estrutura de redes permeáveis, adentrando na vida das pessoas, causando mudanças significativas, e irreversíveis.

O progresso tecnológico leva Rodotà (2008, p. 41) a afirmar que os riscos das tecnologias encontram-se exatamente na impossibilidade de deter tal progresso, que ocorrem

---

indeterminado de processos em interação que se autossustentam ou se inibem. [...] Dizer que a técnica condiciona significa dizer que abre algumas possibilidades, que algumas opções culturais ou sociais não poderiam ser pensadas a sério sem sua presença" (LÉVY, 2010, p. 25-26).

5 Os computadores nesse período eram "grandes máquinas de calcular, frágeis, isoladas em salas refrigeradas, que cientistas em uniformes brancos alimentavam com cartões perfurados e que de tempos em tempos cuspiam listagens ilegítimas".

num ritmo muito acelerado, e, igualmente, são de pronto absorvidas pela sociedade[6], ao passo que o processo para controle social e proteção das pessoas não consegue seguir no mesmo ritmo (RODOTÀ, 2008, p. 42).

Conforme afirma Castells (2020, p. 87-88), o processo de transformação tecnológica não para de crescer, pois possui a faculdade de criar conexões entre a linguagem comum em que a informação é gerada, armazenada, recuperada e transmitida pelas pessoas com os campos tecnológicos. Desta forma, a dependência tecnológica aumenta exponencialmente, adentrando permanente na vida das pessoas[7].

Apesar do rápido avanço, a revolução da tecnologia não se deu do dia para a noite. Esse sistema tecnológico que vivenciamos foi fruto de inovações tecnológicas e transformações organizacionais com enfoque na flexibilidade e na adaptabilidade[8], que permitiram a velocidade e eficiência na sua construção. Inúmeras descobertas surgiram nesse período, que passaram a alargar as funções comerciais e civis como (CASTELLS, 2020, p. 108-109) forma de comunicação, uma vez que as tornaram mais acessíveis ao público em geral, bem como mais baratas, e com uma qualidade cada vez maior[9].

---

6 O tempo necessário para os produtos alcançarem a marca de 50 milhões de usuários está se encurtando com o tempo. O telefone demorou 50 anos. O rádio precisou de 30 anos. Os cartões de crédito precisaram de 28 anos. A televisão levou 18 anos. O computador precisou de 14 anos. O celular, de 12 anos. A internet precisou de sete anos. Os iPods levaram quatro anos. O Facebook precisou de três anos. O Twitter levou dois anos. E esse tempo de penetração de inovações na vida das pessoas tende a diminuir cada vez mais (VIEIRA, 2020). No mesmo sentido: "A internet tem um índice de penetração mais veloz do que qualquer outro meio de comunicação na história: nos Estados Unidos, o rádio levou trinta anos para chegar a sessenta milhões de pessoas; a TV alcançou esse nível de difusão em quinze anos; a internet o fez em apenas três anos após a criação da teia mundial" (CASTELLS, 2020, p. 437).

7 Segundo Lévy (2010, p. 52), "digitalizar uma informação consiste em traduzi-la em números. Quase todas as informações podem ser codificadas desta forma. Por exemplo, se fizermos com que um número corresponda a cada letra do alfabeto, qualquer texto pode ser transformado em uma série de números".

8 A flexibilidade e descentralização dos novos dispositivos tecnológicos foram possíveis graças a empresários inovadores. Contudo, tal revolução não foi iniciada pelo mercado – apesar de o progresso ser essencialmente conduzido por ele, mas sim pelo Estado tanto nos Estados Unidos como em todo o mundo (CASTELLS, 2020, p. 122-123). Ademais, importante mencionar que o "desenvolvimento das cibertecnologias é encorajado tanto por Estados que perseguem a potência, em geral, e a supremacia militar em particular. É também uma das questões da competição econômica mundial entre as firmas gigantes de eletrônica e de software, entre os grandes conjuntos geopolíticos. Mas também responde aos propósitos de desenvolvedores e usuários que procuram aumentar a autonomia dos indivíduos e multiplicar suas faculdades cognitivas. Encara, por fim, o ideal de cientistas, de artistas, de gerentes ou de ativistas de rede que desejam melhorar a colaboração entre pessoas (LÉVY, 2010, p. 24).

9 Dentre os exemplos das tecnologias as mais relevantes podem ser exemplificadas como sendo: "O microprocessador, o principal dispositivo de difusão da microeletrônica, foi inventado em 1971 e começou a ser difundido em meados dos anos 1970. O microcomputador foi inventado em 1975, e o primeiro produto comercial de sucesso, o Apple II, foi introduzido em abril de 1977, por volta da mesma época em que a Microsoft começava a produzir sistemas operacionais para microcomputadores. A Xerox Alto, matriz de muitas tecnologias de software para os PCs dos anos 1990, foi desenvolvida nos laboratórios PARC em Palo Alto, em 1973. O primeiro comutador eletrônico industrial apareceu em 1969, e o comutador digital foi desenvolvido em meados dos anos 1970 e distribuído no comércio em 1977. A fibra ótica foi produzida em

Assim, podemos afirmar que o desenvolvimento e a comercialização do microprocessador impulsionou inúmeros processos econômicos e sociais de enormes magnitudes (LÉVY, 2010, p. 31). Em sentido semelhante, Marineli (2017, p. 9) pontua como as principais inovações a partir de 1975: os microcomputadores ou computadores pessoais (PCs); posteriormente, a linguagem de programação para o primeiro "microcomputador" comercializado, o MITS Altair 8800, criado por Bill Gates e Paul Allen. A linguagem foi um marco importante, pois foi o que permitiu acessibilidade ao público em geral. Um novo salto foi experimentado com a expansão da internet, "a maior rede de intercâmbio de informações já criada". Em 1993, foi lançado o primeiro *smartphone* pela IBM. A Research in Motion (RIM), em 2002, lançou o primeiro celular que possuía acesso à caixa de e-mails via internet – o denominado Blackberry. Também com acesso à internet, em 2010, a Apple lança o iPad. Ao final da exposição, Marineli (2017, p. 9) destaca que essas novas tecnologias possuem como marca a possibilidade ampliada de um "poderoso grau de integração entre todos os seus elementos constitutivos". Com auxílio da tecnologia, as pessoas podem estar conectadas globalmente, possibilitando a comunicação tanto por voz, por vídeos, ou por texto. Possibilitando o compartilhamento de imagens, documentos, bem como o acesso a notícias jornalísticas ou entretenimento de qualquer lugar do mundo.

Dada a importância verificada a expansão da internet, torna-se necessário apresentar uma breve análise sobre o seu desenvolvimento e desdobramentos. Nas últimas décadas do século XX o seu desenvolvimento foi gerado graças à cooperação científica e ao empreendedorismo tecnológico, aliado a uma estratégia militar (FORTES, 2016, p. 58). Essa nova tecnologia possibilitou a abertura de um novo espaço social, desencadeou a coletivização dos dados, revolucionando, novamente, o modo de comunicação e informação da sociedade, aumentando a circulação de informações num montante nunca imaginado. O desenvolvimento da internet proporcionou a criação de uma nova arena de diálogos, mudou e

---

escala industrial pela primeira vez pela Corning Glass, no início da década de 1970. Além disso, em meados da mesma década, a Sony começou a produzir videocassetes comercialmente, com base em descobertas da década de 1960 nos EUA e na Inglaterra, que nunca alcançaram produção em massa. E, finalmente, mas não menos importante, foi em 1969 que a Arpa (Agência de Projetos de Pesquisa Avançada do Departamento de Defesa Norte-Americano) instalou uma nova e revolucionária rede eletrônica de comunicação que se desenvolveu durante os anos 1970 e veio a se tornar a internet. Ela foi extremamente favorecida pela invenção, por Cerf e Kahn em 1973, do TCP/IP, o protocolo de interconexão em rede que introduziu a tecnologia de "abertura", permitindo a conexão de diferentes tipos de rede" (CASTELLS, 2020, p. 109).

ampliou a forma como nos comunicamos, estendeu os tipos de interações sociais, permitindo um maior acesso a uma quantidade infinita de informações (CANCELIER, 2017, p. 39).

A origem da internet está relacionada com um projeto militar iniciado na década de 1960 pela Agência de Projetos de Pesquisa Avançada do Departamento de Defesa dos Estados Unidos com o objetivo de impedir a tomada ou destruição do sistema norte-americano de comunicação em caso de ataques nucleares (CASTELLS, 2020, p. 101)[10]. Esta primeira rede de computadores, denominada Arpanet, em homenagem ao seu patrocinador, começou a operar em 1º de setembro de 1969. Essa rede tornou-se a base de comunicação global composta de milhares de redes de computadores.

No entanto, o sistema da Arpanet começou a ser utilizado por pesquisadores e docentes para comunicação, não apenas para os fins militares inicialmente propostos (CASTELLS, 2020, p. 105). Assim, a academia passou a usar o sistema, possibilitando que sua utilização por estudantes, que passaram a dar à internet aplicações que originalmente não estavam previstas no plano original, o que acabou desenhando a trajetória tecnológica de modo essencial para as características da internet. Dentre as funcionalidades utilizadas que causaram muito entusiasmo, uma foi a utilização do correio eletrônico (CASTELLS, 2020, p. 104). Esse novo meio de comunicação fez surgir nos Estados Unidos uma "contracultura" que passou a utilizar das novas possibilidades técnicas, inclusive levando ao surgimento de importantes invenções como o *modem*[11] e mais adiante o próprio computador pessoal (CASTELLS, 2020, p. 104 e LÉVY, 2010, p. 31).

Em 1983, essa rede sofreu uma divisão entre Arpanet, dedicada para fins científicos, e Milnet, voltada para fins militares. A rede continuou a ser aprimorada por indivíduos e

---

10 O sistema foi idealizado por Paul Baran que visava um modo "de comunicação baseado na tecnologia de comunicação da troca de pacotes", possibilitado pela arquitetura em rede. O sistema não era controlado por nenhum centro, sendo composto por milhares de redes em que as mensagens localizam as suas próprias rotas ao longo dessa arquitetura. A ideia era contornar as barreiras eletrônicas, possibilitando uma troca de informação direta – tanto de ida como de volta – de forma coerente e sem interferências. (CASTELLS, 2020, p. 104).

11 Modem é "o aparelho que permite a modulação e desmodulação da informação digital, e que portanto permite a comunicação de dois computadores via telefone", pois "a informação pode usar a rede telefônica clássica, contanto que seja modulada (codificada analogicamente de forma adequada) ao entrar na rede telefônica e desmodulada (redigitalizada) quando chegar a um computador ou outro equipamento digital na outra ponta do cabo" (LÉVY, 2010, p. 35). A descoberta do modem foi fruto da contracultura que surgiu no período, sendo inventado por dois estudantes de Chicago, em 1978, que com o intuito de evitar se deslocar no frio do inverno de Chicago buscaram utilizar a linha do telefone para transferir programas entre microcomputadores. Obtendo sucesso na empreitada e inventando o protocolo Xmodem, que "permitia a transferência direta de arquivos entre computadores, sem passar por um sistema principal". O mais interessante foi que os dois estudantes, Ward Christensen e Randy Suess, divulgaram gratuitamente a nova tecnologia, pois o intuito dos inventores era espalhar o máximo possível a capacidade de comunicação (CASTELLS, 2020, p. 104).

grupos de pessoas de todas as partes do planeta e com todo tipo de objetivo, desviando da ideia inicial de proteção do banco de dados em caso de guerra (CASTELLS, 2020, p. 65-66). Dentre essas inovações, a invenção do TCP/IP – o protocolo de interconexão em rede, em meados de 1970, foi essencial para a "abertura" do sistema, pois passou a permitir a conexão de diferentes tipos de redes. O outro salto tecnológico que merece destaque foi a criação e distribuição gratuita do aplicativo World Wide Web (www), em 1990, pelo Centre Européen pour la Recherche Nucléaire (CERN). O aplicativo foi capaz de organizar os tipos dos sítios da internet por assuntos, e não por localização, oferecendo aos usuários um sistema fácil de pesquisa (CASTELLS, 2020, p. 105-106).

Em 1990, a Arpanet encerrou as suas atividades, sendo sucedida pelo NSFNET. Porém, em 1995 a internet foi privatizada por conta da pressão comercial existente (CASTELLS, 2020, p. 101-102). E ela não parou de ser aperfeiçoada, destacando-se a criação de novos softwares[12], como o Java e o Jini, que "permitiram que a rede se tornasse o verdadeiro sistema de processamento de dados" (CASTELLS, 2020, p. 107). A internet começava e adentrar em todo tipo de atividade, aumentando cada vez mais o seu alcance. A linguagem digital aumentou a possibilidade de comunicação, bem como ampliou o modo de se comunicar, uma vez que inovações no sistema permitiam a troca de mensagens multimídia integrando texto, áudio e imagens (metalinguagem) (CASTELLS, 2020, p. 101). A metalinguagem levou a mudanças culturais significativas, isto porque os "meios de comunicação são nossas metáforas e as nossas metáforas criam o conteúdo de nossa cultura – isto é, nossos sistemas de crenças e códigos historicamente produzidos" (CASTELLS, 2020, p. 413).

Esse novo mecanismo de comunicação passou a ser utilizado como um instrumento de criação artística, cultural, bem como um meio de organização de banco de dados e planilhas; de simulação com ferramentas de apoio à pesquisa, de diversão com jogos e inúmeras outras aplicações, a depender da criatividade humana que a inova a cada dia numa proporção crescente em todo o globo (LÉVY, 2010, p. 32). Logo, com o passar dos anos a internet, e sua variada gama de aplicações, transformou-se em um dos principais meios de comunicação, sendo utilizada para o "trabalho, conexões pessoais, entretenimento, serviços

12 Software, ou programa, é "uma lista muito organizada de instruções codificadas, destinadas a fazer com que um ou mais processadores executem uma tarefa. Através dos circuitos que comandam, os programas interpretam dados, agem sobre informações, transformam outros programas, fazem funcionar computadores e redes, acionam máquinas físicas, viajam, reproduzem-se etc." (LÉVY, 2010, p. 42).

públicos", inclusive, para fins políticos e de religião (CASTELLS, 2020, p. 18). Assim, a partir dos anos 80, com auxílio da internet e com as demais tecnologias que adentraram na vida das pessoas, pode-se afirmar que "a informática perdeu, pouco a pouco, seu status de técnica e de setor industrial particular para começar a fundir-se com as telecomunicações, a editoração, o cinema e a televisão" (LÉVY, 2010, p. 32).

Hoje podemos descrever a internet como sendo conglomerado de redes informáticas interconectadas que possibilitam a comunicação em todo o globo de milhões de usuários (MARINELI, 2017, p. 13). No mesmo sentido, para Corrêa (2000, p. 8) a internet é composta por várias redes, formando uma rede global de computadores que possibilita o diálogo de informações em escala global, de modo eficiente e rápido, entre várias máquinas conectadas nessas redes, o que levou a um novo modo de interação entre os seres humanos.

Ademais, a internet foi fundamental para o surgimento da Sociedade da Informação, pois por meio dela todas as redes de conexão estão interligadas. Por meio das redes, as distâncias foram encurtadas e as barreiras físicas, levantadas, permitindo uma conexão em nível global. O tempo e o espaço foram alterados nessa nova sociedade, não existem distâncias para o fluxo de informações (CASTELLS, 2020, p. 554). Ela passou a representar um novo meio comunicação entre espaços em rede, "que deixaram de ser estáticas e passaram a ser dinâmicas, baseadas em uma inteligência coletiva que remete a um novo conceito de troca de informações" (MARINELI, 2017, p. 17), sendo marcada pelo uso de redes sociais[13] e pelo compartilhamento de dados, informações e conteúdo. Contudo, o dinamismo das redes, juntamente, com o aparecimento de uma nova geração de tecnologias e aplicações interativas, permitiu a criação de redes pessoais e de comunidades com maior facilidade na publicação, edição, difusão de conteúdo (FORTES, 2016, p. 69). Em sentido semelhante, Bruno (2013, p. 124-126) discorre que houve um alargamento das margens de visibilidade do que outrora era

13 As redes sociais podem ser conceituadas como "serviços on-line, que têm como objetivo construir redes ou relações sociais entre pessoas, que compartilham interesses e atividades em comum. São espaços específicos na internet que abarcam verdadeiras estruturas sociais, compostas por pessoas que buscam o contato virtual fundado em afinidades e objetivos comuns" (MARINELI, 2017, p. 19). Existem centenas de redes sociais. No entanto, entre as mais conhecidas estão: a) Facebook; b) Orkut; c) Twitter; c) Linkedin; e) YouTube; f) Instagram; g) WhatsApp; h) Snapchat; i) Flickr; j) Myspace; k) Google+; l) Waze (MARINELI, 2017, p. 25). Sibila (2016, p. 20) lembra ainda dos serviços para encontrar parceiros tais como o Tinder, Grindr ou Happn. No mesmo sentido Bruno (2013, p. 125) lista as seguintes plataformas cujos conteúdos são gerados pela participação dos usuários: blogs, redes sociais (Facebook, MySpace, Twitter), plataformas de compartilhamento (YouTube, Flickr), folksnomias (Del.icio.us, Technorati Tags), mashups (ChicagoCrime.org, Diggdot.us) etc. Compartilhamos nossas fotografias no Flickr, vídeos no YouTube, dados profissionais no Linkedin, livros que lemos no GoodReads, viagens no Wayan, locais que estamos Foursquare, snapshot de nossas telas de computadores no Snoopon.me, toda sorte de informações no Twitter, Facebook etc.

entendido como intimidade, uma vez que as novas redes sociais envolvem uma exposição voluntária da vida cotidiana com alcance em todas as suas esferas.

Essa evolução de tecnologia levou a internet a sua fase atual, que representaria um novo modelo de inteligência na internet que seria capaz de examinar os dados cedidos, organizando-os de modo a realizar tarefas complexas para os usuários (MARINELI, 2017, p. 18). Possuindo como principal característica a criação e armazenamento de dados, a internet atualmente é "uma base de conhecimento e de informação semântica e qualitativa" (FORTES, 2016, p. 69), pois há uma tendência a guardar informações de seus usuários (gestos, costumes, conectividade, interatividade, usabilidade, entre outros) e, ao mesmo tempo, a combinação de tais informações com os conteúdos existentes nas redes sociais, podendo ser utilizados de diversas maneiras, inclusive como mercadorias para empresas. A internet passou de ser mero instrumento de interação social, focado na criatividade dos seus usuários, "considerados consumidores e produtores das informações que trafegam online", para ser, também, uma ferramenta focada na interligação de conjuntos de dados e objetos (MAGRANI, 2019, p. 34)

Nesse novo modelo de sociedade, a informação é uma matéria-prima muito valorizada, pois com ela o homem pode gerar conhecimento[14], e as tecnologias da informação e comunicação estão em constante aperfeiçoamento para captar e gerar mais conhecimento, a exemplo da inteligência artificial (AI) e aprendizagem de máquina (AM) "como consequência do surgimento de novos modelos sociais e econômicos" (BOFF, 2018, p. 181). Ao passo que, com o passar do tempo, todo tipo de informação passou a ser digitalizada[15], tal como o áudio e o vídeo – a técnica binária[16] desmaterializou a informação em bits, comprimindo tangivelmente a informação e concedendo um acesso mais simples a ela por meio da sua

14 Para "Laudon e Laudon (1999, p. 10), conhecimento é: o conjunto de ferramentas conceituais e categorias usadas pelos seres humanos para criar, colecionar, armazenar e compartilhar informações. O conhecimento pode ser armazenado como um artefato em uma biblioteca – como um livro, por exemplo, ou em um programa de computador como um conjunto de instruções que dá forma a uma sequência de dados que sem ele não teria sentido" (BOFF, 2018, p. 181).

15 Conforme retira-se da obra de Lévy (2010, p. 52-53), digitalizar uma informação é transforma-la em números, abrangendo praticamente todas as informações que podem ser explicitadas ou medidas. Todos os números podem ser expressos em linguagem binária, sob a forma de 0 e 1. "De fato, os números binários podem ser representados por uma grande variedade de dispositivos de dois estados (aberto ou fechado, plano ou furado, negativo ou positivo etc.). É assim que os dígitos circulam nos fios elétricos, informam circuitos eletrônicos, polarizam fitas magnéticas, se traduzem em lampejos nas fibras óticas, microssulcos nos discos óticos, se encarnam em estruturas de moléculas biológicas" (LÉVY, 2010, p. 53).

16 "Com a linguagem binária, permitiu-se um acúmulo de informação inimaginável e em novas plataformas – compact disk (CD), pen drive, computadores pessoais etc. – em comparação ao suporte primitivo dos átomos – papel. [...] A técnica binária permitiu que a informação fosse mais precisamente organizada, facilitando, em última análise, o seu próprio acesso" (BIONI, 2020, p. 7).

inclusão. Como consequência, houve um aumento exponencial no processamento e digitalização das informações (BIONI, 2020, p. 7).

Segundo Lyon (1994, p. 83), a nova tecnologia baseada em microeletrônica tornou-se capaz de controlar com mais precisão informações e pessoas, por meio de sua capacidade de armazenamento e processamento de informações, e também em razão de sua permeabilidade, uma vez que ela adentra rapidamente no cotidiano social. Por tal razão, é necessário refletir sobre seus impactos (DONEDA, 2006, p. 35), pois, diferentemente do que ocorria no passado, hoje praticamente quase todos os aspectos da vida estão direta ou indiretamente interagindo entre bancos de dados computacionais (LYON, 1994, p. 6). Nesta lógica, as Ciências da Informação e da Comunicação transformam-se em um campo do saber que procura soluções para modelos seguros e eficazes para o intercâmbio de informações (LIMA, 2018, p. 133).

Ademais, pode-se complementar que a permeabilidade da internet está diretamente relacionada com o acesso móvel que ampliou e facilitou o acesso a conteúdos digitais (FORTES, 2016, p. 69), bem como "o aumento exponencial das performances dos equipamentos combinado com uma baixa contínua nos preços" (LÉVY, 2010, p. 32). O acesso móvel converteu a tela do computador em versáteis aparelhos móveis como os *tablets* e os smartphones, de uso fácil e com interfaces amigáveis "que driblam quase todos os limites espaciais ou temporais – em janelas sempre abertas e ligadas a quantidades crescentes de indivíduos" (SIBILA, 2016, p. 20). A comunicação pelos aplicativos[17] móveis genéricos como o WhatsApp substituiu as chamadas telefônicas, trocadas por diálogos quase que permanentes em que se digita na tela do aparelho celular e que geralmente vêm ilustrados com fotos, vídeos ou sons (SIBILA, 2016, p. 20).

17 Para melhor compreender os termos utilizados pelo trabalho, utilizaremos a terminologia utilizada por Lévy, que define aplicativos como "programas que permitem uma máquina prestar um serviço específico a seus usuários. Neste sentido, podemos ilustrar como exemplos clássicos de aplicativos: programas que calculam automaticamente o pagamento dos empregados de uma empresa, programas capazes de comandar máquinas em tempo real de acordo com informações fornecidas por sensores. Bem, como os programas de editor de textos que permite a redação, modificação e organização de textos. Gerenciador de bancos de dados que permitem a criação de um ou mais bancos de dados, bem como a localização rápida de uma informação importante de acordo com diversas chaves de pesquisa, como também, apresentação da informação de vários ângulos de acordo com a necessidade" (LÉVY, 2010, p. 43). Ademais, o mencionado autor complementa que os "programas de aplicativos estão cada vez mais abertos à personalização evolutiva das funções, sem que seus usuários sejam obrigados a aprender a programar" (LÉVY, 2010, p. 43). Tal ideia se visualiza nas aplicativos de redes sociais em que os usuários editam seus perfis com fotos, acrescentam textos autorais e vídeos. Alguns dão opções de mudar a cor das telas, acrescentar efeitos nas fotos e nenhuma dessas funções precisa de qualquer conhecimento de programação para ser realizada, sendo de fácil manuseio. Esse fenômeno é consequência da evolução das interfaces de saída que "deu-se no sentido de uma melhoria da definição e de uma diversificação dos modos de comunicação da informação" (LÉVY, 2010, p. 38).

Bioni (2020, p. 19) afirma que o celular no estágio atual da internet é o principal dispositivo de acesso, ultrapassando o uso do computador. Por tal razão, as "pessoas estão cada vez mais conectadas", pois os celulares, aparelhos sem fio, podem ser levados a todos os lugares, sendo difícil distinguir os ambientes on-line e off-line. Igualmente, Lima (2018, p. 134) fala sobre a "conectividade perpétua", fenômeno que ocorre pelo uso constante da comunicação por meio de aparelhos celulares que dificulta a pessoa se desconectar do mundo virtual. Assim, na Sociedade da Informação a disseminação do celular, uma tecnologia de computação, tem distorcido as diferenças entre o mundo digital e o mundo físico (ACQUISTI et al., 2016, p. 3).

Atualmente, a todo momento os aplicativos melhoram suas identidades visuais e o modo de interação entre os usuários, o que acarreta um aumento de tempo de uso e "a quantidade e variedade de informações ali registradas, bem como a abrangência de dispositivos inteligentes conectados" (DAINEZI, 2019, p. 19). Esse aumento do tempo de uso, assim como uma simbiose entre os mundos on-line e off-line, acarretou uma alteração da noção do tempo na Sociedade da Informação, levando Castells (2020, p. 458) a afirmar que "o tempo é apagado no novo sistema de informação"[18].

O tempo mudou, assim como os espaços, o espaço virtual está imbricado ao espaço off-line. Conforme Snowden (2021), antes existia uma diferença entre o mundo on-line e o mundo real, porém hoje essa diferença não existe mais: o mundo on-line é o mundo real, e o mundo real é virtual. A internet é a sociedade, a maior parte dela. Neste sentido, a internet deixou de ser apenas um meio de comunicação para transformar-se num local em que as pessoas desenvolvem e expressam sua personalidade e sua individualidade. Nela são criados e armazenados os dados particulares de cada um, a interação que existe no mundo on-line se iguala ao mundo real, sendo um lugar onde quase tudo acontece (CANCELIER, 2017, p. 40).

Exatamente por ser uma extensão da vida, os aplicativos on-line acumulam os mais variados dados pessoais de seus usuários, que são coletados durante a interação do mesmo com as plataformas interativas. Esses dados são capazes de traçar um perfil do usuário, que

18 [...] A comunicação mediada por computadores possibilita o diálogo em tempo real, reunindo pessoas com os mesmos interesses em conversa interativa multilateral, por escrito. Respostas adiadas pelo tempo podem ser superadas com facilidade, pois as novas tecnologias de comunicação oferecem um sentido de instantaneidade que derruba as barreiras temporais, como ocorreu com o telefone, mas, agora, com maior flexibilidade, permitindo que as partes envolvidas na comunicação deixem passar alguns segundos ou minutos, para trazer outra informação e expandir a esfera de comunicação sem a pressão do telefone, não adaptado a longos silêncios (CASTELLS, 2020, p. 541).

posteriormente é utilizado para o direcionamento de publicidade. Assim, Bioni (2020, p. 18) conclui que "o usuário da rede é a todo momento monitorado, acumulando-se uma série de dados (comportamentais), que são aplicados para a personalização da abordagem publicitária". A internet é uma fonte privilegiada de conhecimento, classificação e intervenção sobre indivíduos e grupos (BRUNO, 2013, p. 145).

Com a facilidade e aprimoramento das técnicas de coleta e armazenamento de dados, surgem inúmeros bancos de dados – públicos e privados – que exercem poderes de vigilância sobre os indivíduos, pondo em risco direitos fundamentais, tais como a privacidade. Lyon (1994, p. 41), citando Simon Davies, prevê que a introdução de novas tecnologias tem o potencial de acabar com as liberdades civis, pois essas tecnologias mudam o equilíbrio de poder existente dentro das sociedades. Nesse assunto, entraremos mais detalhadamente em tópico próprio, mas neste momento é importante pontuar que os mecanismos de coleta de dados e a criação de perfis obtidos por meio desses dados, em sua maioria de dados pessoais, que as pessoas disponibilizam no mundo virtual, bem como esses dados colhidos on-line têm o condão de gerar um perfil virtual da pessoa – perfil que "pode ser o único aspecto visível a uma série de outros sujeitos" e por vezes confundindo-se com a pessoa biológica ou física (DONEDA, 2006, p. 174).

A imensidão de dados coletados on-line é possível graças a alguns fenômenos que passaram a ocorrer por conta das novas tecnologias mencionadas, principalmente com a utilização da internet, que revolucionou os meios de viver as subjetividades humanas e o modo de se comunicar dentre pares[19]. Hoje, as conexões podem ser realizadas imediatamente de qualquer lugar do globo. As funções dos computadores foram reduzidas a pequenos aparelhos, os celulares inteligentes, tornando as conexões ainda mais frequentes e mais fáceis. As pessoas agora estão, conforme mencionado, disponíveis quase a todo o momento, sendo difícil desligar-se da constante interação on-line[20]. A arquitetura dos dispositivos é pensada para prender as pessoas cada vez mais na rede e, assim, disponibilizar dados que poderão ser utilizados futuramente para inúmeros fins (SIBILA, 2016, p. 21). Ademais, um fator que

19 Importante apenas mencionar que o processo de coleta de dados, e em especial de informações pessoais, não é um fenômeno absolutamente novo. A necessidade de coletar informações desenvolveu-se muito com o melhoramento das "estruturas estatais e privadas, particularmente com o advento do estado-nação e principalmente das grandes estruturas estatais burocráticas típicas do *welfare state*" (DONEDA, 2006, p. 175). No entanto, o advento das novas tecnologias, particularmente do computador, permitiu a digitalização das informações, que passou a ser mais utilizada, em praticamente todos os momentos.

20 A dificuldade de ficar off-line advém da própria arquitetura da comunicação digital, que possui sensores que denunciam se o indivíduo está disponível, escrevendo, perto do seu aparelho celular ou, inclusive, se leu a última mensagem, por meio de marcas de leitura e de recebimento.

contribui para o aumento da utilização e coleta de informações está relacionado com a diminuição dos custos de manutenção das redes, possibilitando estarem por todo o planeta, mais dispersas e com maior qualidade.

O gerenciamento e organização de bancos de dados evoluíram graças às novas tecnologias (LYON, 1994, p. 48). As máquinas (computadores, aparelhos celulares, dentre outros) estão conectadas ao ciberespaço de modo que podem se utilizar de memória e de cálculo de outros aparelhos da rede. "Todas as funções da informática são distribuíveis e, cada vez mais, distribuídas" (LÉVY, 2010, p. 44). De modo que todas as ações realizadas na rede informacional podem, por meio das novas técnicas, ser rastreadas e arquivadas. Neste sentido, Bruno (2013, p. 123) afirma que toda ação realizada na estrutura nesta rede de comunicação "deixa um rastro potencialmente recuperável, constituindo um vasto, dinâmico e polifônico arquivo das escolhas, interesses, hábitos, opiniões das pessoas"[21]. Com o avanço tecnológico e diminuição dos custos de obtenção de informações pessoais, passou a ser fácil obter dados, tais como as preferências do consumidor. Algo muito útil e valioso quando se pensa em marketing comercial. Informações que antes eram de difícil acesso e estavam à margem das relações comerciais começam a se tornar mercadorias, compradas e vendidas (LYON, 1994, p. 45).

Por outro lado, as mesmas informações úteis para o marketing comercial também podem beneficiar serviços sociais. Por exemplo, tais informações podem ser usadas para mapear os cidadãos que necessitam de determinado serviço público, dando ferramentas para a Administração Pública ser mais eficiente e assertiva na disponibilização de serviços públicos, bem como melhorar o planejamento dos serviços ofertados. Nesse sentido, Lyon (1994, p. 96) faz referência ao sistema Health Number, implantado em 1990 no Canadá.

Inegável é que todas essas mudanças despertaram novas formas de sociabilidade, um novo mercado, uma nova forma de vida urbana – as pessoas estão conectadas e interligadas em redes o tempo todo –, e os serviços tanto públicos como privados passam a se moldar

21 Empresas e Estados conseguem hoje absorver uma gama enorme de informações pessoais, detalhando a vida do individuo com facilidade. Dados como situação financeira, registros de saúde, preferências do consumidor, transações de telefone, elegibilidade de bem-estar, residência, nacionalidade e formação étnica, experiência educacional e atividades criminais estão prontamente disponíveis por contas utilizadas das novas tecnologias (LYON, 1994, p. 83). Tais informações circulando entre os centros de processamento são capazes de compreender dados sobre as pessoas e suas ações, uma vez que os eventos cotidianos da vida são armazenados sistematicamente de forma legível por máquinas que, usualmente, são transmitidos para outras máquinas viajando de dentro do setor privado para setores governamentais, utilizados para a segurança estatal como também para operações comerciais (DONEDA, 2006, p. 175-176).

dentro desse novo meio ambiente tecnológico (CASTELLS, 2020, p. 441). A utilização de tecnologias derivadas da Revolução Tecnológica não significa que elas serão usadas apenas para o bem, ou para o mal, ou para ambos; logo, cabe ao homem realizar algumas escolhas no tocante à utilização desses dispositivos e delimitar os usos que podem ser feitos deles (DONEDA, 2006, p. 53). Afinal, por detrás das tecnologias existem pessoas com ideias, sonhos, utopias, interesses econômicos, estratégias de poder, etc. Logo, dar um único conceito à técnica como boa ou ruim, bem como dizer que ela é neutra[22], pode gerar ambiguidades (LÉVY, 2010, p. 24).

Por tal razão, Lemos (2014, p. 115-117) adverte que os limites às tecnologias serão ditados pelo Direito, mas um direito robusto que impeça práticas que violem a ética e os direitos fundamentais. Sendo importante afastar o pensamento de que mudanças não são possíveis, por característica técnica da rede ou por ser algo inevitável da sua utilização. Muito pelo contrário, o modo de operar as tecnologias é uma escolha humana. Pessoas que ditam como as máquinas vão operar, bem como que dados irão coletar e armazenar. São pessoas que arquitetam as redes e, também, são pessoas que definem os usos. Logo, é possível ditar limites e proteger a dignidade de todas as pessoas humanas.

2.2 PRIVACIDADE

A privacidade, segundo Cancelier (2017, p. 52), é uma necessidade eminentemente humana. Para uma melhor compreensão da privacidade precisamos analisar a sua história recente e as alterações que sofreu ao longo do tempo por influência das organizações econômicas, sociais e políticas de cada período, sendo imperioso identificar a própria evolução do conceito ou aquilo que representa numa perspectiva histórica e jurídica (CACHAPUZ, 2006, p. 43). Ademais, de acordo com Solove (2008, p. 754), a discussão social e filosófica sobre a conceituação da privacidade normalmente é esquecida nos debates

22 "Uma técnica não é nem boa, nem má (isto depende dos contextos, dos usos e dos pontos de vista), tampouco neutra (já que é condicionante ou restritiva, já que de um lado abre e de outro fecha o espectro de possibilidades). Não se trata de avaliar seus 'impactos', mas de situar as irreversibilidades às quais um dos seus usos nos levaria, de formular os projetos que explorariam as virtualidades que ela transporta e de decidir o que fazer dela" (LÉVY, 2010, p. 26). Em sentido semelhante Doneda (2006, p. 42) afirma que a tecnologia precisa ser analisada a partir de seu perfil dinâmico, pois por meio dele é possível abranger o máximo dos efeitos da tecnologias e colocar em questão todos os seus aspectos relevantes, visto que a realimentação que a sociedade fornece à tecnologia depende também de juízos de valor. Por outro lado, se considerar a tecnologia como um perfil estático ligada apenas ao seu aspecto utilitarista – o de ferramenta, instrumento para atingir um fim – consequentemente, neutralizaria o discurso em torno da tecnologia.

jurídicos. Problemas que envolvem privacidade são debatidos sem se analisar o conceito de privacidade, sem adentrar no seu valor e significado. Tal análise é fundamental para o enfrentamento dos problemas que envolvem essa temática. Até porque todas as pessoas possuem um conceito implícito de privacidade. No entanto, a conceituação do significado do que é privacidade não aparece nos julgados e discussões jurídicas e legislativas com a exuberância que o tema demanda.

A revolução da tecnologia trouxe alguns problemas antes desconhecidos, alterando noções clássicas de público e privado. Neste sentido, Doneda (2006, p. 60) constata que é razoável considerar que a privacidade sempre esteve "diretamente condicionada pelo estado da tecnologia em cada época da sociedade". Inclusive, continua o mencionado autor, as soluções jurídicas apresentadas e consolidadas foram respostas aos problemas que surgiram com o advento de novas tecnologias que alteraram a condição da informação e o modo de propagação da mesma. Ademais, a privacidade acaba sendo tema de destaque no Brasil e no mundo, pois há um vínculo entre inovação tecnológica, força motriz na sociedade atual, e a potencial corrosão de valores fundamentais, motivos pelos quais a discussão sobre esse tema está longe de um fim, apesar das recentes reformas legislativas ocorridas tanto no Brasil como em diversas outras partes do mundo (ZANATTA; ABROMAVAY, 2019, p. 423).

Não pretendemos neste trabalho remontar toda a história do conceito de privacidade, que foi ganhando forma e se moldando de acordo com o tempo e a sociedade existente. Porém, para compreender o estado atual, precisamos regressar alguns anos, mais especificamente para o ano 1890 – data de publicação do famoso artigo de Samuel Warren e Louis Brandeis na *Harvard Law Review*, intitulado de "The Right to Privacy" [O direito à privacidade], que definiu a privacidade como um "direito de ser deixado só" (CORRÊA, 2016, p. 12). O referido artigo se enquadra como o grande marco doutrinário, pois o estudo chamou a atenção para o direito à privacidade de forma autônoma e protagonista, encontrando uma solução para os anseios da burguesia norte-americana do século XIX, que demonstrava elevada preocupação com o modo intrusivo com que os novos aparatos tecnológicos (fotografia[23], jornais) passaram a adentrar os domínios da vida privada e doméstica

23 "Em 1889, tirar fotos instantâneas era descrito como um hobby comum e até mesmo uma mania. Com câmeras automáticas baratas oferecidas aos consumidores, a frase 'demônios da Kodak 'entrou para o vernáculo. [...] Surgiu um novo tipo de invasões, seja de caçadores de fotos esperando fotos inocentes dos desavisados ou da imprensa urbana de massa. A súbita onipresença da fotografia e dos fotógrafos na América

(MENDES, 2008, p. 27). Neste sentido, os mencionados autores buscavam encontrar uma resposta adequada para abrigar a esfera privada das pessoas sem que isso estivesse necessariamente ligado a uma noção patrimonial. Houve a tentativa de relacionar esse direito a um patrimônio imaterial (CACHAPUZ, 2006, p. 77). Bem como, houve a tentativa de demonstrar a existência de um direito com aspectos imateriais, uma forma de tutelar a personalidade de seu titular, distanciando a sua tutela de uma matriz proprietária utilizada até então para proteger aspectos da vida privada (CANCELIER, 2017, p. 76).

A motivação do artigo surgiu pela necessidade do reconhecimento da possibilidade de as pessoas não serem perturbadas em momentos nos quais não existe interesse ou vontade de que sejam conhecidos por todas as pessoas de uma comunidade. Buscava-se demonstrar que existia uma garantia de imunidade contra a intrusão da vida privada (ZANATTA; ABROMAVAY, 2019, p. 43). O fato que impulsionou a redação do artigo foi a divulgação não autorizada, na imprensa da época, de detalhes íntimos do casamento de Samuel Warren, que posteriormente tomou posse como juiz da Suprema Corte dos EUA[24] (CANCELIER, 2017, p. 76), razão pela qual o artigo começa descrevendo as ameaças existentes nas novas tecnologias, que penetram os espaços sagrados e privados dos lares, ameaçando tornar real a profecia de que "aquilo que é sussurrado no quarto será proclamado nos telhados" (LEONARDI, 2011, p. 53 e CANCELIER, 2017, p. 77). Essas intrusões, segundo os autores, causavam dor e angústias no espírito do homem, superando meros danos pessoais (BOFF, 2018, p. 64), pois a dor e a angústia mental causada pela invasão à privacidade são muito superiores às dores físicas (BRANDEIS; WARREN, 1890, p. 2).

Brandeis e Warren (1890, p. 2) afirmam que a intensidade e a complexidade da vida, juntamente com os avanços da civilização[25], fazem surgir a necessidade ao homem de ter um

---

do final do século XIX, argumenta a historiadora Jessica Lake, 'alterou radicalmente a experiência de ver e ser visto por outras pessoas'" (IGO, 2018, p. 30).

24 Os autores, além das novas tecnologias, viam com preocupação a "indústria dos jornais", fazendo uma alusão aos jornais extremamente sensacionalistas, voltados à veiculação de boatos, rumores e fofocas a respeito das pessoas importantes do momento. "Não se pode perder de vista, também, que Warren tinha uma motivação especial para escrever o artigo, qual seja, a cobertura sensacionalista de seu casamento com Mabel Bayard, filha do senador norte-americano Thomas F. Bayard" (LEONARDI, 2011, p. 52).

25 No período em que Warren e Brandeis escreveram o artigo, houve inúmeros avanços tecnológicos, dentre os quais se destacam: "a máquina de escrever comercial (1874), o microfone (1876) e o ditafone (1889) – permitiram que as informações fossem transferidas de maneira ainda mais precisa e eficiente. Enquanto isso, a transmissão de imagens foi revolucionada com a introdução da fotogravura em 1881 e do filme em rolo em 1889. Cada uma dessas tecnologias carregava o potencial de alterar a forma como as notícias de natureza pública e privada viajavam. Palavras e imagens poderiam ser disseminadas com muito mais rapidez e suavidade por esses meios – mas também com menos segurança. Assim, os novos meios de comunicação do final do século XIX, assim como os de hoje, fascinavam e perturbavam seus usuários" (IGO, 2018, p. 26).

espaço solitário, um espaço privado. Para eles, a base da privacidade seria "a inviolabilidade da personalidade, e não a propriedade privada; seu valor não está no direito de receber indenização em decorrência da publicação", porém na segurança de não virar de conhecimento público aspectos da vida privada, bem como na paz de espírito e tranquilidade de não sofrer nenhum tipo de exposição (LEONARDI, 2011, p. 53).

A privacidade protegeria qualquer pessoa, independentemente de status ou posição, de serem expostos aspectos da sua vida que não tenham qualquer interesse coletivo, protegendo as pessoas de uma publicidade indesejável e indesejada, sobre assuntos que não tenham nenhuma vontade de compartilhar com os demais (BOFF, 2018, p. 65 e CANCELIER, 2017, p. 78).

Rodotà (2008, p. 16) afirma que "The Right to Privacy" fez surgir um entendimento no qual a privacidade protegia a livre manifestação dos sentimentos e manifestação dos pensamentos, bem como um livre desenvolver da personalidade. Dessa forma, ela também protegeria as minorias e opiniões dissonantes.

No entanto, conforme bem delimitado por Leonardi (2011, p. 53), Warren e Brandeis não apresentaram uma definição para o termo privacidade, apenas afirmaram que o direito norte-americano permitia a cada pessoa o direito de determinar se expressará ou não seus sentimentos e emoções aos demais. "Esse direito de ser deixado só é, para eles, um direito geral à imunidade da pessoa, o direito à sua própria personalidade" (LEONARDI, 2011, p. 53). Para Cancelier (2017, p. 79), a principal contribuição do texto é a desvinculação do direito à privacidade dentro da ideia de propriedade material. O destaque estaria na afirmação de que o respeito à privacidade estaria concedido pelo direito de a pessoa "pensar, sentir e emocionar-se" efetuando o "resguardo à inviolabilidade da personalidade do indivíduo".

Contudo, o direito a ser deixado só não representa exatamente o conceito de privacidade. Tal ideia é um conceito vago que não serve como guia para definir o escopo de proteção da privacidade. No decorrer das páginas do mencionado artigo não é apresentado em nenhum momento em quais situações nem sobre quais assuntos as pessoas têm o direito a serem deixadas em paz. Tal conceito apresenta falhas, uma vez que é demasiadamente amplo, de modo que se pode interpretar que "qualquer conduta direcionada a outra pessoa, quer ilícita ou não – uma agressão física, ou simplesmente pedir informações – seria uma violação de sua privacidade" (LEONARDI, 2011, p. 54).

Apesar de o conceito de privacidade como direito a ser deixado sozinho ser vago, não se pode negar que o artigo faz emergir uma importante discussão sobre a privacidade, e o faz ligando esse conceito a ideias de propriedade imaterial e liberdade, que estão unidas enquanto "liberdade estiver associada à não interferência e à razão individual". Entretanto, o conceito de privacidade foi sofrendo transformações ao longo do século XX em decorrência das mudanças sociais, econômicas e culturais que advieram (DAINEZI, 2019, p. 97). Neste sentido, Silveira et al. (2016, p. 218) reforçam que a ideia que as pessoas têm de privacidade muda de acordo com as tecnologias de intrusão, invasão dos espaços pessoais, não públicos; porém, além desses fatores, existem diferentes formas de entender a privacidade envolvendo práticas discursivas, visões de mundo, ideologias e, inclusive, interesses econômicos.

A privacidade é um conceito que ainda não detém um consenso sobre o que ela exatamente engloba, e quando tratamos sobre direito à privacidade essa falta de definição é percebida pela falta de clareza sobre o que deve ser protegido ou não, quais os seus limites e qual a sua abrangência. A explicação a tal fato pode ser correlacionada às diferenças existentes em cada cultura, o que gera uma noção diferente sobre privacidade. "As reivindicações de privacidade são interpretadas e aplicadas em diferentes sociedades, dependendo de suas expectativas culturais, históricas e práticas aceitas" (LIMA, 2018, p. 142).

> [...] A noção de privacidade é, até certo ponto, em relação à própria cultura, visto que o que é certo ou errado, bom ou ruim, com respeito à privacidade é em parte determinado culturalmente. Ou seja, a forma como as reivindicações de privacidade são interpretadas e aplicadas nas diferentes sociedades também depende das expectativas culturais, da história, das práticas aceitas, das leis existentes, entre outros fatores, de onde deriva sua alta complexidade e amplo espaço para controvérsias (LIMA, 2018, p 143).

Solove (2008, p. 754), citando autores como Arthur Miller, Hyman Gross e Colin, relata que o conceito de privacidade pode ser entendido como de pouca utilidade, pois para esses autores é um conceito confuso, infectado de ambiguidades, e que em todas as tentativas de definição de privacidade foram incapazes de realmente definir o que a privacidade é. Dentre as várias conceituações de privacidade, ditas como fracassadas, Solove (2008, p. 754) percebe que os autores buscavam definir a essência do conceito, o seu núcleo duro, sua característica principal, capaz de identificar e classificar várias situações dentro do conceito de privado. Contudo, da leitura das definições de privacidade ao longo da história, esta possui sentidos diversos, mudando de pessoa para pessoa. No seu sentido clássico, conforme

definido por Warren e Brandeis, privacidade é o direito de ser deixado em paz; para Westin ela é entendida como o controle e proteção de informações pessoais; por outro lado, Schoeman afirma que privacidade é um aspecto de dignidade, autonomia e liberdade[26] (ACQUISTI et al., 2016, p. 2).

Dentro de uma perspectiva histórica, a privacidade na década de 1970 manteve muito da ideia inicialmente apresentada por Warren e Brandeis[27] como sendo um "desejo por isolamento e anonimato". Contudo, ela começou a se transformar por conta das mudanças urbanísticas e principalmente pela entrada de tecnologia na vida das pessoas, que começaram a ter uma preocupação em relação à disseminação de informações pessoais (BOFF, 2018, p. 67).

Em cada período histórico da humanidade a privacidade ganhava contornos diferenciados e, por essa razão, a privacidade é um conceito de difícil definição, "justamente em função de seus contornos indefinidos, afinal a noção de privado acompanha o desenvolvimento da Sociedade e, por lógica, do ser humano" (CANCELIER, 2017, p. 53). No entanto, analisando a obra de Daniel Solove (2008, p. 755), retira-se que o autor examinou inúmeros conceitos de privacidade, tanto no campo jurídico como no filosófico, na busca de um núcleo em comum entre os vários conceitos existentes. Nessa análise o autor percebeu que a privacidade poderia ser entendida como intimidade, porém entender a privacidade apenas como intimidade seria equivocado, pois ela é mais ampla que apenas aspectos relacionados com a intimidade. Por outro lado, Solove também visualizou problemas em conceituar a privacidade de um modo muito amplo, como realizado por Warren e Brandeis. Nesse caso, o "direito de ser deixado sozinho" significa muitas coisas, pois há inúmeras formas de as pessoas se sentirem invadidas que não são propriamente uma violação de privacidade – se a

26 Em igual sentido, para Zanatta e Abromavay (2019, p. 423) a privacidade não pode ser vista dentro dos moldes clássicos de garantia de uma imunidade contra a intrusão da vida privada, como sustentou Louis Brandeis em 1890. Também não pode ser vista como capacidade de controlar os fluxos de dados produzidos por um indivíduo, como sustentou Alan Westin em 1968.

27 Além do contexto histórico e tecnológico de cada tempo para definir o entendimento sobre o que seria privacidade, Rodotà (2008, p. 28) também traz à luz características pessoais dos autores que são referenciados como os "pais da privacidade", pois, para o referido autor, "para compreender a real dinâmica à qual está ligado o conceito de privacidade, é necessário considerar, sobretudo, as diversas funções a ele atribuídas segundo a cultura comum a cada grupo. Foram oportunamente esclarecidas as distintas inspirações que moveram os próprios 'pais fundadores' da privacidade em terreno jurídico, Warren e Brandeis. O primeiro, um conservador de cunho tradicional, mostrava-se interessado somente nos privilégios da alta burguesia, encarando com ressentimento a ação da imprensa à caça de escândalos políticos e mundanos; o outro, liberal-progressista, ainda que preocupado com a privacidade das pessoas de maior projeção, enfatizava o dano que poderia derivar das indiscrições jornalísticas às minorias intelectuais e artísticas, podendo provocar o aumento da impopularidade destes".

pessoa recebe um empurrão ela será prejudicada, porém não teve a sua privacidade violada (SOLOVE, 2008, p. 755).

Neste sentido, Solove (2008, p. 755-759) relata um dilema difícil de resolver, pois, ao tratar privacidade dentro de um conceito mais abrangente, corre-se o risco de o conceito ser muito inclusivo ou muito vago, ao passo que, se se escolhe um conceito mais específico, a concepção pode ser muito delimitada. Por tal razão, o autor conclui que o foco deve ser na solução dos problemas, que existem independentemente da concepção que se dá para privacidade. Se existem vários problemas envolvendo privacidade, o valor da privacidade será alterado de acordo com o seu dano ou o problema do caso concreto. Nem todos os danos serão iguais, nem todos os problemas envolvendo as várias concepções de privacidade são iguais; alguns são mais prejudiciais que outros, porém não deixam de serem problemas. Por tal razão, Solove (2008, p. 763) afirma que o valor da privacidade depende da situação (problema), o conceito de privacidade e o seu valor são definidos de modo pluralístico, pois a privacidade é, para o autor, um conjunto de proteções contra um conjunto de problemas relacionados com a privacidade. Esses problemas não estão relacionados da mesma forma, nem dizem respeito às mesmas coisas, porém eles se parecem. Por exemplo, existe diferença significativa entre utilização de dados de terceiro pelo governo ou quando agentes federais invadem uma casa. São problemas diferentes, mas ambos envolvem questões de privacidade.

Contudo, nesse ponto é importante destacar que nos Estados Unidos, país em que a obra de Solove foi escrita, não existe uma legislação específica para proteção de dados, bem como não existe uma norma que proteja direitos de personalidade de modo geral. Assim, existe um movimento de tentar enquadrar essa proteção na Quarta Emenda[28], buscando alargar o conceito de privacidade (*privacy*). Porém, no direito brasileiro existe um sistema de proteção da personalidade para proteger tanto a privacidade quanto os dados pessoais (BIONI, 2020, p. 96)[29]. A contribuição da obra de Solove é a concepção de que a privacidade possui várias facetas e pode ser entendida de modo pluralista, bem como podem existir problemas de privacidade pela utilização de dados pessoais.

---

28 Por tal razão o autor apresenta ao debate que o Supremo Tribunal dos Estados Unidos não reconhece que as pessoas têm proteção da Quarta Emenda sobre os dados coletados pelo governo federal, pois as pessoas não têm uma expectativa razoável de privacidade nas informações expostas para outros (SOLOVE, 2008, p. 764).

29 Em sentido semelhante, Sawaris (2017, p. 64) apresenta o entendimento de Paulo Mota Pinto de que não se deve confundir "o direito à reserva sobre a intimidade da vida privada com o direito à proteção da vida privada e a *privacy*. Segundo o autor citado, a *privacy*, reconhecida no direito norte-americano, tem uma amplitude que se aproxima no Direito português do conteúdo do direito geral de personalidade".

A privacidade, em muitos casos, não é ameaçada pela utilização ou coleta de alguns dados pessoais, mas por uma série lenta de aspectos menores, cedidos pela pessoa, que começam, gradualmente, a serem somados, piorando quando retirados de contexto. Solove (2008, p. 769), citando a obra de Bartow, aponta que na maioria dos casos os problemas de privacidade não estão relacionados com uma grande exposição, fazendo uma analogia a um problema ambiental como um grande vazamento, mas sim como poluição gradual realizada por uma multidão de diferentes atores, mas que no fim criam problemas mais impactantes.

É importante ressaltar que entender a privacidade como um conjunto de proteções contra uma pluralidade de problemas distintos relacionados entre si já recebeu críticas da doutrina nacional. Leonardi (2011, p. 84-90), ao analisar a obra de Daniel Solove, tece importantes comentários, principalmente quanto à importação de seus conceitos para o Brasil, pois precisa-se analisar que soluções propostas por Solove foram pensadas para um sistema de *commom law* que tem como a solução do caso concreto sem se preocupar com a formação de um sistema normativo. Ademais, "pela rejeição à existência de qualquer ponto central falta-lhe qualquer referência à dignidade da pessoa humana" (LEONARDI, 2011, p. 88), princípio consagrado no ordenamento pátrio.

Para Leonardi (2011, p. 85), quando Solove conceitua a privacidade como um "conjunto de proteções contra uma pluralidade de problemas distintos, relacionados entre si", como se esses problemas não estivessem ligados a um núcleo comum, existe ligação entre elementos, porém não necessariamente ao mesmo elemento – "os problemas compartilham semelhanças de família entre si". Logo, percebe-se que Solove rejeita a ideia de um conceito de privacidade em termos gerais, como uma categoria unitária e abrangente. O conceito de Solove estaria voltado para o caso prático, o problema que envolve um conflito de privacidade (LEONARDI, 2011, p. 86).

> Para Solove, um conceito plural não significa o abandono da expressão "privacidade", ainda que diversas questões de privacidade sejam diferentes entre si e que não tenham um característica essencial em comum, ainda assim compartilham muitas semelhanças importantes, e que a palavra "privacidade" mantém sua utilidade como um atalho, como uma maneira de falar coletivamente sobre uma rede de coisas conectadas, ainda que distintas (LEONARDI, 2011, p. 86).

Dentre os problemas de privacidade, ela poderia ser dividida em quatro gêneros de dezesseis espécies. Os gêneros seriam: 1) coleta de informações; 2) processamento de informações; 3) disseminação de informações, e 4) invasão. No gênero "coleta de

informações" as espécies de problema de privacidade podem ser divididas em: (a) vigilância e (b) interrogação. Em "processamento de informações" subdivide-se em cinco espécies: (a) agregação, (b) identificação, (c) insegurança, (d) uso secundário e (e) exclusão. Em "disseminação de informações" as espécies são (a) quebra de confidencialidade, (b) revelação, (c) exposição, (d) aumento da acessibilidade, (e) chantagem, (f) apropriação e (g) distorção. Por fim, "invasão" encontra-se dividida em (a) intrusão e (b) interferência em decisões.

No tocante às espécies, Leonardi (2011, p. 87) sintetiza as explicações de Solove da seguinte forma:

> a) *vigilância*: ver, ouvir ou gravar as atividades de um individuo; b) *interrogação*: questionar ou sondar um indivíduo para obter informações; c) *agregação*: combinar diversos fragmentos de dados esparsos sobre um determinado indivíduo, d) *identificação*: estabelecer uma ligação entre uma informação e um determinado indivíduo; e) *insegurança*: descuido na proteção de informações armazenadas, gerando vazamentos ou acesso indevido aos dados; f) *uso secundário*: utilização de informações originalmente coletadas com determinado propósito para uma outra finalidade, sem o consentimento do indivíduo: g) *exclusão*: negar ao indivíduo a possibilidade de saber quais dados e informações, previamente coletados, são do conhecimento de terceiros, bem como a possibilidade de controlar seu processamento e sua utilização; h) *quebra de confidencialidade*: ignorar um dever de sigilo de informações, previamente estabelecido; i) *revelação*: veicular informações verdadeiras que causem impacto à reputação de um indivíduo; j) *aumento da acessibilidade:* amplificação do acesso a uma determinada informação; k) *chantagem:* ameaçar revelar publicamente informações a respeito de um indivíduo; 1) *apropriação*: usurpar a identidade de um indivíduo em benefício de outro; m) *distorção*: disseminar informações falsas ou deturpadas a respeito de um indivíduo; n) *intrusão*: praticar atividades invasivas que interfiram na tranquilidade ou solidão de um indivíduo; o) *interferência em decisões*: a incursão do Estado nas decisões de aspectos da vida privada de um indivíduo (LEONARDI, 2011, p. 87-88).

De acordo com a explicação sobre as espécies, percebe-se que podem ser retiradas dois tipos de proteção, uma envolvendo a proteção aos dados pessoais e outra envolvendo a privacidade. Em algumas espécies parece existir tanto um problema de privacidade como um problema de proteção de dados pessoais, como pode ser observado na "interrogação", "agregação", "insegurança", "aumento da acessibilidade", "chantagem" e "interferência de decisões". Ao passo que a "vigilância", "quebra de confidencialidade" e "intrusão" são espécies ligadas ao conceito clássico de privacidade. Já as espécies da "identificação", "uso secundário", "exclusão", "apropriação" e "distorção" estão mais ligadas ao problema de proteção de dados e não tanto com a privacidade, apesar de que esses problemas podem se sobrepor. Com base nesse raciocínio, o modelo proposto por Solove analisa inicialmente a pessoa diretamente prejudicada pelo uso de dados pessoais, incluindo nesses aspectos

problemas do processamento de dados, tais como: “coleta, armazenamento, combinação, manipulação, pesquisa e utilização”; nesse primeiro momento destaca-se os problemas envolvendo proteção de dados pessoais e algumas situações que podem levar a um dano à privacidade do indivíduo; a seguir, o modelo “trata da disseminação da informação, procedimento que fica mais distante do controle do indivíduo”. Nesse aspecto também percebe-se que a proteção de dados ganha tons de protagonista, porém em algumas situações podem surgir, também, problemas de privacidade; “e, por fim, trata das invasões, ou seja, de procedimentos que causam danos diretos aos indivíduos” – nesse aspecto a privacidade é a que se destaca na violação (LEONARDI, 2011, p. 88).

Apesar das ressalvas na utilização do modelo proposto por Solove, Leonardi (2011, p. 89) admite que ele pode ser útil para sistemas legislativos a exemplo do brasileiro, principalmente porque o conceito plural e fragmentado de privacidade possibilita enxergar a privacidade segmentada em inúmeros conceitos e fica mais fácil compreender com base nessa segmentação as diferenças entre a privacidade e a proteção de dados, e que em determinados momentos elas se encontram. O modelo proposto por Solove, então, auxilia, pois a taxonomia permite “identificar as situações mais comuns que ameaçam a privacidade” (LEONARDI, 2011, p. 89).

A necessidade de formular um conceito sólido de privacidade possui implicações práticas, pois, como bem enunciado por Rodotà, (2008, p. 31) a dignidade humana não pode ser protegida por meio de enunciados e referências genéricas que, colocadas à luz do caso concreto, tenham soluções muito diferentes. A privacidade precisa ser protegida em todas as situações e em todos os tipos de relações, pois, “caso contrário, coloca-se no mesmo nível de inúteis, ainda que consoladores, desafogos paroquiais” (RODOTÀ, 2008, p. 31).

O conceito de privacidade sempre esteve muito ligado com a dicotomia público e privado. Nesse sentido, o enfoque dado era que algumas atividades eram realizadas na esfera pública, como a vida política e outras atividades estariam ligadas à vida privada (BIONI, 2020, p. 91). Privado estaria relacionado ao ambiente familiar, íntimo e pessoal, em oposição ao público, que estaria na esfera da política, da vida em sociedade, da cidadania, da opinião coletiva e até mesmo no Estado[30] (CANCELIER, 2017, p. 58).

30 “Nomeadamente quando se emprega o conceito de público como sinónimo do conceito de *estatal*. A partir do século XVIII, a afirmação da sociedade civil perante o domínio estatal é designada como *esfera pública*, portanto, embora aquilo que é do domínio do Estado seja designado com o conceito de público, a

Neste sentido, a casa "estabeleceria os contornos dessa dicotomia, sendo, por excelência, o espaço para que as pessoas se refugiassem do escrutínio público"[31] (BIONI, 2020, p. 91). A privacidade estaria protegida, uma vez que permitiria a pessoa de se isolar dos demais, da comunidade, do espaço público e se recolher em sua residência, seu espaço privado.

No entanto, a privacidade não possui uma relação direta com o local, como a casa ou o espaço de trabalho (escritório), a privacidade pode estar relacionada com a consciência de cada pessoa (crenças religiosas, afinidades político-partidárias e morais) e a sua vontade ou não de tratar sobre esses assuntos, e esse controle de sua privacidade pode se dar dentro de casa, bem como pode manter esses assuntos privados mesmos estando na rua (CORREIA, 2018, p. 28). Adriana Sawaris (2017, p. 66-67), ao defender que o local não é determinante para definir aspectos da vida pública ou privada, apresenta o exemplo de uma discussão matrimonial ocorrida em um restaurante: "apesar do local ser público, as palavras proferidas pelo casal estão sob a proteção da reserva da intimidade e sobre a vida privada".

Em igual sentido, Cancelier (2017, p. 59), ao trabalhar a obra de Habermas, descreve que a privacidade não está em oposição ao público, mas sim a indiscrição. Logo, se privacidade não se encontra em choque com o público, existe "a possibilidade para o exercício da privacidade em público, entendimento essencial para compreensão do que é a privacidade contemporânea" (CANCELIER, 2017, p. 59). Por tal razão, a dicotomia público-privado apresenta dificuldades de conceituação semântica, o que acaba deixando ambíguo seu significado, pois não deixa claro do que essa dicotomia trata (CORREIA, 2018, p. 33). A privacidade se faz presente em casa, porém também pode existir na rua, na praça, no trabalho, tanto para pessoas desconhecidas como para celebridades (CANCELIER, 2017, p. 59). A diferença entre público e privado independe "da natureza intrínseca dos seus conteúdos. Isto

própria contraposição ao Estado é também, ela própria, designada com o conceito de *público,* como sucede neste caso em autores como Habermas" (CORREIA, 2018, p. 26). O espaço público passou a ser utilizado como arena para discutir o monopólio Estatal da coisa pública pela burguesia emergente do século XVII e XVIII, havendo uma ascendência da esfera social. Os espaços passaram a abrigar não apenas a política do Estado e sua administração, mas também a sociedade, espaços em que as pessoas podiam discutir, avaliar e analisar as suas ideias (CORREIA, 2018, p. 27). Nesse período, adentrando na modernidade, a ascensão da classe burguesa, cria uma nova dicotomia: a social-individual, "o privado passa a ser também social, sendo o terreno das trocas e do comércio. O Estado aparece como elemento que possibilita uma melhor definição dessas esferas e as concepções de social dividem-se, manifestando-se como o *social-público* (área da política) e o *social-privado* (área do econômico)" (CANCELIER, 2017, p. 25).

31 Por tal razão, alguns autores como Vieira (2007, p. 32), afirmam que os ingleses no século XVI protegiam indiretamente a privacidade das pessoas, pois existia um princípio em relação à inviolabilidade do domicílio, por meio do brocardo *man's house is his castle* (a casa do homem é o seu castelo).

significa que público e privado não são fundamentados ontologicamente, mas que são relacionais" (CORREIA, 2018, p. 33).

Assim, para melhor compreender o conceito de público e privado, utiliza-se a teoria das esferas de Hubmann. Segundo Marineli (2017, p. 85-87), o autor alemão foi o primeiro a visualizar âmbitos de proteção distintos para a privacidade. Ele dividiu a vida privada em três círculos concêntricos, um dentro do outro: a) a esfera privada – o círculo que contém a maior circunferência, guardando as relações interpessoais mais superficiais. As pessoas nessa esfera não precisam manter acesso íntimo, o contato pode ser eventual, as informações obtidas nessa esfera são acontecimentos casuais, no entanto o resto da coletividade não tem acesso; b) a esfera do segredo – é a esfera do meio, estando dentro da camada anterior. Aqui as informações são compartilhadas com um número menor de pessoas, sendo apenas aquelas que fazem parte da vida cotidiana da pessoa, como família e amigos íntimos, tendo acesso a segredos dessa pessoa; c) a esfera íntima – aqui é a esfera de menor raio, representando o maior grau de intimidade e tutela da pessoa de todo e qualquer acesso por parte de quem quer que seja, em grau irrestrito, longe do conhecimento de todos. Deste modo, percebe-se que a intenção do autor foi dar maior proteção à privacidade da pessoa na medida em que o raio de alcance das esferas diminui. Heinrich Henkel, após a publicação da teoria de Hubmann, em 1957, reelaborou a teoria das esferas, adicionando o segredo no centro da esfera. A intimidade nesse modelo passou a ser um circulo intermediário. Henkel dividiu a vida privada em: esfera privada, esfera da confiança e esfera do segredo (da maior esfera para a menor esfera). Além disso, o autor acredita que mesmo na esfera do segredo pode ser acessado por poucas pessoas, amigos muito chegados, ao passo que Hubmann acreditava que a esfera do centro era uma esfera de proteção absoluta (MARINELI, 2017, p. 87). Em ambas as teorias, para fora das esferas estariam o espaço público de conhecimento de todos.

Neste sentido, os conceitos público e privado poderiam ser entendidos como camadas de uma cebola. A camada externa da cebola está dentro de outra que também estará dentro de outra camada, logo "aquilo que é público em relação a uma esfera da vida privada, pode também ser privado em relação a uma outra esfera, que é pública, e assim sucessivamente" (CORREIA, 2018, p. 33). Contudo, não há como tipificar com perfeição, em matéria de privacidade, uma esfera da outra (DONEDA, 2006, p. 109). Ademais, o grau de privacidade altera a depender do indivíduo: "aquilo que para algumas pessoas pode ser considerado apenas como privado, mas não íntimo, para outras pessoas pode ser considerado

íntimo, e não privado" (CORREIA, 2018, p. 29). Por tal razão, mais importante que se preocupar com esferas no âmbito teórico é analisar o relacionamento das pessoas com os outros. "Nesse campo, se há que distribuir estratos, não se encontra justificação para que sejam apenas três" (VASCONSELOS, 2014, p. 80).

Cancelier (2017, p. 89) aponta ser extremamente relevante o papel da vontade dos indivíduos quando se procura determinar se algo é íntimo ou faz parte da vida privada, sendo que cada pessoa irá estabelecer por meio de suas emoções e vivências o que é íntimo, o que é privado e o que pode ser público, dependendo do caso concreto que, juntamente com a vontade, vai sinalizar o contexto em que a informação ou a situação se dá, pois "nada é privado ou público em si mesmo, mas sim de forma contextualizada, e segundo o significado de cada um destes conceitos. As mesmas coisas que em determinadas situações são privadas, noutras são públicas" (CORREIA, 2018, p. 33). Assim, levando em consideração a vontade do indivíduo, a teoria das esferas é de grande valia para demonstrar que as informações possuem graus de importância para cada pessoa, de modo que sua revelação se dá de forma seletiva, "segredo, intimidade ou vida privada são as esferas que, com maior ou menor grau de intensidade, procuram delimitar os espaços da vida privada e pública" (BIONI, 2020, p. 92).

Contudo, não há como abandonar totalmente a dicotomia público-privado, devendo-se, outrossim, trabalhar ela com ressalvas, pois nem toda ação realizada em público é, realmente, pública. Existem ações realizadas em público que são privadas, nem todo movimento executado fora das fronteiras físicas da esfera privada terá como consequência a falta de proteção da privacidade (CANCELIER, 2017, p. 59-60).

Nesta perspectiva, Cancelier (2017, p. 98) desenvolve o conceito de integridade contextual trabalhado por Helen Nissenbaum (2011), em que a privacidade estaria relacionada com o conteúdo disponibilizado, com as pessoas envolvidas e com o local. Em outras palavras, a privacidade estaria relacionada com o contexto, devendo se ater para o conteúdo e quem são as pessoas envolvidas na situação fática. Existe uma proteção à privacidade, porém ela é flexibilizada para vivermos em sociedade. Por exemplo, em uma consulta médica, mesmo que o paciente realize exames e confesse ao médico suas dores e doenças mais vexatórias, essa informação continua sendo privada, mesmo com o relato do paciente ao médico. Mesmo com a inscrição dos resultados no laudo dos exames feitos pelo laboratório, não transformou-se a informação privada em pública, pois ela está dentro de um contexto que se entende como protegido pelo manto da privacidade. Sobre a privacidade dentro do contexto

hospitalar, vamos discorrer mais para frente, mas por ora podemos adiantar que são hipóteses em que se espera que a privacidade seja respeitada, aproximando-se, inclusive, com o sigilo.

Dificilmente haverá uma situação totalmente pública ou totalmente privada, pois algo inteiramente público, em todos os sentidos, seria algo "de todos, para todos, ser usado por todos, estar à vista de todos, todos saberem que existe e poder estar sob o controle de todos" (CORREIA, 2018, p. 24). Ao passo que algo totalmente privado seria exclusivo de uma pessoa, ser para ela, "ter vindo apenas dela, ser usada apenas por ela, não haver controlo exterior sobre o seu uso, não estar à vista de ninguém e apenas essa pessoa saber que existe" (CORREIA, 2018, p. 24). Ambas as situações, algo totalmente público ou totalmente privado, é impossível de existir, público ou privado são conceitos que interagem e acabam se fracionando, tendo limitações. Logo, nada pode ser inteiramente público ou inteiramente privado.

> Nenhum espaço é totalmente privado no sentido de ficar completamente, sob todos os pontos de vista, em relação a todos os outros indivíduos, em todos os momentos, e para todo o sempre, fora da autoridade pública, ou fora do olhar público, ou do uso público (CORREIA, 2018, p. 25).

A inserção da pessoa em determinados espaços depende do compartilhamento de informações: a relação médico-paciente precisa de informações de saúde; em uma relação profissional, informações sobre o ofício; em uma relação com a igreja, a crença que a pessoa profere e crê; na relação amorosa, as confissões a dois de sentimentos e afetos; em todos esses espaços existem informações compartilhadas, existe um fluxo de informações pessoais e privadas e são informações necessárias para que as pessoas realizem seus papéis e tenham uma convivência adequada em cada um desses ambientes, porém o compartilhamento dessas informações apenas se faz necessário dentro de um contexto, fora dele o fluxo informacional seria inapropriado, uma vez que o contexto é desvirtuado (BIONI, 2020, p. 199-200). O fato de a informação ser compartilhada no espaço privado ou público em nada define o seu caráter público ou privado. Existem informações reveladas em espaço público que são privadas, "como uma conversa entre dois amigos, na rua, na esplanada ou no banco do jardim"; bem como existem informações públicas feitas em espaços privados, tais como uma entrevista televisiva da casa de uma pessoa (CORREIA, 2018, p. 191).

Podemos afirmar que a privacidade apenas ganha forma quanto confrontada com o caso concreto. Sem os aspectos da realidade fática, a privacidade é apenas uma categoria

formal (CACHAPUZ, 2006, p. 127-128). A privacidade necessita que os atos privados se formem no mundo. Estes atos serão entendidos de acordo com o conteúdo e com a expectativa que existe que a informação mantenha-se em um espaço privado. Esta exclusividade pode se dar entre um grupo de amigos, família, ou internamente, tanto em um local fechado ou como num local aberto. O privado não é um local físico, mas sim uma expectativa que um conteúdo ou situação mantenha-se opaca para as demais pessoas. Nesse sentido, a privacidade está relacionada a um agir humano, bem como a expectativa de resguardo que este agir[32] deve ter.

A privacidade, então, protege situações e conteúdos frequentemente opostas ao social (CANCELIER, 2017, p. 57), de modo que a pessoa, ao se opor a esfera social, tem o poder de determinar quais aspectos de sua vida privada podem ser descortinados e quais ficam fora das luzes da publicidade (LEONARDI, 2011, p. 83). Esse afastamento do olhar dos demais é essencial ao ser humano, pois permite a pessoa "conhecer, construir, desenvolver e expressar" a sua personalidade (CANCELIER, 2017, p. 60). "Seria na esfera privada que as pessoas refletiriam e pensariam criticamente para voltar a público e discutir os mais variados assuntos" (BIONI, 2020, p. 91). Nesse sentido, a privacidade também é compreendida como uma liberdade, pois por meio dela as pessoas podem criar a sua personalidade sem a pressão social, formando a sua individualidade com base nas suas escolhas pessoais e compartilhar tais vivências de modo exclusivo[33] com pessoas selecionadas e não com todos (CANCELIER, 2017, p. 65).

Cancelier (2017, p. 66) afirma que apesar da dificuldade de definir privacidade em um único conceito, é razoável a constatação de que ela sempre estará relacionada ao nível de

---

32 Tal entendimento possui divergências, para Hartzog (2017, p. 14) existem algumas confusões em torno de informações particulares se manterem privadas mesmo em espaços privados. Segundo o mencionado autor, o caso Kartz vs. Estados Unidos é emblemático para ilustrar o problema. Na decisão do juiz Stewart, o magistrado começa seu texto explicando que a pessoa que deseja expor algo ao público, sabendo disso, mesmo que em sua própria casa ou seu escritório não pode evocar proteção à privacidade prevista na quarta emenda da Constituição americana, contudo mais a frente em sua decisão o mesmo juiz afirma que o que a pessoa busca preservar como particular, mesmo em área acessível ao público, pode existir proteção constitucional. Os conceitos apresentados foram interpretados de modo confuso pela doutrina, o que levou a maioria dos juízes nas decisões subsequentes serem fies a primeira parte da decisão de Stwart no caso Kartz vs. Estados Unidos, ou seja, nenhuma privacidade em público, sendo público e livre acesso tratados como sinônimos na maioria das decisões envolvendo proteção à privacidade (HARTZOG, 2017, p. 14).

33 Cancelier (2017, p. 65-66) explica que Hannah Arendt relaciona privacidade à exclusividade, a esfera privada é exclusiva, ao passo que a esfera pública é um local comum. A exclusividade é para Hannah Arendt um princípio que limita o direito à informação, limitando que fatos íntimos ou da vida particular das pessoas sejam divulgados indiscriminadamente. "Os fatos que contornam a individualidade de cada ser humano devem ser compartilhados de acordo com suas respectivas opções para que ele revele e desenvolva a sua personalidade" (BIONI, 2020 p. 92).

desenvolvimento tecnológico da sociedade. A nova prática social na Sociedade da Informação, no espaço virtual, em que os indivíduos confessam detalhes de suas vidas privadas pela alegria de serem notados nesse novo mundo, levou muitos autores a afirmarem que os limites entre os espaços públicos e privados foram apagados (BELLO, 2011, p. 140). Cancelier (2017, p. 42) alerta que, "com a popularização da internet", as pessoas começaram a expor a sua privacidade, exercendo um movimento de evasão de suas privacidades, "um movimento crescente em busca de exposição e audiência" (BELLO, 2011, p. 140). Pessoas comuns expõem suas vidas privadas com muita facilidade nas redes sociais em busca de protagonismo ou atenção dos demais membros da comunidade, transformando o privado em público.

> A vida privada do homem comum transformou-se numa espécie de espetáculo, numa banalização, levando a que todos os indivíduos se interessem por esta e a recebam como um assunto que lhes passa também a dizer respeito (CORREIA, 2018, p. 39).

Essa mudança de comportamento – a exposição de assuntos ditos como privados em público – levantou uma série de questionamentos sobre a existência da privacidade na sociedade hodierna. Autores como Bauman (2012, p. 24) passaram a afirmar que as pessoas estão matando voluntariamente o seu direito à privacidade, uma vez que a lógica da atualidade passou a ser a da maior visibilidade possível, como se existência só se tornasse significativa quando exposta ao público[34].

No entanto, como bem colocado por Cancelier (2017, p. 67), a exposição virtual não pode ser observada como uma futilidade, ou uma vontade de ser notado. A internet e o mundo on-line são a sociedade, o real e o virtual se misturam e se confundem, logo, influenciadas pela lógica do capitalismo conexionista[35], as pessoas são persuadidas a exporem

---

34 Complementa o autor que as pessoas aparentemente ficam felizes por revelar detalhes de sua vida privada, postar informações preciosas e compartilhar suas imagens nas redes sociais. Assim, "o medo da exposição foi abafado pela alegria de ser notado" (BAUMAN, 2012, p. 47).

35 Thibes (2014, p. 152-154) trabalha a ideia de capitalismo conexionista (ou terceiro capitalismo). Diferentemente do seu antecessor, volta a dar importância a aspectos da vida da pessoa, pois características individuais podem trazer benefícios para o sistema produtivo e saber quais os indivíduos que se enquadram nos padrões que o mercado entende por vantajosos poderá dar vantagens para algumas pessoas frente aos demais. "Os critérios de seleção passaram a privilegiar os mais adaptados às novas exigências do mercado de trabalho. Além dos tradicionais critérios de idade, sexo e nacionalidade, as provas que a sociedade contemporânea passou a exigir, por meio das quais se efetua a seleção social das pessoas e é decidido quais serão bem-sucedidas e quais não o serão, passaram a ser relacionadas às características de autonomia, empreendedorismo,

características pessoais e individuais para reconhecimento social, que poderão ser revertidas em aceitação entre os demais, melhores propostas de trabalho, conquistas amorosas e criação de amizades. Plataformas voltadas para os aspectos profissionais, como LinkedIn, outras voltadas mais para a sociabilidade, como Facebook e Instagram, porém também analisadas pelas empresas[36] e pelos demais indivíduos. Os objetivos das análises dos perfis expostos nas redes sociais são vários, tais como analisar características pessoais para saber se seria interessante começar ou não um relacionamento, romântico ou de amizade.

A imagem conta muito na nova sociedade e muitos de seus aspectos são construídos virtualmente. Por tal razão não é exagero falar que "em tempos de internet, não basta ter um bom currículo e obter bom desempenho durante as entrevistas de empregos, a imagem *online* necessita ser correspondentemente atrativa". Ter uma boa imagem no mundo virtual leva a benefícios reais, como um bom emprego e mais amigos (THIBES, 2014, p. 153-154). De modo semelhante, uma imagem on-line que não atenda às expectativas do mercado e da sociedade pode trazer consequências negativas para as pessoas[37]. Neste sentido, criar uma boa

---

equilíbrio psicológico (capacidade de suportar pressão), sociabilidade (para fazer contatos), entre outras tantas outras características pessoais, individuais, que devem ser cultivadas e reveladas".

36 "Uma pesquisa realizada pela empresa CareerBuilder descobriu que pelo menos 37% dos 2.303 gerentes e profissionais de RH pesquisados utiliza(va)m redes sociais para verificar potenciais candidatos. Isso significa que 2 em cada 5 companhias procuram informações online sobre seus candidatos, a fim de avaliar seu "caráter de personalidade". Acerca das razões do uso das redes socais com esse propósito, 65% afirmaram que o fazem para verificar se o candidato se apresenta "profissionalmente" online, 50% queriam saber se o perfil do candidato se encaixava na cultura da empresa e outros 45% queriam conhecer melhor suas qualificações." A mesma pesquisa foi capaz de demonstrar que um terço dos empregadores não contrataram candidatos por causa dos seus perfis on-line, fazendo alusão a fotos provocativas, informações inapropriadas ou evidência de uso de álcool e outras drogas, bem como demonstração de poucas habilidades de comunicação, posts ofensivos relacionados a antigos empregos, gênero, etnia ou religião. Por outro lado, os empregadores também mencionaram que empregaram pessoas com base nos seus perfis on-line – "o candidato criou uma boa imagem profissional ou apresentou evidências de que as informações de seu currículo eram verdadeiras. Houve ainda casos de postagens de boas referências sobre as candidatas feitas por colegas ou demonstração de qualidades, tais como criatividade, boas conexões e habilidades comunicacionais" (THIBES, 2014, p. 156-157).

37 Nesse sentido, a "professora americana Ashley Payne, de 24 anos, foi obrigada a pedir demissão de uma escola no estado da Geórgia (EUA), porque publicou fotos suas na internet em que ela aparece segurando bebidas alcoólicas", as fotos foram tiradas em 2009 durante suas férias na Europa e estavam publicadas em sua rede social, que nenhuma relação tinha com a escola, no entanto pais de alunos ao visualizarem suas redes sociais não gostaram, o que motivou o diretor da escola a pedir que Ashley pedisse demissão ou fosse suspensa por causa de suas publicações tidas como inapropriadas (G1, 2011). Thibes (2014, p. 155), também comentando sobre os efeitos negativos que a internet pode trazer para o indivíduo, apresenta a história de uma jovem que "durante sessão de apresentação da universidade para estudantes em fase de ingresso, postou, em seu perfil do Twitter, comentários desrespeitosos sobre os colegas presentes no mesmo evento", isto acabou lhe custando a negativa de admissão nas universidades. Ademais, as universidades admitem que realizem monitoramento on-line para seleção dos candidatos, justificando que por não existir uma política formal de admissão, recorrem à pesquisa on-line para suplementar o registro dos estudantes. No mesmo sentido, "em 2012, um estudante de graduação do Pitzer College, na Califórnia, denunciou um amigo do Facebook que estava concorrendo a uma vaga na universidade porque notou que o candidato havia postado comentários ofensivos sobre um dos seus antigos professores" o que acarretou na negativa da admissão do estudante.

imagem de si e apresentar ao público aspectos de sua vida privada se mostra essencial, porém, nesse ponto, precisamos ter cuidado em dizer que as pessoas estão abrindo mão de sua privacidade, pois ao criar um perfil mais vantajoso ou selecionar o que será postado ou não, de uma certa forma, as pessoas têm conhecimento de que essas informações estão indo a público – a privacidade não acabou – e o mesmo sentimento de necessidade de recato das sociedades burguesas se faz ainda presente. Aparece, outrossim, que junto com a privacidade outro direito da personalidade começa a se destacar, um direito que se relaciona com os dados pessoais públicos, com a identidade da pessoa, e que os dados que estão disponíveis aos demais digam respeito de forma fidedigna com seu titular.

Em outra posição ao argumento apresentado, Igo (2018, p. 361) apresenta o pensamento de Andreas Wigend, ex-cientista chefe da Amazon, para quem o conceito de privacidade não consegue proteger as pessoas na era dos dados pessoais. Segundo Wigend, ao invés de temerem uma sociedade em que tudo se sabe, as pessoas deveriam enxergar essas mudanças com positividade, e, conforme exposto acima, tirar vantagens com os valores que as pessoas podem adquirir de acordo com o que expõem sobre si e visualizar as diversas oportunidades e otimizações que isso pode gerar, tais como o auxílio em tomadas de decisões pessoais, como escolha de parceiros românticos, local e modos de trabalho, quais remédios são os mais adequados, ou que tipo de matéria estudar, todas essas decisões baseadas em dados pessoais. Assim, a ex-cientista, chefe da Amazon, conclui com a afirmação que as pessoas deveriam deixar de lado a ilusão de privacidade (IGO, 2018, p. 363).

Apesar de parecer que a sociedade está se tornando transparente, e que as concepções de público e privado estão se dissolvendo, ou que a privacidade é uma ilusão, precisamos ter em mente qual o tipo de contexto que as informações são fornecidas e qual o grau de abrangência que essas informações são distribuídas. As antigas concepções de público e privado não auxiliam nas situações que vivemos na atualidade, principalmente com o advento da internet e das redes sociais[38]. Diariamente ocorrem transações envolvendo dados pessoais cedidos por seus titulares para poder utilizar serviços on-line. Ao utilizar uma rede social, como o Facebook, os membros aceitam ceder seus dados sobre interesses, localização, redes de amigos, dentre outros dados para ter a autorização de utilizar a plataforma. Tal fenômeno

38 Atualmente, o Facebook pode vender informações pessoais para empresas sem violar a privacidade, uma vez que tudo que se coloca no Facebook, se faz publicamente, as pessoas deixaram de ser anônimas ou desconhecidas, e passaram a ser tratadas como celebridades dentro do contexto das redes sociais (LEMOS, 2014, p. 119).

poderia demonstrar que as pessoas valoram a sua privacidade de acordo com o que podem fazer com as plataformas e ferramentas on-line (ACQUISTI et al., 2016, p. 5).

No entanto, conforme demonstrado, a privacidade está sujeita a variações históricas e a sua variação nunca se deu de modo estável. A privacidade mesmo "consolidada jurídica, social e subjetivamente na Modernidade, já em seu nascimento o seu valor e os seus limites eram objeto de tensões, deslocamentos e disputas políticas e sociais" (BRUNO, 2013, p. 128). Algo ainda presente na atualidade, pois a privacidade encontra-se em disputa, e sua existência e grau de existência são disputados por diversos atores sociais (empresas, consumidores, cidadãos, Estado, o mercado, dentre outros). Apesar de discursos como de Andreas Weigend ou Michal Kosinski (2018, p. 77), para quem a "privacidade acabou", e as pessoas deveriam agora angariar esforços para pensar em novos mecanismos para garantir a segurança e a habitabilidade num mundo "pós-privacidade". Mesmo considerando as importantes críticas dos autores, é difícil acreditar que de fato a privacidade tenha acabado, mesmo com as possíveis modificações. Independentemente da visão negativa, privacidade não se encontra enterrada ou fadada à morte.

Ademais, antes de decretar o fim da privacidade ou não, colhemos do texto de Bruno (2013, p. 129) que o mais importante na discussão sobre a privacidade na atualidade é compreender os discursos, as forças e as práticas que atualmente buscam conceituar, valorar e ditar qual é o sentido e a experiência da privacidade, uma disputa notada com mais nitidez no campo da comunicação, em especial na internet (BRUNO, 2013, p. 129). A privacidade precisa ser compreendida relacionada com o contexto político e econômico vigente, pois ela existe e é bastante valiosa.

> É preciso entrecruzar a disputa em torno da privacidade e as disputas políticas, econômicas, sociais, cognitivas e estéticas que se travam no âmbito dessas redes, de seus "bens" matérias e imateriais, de seus modelos de comunicação, circulação e produção de informação, conhecimento, cultura etc. Não raro (embora não necessariamente) os que clamam pelo fim da privacidade também clamam pelo controle de liberdade e do anonimato, ou pelo controle de práticas de compartilhamento e colaboração na rede (BRUNO, 2013, p. 129).

Vivemos uma nova economia que é movida por dados[39], e nesse sistema dados pessoais são valiosos, existindo interesses de agentes econômicos na sua circulação e comercialização. Os dados são usados para inúmeras ações, Silveira et al. (2016, p. 228)

39 Vamos trabalhar melhor essa nova economia no item 2.3 deste trabalho.

estimam que o uso de dados pessoais "terá efeitos ambivalentes em nossa sociedade", defendendo que "o mercado de dados dará maior poder às corporações do que aos cidadãos em relação às trocas que realizam". As consequências de um uso indiscriminado de dados pessoais pode levar a marginalização de grupos sociais, ou segregação por algumas condições individuais. Para exemplificar, Silveira et al. (2016, p. 228) citam Lori Andrews, que comenta que seguros de saúde podem ser negados tendo por base pesquisas realizadas na plataforma do Google sobre determinada doença ou condição de saúde, ou financiamentos bancários ou concessão de créditos com limites mais baixos podem ser negados, levando em consideração para a pontuação não o histórico de crédito, mas sim características raciais, sexuais, bem como os tipos de sites visitados ou a localização da residência e/ou trabalho. Mesmo com os efeitos negativos gerados pelo uso indiscriminado, "muitos operadores do direito e corporações defendem que a privacidade é anacrônica, e sua manutenção como direito impede a oferta de serviços e produtos adequados à melhor experiência dos consumidores" (SILVEIRA et al., 2016, p. 228). Porém, precisamos ter cuidado com esse tipo de discurso, pois existem muitos interesses envolvendo dinheiro e poder quando analisamos o direito das pessoas à privacidade. Organizações muito poderosas se beneficiam de seu enfraquecimento, e por tal razão a leitura dos defensores do fim da privacidade, ou a de que ela seria um direito "inútil"[40], precisam ser analisadas com ressalvas. É nessa toada que as legislações e a cultura

40 Nesse sentido, Daniel Solove (2008, p. 752- 753) critica o argumento de que a privacidade não seria um direito útil, pois as pessoas "de bem" nada teriam o que esconder, não existindo nenhum tipo de dano. O argumento de que "eu não tenho nada a esconder" e suas variações estão presentes em inúmeros discursos contrários à privacidade, tanto no ambiente acadêmico como fora dele. Tal argumento pode ser utilizado ao se comparar privacidade e segurança. Nesse sentido, da desvalorização da privacidade argumentam que as pessoas não têm privacidade ao fornecerem informações pessoais, pois a informação pessoal em geral não é confidencial. Logo, apenas as pessoas que estão envolvidas em condutas ilegais precisam se preocupar em ocultar algo, o que não deveria ser tolerado, fazendo o valor da privacidade ser baixo ou inexistente. A segurança, por outro lado, teria um valor muito alto. Por tal razão não haveria danos às pessoas se computadores governamentais analisassem números de telefones todos os dias. As informações colhidas, provavelmente, não serão reveladas ao mundo, pois a máquina simplesmente seguirá em frente, alheia a qualquer informação que, por padrão, não seja considerada suspeita. Logo, se nada de errado está acontecendo, não tem com o que as pessoas se preocuparem (SOLOVE, 2008, p. 753). Contudo, o argumento do "nada a esconder" provém de uma premissa falha, pois, para o argumento, a privacidade existe para proteger um erro, e não é disso que a privacidade trata. Logo, "a vontade de privar não pode ser igualada à vergonha ou ao errado, mesmo que a motivação para esconder seja essa. Ao contrário do que possa parecer, diante de uma Sociedade que valoriza como nunca a exposição, querer não mostrar não é condenável" (CANCELIER, 2017, p. 62). Inclusive, inúmeras ações que as pessoas realizam não são erradas, porém elas não querem compartilhar com as demais. Um argumento mais grotesco contrário ao nada esconder, como se a privacidade apenas protegesse atos ilícitos, seria : "se você não tem nada a esconder, então tire suas calças". Apesar de não muito polido, podemos ilustrar bem a situação de que as pessoas têm coisas a esconder e não estão fazendo nada de errado. "Todos têm algo a esconder, felizmente, [...] pois, nem tudo aquilo que deve ser ocultado constitui uma privação ou representa algo moralmente condenável e vergonhoso, ou seja, tem para a comunidade política o

de proteção da privacidade e dados pessoais tornam-se importantes. O discurso de que "as pessoas não se importam com a sua privacidade, uma vez que divulgam inúmeros aspectos da sua vida para o mundo" encontra falhas, uma vez que as pessoas divulgam fragmentos da sua vida, fragmentos que entendem que podem ir a público. As pessoas, ao viverem em comunidade, expõem pedaços de sua vida. No entanto, ainda há um espaço que é considerado íntimo, e que as pessoas querem manter longe de interferências alheias. Ademais, a ação de compartilhar informações pessoais está dentro de um contexto que se espera ser respeitado, logo, existe uma legítima expectativa sobre a forma como essas informações serão utilizadas. Espera-se que a sua divulgação não causará danos ao seu titular, bem como que elas digam respeito à realidade. Nesse sentido, discursos impulsionados por uma agenda neoliberal da economia informacional e que encontra como aliada uma sede por vigilância, antiga, dos Estados, "que buscam restringir ao máximo o direito à privacidade" (SILVEIRA et al., 2016, p. 228), como se houvesse uma alteração no valor desse direito como fruto de um novo circuito cultural (PERES-NETO, 2018, p. 3) parecem frágeis, pois seus objetivos são proteger o lucro, não as pessoas.

Assim, a alegação de que a privacidade acabou porque houve um "processo de publicização da vida privada nos ambientes de comunicação contemporâneos (dos reality shows às redes sociais)" (BRUNO, 2013, p. 130) não merece prosperar. Esse processo, ilustrado como "cultura confessional", em que histórias altamente pessoais são divulgadas ao público, histórias que décadas atrás seriam segredos guardados em diários lacrados, e hoje são páginas de um livro aberto (IGO, 2018, p. 307), está relacionado com uma vontade de querer mostrar momentos, como se uma celebridade fosse, visando a "existir" no mundo – ser visto, admirado, enaltecer qualidades, enfim, criar um avatar virtual pessoal que possui implicações diretas no mundo real. Porém, essa divulgação não é sinônima de inexistência de privacidade.

Ademais, "encenar a privacidade em público pode (com algum risco) implicar sobre ela um controle maior e não menor" (BRUNO, 2013, p. 130). De acordo com Bruno (2013, p. 133), existem estudos que buscam relacionar a maior exposição, principalmente, por parte dos jovens, com a criação de um perfil público e social de si mesmo. Nesse sentido existiria algo a ser escondido e o que é publicado na internet seria apenas a parte que as pessoas gostariam de

---

efeito deletério da mentira. O amor, por exemplo como a dor, as paixões, os sentidos, em síntese, as grandes forças da vida íntima são validadas na penumbra, tanto que só surgem em público, quando desindividualizadas e desprivatizadas" (CANCELIER, 2017, p. 62). Neste sentido, o argumento "você não tem nada a esconder, logo, não precisa se preocupar com a privacidade" é tão falacioso quanto "você não tem nada para falar, logo, não precisa se preocupar com a liberdade de expressão".

contar ao mundo sobre si, e não o que elas reservam para algumas pessoas, e muito menos o que elas reservam apenas para si mesmas. Também, considerando todo o aparato de vigilância, melhor jogar luz para o que gostaria de ser notado, se expor aos seus próprios termos e gostos, uma revelação que estaria a serviço de uma autoafirmação ou autodeterminação (IGO, 2018, p. 317). Outro argumento contrário ao fim da preocupação das pessoas com a privacidade é apresentado por Igo (2018, p. 364): a autora comenta sobre o fenômeno de publicação de inúmeros livros de autoajuda para controlar informações privadas e de guias de como navegar em uma sociedade que sabe demais. Enquanto alguns aconselham trituradores de papel e a realização de pagamento apenas em dinheiro, outros apresentam como opção o uso de, criptografia, servidores proxy, hardware, software seguros e, inclusive, outros mecanismos de bate-papo online[41].

Nesse contexto, as atenções se voltam para as mídias sociais on-line. Inclusive, pode se fazer um paralelo entre as redes sociais e os cabos telegráficos e as linhas telefônicas da época de Warren e Brandeis, uma vez que ambos geraram discussões significativas para as questões envolvendo a privacidade (IGO, 2018, p. 340). Assim como na época de Warren e Brandeis, ainda existe um forte medo de que imagens e fatos íntimos constrangedores ou vergonhosos cheguem a público, e, tal como ocorrido naquela época, as tecnologias têm o condão de ameaçar reputações. Por tal razão ainda existe um cuidado por parte das pessoas, em especial dos jovens, com o que é publicado nas redes sociais, pois, num mundo conectado, a vida pode ser destruída em questões de segundos (IGO, 2018, p. 360). Contudo, o medo foi para além das fotografias instantâneas, englobando proteção das redes na nuvem e cruzamento de dados. Em vez de preocupações com invasões a diários, as pessoas passaram a se preocupar com rastreamento de geolocalização e com adulterações em contas em redes sociais, tais como o Facebook. Apesar dos novos tons, os temas são familiares e os problemas, semelhantes: quem está autorizado a nos conhecer e como pode nos conhecer, quais os detalhes a que os demais podem ter acesso, quais os limites e o que pode ser alterado

41 Manuais de privacidade populares proliferaram, com títulos como: Você está em risco: um guia completo para você e sua família ficarem seguros online; O Guia para a Privacidade da Garota Inteligente; Vida sob vigilância: um guia de campo; e À prova de hack da sua vida agora! Como proteger (ou destruir) sua reputação online. Novos especialistas surgiram, em coisas como andar pela sociedade americana sem ser visto, e em livros como How to Disappear, The Incognito Toolkit e The Art of Invisibility eles explicam como se esconder. “Não, enquanto você viver, nunca mais permita que seu nome verdadeiro seja associado ao seu endereço residencial” é o primeiro passo, de acordo com o autor de Como ser invisível: proteja sua casa, seus filhos, seus bens e sua vida, atualmente em sua terceira edição (IGO, 2018, p. 364).

por outros em posse dessas informações. Tais perguntas são tão ou mais importantes hoje como foram na época de Warren e Brandeis (IGO, 2018, p. 351).

Apesar de parecer que a sociedade caminha para uma era "pós-privacidade", Igo (2018, p. 355) aponta, com base nos estudos realizados por John Giliom e Torin Monaham, que os americanos não concordariam com qualquer programa estatal que exigisse das pessoas a utilização de dispositivos que fornecessem em tempo real dados de localização, comunicação e interações pessoais, arquivando tudo em banco de dados – e autorizando, quando considerado necessário, o monitoramento de conversas e mensagens particulares. Apesar da não concordância, esse cenário é o que acontece com mais de 90% dos americanos, por meio de dados coletados de cartões de crédito e telefones celulares. A dinâmica da vida moderna induz as pessoas a estarem conectados a todo o momento, carregando consigo aparelhos celulares com disco rígido de 16 GB "com o qual se pode em qualquer lugar copiar informações e coisas do tipo, guardar um segredo fica muito difícil" (LEMOS, 2014, p. 122). Contudo, mesmo com a dificuldade de manter a proteção da privacidade, é possível, e mais, se torna necessário, até porque todos possuem algo a esconder (e ainda bem).

O embate envolvendo a privacidade aumenta na mesma proporção do aparecimento de novos meios tecnológicos, principalmente quando envolve novos meios de comunicação[42]. Trazendo a discussão para os dias atuais, como a segurança das conversas e a privacidade nas comunicações em redes sociais estaria assegurada? Interessante registrar que, conforme o exposto, ainda existe muito interesse nessa proteção. Inclusive, diversos atores vêm alterando seus discursos por conta das repercussões negativas referente a violações de privacidade ocorridas recentemente. O Facebook, por exemplo, após o escândalo envolvendo a empresa Cambridge Analytica[43], passou a alterar o seu discurso, que em meados de 2010 era no

42 Os conflitos que vivenciamos hoje em certa medida já foram vivenciados com a aparição do sistema postal, em 1860. Autores da época, como Ralph Waldo Emerson, refletiam sobre a proteção da confidencialidade das correspondências, pois dentro de uma carta podiam estar contidos os pensamentos mais secretos de alguém, e o que assegura a sua confidencialidade é apenas um selo (IGO, 2018, p. 26).

43 Em 2018 uma reportagem do *New York Times* revelou um vazamento de informações por meio de um aplicativo do Facebook para a empresa Cambridge Analytica, onde inicialmente 50 milhões de usuários teriam tido suas informações vazadas. A empresa Global Science Research teria se aproveitado de uma falha na rede social para coletar informações dos usuários e amigos dos usuários que participaram de um quiz chamado "thisisyourdigitallife". Posteriormente a empresa chegou a afirmar que devido a falhas em seu sistema de proteção de dados seus dois bilhões de usuários poderiam ter tido suas informações expostas (AGRELA, 2018). O escândalo tomou proporções ainda maiores quando foi relevado a possibilidade da utilização desses dados para a campanha do então presidenciável Donald Trump (GLOBO, 2018), além de participação da Cambridge Analytica na campanha do pró-brexit no plebiscito realizado no Reino Unido. A relevância dos fatos levou o CEO do Facebook a depor perante o congresso Norte Americano, inclusive sendo posteriormente convidado pelo parlamento Britânico para expor explicações (LLANO; SÁNCHES, 2018).

sentido do fim da privacidade, para afirmações do tipo "a privacidade é o futuro"[44] (O'NEILL, 2019).

Se ela é o futuro, precisa ser definida. Nesse sentido, podemos afirmar que a privacidade seria um limite ao direto à informação, um respeito à liberdade do indivíduo de escolher com quem compartilha sua vida privada e sua intimidade. Logo, ao realizar um post público, existe o entendimento de que essa postagem pode atingir um número indeterminado de pessoas, exatamente pelo alcance da internet como uma rede global, não tendo como invocar a privacidade – quem sabe outro direito, porém não este. No entanto, o mundo on-line, como visto, abriga inúmeras esferas da vida e, por consequência, também seus aspectos privados e íntimos – locais em que a privacidade deve existir. Levando em consideração a própria arquitetura das redes socais, quando se fala com um amigo no "privado" – direct message (Instagram), chat (Facebook), ou pelo WhatsApp – existe a crença de estar conversando apenas com aquela pessoa, semelhante a uma conversa a "sós" do mundo concreto. Assim, "uma pessoa que envia determinada informação, íntima, para um amigo (via Facebook ou WhatsApp, por exemplo) continua tendo resguardada sua Privacidade" (CANCELIER, 2017, p. 69).

Por tal razão, entendendo as expectativas criadas pela arquitetura das redes sociais, torna-se difícil defender que a privacidade não existiria, ou que as pessoas não se importam mais com a sua vida privada, transformando tudo em um grande livro aberto em que não existe a "possibilidade de separação dos outros, da massa, do público" (CANCELIER, 2017, p. 60). Logo, mesmo em ambientes virtuais – locais em que existiu o questionamento sobre a importância e a existência da privacidade –, ela se mostra presente. Possuindo os mesmos contornos quando analisada no mundo fático, onde as pessoas têm como impedir a invasão de terceiros na sua vida privada, a assuntos que não existe interesse que se tornem públicos, havendo a mesma "possibilidade de controlar o acesso de terceiros a informações (seja uma

---

44 No palco da conferência anual de desenvolvedores do Facebook no Vale do Silício, o CEO do Facebook chegou a afirmar que a privacidade é o futuro e que sua empresa passará a adotar medidas de privacidade, uma vez que o modelo de negocio do Facebook, segundo seu CEO , não é incompatível com a privacidade dos usuários. Todo o evento de 2019 foi pensado buscando desvincular a imagem da rede social com falhas de privacidade, desinformação. Uma das mudanças anunciadas é oferecer mensagens criptografadas de ponta a ponta, isso significa que "que nem os funcionários da empresa nem seus algoritmos poderão mais ver o que é dito em mensagens particulares. Esse processo parece estar apenas nos estágios iniciais e envolverá uma consulta de um ano com especialistas, governos e agentes da lei sobre como implementá-lo". A privacidade é o futuro é uma frase forte, no entanto, o Facebook ainda rastreia sua localização física o tempo todo, ainda o segue pela internet, e ainda assim ganha dinheiro capturando sua atenção (O`NEILL, 2018).

imagem, um escrito, uma fala) o mesmo pode, e deve ser exigido no mundo virtual" (CANCELIER, 2017, p. 69).

Contudo, ao falarmos de proteção e autoafirmação, chegamos num impasse que esse trabalho precisa decidir: se tal assunto encontra-se dentro do conceito de privacidade ou se é um conceito autônomo, que possui uma nova esfera de proteção. Hoje, com a internet, houve o aumento de um fenômeno que foi pouco discutido quando da primeira grande discussão sobre a privacidade. Hodiernamente grande parte das informações cedidas a terceiros não advém da devassa do lar, da violação de cartas, de fotografias, mas sim através de coletas das informações pessoais em transações abstratas (RODOTÀ, 2008, p. 128). A dúvida que surge é se essas informações pessoais são informações que se encontram dentro do conceito de privacidade ou pertencem a outra categoria, assunto que trataremos no próximo tópico.

2.3 DIFERENÇA ENTRE DADOS PESSOAIS E PRIVACIDADE

O ponto de maior divergência está na conceituação de privacidade. A privacidade continua existindo, porém ela se alterou com o tempo e com as novas tecnologias. Conforme visto, a privacidade é um conceito subjetivo relacionado com a sensibilidade individual e com seu grau de tolerância em relação ao que seria ou não privado. A dificuldade gira em torno da falta de um tratamento semântico bem definido para o termo privacidade, e como bem aponta Danilo Doneda (2006, p. 102), essa falta de definição não é um problema exclusivo da doutrina brasileira. Nesse sentido, tomando como exemplo a doutrina americana, o termo "*privacy*", fortemente reconhecido como *right to privacy*, faz referência a inúmeras situações fáticas e jurídicas. Dentre essas, alguns doutrinadores de tradição de *civil law*, incluindo o Brasil, não conseguem visualizar como sendo questões de privacidade. Quem sabe, a questão de diferenciação entre dados pessoais e privacidade seja, exatamente, o fato de que não são todas as situações que proteção aos dados pessoais esteja abarcada dentro do escopo da privacidade[45].

45 De acordo com Bioni (2019, p. 96), muitos equívocos doutrinários foram cometidos em torno da construção do conceito da privacidade, alargando-o em demasia, exatamente porque no sistema norte-americano inexistem direitos da personalidade para proteger de forma ampla a pessoa. Assim, o vocábulo *privacy* é utilizado de forma genérica para diversas situações, que "tradicionalmente pela *civil law* sequer se relacionam com o conceito de privacidade", sendo necessário considerar interpretações distintas a depender do modelo jurídico utilizado (MIRANDA, 2018, p. 86).

Ademais, como precisamos de um conceito mais genérico para abarcar a generalidade de todas as pessoas que convivem em sociedade, a privacidade acaba por ter uma conceituação extremamente ampla, pois existe uma diversidade de pontos de vista e de mesma forma várias tentativas de achar um termo único, essa "dificuldade metodológica em definir um ponto de vista comum sobre a questão como pela tentação em fazê-lo abranger um leque demasiadamente amplo de situações" (DONEDA, 2006, p. 105), que, muitas vezes, acabam aglutinando situações que não têm a ver com a privacidade. Paulo Mota Pinto escreve:

> Grande parte dos problemas com o conceito de *privacy* têm a ver com um esclarecimento teleológico e conceitual insuficiente ou, pelo menos, incapaz de resistir à tendência para se colocar sobre a alçada da 'privacidade' coisas que não têm a ver com ela. Impõe-se, por isso, pelo menos tentar colocar uma barragem a essa tendência (PINTO, 1993, p. 506, apud DONEDA, 2006, p. 103).

Uma solução a esse empate seria a utilização da ficção jurídica do "homem médio", um conceito de raiz social e moral que advém de um conceito geral já sedimentado na "cultura social-moral". Logo, são valores e entendimentos "consensualmente admitido pelos membros da comunidade" mais ou menos estáveis durante a passagem do tempo. Neste sentido, o conceito de "homem médio" pode ser entendido como "uma aquisição cultural atualizável no tempo de cada civilização humana, derivada da base comum das diferentes ideologias vigentes na comunidade, temperada por um senso da razoabilidade e do respeito pela dignidade humana" (LEONG, 2017, p. 323). Logo, apenas seriam considerados danos à privacidade aquelas violações em que a média da sociedade assim identifica como prejudicial, evitando argumentações que entendem a privacidade como "egoísmo pessoal" (SAWARIS, 2017, p. 71).

Neste sentido, se não for estabelecida uma espécie de limite, a utilização de um conceito muito aberto ou muito geral pode causar problemas em um mundo altamente interligado e informatizado que, por seu turno, depende de um enorme fluxo de informações e dados para gerar riquezas, prestar serviços, conectar pessoas, gerar empregos, dentre tantas outras atividades vitais. O mundo, no seu atual estágio de desenvolvimento, depende de dados e informações, sendo que eles serão utilizados, e é inegável que sua utilização possibilitou e

possibilita inúmeros "benefícios para a sociedade, mas ao mesmo tempo apareceram novos riscos, dentre eles à privacidade das pessoas" (AMARAL, 2019, p. 113)[46].

O dilema é como permitir esse tratamento de dados, esse fluxo informacional, sem deixar de proteger a dignidade humana. Importante ter em mente que podemos incorrer na falácia de tentar tudo proteger e, assim, não proteger nada. Uma visão muito restritiva de privacidade não protege a pessoa, assim como uma visão muita ampla. Precisamos delimitar um núcleo duro, algo que para o "homem médio" seja entendido como privacidade, e quais os procedimentos adequados para a utilização de dados pessoais. Essa delimitação busca evitar que informações pessoais sejam "submetidas a regimes jurídicos diferenciados", levando em consideração aspectos subjetivos e de ocasião do julgador que podem variar "do máximo de opacidade ao máximo de transparência, segundo se considerasse prevalecente o interesse privado à intimidade ou o interesse coletivo à publicidade" (RODOTÀ, 2008, p. 77).

Assim, conforme já mencionado, a proteção à privacidade, que teve a sua origem na definição de Warren e Brandeis como "o direito de ser deixado em paz", passou a ter outras definições desenvolvidas para outros tempos e outros clamores sociais – com o aumento do fluxo informacional, passou a se buscar uma forma de proteger as pessoas de abusos e dar aos cidadãos instrumentos para controlar a maneira como seus dados pessoais eram utilizados (RODOTÀ, 2008, p. 15). Faltando um conceito melhor, passou-se a buscar proteger o controle de informações como parte da privacidade. Apesar de muito próximos, percebe-se que o que realmente busca-se proteger é o modo como informações pessoais podem ser utilizadas por terceiros, uma vez que a coleta de "dados sensíveis e perfis sociais e individuais pode levar a discriminação" (RODOTÀ, 2008, p. 15). Desta forma, a ampliação do conceito de privacidade foi, num primeiro momento, utilizada para abarcar em seu bojo a proteção de dados pessoais, pois não existia um conceito que visasse a proteger os dados pessoais dos indivíduos. "Os sinais desta mudança são claros: basta verificar que a partir de 1970 o direito associou cada vez mais privacidade com casos de informações armazenadas em banco de dados" (DONEDA, 2006, p. 141)[47]. Tais legislações foram respostas aos desafios gerados pelas novas tecnologias envolvendo privacidade e dados pessoais (ANDRADE, 2011, p. 91).

---

46 Sobre a utilização e a economia de dados pessoais, vamos tratar com mais afinco no item 3.3 desse trabalho.

47 "A lei considerada a primeira lei norte-americana sobre *privacy* é justamente o *Fair Credit Reporting Act* de 1970, que regulava escritórios de proteção ao crédito e cadastro de consumidores – ou seja, basicamente banco de dados de consumidores" (DONEDA, 2006, p. 141).

Neste novo contexto, urge a necessidade de evitar um controle social, em que a pessoa estaria a todo momento sob o comando de ingerências externas que, consequentemente, ceifariam sua individualidade, bem como limitaria a possibilidade de escolhas, a autonomia privada, de modo a inviabilizar seu livre desenvolvimento da personalidade (DONEDA, 2006, p. 142). Bem por isso, o direito à privacidade começou a ser invocado para tutelar a pessoa humana frente às mudanças tecnológicas.

Para Doneda (2006, p. 141), a privacidade não poderia mais ser entendida dentro de um direito subjetivo, em que cada pessoa estabeleceria os seus limites de exposição, ou não, ao público, mas a privacidade precisa ser entendida dentro de uma posição de destaque na proteção da pessoa humana, "não somente tomada como escudo contra o exterior – na lógica de exclusão – mas como elemento positivo, indutor da cidadania, da própria atividade política em sentido amplo e dos direitos de liberdade de uma forma geral" (DONEDA, 2006, p. 142). Assim, a privacidade passaria a se desassociar de sua antiga lógica patrimonialista, que esteve presente em sua formação. Agora a privacidade incorpora uma complexidade de situações para além de uma pessoa em particular. A privacidade é ampliada para uma dimensão coletiva, buscando a promoção e proteção da dignidade da pessoa humana, considerada singular e parte de um coletivo.

Logo, para Doneda (2006, p. 142) a privacidade teria angariado um aspecto positivo, uma função promocional, adquirindo mais um aspecto ao seu conceito tradicional, deixando de ser apenas uma liberdade negativa, uma barreira ao espaço considerado privado – o não invadir, originário de uma lógica de não adentrar na propriedade alheia sem autorização. Passando, por seu turno, a ser considerada uma liberdade positiva, a privacidade passa a promover, também, um controle sobre as informações pessoais e determinar as modalidades de construção da esfera privada, permitindo assim o livre desenvolvimento da personalidade (DONEDA, 2006, p. 142-147).

A privacidade em seu sentido tradicional, relacionada com seu aspecto negativo, encontra-se enfraquecida, pois é "cada vez menos relevante o raciocínio em termo de 'espaço' ou 'bens' protegidos pela privacidade" (DONEDA, 2006, p. 145). Em contrapartida, existe um aumento na intenção de proteger a personalidade da pessoa no exterior. Desse modo, a privacidade estaria sendo chamada para o controle de informações pessoais e, neste sentido, determinar o modo como as pessoas querem se relacionar com os demais e formar a sua

individualidade, sem serem obrigadas a ceder a pressões estranhas advindas do Estado ou da Sociedade (DONEDA, 2006, p. 146).

Do mesmo modo, Rodotà (2008, p. 92) afirma que a privacidade apresenta-se como uma "noção fortemente dinâmica", possuindo estreita relação com as alterações ocorridas em função das tecnologias da informação, pois os dados em circulação necessitam de uma tutela que seja dinâmica, bem como essa tutela não pode mais se "concentrar no sujeito (como geralmente acontece quando se considera o direto à privacidade)". Nesse novo paradigma, a informação pessoal não está mais vinculada à pessoa e "torna-se exterior a esta: ela pode circular, submeter-se a um certo tratamento, ser comunicada, etc." (DONEDA, 2006, p. 168). Segundo Mendes (2008, p. 58), esse alargamento no conteúdo da privacidade decorre do fato de que sua antiga concepção "não funciona mais como uma solução para os problemas relativos à seleção, classificação e discriminação do fluxo de informações na sociedade" cada dia mais vigilante[48].

Nesse sentido, os tratamentos de dados pessoais causaram inúmeras invocações à proteção da privacidade, paralelamente, cresce "a consciência da impossibilidade de confinar as novas questões que surgem dento do quadro institucional tradicionalmente identificado por este conceito" (RODOTÀ, 2008, p. 23). A privacidade precisava ser reinventada, sua definição clássica como "direito de ser deixado só", apesar de ainda existir em situações específicas, precisava ser alargada na Sociedade da Informação, a privacidade precisa passar a abranger o conceito de uma privacidade funcional. Assim, Rodotà (2008, p. 92) passa a conceituar as definições funcionais da privacidade, sendo consideradas como as possibilidades de o sujeito controlar suas informações pessoais. Deste modo, a pessoa tem a faculdade de "conhecer, endereçar, interromper o fluxo de informações a ela relacionadas".

Nesta toada, a privacidade ganha um novo valor, passa a ser entendida como um "direito à autodeterminação informativa" – o qual atribui poder aos indivíduos de controlar as

---

48 "A vigilância na sociedade da informação, no entanto, adquire características e contornos próprios. Primeiramente, ela passa a ser realizada, não mais apenas pelo Estado, mas diversos organismos privados, atingindo consumidores, trabalhadores e cidadãos em geral. Segundo, ela utiliza-se de tecnologias extremamente modernas, como as diversas técnicas para tratamento de dados pessoais, que permitem a consolidação de um quadro da personalidade do indivíduo relativamente completo. Por fim, ressalta-se que a principal característica da nova vigilância, concretizada por meio da coleta e do processamento de dados pessoais, é a sua ocorrência cotidiana, tanto local quanto globalmente. Isto é, tornou-se uma vigilância do dia-a-dia e de todos os aspectos corriqueiros da vida: do trabalho, da casa, do consumo" (MENDES, 2008, p. 59). Diversos dados pessoais são manipulados dentro desse processo de vigilância, tais como dados biométricos, dados de saúde, dados genéticos, imagens e vídeos, registros de consumo, arquivos administrativos. Ao fim, a vigilância tem como finalidade o planejamento, realização de prognósticos, prevenção de riscos das atividades administrativas e empresariais, mediante classificação e avaliação dos perfis pessoais (MENDES, 2008, p. 59).

informações pessoais existentes sobre si mesmos. A privacidade, então, teria evoluído – partindo do conceito clássico elaborado por Warren e Brandeis para chegar à privacidade como direito "de manter o controle sobre as próprias informações e de determinar as modalidades de construção da própria esfera privada" (RODOTÀ, 2008, p. 7). A proteção de informações pessoais seria o resultado de um longo processo evolutivo do conceito de privacidade, que no início foi vinculado com um direito de ser deixado em paz, transformando-se no direito de poder controlar as informações pessoais com o intuito de controlar e "determinar como a esfera privada deve ser construída" (RODOTÀ, 2008, p. 17).

Tal entendimento tem forte ressonância na doutrina sobre o direito à privacidade. Contudo, este trabalho irá se filiar à posição que considera que a privacidade não possui "uma faceta positiva" nem estaria a serviço de manter o controle das informações pessoais. Em vista disso, a proteção de dados não se encontra dentro do escopo da privacidade nem é "uma mera evolução do direito à privacidade" (BIONI, 2019, p. 94-96). A compreensão que adotamos é que a privacidade e a proteção de dados são dois valores diferentes, que protegem diferentes bens da vida e, por consequência, tratam de dois direitos autônomos.

Rodotà afirma:

> Uma definição da privacidade como 'direito de ser deixado só' perdeu há muito tempo seu valor genérico, ainda que continue a abranger um aspecto essencial do problema e possa (deva) ser aplicada a situações específicas. Na sociedade da informação tendem a prevalecer definições funcionais da privacidade que, de diversas formas, fazem referência à possibilidade de um sujeito conhecer, controlar, endereçar, interromper o fluxo de informações a ele relacionadas. Assim a privacidade pode ser definida mais precisamente, em uma primeira aproximação, como o direito de manter o controle sobre as próprias informações (RODOTÀ, 2008, p. 92).

À vista disso, a "ampliação progressiva da esfera privada" (RODOTÀ, 2008, p. 92) para uma privacidade com definições funcionais estaria contemplada dentro do escopo do conceito de privado. Ou estaríamos diante de um novo conceito que adveio da preocupação que surgiu com o poder das novas tecnologias de coletar e cruzar dados pessoais, possibilitando novos mecanismos de controle e discriminações? Entendemos que a privacidade não teria expandido o seu conceito para "além do seu tradicional poder de exclusão" para passar a, também, abranger um poder de controle. A privacidade, ao contrário do que defende Rodotà, continuaria a ser compreendida dentro de "áreas às quais se atribui uma proteção especial por razões de intimidade". Ao passo que a proteção de dados pessoais,

e não uma ampliação da privacidade, estaria voltada a "abranger o conjunto de atividades e situações de uma pessoa que tem um potencial de 'comunicação', verbal e não-verbal, e que pode, portanto, se traduzir em informações" (RODOTÀ, 2008, p. 93).

Logo, a noção "pessoa-informação-circulação-controle" diz respeito à proteção de dados pessoais. A privacidade visa a proteger informações para que não se tornem públicas. Mesmo entendendo a privacidade dentro de um contexto da vida privada, ela tem limites, e a ideia da tutela é impedir que as informações ultrapassem o limite de uma esfera dita como privada (que como visto não é um local físico, mas sim assuntos e ações que se entendem privados dentro de um contexto que o "homem médio" compreenderia como fora da ideia de público). Assim, a privacidade visa interromper/barrar o fluxo da informação, diferentemente da proteção de dados, que visa controlar esse fluxo informacional, porém permitindo que ele flua. A proteção de dados pode exigir "formas de 'circulação controlada'", afastando-se do direito à privacidade que visava apenas a estancar o fluxo de informações pessoais (RODOTÀ, 2008, p. 93).

A transição de um conceito amplo de privacidade para um novo valor, de proteção de dados, foi marcada pela busca de uma tutela dinâmica visando a objetividade, "promover funcionalidade" e "elevar-se a uma dimensão coletiva. A clássica sequência 'pessoa-informação-sigilo' é superada para alcançar a noção 'pessoa-informação-circulação-controle', na qual o imperativo é a circulação controlada de dados" (KORKMAZ, 2019, p. 38). Dentro dessa perspectiva, sendo possível ao indivíduo a gerência sobre o seus dados pessoais, igualmente, tornou-se possível "liberdade de acesso às informações em mãos públicas", promovendo uma mudança em regras gerais de circulação de informações, pessoais ou não, pois passou-se a dar mais ênfase em como essas informações seriam utilizadas pelo poder público (RODOTÀ, 2008, p. 44). O controle de circulação de informações se volta para interesses coletivos e das gerações futuras, não estando apenas delimitado em uma expectativa individual do sujeito (KORKMAZ, 2019, p. 38-39). Expectativas que podem ser entendidas como ter o "controle de informações pessoais do que seja algo íntimo ou privado do sujeito" (BIONI, 2019, p. 58). Destarte, a proteção de dados pessoais pode englobar dados que estão sob a esfera pública, em casos em que se discute apenas a sua exatidão, como bem exemplifica Bruno Bioni (2019, p. 58). A proteção de dados não se insere dentro de uma dicotomia público/privado, pois a proteção dos dados deriva de uma "perspectiva da identidade do sujeito", e como diz respeito à identidade da pessoa, os dados que circulam necessitam ser exatos e corretos.

Para entender a diferença entre a privacidade e a proteção de dados, Andrade (2011, p. 94) utiliza analogia desenhada por De Hert e Gutwirth, para quem a privacidade seria uma "ferramenta de opacidade" ou "*tool of opacity*", e a proteção de dados, por outro lado, seria uma "ferramenta de transparência" ou "*tool of transparency*". Nesse desenho, as ferramentas de opacidade auxiliam em escolhas normativas para a limitação do poder, ao passo que ferramentas de transparência são utilizadas para o controle e uso legítimo do poder (ANDRADE, 2011, p. 94).

Historicamente, a privacidade pressupõe a presença de dois lugares, dois espaços separados (público/privado) concebendo a própria razão de ser da privacidade. Esta dicotomia sempre esteve no panorama do direito à privacidade, em que existiria uma delimitação entre as ações exercidas em público e aquelas realizadas privativamente (BIONI, 2019, p. 91). Sob o mesmo ângulo, pode-se dizer que existem dois espaços,

> De um lado, tem-se a 'casa': a esfera privada como espaço íntimo – e por vezes até sigiloso – no qual o indivíduo se refugia do escrutínio público e da própria intervenção estatal. De outro, tem-se a 'Ágora': a esfera pública como espaço no qual são desenvolvidas as virtudes cidadãs do indivíduo, que se posiciona na sociedade e se expõe. Nesse cenário, o direito à privacidade atua como elemento delimitador dessas duas esferas dicotômicas, permitindo o controle da individualidade (DONEDA et al., 2021, p. 76).

Logo, a ordem da inviolabilidade da vida privada advém dessa oposição entre público e privado (BIONI, 2019, p. 93), pois concebe a privacidade como o direito de "ser deixado só", livre de intromissões, abarcando em seu conceito aquelas informações que a pessoa não quer que sejam divulgadas ou quando compartilhadas com alguém "exigem do receptor extrema lealdade e alta confiança, e que, se devassadas, desnudariam a personalidade, quebrariam a consistência psíquica, destruindo a integridade moral do sujeito" (FERRAZ JÚNIOR, 1993, p. 448-449). A privacidade protege as informações "que por qualquer razão não gostaríamos de ver cair no domínio público; é tudo aquilo que não deve ser objeto do direito à informação nem da curiosidade da sociedade moderna" (BIONI, 2019, p. 92).

Assim, a privacidade, como "uma ferramenta de opacidade" traça garantias para que não haja perturbação de questões particulares, produzindo um local livre de intromissão. É um direito negativo, protegendo os indivíduos contra interferências em sua autonomia por parte do governo e/ou atores privados (ANDRADE, 2011, p. 94). Como bem leciona Frazão (2020,

p. 107) o ser humano necessita de um local livre do controle social, em que se sintam seguros para “deixar as máscaras e exercer suas verdadeiras identidades”, uma espécie de “santuário”, um local de “refúgio inviolável”.

A conceituação da privacidade, dentro de sua definição clássica, não lhe retira valor ou importância, muito pelo contrário, trazendo luz ao seu conceito a privacidade pode proteger “a integridade moral da pessoa” (FERRAZ JÚNIOR, 1993, p. 448). No que diz respeito à liberdade negativa de cada indivíduo, significa dizer que cada um tem o condão de determinar “quais fatores da sua vida deveriam ser excluídos do domínio público”, sendo um conceito de resguardo possível (BIONI, 2019, p. 93). Protegendo a vida privada e familiar que exterioriza “o momento individualista e o poder exaure-se substancialmente na exclusão da interferência de outrem; a tutela, portanto, é estática e negativa” (BODIN, 2008, p. 8).

No entanto, tais definições ainda não conseguem precisar de modo objetivo a privacidade, pois, por tratar de um direito de cunho subjetivo, cada pessoa poderia ter uma definição de sua esfera privada (mais larga ou mais estreita). Por tal razão há a necessidade de o parâmetro de esfera privada ser vinculado dentro do seu conceito clássico de privacidade como o direito de ser deixado só ou em paz, como o direito à exclusão, de resguardo. Sendo que privados são aquelas situações e espaços que, dentro do ideal do “homem médio”, não devem ser violados, situações tais como aquelas que envolvem a inviolabilidade da casa, correspondência, das comunicações (BIONI, 2019, p. 93).

Por outro lado, perante as mudanças tecnológicas ocorridas, houve a necessidade de invocar um novo meio de proteção da pessoa humana “vinculado à tutela da dignidade e da personalidade dos cidadãos no seio da sociedade da informação” (MENDES; FONSECA, 2021, p. 77). Uma proteção que precisava transcender a proteção conferida à esfera íntima da pessoa, para englobar o controle dos dados pessoais (RODOTÀ, 2008, p. 95). Apesar de a proteção de dados pessoais possuir o mesmo fundamento ontológico da privacidade, que é a dignidade humana, diferentemente dela, “passa a ostentar um caráter significantemente dinâmico e a elevar-se a uma dimensão coletiva” (KORKMAZ, 2019, p. 38). Diferentemente da privacidade, que é uma ferramenta de opacidade, a proteção de dados é uma ferramenta de transparência (ANDRADE, 2011, p. 94), envolvendo dentro de seu escopo de proteção direitos de acesso e retificação desses dados. Tais salvaguardas permitem que dados que “transitam na esfera pública e não na privada” sejam fidedignos com os de seus titulares, logo é um conceito que atua “fora da lógica binária do público e do privado, bastando que a informação esteja atrelada a uma pessoa” (BIONI, 2019, p. 95).

Ademais, a ideia de proteger os dados pessoais não está a serviço de evitar a sua circulação, mas sim que esse fluxo informacional seja regulado de modo a promover responsabilidades públicas significativas para os agentes que tratam dados pessoais. A lógica é de natureza pragmática e instrumental, pois define o procedimento de como esses dados podem ser utilizados e tratados. Nesse sentido, o direito à proteção de dados poderia também ser denominado como o direito ao processamento de dados, pois permite que entidades públicas e privadas coletem e utilizem informações pessoais. Obviamente que a coleta não pode ser de qualquer modo, estando sujeita a condições, procedimentos, limitações e exceções (ANDRADE, 2011 p. 95). Assim, proteção de dados diz respeito a diretrizes, os modos de tratamento, o "processamento de dados e estabelece a legitimidade para a tomada de medidas – i.e. é um tipo de proteção dinâmica, que segue o dado em todos os seus movimentos" (BODIN, 2008, p. 17).

Ademais, a proteção de dados pessoais teria o objetivo de conferir amparos processuais especiais para amparar a pessoa humana de discriminações e abusos, bem como promover responsabilidades por parte dos agentes públicos e privados que possuem bancos de dados com informações pessoais (ANDRADE, 2011, p. 97). Tal entendimento pode ser retirado da obra de Rodotà (2008, p. 92), quando este comenta sobre "as definições funcionais da privacidade". É inegável que a proteção de dados visa a regular a circulação de informações pessoais, mesmo que não digam respeito à vida privada ou íntima, mas sim todos os dados que digam respeito a uma pessoa, ou, em outros termos, "informações em seu conjunto". Nesse sentido,

> [...] a proteção de dados não pode mais se referir a algum aspecto especial, mesmo que seja em si muito relevante, porém requer que sejam postas em operação estratégias integradas, capazes de regular a circulação de informações em seu conjunto (RODOTÀ, 2008, p. 50).

Assim, a proteção de dados é um instrumento ou uma ferramenta que visa a definir os meios e os procedimentos para garantir a proteção de valores que encontramos em outros direitos, tais como o direito à privacidade, ao nome, liberdade de expressão e informação, dentre outros. Por tal razão, Andrade (2011, p. 97), citando Poullet, afirma que a proteção de dados é uma ferramenta a serviço da dignidade e liberdades e não um valor como tal. Aliás, é importante mencionar que a proteção de dados está a serviço da proteção da dignidade humana, relacionando-se com o direito à privacidade. Contudo, outros direitos também estão

absorvidos dentro do seu âmbito de proteção (BIONI, 2019, p. 57). Entendidos como conceitos apartados, apesar da forte conexão entre a proteção de dados e a privacidade, "tal relação não se traduz numa superposição completa dos respectivos âmbitos de proteção. Proteção de dados pessoais, e da mesma forma, autodeterminação informativa vão além da privacidade e de sua proteção" (SARLET, 2021, p. 32).

Em igual sentido, Bioni (2019, p. 95) entende que a proteção de dados não se configura como uma evolução do conceito de privacidade[49], mas um novo valor com autonomia própria, abarcando os dados pessoais em qualquer espaço, seja ele público ou privado. Assim,

> cadastros e bancos de dados formados com dados pessoais que não envolvem aspectos da intimidade e vida privada do indivíduo submetem-se a regras do direito à proteção dos dados pessoais. Essa concepção depende, sobretudo, da percepção de que até as informações aparentemente mais inócuas podem ser integradas a outras e provocar danos ao seu titular (BIONI, 2019, p. 95).

No mesmo sentido, Amaral (2019, p. 144) argumenta que a disseminação ilegítima de dados pessoais pode causar danos a vários direitos da personalidade, além da privacidade e da intimidade, "tais como o direito ao bom nome ou ao crédito, à honra e à reputação, que estão diretamente ligados à dignidade humana".

Por tais razões, coadunamos com o entendimento de que o controle do fluxo das informações pessoais está relacionado à proteção de dados, obviamente, que dados pessoais podem conter informações que fazem parte da esfera privada da pessoa, e nesses casos haverá uma sobreposição dos direitos. Bem como existirão situações em que não haverá tal intersecção.

> Visto que nem toda recolha e tratamento concedido aos dados pessoais caracterizam infringências à esfera íntima. No mesmo sentido nem tudo que concerne à *privacy* tem a ver com o direito à proteção de dados, mas não se desconsidera que efetivamente há um ponto de encontro entre eles (SAWARIS, 2017, p. 83).

Os dados pessoais compõem uma soma de contextos que, geralmente, são comunicados sem nenhuma inibição. "São dados que, embora privativos – como o nome,

---

49 Existe uma corrente doutrinária que entende que o direito à proteção de dados está dentro do escopo da privacidade, "consistiria em uma proteção dinâmica e em uma liberdade positiva do controle sobre as informações pessoais" (BIONI, 2019, p. 94). Para essa linha doutrinária a privacidade teria uma faceta positiva, que estaria configurada como manter o controle das informações pessoais.

endereço, profissão, idade, estado civil, filiação, número de registro público oficial, etc. –, condicionam o próprio intercâmbio humano em sociedade", uma vez que formam os subsídios para a identificação da pessoa, necessários para a apresentação e interlocução em sociedade (FERRAZ JÚNIOR, 1993, p. 449). Exatamente nesse limiar da vida privada com o intercâmbio humano em sociedade é que se encontra a proteção de dados pessoais, que, apesar de dizer respeito à personalidade humana, assim como a privacidade, com ela não se confunde. [50]Nessa lógica, os dados pessoais, assim como o nome, a imagem e a reputação são condições de comunicação, apesar de exclusivos (próprios) estão "*perante* os outros", diferentemente da privacidade, que demarca a "individualidade em face dos outros" (FERRAZ JÚNIOR, 1993, p. 442)[51].

Privacidade e dados pessoais, apesar de distintos em vários pontos, possuem algumas semelhanças. Surgindo a necessidade de ter em mente que existe uma zona de intersecção entre os conceitos de privacidade e dados pessoais, há momentos em que eles se encontram, havendo uma sobreposição, e a situação poderá ser abarcada dentro de duas esferas de proteção, tanto da proteção de dados quanto da privacidade. Os dados pessoais podem ser utilizados, devem fluir, pois o intercâmbio de dados traz benefícios para a economia, bem como é importante para o bom funcionamento dos governos e das instituições. A utilização dos dados pessoais traz inúmeros benefícios, porém pode trazer muitos malefícios – o modo de utilização da tecnologia é que vai definir a qualidade do uso.

No tocante às zonas de intersecção, elas serão frequentes quando o tratamento envolver dados sensíveis. São dados, conforme veremos adiante, passíveis de gerar discriminação. Diferentemente dos dados pessoais simples, os dados sensíveis estão

---

50 Fortalecendo o argumento que há uma diferença entre proteção de dados e proteção à privacidade é é interessante mencionar a analise realizada por Fortes (2016, p. 142) do Relatório do Comitê de Proteção de Dados da Parlamento Britânico, apresentado em 1978, "Para a elaboração do referido relatório, o comitê temático do Parlamento Britânico conduziu uma série de estudos, examinando a relação entre privacidade e proteção de dados pessoais, e conclui que a função do direito de proteção de dados deveria ser diferente do direito à privacidade. Em vez de estabelecer direitos, deveria fornecer parâmetros para buscar o equilíbrio entre os interesses dos indivíduos, dos usuários dos dados e da sociedade em geral". Apesar de o relatório encontrar pontos de convergência entre a privacidade e a manipulação de dados, há vários aspectos "da proteção de dados que não possuem qualquer relação com a garantia de privacidade. Por exemplo, o uso de informações imprecisas ou incompletas para a tomada de decisões sobre pessoas é um assunto exclusivamente de proteção de dados, mas, nem sempre, terá relação com questões envolvendo a privacidade de alguém" (FORTES, 2016, p. 143).

51 Para exemplificar essa situação, imaginemos um pagamento via PIX em que se utiliza o CPF como chave para ser possível a operação de transferência de dinheiro. Nesse caso, não há como defender que, ao passar o número CPF para realização do pagamento via PIX, a pessoa está compartilhando elementos da sua esfera privada. Existe a troca de um dado pessoal, um dado passível de identificar seu titular, e no exemplo em tela a identificação é necessária (e bem-vinda) para o recebimento do dinheiro na conta-corrente do dono do CPF.

localizados numa linha tênue com a privacidade. Sobre os dados pessoais, pela importância que eles possuem no presente trabalho, iremos melhor trabalha-los no segundo capítulo, bem como a implicação que eles possuem na nova ordem econômica da Sociedade da Informação.

3 DADOS PESSOAIS

3.1 CONCEITO DE DADOS PESSOAIS

Feita essa digressão da diferença entre privacidade e proteção de dados pessoais, reconhecendo a proximidade que existe entre esses conceitos, ainda mais dentro do paradigma atual, em que há uma "ampla gama de oportunidades de coleta, análise, uso e armazenamento de dados pessoais" (BOFF, 2018, p. 117), passamos a analisar com mais detalhes os dados pessoais.

A palavra dado deriva do plural do vocábulo *datum*, do latim (AMARAL, 2019, p. 113), e em inglês *data*[52], definido pelo dicionário Oxford *on-line* (2013) e traduzido por Semidão (2014, p. 71) como:

> Substantivo (usado como singular ou plural):
> • Fatos e estatísticas coletadas juntas para fim de referência ou análise.
> • Computação de quantidades, caracteres ou símbolos em que as operações são executadas por um computador, sendo armazenados e transmitidos na forma de sinais elétricos, e gravados em mídias de gravação magnética, óptica ou mecânica.[...]

No entanto, o termo "dado" para Miranda (2018, p. 88) são informações coletadas que passaram por alguma forma de tratamento, manual ou eletrônica, para atingir um determinado fim. O dado, então, seria uma "espécie de pré-informação, uma informação em potencial" (SCHAEFER, 2010, p. 48). Assim, "dado" constitui uma minúscula parte da informação, podendo ter um valor próprio ou não. Se possuir um valor intrínseco, o dado – de forma isolada – tem a capacidade de transmitir uma mensagem; porém, caso o dado não possua valor próprio, necessita agrupar-se com outros dados para conseguir transmitir uma mensagem (VIEIRA, 2007, p. 224). Nesse sentido, Mendes (2008, p. 70) dispõe que é admissível compreender dado como "informação em potencial", ou seja, é viável ao dado se

52 Na língua inglesa, "o substantivo data é classificado como um substantivo incontável, podendo ser usado no plural (data), mas com significação singular" (SEMIDÃO, 2014, p. 70).

tornar informação, desde que ele seja "comunicado, recebido e compreendido". Arrematando, Bioni (2019, p. 31-32) conceitua "dado" como a informação em estado primitivo, uma vez que o dado em si não acresce conhecimento. Neste sentido, "dados são simplesmente *fatos brutos* que, quando processados e organizados, se convertem em algo inteligível, podendo ser deles extraída uma informação".

Logo, "dado" e "informação" possuem significado diverso, muito embora, conforme alerta Mendes (2008, p. 70), esses conceitos sejam utilizados como sinônimos. À vista disso, Doneda (2006, p. 152) discorre que os termos "dados" e "informações" são, frequentemente, utilizados como se possuíssem o mesmo sentido, pois ambos são utilizados para "representar um fato, um determinado aspecto da realidade". Contudo, apesar das semelhanças, os vocábulos "dados" e "informações" não se confundem, possuindo significados próprios. "Dado", de acordo com o exposto acima, é uma espécie de "pré-informação", ou um conceito mais primitivo e fragmentado quando comparado com a informação. Por outro lado, a "informação" estaria localizada numa etapa posterior, sendo o "resultado do processo de elaboração dos conteúdos fornecidos pelos dados", os dados são a matéria-prima para se obter uma informação que nasce de "um mecanismo (processo) de compreensão desses dados" que se transmutam em informações (SCHAEFER, 2010, p. 48). A informação é o resultado da interpretação dos dados, passando a possuir um significado mais amplo do que o existente no dado, chegando ao começo da cognição pelo receptor dessa informação. Assim, "na informação já se pressupõe uma fase inicial de depuração de conteúdo" (DONEDA, 2006, p. 152).

Ainda que, dentro do escopo de proteção de dados, os conceitos "dados" e "informações" estejam interligados[53], é necessário compreender que há diferença entre eles. Sarlet (2021, p. 40) discorre que o termo "informação" é muito variável e depende do contexto em que é utilizado, bem como da área do conhecimento a que faz referência[54]. Os dados possuem uma natureza formalizada, tais quais os algarismos – "dados são 'sinais' ou

53 Em igual sentido Doneda (2011, p. 94) comenta que "dado" e "informação" em várias situações se sobrepõem e, por tal razão, muitas vezes são utilizado como sinônimos. "Ambos os termos servem para representar um fato, determinado aspecto de uma realidade."

54 O termo "informação" pode estar relacionado com ordens de valores distintas, de acordo com o contexto que está relacionado. Nesse sentido, "liberdade de informação" entendida como o fundamento de uma imprensa livre juntamente com o "direito à informação", bem como "dever de informação" pré-contratual previsto no Código de Defesa do Consumidor detém um tipo de conotação. Ao passo que a informação pessoal tem outro tipo de conotação, que para Danilo Doneda (2011, p. 94) num primeiro momento encontrou guarida junto ao direito de privacidade.

‘símbolos’ não interpretados” – precisando de um meio técnico para serem “reproduzidos e transmitidos mediante determinados procedimentos” (SARLET, 2021, p. 40). A informação, resultado da interpretação dos dados, “pode apresentar-se como numérica, gráfica, fotográfica, acústica, enfim, de qualquer tipo, importa que represente um dado, que já tem significado por si só, ou um conjunto de dados reunidos” (VIEIRA, 2007, p. 224)[55]. A informação ganhou mais importância com a tecnologia, pois passou a ser possível armazená-la e organizá-la para utilização posterior, passando a ser utilizada para diversos fins. Ao passo que quanto mais as atividades dependem de informações para serem realizadas, maior a sua importância, bem como maior a possibilidade de influir no dia a dia das pessoas (DONEDA, 2006, p. 153).

Segundo Doneda (2006, p. 155), as primeiras interpretações em torno do termo informação estavam mais relacionadas com fenômenos relacionados a ela, tais como a fala ou a comunicação. Nesse primeiro estágio a informação era classificada com um tom mais fenomenológico – tinha-se o entendimento de que “toda mensagem comunicável a alguém por um meio qualquer constitui uma informação” (DONEDA, 2006, p. 155).

A noção da informação relacionada com sua faceta funcional para a sociedade, economia ou política surgiu mais tarde. O termo “informação” apenas chamou atenção dos estudiosos em meados do século XX, com o desenvolvimento da tecnologia. Nesse sentido, é interessante pontuar que em 1962 foi inserido no dicionário oficial da língua francesa o conceito de “tratamento automatizado de informações”. Esse conceito expandiu-se atingindo outros idiomas – dessa expansão surgiu o termo “informática” na língua portuguesa, sendo considerado um marco, pois revolucionou a disciplina jurídica sobre informação (DONEDA, 2006, p. 169). O novo conceito ganhou novos desdobramentos, pois estava interligado com as mudanças que vinham ocorrendo na sociedade, tais como o desenvolvimento das tecnologias da informação (DONEDA, 2006, p. 15).

As informações podem estar vinculadas a diversas modalidades, e, no presente trabalho, focaremos na modalidade da informação que diz respeito aos indivíduos e aos seus bens – aquela informação que possui um “vínculo objetivo com uma pessoa, revelando algo

55 Ademais, a informação contém um atributo de sentido que depende do contexto em que é obtida, “mediante observação, comunicação ou dados para posterior utilização, sempre dependentes (ou associados) a um processo de interpretação”. Logo, podem existir informações que não estão relacionadas ao tratamento de dados (coleta, processamento, transmissão, interpretação), o contexto social da informação em si está relacionado a outros valores também relevantes, tais como a privacidade ou a imagem (SARLET, 2021, p. 40-41).

sobre ela", ou seja, o objeto da informação são características ou ações de uma pessoa. Abarcando nessa modalidade de informação apenas o sentido de "pessoal". Assim, mesmo que relacionadas com uma pessoa, encontram-se fora do sentido de "pessoal" as opiniões formuladas por terceiros referentes a uma pessoa, bem como a produção intelectual, que, considerada em si mesma, não é tida como uma informação que possua um vínculo objetivo com o seu autor ou inventor, pois "não é *per se* informação pessoal (embora o fato de sua autoria o seja)" (DONEDA, 2005, p. 156).

Tal modalidade de informação que mantém uma ligação estreita com uma pessoa é classificada como "pessoal", ao passo que essa informação trazer elementos que compõem um sujeito de direito ganha tamanha relevância que é considerada um atributo da personalidade. Esse entendimento foi utilizado pelo Conselho da Europa, por meio da Convenção de Strasbourg ou Convenção nº 108, de 1981, definindo informação pessoal em seu artigo 2º como "qualquer informação relativa a uma pessoa singular identificada ou susceptível de identificação". Assim, é nítido que o fato que define uma informação como pessoal é a característica de estar ligada diretamente a uma pessoa, "revelando algum aspecto objetivo desta" (DONEDA, 2011, p. 94).

Nesse sentido, informação pessoal é aquela que possui um vínculo objetivo com a pessoa, ou seja, por refletir características que lhe dizem respeito. Dentro da informação pessoal encontram-se os dados *per se* que igualmente detêm aspectos da pessoa que fazem referência. Logo, esses dados podem ser denominados como dados pessoais e dizem respeito a circunstâncias, relações, intimidades, comportamentos que se relacionam a circunstâncias pessoais ou matérias de uma pessoa identificada ou identificável (MENDES, 2008, p. 70-71). Ademais, informação pessoal está relacionada a uma pessoa física identificável ou identificada, são fragmentos de informações capazes de se relacionar a uma pessoa em concreto (SCHAEFER, 2010, p. 48), "independentemente do suporte em que se encontre registrado (escrita, imagem, som ou vídeo)" (VIEIRA, 2007, p. 224).

No tocante à expressão "pessoa identificada ou identificável", se faz importante ressalvar que existem duas interpretações possíveis sobre a abrangência do conceito de dados pessoais. A primeira interpretação de dados pessoais é denominada expansionista, possuindo uma definição alargada de dados pessoais, entendendo como dados pessoais aqueles relacionados a uma pessoa identificada – uma pessoa já conhecida – bem como entende ser dado pessoal se a pessoa for identificável, ou seja, a pessoa num primeiro momento pode não

ser determinada de pronto (BIONI, 2019, p. 60). Contudo, apesar do vínculo ser mediato, indireto ou inexato, é possível reconhecer a pessoa "através de recursos e meios à disposição de terceiros. Um exemplo de dado pessoal é o IP atribuído a um determinado computador quando este se conecta à rede" (VIEIRA, 2007, p. 224). Nesse sentido, podemos dizer que a corrente expansionista alarga a qualificação do dado como pessoal[56].

Por outro lado, outra corrente retrai a qualificação do dado como pessoal. A interpretação reducionista entende que dados pessoais são aqueles que ligam a uma pessoa identificada, já conhecida, uma pessoa específica e determinada em que o vínculo é imediato, direto, preciso e exato. A definição reducionista retrai a qualificação do dado como pessoal, retirando do seu conceito a hipótese de pessoa identificável (BIONI, 2019, p. 60).

No entanto, existem dados que podem estar relacionados a pessoas indeterminadas, tais como ocorre na representação de informações referentes a um determinado grupo ou alguma comunidade, sem que haja a individualização das pessoas pertencentes a esses arranjos. Por exemplo, "os dados relativos ao fluxo telefônico de uma determinada concessionária de telecomunicações, sem a identificação pessoal de quem realizou as chamadas" (DONEDA, 2006, p. 157). Estes dados podem ser considerados como dados anônimos[57], pois não estão relacionados com uma pessoa identificada, e nem há como identificar a pessoa com base nas informações existentes. O dado sendo anônimo, sendo incapaz de revelar a identidade de uma pessoa, não chama para si a qualidade de pessoal, sendo outra espécie de informação – que não terá a proteção especial que existe para os dados pessoais. Assim, dados anônimos são dados que após um processo de tratamento tornam-se incapazes de qualquer tipo de identificação pessoal (MENDES, 2008, p. 72), ou, como definido pelo Grupo de Trabalho (29 Working Party), dados anônimos seriam dados que num momento posterior faziam referência a uma pessoa identificável, porém, após o processo de

---

56 A legislação brasileira adota o conceito expansionista de dados pessoais, seguindo o exemplo da União Europeia. Em contrapartida, países como os Estados Unidos da América adotam uma concepção reducionista de dados pessoais, pois na perspectiva adotada dado pessoal é o dado que identifica determinada pessoa (SCHWARTZ; SOLOVE, 2011, p. 1837).

57 Existem várias técnicas de anonimização de dados. A técnica mais comum é a da supressão. Nessa técnica um administrador de dados suprime algumas partes, excluindo ou omitindo. Por exemplo, o administrador de dados de um hospital retira o nome dos pacientes das prescrições. Dessa forma não estaria identificando uma pessoa, o que poderia ser considerado como anônimo. Contudo, uma supressão "exagerada" pode fazer com que os dados sejam inúteis. Nesse sentido, buscando um equilíbrio entre privacidade e utilidade, a técnica da supressão é aliada à técnica da generalização. Aqui, ao invés de suprimir identificadores, eles serão trocados por um elemento geral – por exemplo, ao invés de deixar a data de nascimento, deixar apenas o ano; ao invés de deixar o endereço completo, manter apenas os três primeiros dígitos do Código Postal (OHM, 2010, p. 1708-1710).

tratamento, não é mais possível identificar a pessoa, isto é, as técnicas de anonimização impedem que o dado volte ao estado de dado pessoal (29 WORKING PARTY, 2016, p. 8).

Segundo Schaefer (2010, p. 49), para caracterizar um dado como identificável ou não se leva em "consideração do conjunto de meios que se possam razoavelmente utilizar para identificar tal dado. Quanto maior o esforço exigido, maior é a dissociação entre a pessoa e seus dados". Existindo meios razoáveis de identificar a pessoa, não podemos definir os dados como anônimos, sendo ainda considerados dados pessoais – dentro da concepção expansionista de qualificação de dados pessoais (em que faz referência também a uma pessoa identificável e não somente uma pessoa identificada). Logo, para que o dado seja considerado como pessoal, precisa existir uma correlação entre o dado e uma pessoa, bem como o esforço exigido para relacionar o dado à pessoa não passe dos limites do razoável. A possibilidade de um dado ser atrelado a uma pessoa por meio de esforços desarrazoáveis não é capaz de atrair a definição de identificável e, assim, ser considerado um dado pessoal. Há a necessidade de um esforço razoável. A razoabilidade é o filtro que define quais os dados de pessoas identificáveis que serão considerados como dados pessoais (BIONI, 2019, p. 66). Nesse sentido, a Lei Geral de Proteção de Dados (Lei nº 13.709/2018), LGPD, definiu dado anonimizado como sendo o "dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento", bem como definiu o conceito de anonimização como a "utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo".

O filtro da razoabilidade é necessário, até porque existe uma impossibilidade teórica no processo de completa anonimização de dados pessoais. Segundo Bioni (2019, p. 63), "a representação simbólica de que os vínculos de identificação de uma base de dados poderiam ser completamente eliminados, garantindo-se, com 100% (cem por cento) de eficiência, o anonimato das pessoas, é um mito". Isto ocorre porque existe uma gama enorme de dados pessoais disponíveis, existindo o risco de cruzamento de dados, *a priori* não identificados, que com a sobreposição com outra base de dados[58] anonimizada passe a reidentificar as pessoa.

58 Banco de dados, segundo Bioni (2019, p. 33), deve ser atrelado com a ideia de sistema de informação, "cuja dinâmica explicita, sequencialmente, um processo que se inicia pela coleta e estruturação dos dados, perpassa a extração de uma informação que, por fim, agrega conhecimento". Logo, um sistema de informação é uma reunião de dados que foram coletados (entrada), manipulados (processo) e disseminados (saída) com algum fim específico. "A dinâmica de um banco de dados envolve entrada (*input*) e o processamento de dados

Logo, há a necessidade de analisar os dados dentro de um contexto (SCHWARTZ; SOLOVE, 2011, p. 1836). O caso Netflix Prize é emblemático na possibilidade de reidentificação de dados anônimos. Dois pesquisadores – Arvind Narayanan e Vitaly Schmatikov – desenvolveram um algoritmo para facilitar o processo de reversão de dados anônimos. No mesmo período a Netflix[59] lançou um concurso visando a melhorar o seu algoritmo de sugestões de filmes. Para isso a provedora de streaming forneceu a sua base de dados com todas as apreciações dos filmes do seu catálogo realizadas pelos usuários no período de 1998 a 2005. Os nomes dos usuários foram excluídos, estando disponível apenas a data e a nota dada ao filme. Os pesquisadores rodaram o seu algoritmo na base de dados, entendida como anônima, disponibilizada pela Netflix e descobriram que seria possível reverter o processo de anonimização com 3 (três) a 9 (nove) bits de informação. E que as informações necessárias estavam disponíveis on-line no site do seu catálogo / IMDB – base de dados on-line de informação sobre cinema, TV, música e games – em que as pessoas compartilham suas opiniões sobre filmes. Por conseguinte, os pesquisadores "cruzaram" as informações contidas na base de dados do IMDB com a base de dados disponibilizada pela Netflix, "correlacionando as datas das avaliações dos filmes e seus respectivos *scorings*. Assim, a peça faltante do quebra-cabeça – a identidade dos usuários da Netflix – foi desvendada com base nos nomes contidos nas avaliações do IMDB" (BIONI, 2019, p. 64).

Em complemento ao exemplo apresentado, Schwartz e Solove (2011, p. 1836) apontam o estudo da professora de Ciência da Computação de Harvard Latanya Sweeney, que demonstrou que a combinação de um CEP, data de nascimento e gênero são os dados necessários para identificar 87% (oitenta e sete por cento) das pessoas residentes nos Estados Unidos, dados que, num primeiro momento, eram compreendidos como incapazes de

---

e a saída (*output*) de uma informação. É imprescindível, portanto, o gerenciamento, manual ou automatizado, de um banco de dados, para que dele seja extraído algum conhecimento" (BIONI, 2019, p. 32). Por tal razão, Lyon (1994, p. 46) conceitua banco de dados como todo sistema de processamento de dados que permite a recuperação seletiva de informações. Assim, os dados são o coração do banco de dados, e podem ser constantemente coletados e atualizados. Dentro de um banco de dados, dados são organizados de modo que um fato esteja arquivado e codificado dentro de uma linguagem padrão. Além do mais, o banco de dados pode ser relacional, ou seja, assume a forma de uma lista tabular e, portanto, pode ser comparado com outros bancos de dados, como no caso Netflix. Para arrematar, podemos dizer que banco de dados é a ferramenta que organiza o tratamento de dados pessoais, sendo um conjunto organizado e lógico de dados, de fácil utilização e acesso (MENDES, 2008, p. 73). E que não deve ser entendido como somente um agrupamento lógico e inter-relacionado do estado primitivo da informação, mas são, também, um ferramental que deve criar uma interface para auxiliar na tomada de decisão (BIONI, 2019, p. 30). A legislação brasileira de Proteção de Dados, LGPD, conceituou banco de dados como "conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico".

59 Provedora global de filmes e séries de televisão via *streaming* – forma de distribuição digital de dados, geralmente através da internet –, e que atualmente possui mais de 208 milhões de assinantes.

identificar uma pessoa. Ademais, outro estudo da professora Latanya Sweeney demonstrou preocupação com muitos bancos de dados de saúde ditos anônimos, pois, mesmo que não identificado os titulares desses dados, considerando a individualidade que esses dados possuem, torna-se fácil reverter a anonimização. Segundo a professora, dados médicos desprovidos de informações, como nomes, endereços, números de telefone e número do Seguro Social não podem ser considerados realmente anônimos, uma vez que o restante dos dados existentes pode ser utilizado para identificar as pessoas – ligando, combinando, cruzando esses dados com outros bancos de dados, bem como pela análise de características únicas dos dados de saúde disponíveis nesses bancos de dados ditos anônimos. Em outro estudo, Sweeney, em coautoria com Bradley Malin, demonstrou que os dados do genoma humano podem ser facilmente identificados caso a instituição de saúde realize troca de informações (SCHWARTZ; SOLOVE, 2011, p. 1845)[60].

Dentro dessa perspectiva, qualquer banco de dados anônimos ainda detém o risco de "se transmutar em um dado pessoal" (BIONI, 2019, p. 65). Pois mesmo que as informações identificadoras em um banco de dados sejam suprimidas, o mundo está inundado de dados sobre as pessoas, de modo que cruzando as informações com bancos de dados externos é possível identificar dados anônimos (OHM, 2010, p. 1724)[61]. "Agregação de diversos 'pedaços' de informação (dados) pode revelar (identificador) a imagem (sujeito) do quebra-cabeça, a qual era até então desfigurada (anônimo) – o chamado efeito mosaico" (BIONI, 2019, p. 65). Pois, conforme os exemplos expostos, a tecnologia tornou possível que

60 Outro exemplo de que os dados anônimos podem se tornar identificáveis é o caso AOL. Buscando criar uma comunidade de pesquisa aberta, a AOL teve a ideia de divulgar num site as consultas realizadas em seu buscador. Nesse site, divulgou 20 milhões de consultas realizadas por 650.000 usuários dentro de um período de três meses. No entanto, antes de divulgar a AOL tentou tornar esses dados anônimos. Para isso ela suprimiu as informações de identificação óbvias, tais como nome, endereço de IP, dentro outros. Para preservar a utilidade, substituiu esses identificadores por números. Assim, os pesquisadores conseguiriam relacionar as pesquisas com usuários individuais (no caso, um número). Contudo, o repórter Michael Barbaro conseguiu identificar o usuário 4417749 com base nas suas pesquisas como "paisagistas em Lilburn, Georgia"; "Várias pessoas com sobrenome Arnold", encontrando Thelma Arnold, uma senhora de 62 anos de idade, viúva de Lilburn, Georgia, que reconheceu ser autora das pesquisas, incluindo outras consultas um pouco embaraçosas, tais como "dedos dormentes"; "homens 60 solteiros" e "cachorro que urina em tudo". Tal caso veio a demonstrar a fragilidade que pode existir num processo de anonimização (OHM, 2010, p. 1718).

61 Ohm (2010, p. 1725-26) utilizou um exemplo fácil de entender como funciona a reidentificação – imagine uma pessoa cruzando os dedos das mãos como se fosse realizar uma prece, agora imagine que a mão direita detém dados anônimos, a mão esquerda são as informações extras, e entre os dados intercalados são lugares onde as informações se ligam com as informações faltantes, identificando a pessoa. Essa operação é denominada de "junção interna", uma operação que combina duas tabelas de dados de bancos de dados distintos, conectando as linhas de uma tabela com a da outra. Quando essas linhas representam pessoas, a sua junção com outras tabelas pode identificar as pessoas.

informações sejam pesquisadas e organizadas por diferentes tipos de atributos, não precisando mais de indicadores específicos como nome ou sobrenome para identificar uma pessoa na multidão. Essa nova tecnologia mudou a forma como as informações podem ser vinculadas a uma pessoa. No passado essa ligação entre dados e pessoas específicas quase que invariavelmente teria que vincular ao nome ou algo semelhante. Hoje não existe mais essa necessidade. Sistemas computadorizados de registro e técnicas de agregação de dados permitiram a análise de muitos pedaços de dados pessoais que, cruzados, podem individualizar com precisão uma pessoa (SCHAWARTZ; SOLOVE, 2011, p. 1820).

Assim, o conceito de dado pessoal como o oposto de um dano anônimo apenas poderia ser aceito se dado pessoal fosse considerado dentro do conceito reducionista. Caso contrário, como todo dado tem o potencial de identificar alguém e estaria atrelado a uma pessoa identificável. Assim, todo dado – mesmo anônimo – seria um dado pessoal. No entanto, esse raciocínio não deve prosperar, pois, além do adjetivo "identificável" para o dado ser considerado um dado pessoal, precisa acrescentar um critério de razoabilidade. Assim, o esforço para relacionar um dado a uma pessoa precisa ser razoável, para que esse dado seja considerado como pessoal (BIONI, 2019, p. 66-67). Nas palavras de Bioni (2019, p. 66), o vinculo que existe entre o dado e a pessoa

> [...] deve ser objeto de um "esforço razoável", sendo esse o perímetro de elasticidade do conceito de dado pessoal como aquele relacionado a uma pessoa identificável. A *contrario sensu*, se para a correlação entre um dado e uma pessoa demanda-se um esforço fora do razoável, não há que se falar em dados pessoais. Nessa situação, o dado é considerado como anônimo, uma vez que o "filtro da razoabilidade" barra o seu enquadramento como aquele relacionado a uma pessoa identificável.

Ademais, existiria uma espécie de dado que estaria a "meio do caminho" entre um dado pessoal e um dado anônimo. Seriam dados pseudoanonimizados – isto é, dados que sofreram um processo de retirada de identificadores, minimizando os riscos de uma atividade de tratamento de dados (BIONI, 2019, 69-70). Logo, a pseudononimização é um processo que visa a mitigar os riscos no tratamento de dados pessoais, em que há uma "transposição de identificadores (como nomes e datas de nascimento) numa nova designação, de preferência por criptografia, para que o destinatário da informação não possa identificar a pessoa em causa" (BARBOSA; LOPES, 2021, p. 46). No entanto, apesar de mitigar os riscos, os dados não perdem por completo o caráter de pessoal (BIONI, 2019, p. 70).

Nesse sentido, como bem destacado pelo Grupo de Trabalho de Proteção de Dados (29 Working Party), a pseudonimização não é um método de anonimização. Nesse processo há uma diminuição na capacidade de ligação dos dados com a pessoa (29 WORKING PARTY, 2016, p. 4), é um instrumento de segurança útil. As técnicas de pseudonimização mais utilizadas são: a criptografia, *hash function*, *keyed-hash function with stored key*, *keyed-hash function with deletion of the key* e tokenização (29 WORKING PARTY, 2016, p. 20-21). No entanto, mesmo com a utilização dessas técnicas a informação pseudoanonimizada continua sendo um dado pessoal, já que o processo é reversível, não afastando a proteção de dados nesses casos (BARBOSA; LOPES, 2021, p. 49).

Ademais, mesmo não sendo uma técnica de anonimização, as legislações reconhecem que a pseudonimização aumenta a segurança e incentivam a sua prática. O GDPR, Regulamento Geral sobre Proteção de Dados da Europa, define pseudonimização em seu artigo 4º da seguinte forma:

> Pseudonimização, o tratamento de dados pessoais de forma que deixem de poder ser atribuídos a um titular de dados específico sem recorrer a informações suplementares, desde que essas informações suplementares sejam mantidas separadamente e sujeitas a medidas técnicas e organizativas para assegurar que os dados pessoais não possam ser atribuídos a uma pessoa singular identificada ou identificável.

A Lei de Proteção de Dados brasileira, LGPD, define pseudonimização no § 4º do artigo 13, como sendo "tratamento por meio do qual um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo, senão pelo uso de informação adicional mantida separadamente pelo controlador em ambiente controlado e seguro". Tal artigo faz referência à realização de estudos em saúde pública, em que órgãos de pesquisa poderão ter acesso a bases de dados pessoais, que dentre outros comandos recomenda a anonimização ou pseudonimização dos dados como forma de manter a segurança dos mesmos, bem como que sejam levados em consideração os devidos padrões éticos relacionados a estudos e pesquisas.

Ainda sobre o conceito de dados pessoais, podemos afirmar que eles dizem "respeito às informações inerentes a cada ser humano. Pode-se dizer que os elementos que o compõem equivalem-se a um código de barras" (AMARAL, 2019, p. 115). A analogia utilizada por Amaral é interessante, pois, assim como os códigos de barras são utilizados para diferenciar e auxiliar na localização dos bens, os dados pessoais diferenciam as pessoas e do mesmo modo

podem localizar ou especificar pessoas dentre as demais. Tal fenômeno foi exemplificado com os usos de bancos de dados pessoais.

Ademais, conforme visto, a sociedade hodiernamente depende de informações. “As sociedades informacionais são sociedades pós-industriais que têm a economia fortemente baseada em tecnologias que tratam informações como seu principal produto” (SILVEIRA, 2017, p. 16). Os dados pessoais possuem um valor na sociedade tendo em vista o surgimento de uma economia de dados, que será mais bem trabalhada no item 3.3, mas, adiantando um pouco a temática, o dado pessoal possui um valor de mercado pois os dados são coletados, tratados e difundidos com finalidades comerciais (RODOTÀ, 2008, p. 99). Então os dados pessoais poderiam ser considerados bens de propriedade do titular dos dados? Ou, conforme questionou Mendes (2008, p. 113), citando Simson Garfinkel, “a quem pertencem os dados pessoais?” Esses questionamentos não possuem uma resposta simples, principalmente pelo valor que os dados pessoais possuem na Sociedade da Informação, que desenvolveu um verdadeiro mercado de informações pessoais (MENDES, 2008, p. 113).

Diante da viabilidade de comercialização dos dados pessoais, uma parte da doutrina passou a admitir a possibilidade de “garantir um direito de propriedade sobre os dados pessoais, sob o pretexto de que o direito tem de se adequar à realidade social” (MENDES, 2008, p. 113). Assim, na sociedade pós-industrial, em que há o fenômeno da desmaterialização das riquezas, desenvolvimento dos mercados financeiros e valorização de bens incorpóreos, não seria estranho atribuir a qualidade de bem patrimonial ao dado pessoal (um bem imaterial) (DONEDA, 2006, p. 165).

Exatamente por existirem interesses em jogo, tanto sociais como econômicos, a definição de dados pessoais não é pacífica, nem meramente científica, pois, dependendo da qualificação atribuída ao dado pessoal, pode existir maior facilidade ou dificuldade legal a um corretor de dados (*broker*) para coletá-lo e vendê-lo (SILVEIRA, 2017, p. 60). Nesse sentido, alerta Rodotà (2008, p. 100) que existem duas formas de enxergar a situação: uma aceitando incondicionalmente a lógica de mercado, e a outra fixando normativas para proteção de dados; de um lado temos os dados como atributos da personalidade humana, do outro a qualificação dos dados pessoais como “mera atribuição de títulos de propriedade livremente negociáveis no mercado; entre situações de inalienabilidade dos direitos individuais e a possibilidade de dispor de tais direitos”. Ilustrando esse cenário de jogo de interesses, Silveira (2017, p. 60) escreve:

> Representantes de agências de análise de crédito, por exemplo, defendem que dados cadastrais e biométricos não devem ser considerados dados pessoais, não devem requerer autorização para o seu tratamento, uma vez que são de interesse dos agentes econômicos, da polícia e, por conseguinte, seriam de interesse de toda a sociedade. Para alguns segmentos da economia informacional, quase nada deveria ser considerado um dado pessoal.

Lawrence Lessig, conhecido como um dos defensores da uma visão patrimonialista dos dados pessoais, acredita que a proteção que deve ser dada aos dados pessoais deve ser a mesma que é fornecida às criações e invenções, uma espécie de proteção equivalente à existente na propriedade intelectual. Isto porque a propriedade intelectual é mais bem protegida, uma vez que existe investimento visando a essa proteção. Ao passo que os dados pessoais, apesar de valiosos, não têm o mesmo investimento visando a sua proteção e controle. Logo, se houvesse maior investimento em proteger esses dados, eles seriam mais bem protegidos e para isso a lógica seria dar a eles um tratamento de bem imaterial. Os dados pessoais poderiam ser negociados dentro dos já existentes mercados digitais, porém os termos seriam mais transparentes e as pessoas teriam maior liberdade nas negociações. Ademais, dando aos dados pessoais conotações de proprietárias, os usos indevidos de dados ou sua apropriação indevida teriam o mesmo tipo de punição do "roubo" (LESSIG, 2002, p. 250-55). Nesse sentido, considerando o alto valor atribuído aos dados pessoais, que incentiva o seu comércio e que ao mesmo tempo acarreta na violação de direitos, tais como a privacidade dos titulares dos dados pessoais que não sabem ou que não consentiram no tratamento de seus dados. Visando minimizar essas externalidades negativas, existe a defesa que "tal custo seja internalizado por quem usa o dado, exigindo que ele pague por isso" (MENDES, 2008, p. 114).

Porém, defender que dados pessoais possam ser qualificados como bens patrimoniais na visão de Mendes (2008, p. 114-15) apresenta três problemas graves. O primeiro é que esse modelo de negócio acabaria violando o princípio da igualdade, pois apenas quem possui condições financeiras conseguiria optar pela proteção de seus dados. O segundo reside no fato de que haveria uma diminuição da individualidade e o surgimento de indivíduos direcionados ao mercado, pois poderia induzir as pessoas a mentirem a sua personalidade, moldando para atrair condições no mercado de dados, e assim "conseguir melhores condições de comercialização de suas informações pessoais". O terceiro diz respeito à ameaça ao princípio da democracia, uma vez que a efetividade da democracia tem como "fundamento a proteção

da liberdade e da igualdade dos cidadãos, bem como de sua personalidade, que seriam afetados, caso essa hipótese fosse implementada".

Em sentido semelhante, Doneda (2006, p. 166) não entende como uma solução adequada tutelar dados pessoais como sendo bens patrimoniais, uma vez que os dados pessoais abarcam em seu conceito inúmeras situações, não se limitando apenas aos vetores patrimoniais. Assim, Doneda (2006, p. 168) procura conceituar dados pessoais dentro de uma lógica mais objetiva, sem tender a uma patrimonialização do dado pessoal. Busca-se "estabelecer referências objetivas na informação em si e não somente no sujeito ao qual ela é relacionada". A objetivação significa que os dados pessoais devem possuir um tratamento pragmático – a proteção a esse tipo de bem deve voltar-se a um caráter instrumental. "A informação pessoal em certo sentido pode ser desvinculada da pessoa e tornar-se exterior a esta: ela pode circular, submeter-se a certo tratamento, ser comunicada, etc." (DONEDA, 2006, p. 168) Contudo, fazendo referência a um dado pessoal continua existindo um vínculo especial com o seu titular, e o dado pessoal deve ser valorado com base neste vínculo que confere a esse dado uma qualificação especial, confere ao dado pessoal um atributo da personalidade, pois é "uma representação direta da personalidade" da pessoa – "tal informação deve ser entendida como uma extensão da sua personalidade". Esse reconhecimento supera o "critério formal da posse das informações. Acima do critério proprietário, fundado na legitimidade da coleta e do tratamento de informações relativas a outras pessoas, prevalece o direito fundamental da pessoa à qual se referem as informações" (RODOTÀ, 2008, p. 97).

Traçado esse panorama, pode-se concluir que "dados pessoais referem-se às informações inerentes a uma pessoa singular, estabelecendo uma ligação direta com o tratamento informático e os direitos voltados à dignidade humana" (AMARAL, 2019, p. 115). Os dados pessoais são vinculados a uma pessoa identificável ou identificada, que no contexto das novas tecnologias de comunicação e informação são obtidos por meio de inúmeras ações da vida cotidiana. Por conseguinte, dados pessoais podem ser retirados dos pagamentos com cartão de crédito, que detêm as informações do valor da compra, o local, a data da transação de determinada pessoa; os dados registrados por empresas de telefonia: registros de ligação, duração, data e os destinatários das ligações; antenas de celulares que captam a passagem das pessoas em determinadas regiões, mecanismos de geolocalização, dentre outros. "Além disso, há todo o conjunto de dados (texto, vídeo, fotos, etc.) despejados diariamente nas redes

sociais[62], em sites, blogs, em cadastros virtuais" (MARINELI, 2017, p. 134). Dentre os exemplos citados, é possível traçar um paralelo com o conceito atribuído aos dados pessoais disposto no Relatório do Fórum Econômico Mundial como sendo

> [...] informações e metainformações criadas por e sobre as pessoas, abrangendo: dados oferecidos voluntariamente (exemplo: perfil na rede social), dados observados (como: dados de localização ao usar os celulares) e dados inferidos (exemplo: análise de informações oferecidas ou observadas com a finalidade de construir uma pontuação de crédito) (SILVEIRA, 2017, p. 60).

Seguramente, dados pessoais retratam qualidades e particularidades de seus titulares, descrevendo peculiaridades de suas vidas, e por tal razão requerem cuidado especial, pois "estão, inquestionavelmente, entrelaçados com inúmeros direitos, liberdade e garantias essenciais para o desenvolver da vida humana" (AMARAL, 2019, p. 115). Os dados pessoais devem ser compreendidos como prolongamentos de um sujeito, não estando limitados apenas a um tipo de "projeção imediata, mas, também, a um referencial mediato que pode ter ingerência na esfera de uma pessoa" (BIONI, 2019, p. 65). Assim, a formulação de "dados pessoais", qualquer informação relativa a uma pessoa física identificada ou identificável, abarca uma estreita relação entre "o tratamento informático e os direitos à dignidade da pessoa humana, do desenvolvimento da personalidade, da integridade pessoal e da autodeterminação informativa" (AMARAL, 2019, p. 113).

A proteção de dados tem por objetivo final proteger a dignidade da pessoa humana, "valor-fonte do ordenamento jurídico brasileiro (art. 1º, III, CF)" (SCHAEFER, 2010, p. 169)[63]. Deve ser entendida, tal proteção, como um novo direito da personalidade, pois os dados pessoais "influem na projeção de uma pessoa e na sua esfera relacional" (BIONI, 2019, p. 59). Dessa forma, o olhar da proteção deve voltar-se ao indivíduo, à pessoa humana, e não na base de dados em si, "especificamente se o perfil comportamental pode ser ou não atribuído a uma pessoa em específico. Ou seja, o foco não está no dado, mas no seu uso – para

62 "O pesquisador de segurança da informação Bruce Schneier define seis tipos de dados pessoais com base nas plataformas de relacionamento social online: dados de serviços, fornecidos para abrir uma conta (por exemplo, nome, endereço, informações de cartão de crédito, etc.); dados divulgados, que são introduzidos voluntariamente pelo usuário; dados confiados, como comentários feitos sobre outras pessoas; dados incidentais, sobre um usuário específico, mas enviados por outra pessoa; dados comportamentais, que contêm informações sobre as ações que os usuários realizam ao utilizar um site e são utilizados pela publicidade segmentada; e os dados inferidos, que são as informações deduzidas dos dados, perfil ou atividade" (SILVEIRA, 2017, p. 61).

63 A proteção jurídica da privacidade será melhor trabalhada no item 4.1.

formação de perfis comportamentais –, sua consequente repercussão na esfera do indivíduo" (BIONI, 2019, p. 78). A proteção de dados volta-se ao uso dos dados pessoais, podendo ser entendida como um instrumento necessário, dentro da nova conjuntura social, para garantir o livre desenvolvimento da personalidade humana, havendo uma forte conexão entre a proteção de dados e os direitos de liberdade, dignidade, privacidade, igualdade, de modo que a proteção dos dados pessoais se torna fundamental para caracterizar a cidadania (e até o ideal democrático) no novo milênio. Isto porque, com o enorme fluxo informacional, as pessoas correm o risco de serem discriminadas em razão de suas opiniões, crenças religiosas, condições de saúde, ideologias, convicções políticas (RODOTÀ, 2008, p. 233). Desse modo, proteger dados pessoais não é uma consequência de um aspecto proprietário, mas sim é um meio de proteger a personalidade, "sendo, por isso, um direito fundamental que confere instrumentos que possibilitam tornar mais controlável a esfera privada e possível promoção da cidadania" (SCHAEFER, 2010, p. 170).

Ademais, a Lei Geral de Proteção de Dados (LGPD) – Lei nº 13.709/2018 – conceitua dado pessoal como "informação relacionada a pessoa natural identificada ou identificável". Conforme visto, a proteção de dados está atrelada ao recurso da identificabilidade, que pode se dar de modo direto ou indireto, por meio de um número de identificação ou por meio de "mais fatores específicos de sua identidade física, psicológica, mental, econômica, cultural ou social" (ANDRADE, 2011, p. 92). O conceito adotado pela legislação brasileira tem muita semelhança com o elegido pelo Regulamento Geral sobre Proteção de Dados da Europa (GDPR), que definiu dados pessoais, em seu artigo 4º, como "informação relativa a uma pessoa singular identificada ou identificável (titular dos dados)". O GDPR também define o conceito de "pessoa identificável" como

> [...] uma pessoa singular que possa ser identificada, direta ou indiretamente, em especial por referência a um identificador, como por exemplo um nome, um número de identificação, dados de localização, identificadores por via eletrônica ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, económica, cultural ou social dessa pessoa singular.

Percebe-se que a proteção conferida aos dados pessoais não está limitada a dados sensíveis, porém existem dados que requerem um nível de proteção maior, "quando estiver em causa a esfera mais interna da privacidade, designadamente, a intimidade" (DONEDA, 2021, p. 33). Quanto mais as informações pessoais estiverem relacionadas ao direito de privacidade, bem como de igualdade e não discriminação, "mais restrições deverão ser

impostas no que se refere a utilização e recolha desses dados, que constituem os bancos de dados" (AMARAL, 2019, p. 113).

Nesse sentido, Vieira (2007, p. 228) classifica os dados pessoais em três espécies: não sensíveis; sensíveis; e de tratamento proibido. A autora, para facilitar o entendimento dessas três espécies de dados pessoais, classifica-os segundo a teoria alemã das esferas. Assim, os dados não sensíveis estariam na primeira esfera, a esfera da privacidade. Os dados sensíveis estariam na segundo nível, a esfera da intimidade. Por fim, os dados de tratamento proibido estariam no centro, na esfera do segredo. Apesar de concordar que existem espécies diferentes de dados pessoais, a relação direta entre dados sensíveis e a intimidade, mesmo que existente, não parece ser a melhor definição. Assunto que iremos trabalhar melhor no próximo item.

3.2 DADOS SENSÍVEIS

Os dados pessoais podem ser divididos em diferentes espécies. Contudo, todo e qualquer dado pessoal merece proteção (VIEIRA 2007, p. 231). Porém, existem tipos de "informações que, caso sejam conhecidas e processadas, prestar-se-iam a uma potencial utilização discriminatória ou particularmente lesiva e que apresentaria maiores riscos potenciais que a média, para a pessoa e não raro para a coletividade" (DONEDA, 2006, p. 160-161). Desse modo, levando em consideração o maior risco de alguns dados serem utilizados como ferramentas de discriminação de pessoas, tornou-se necessária a criação de uma categoria autônoma de dados para preservar princípios caros, tais como o da igualdade (RODOTÀ, 2008, p. 236).

Assim, existindo a necessidade de uma maior proteção, foi criada uma categoria específica de dados pessoas: os dados pessoais sensíveis. "Trata-se de informações relacionadas a uma esfera absoluta de intimidade, tratados coletiva e individualmente, e que são mais suscetíveis a lesões e discriminações" (SANTOS et al., 2021, p. 273). Nesse sentido, a criação de uma categoria autônoma de dados pessoais está intimamente ligada aos riscos que o armazenamento, tratamento, processamento e fluxo de certas informações pessoais poderiam causar à personalidade da pessoa humana, principalmente no tocante a práticas discriminatórias (KORKMAZ, 2019, p. 42).

Tais dados, na prática, possuem efeitos distintos quando comparados com os demais dados pessoais. Esses efeitos diferenciados, segundo Doneda (2006, p. 161), advêm da necessidade de garantir o princípio da igualdade material, bem como o da privacidade, pois são dados que, pela natureza das informações, quando tratados apresentam um elevado potencial lesivo aos seus titulares. Então, designar um dado pessoal como sensível significa dizer que esse dado pessoal "deve ser especialmente protegido uma vez que a revelação de seu conteúdo pode potencialmente causar lesão ao seu titular ou a pessoa a ele vinculada" (SCHAEFER, 2010, p. 62).

Segundo Rodotà (2008, p. 78), os dados sensíveis seriam a representação do "núcleo duro da privacidade", pois são "dados relativos a opiniões políticas, sindicais ou de qualquer outro gênero, fé religiosa, raça, saúde, hábitos sexuais". Dessa forma, o resguardo aos dados sensíveis protegeria a privacidade, bem como evitaria a discriminação. Tais dados possuem em seu conteúdo uma forte intersecção com a privacidade. Portanto, pode-se constatar que os dados sensíveis são constituídos por dados que detêm uma forte carga privada (por exemplo, aqueles relacionados à saúde e aos hábitos sexuais). Apesar da grande proximidade, contudo, não são todos os dados sensíveis que estarão relacionados com a privacidade, pois, como bem pontuou Rodotà (2008, p. 96), os dados sensíveis também possuem em seu rol de proteção os dados que são manifestados em público, tais como as opiniões políticas e sindicais, bem como o credo religioso. "Ora a particularidade decorre do fato que as opiniões políticas e sindicais não podem ser confinadas somente à esfera privada: pelo menos nos Estados democráticos de direito elas são destinadas a caracterizar a esfera pública". Nesse sentido, as opiniões ou crenças do indivíduo fazem parte dele, e são manifestadas em público, porém, tais informações devem ser tuteladas com mais afinco para evitar que com sua circulação floresçam situações de discriminação.

Importante destacar que essa lesão não está apenas relacionada a violações de intimidade, "mas também, e às vezes, sobretudo, pelo risco que seu conhecimento possa provocar discriminação" (RODOTÀ, 2008, p. 106). Nesse sentido, podemos concluir que uma das características que diferem os dados sensíveis dos demais é a sua proximidade com uma vulnerabilidade específica: a discriminação (BIONI, 2019, p. 83). Alguns dados sensíveis estão "intrinsecamente ligados à privacidade, à intimidade das pessoas" (SANTOS et al., 2021, p. 277). São dados que podem revelar informações muito íntimas, abarcando um "fortíssimo estatuto 'privado'" (RODOTÀ, 2008, p. 96). Podemos concluir que a proteção dos

dados pessoais sensíveis abarca em seu entorno a salvaguarda de diferentes, e fundamentais, necessidades humanas.

Conforme visto, uma das características que definem um dado pessoal como sensível é a possibilidade de contribuir para a ocorrência de "processos sociais de exclusão e segregação" (KORKMAZ, 2019, p. 42). Para Mendes (2008, p. 231), possuem essa qualidade de sensível os dados: "genéticos, informações relacionadas com a saúde do indivíduo, filiação partidária ou sindical, convicções religiosas ou filosóficas, vida sexual". Complementando o quadro exemplificativo, Doneda (2006, p. 161) elenca, também, os dados sobre raça e o histórico médico.

Tal enumeração dos tipos de dados que seriam considerados sensíveis aparece nas definições legislativas que tratam sobre proteção de dados. Nesse sentido, a Regulamentação Geral sobre a Proteção de Dados (RGPD)[64] dispõe em seu artigo 9 um tratamento diferenciado a uma categoria especial de dados (dados sensíveis), sendo proibido, com algumas exceções elencadas no parágrafo segundo, o tratamento de dados que

> revelem a origem racial ou étnica, opiniões políticas, crenças religiosas ou filosóficas ou filiação sindical e o processamento de dados genéticos, dados biométricos com o objetivo de identificar de forma única uma pessoa singular, dados relativos à saúde ou dados relativos a um natural, à vida sexual ou à orientação sexual da pessoa.

Em sentido semelhante, a legislação brasileira passou a conceituar dados sensíveis (art. 5º, II, LGPD) como sendo: "dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural".

Ademais, a legislação brasileira abre o rol de dados que podem ser considerados sensíveis, por meio do §1º, do artigo 11 da LGPD, que dispõe que as hipóteses de tratamento de dados sensíveis se aplicam a qualquer dado sensível e a dados que possam causar danos ao seu titular. Demonstrando que tal categoria diferenciada de dados pessoais está diretamente relacionada com o alto risco existente quando da sua utilização, que podem causar danos – como discriminação e violação ao foro íntimo da pessoa (SANTOS et al., 2021, p. 277). A

64 "À semelhança do que acontecia com a Diretiva de 95, o Regulamento proíbe o tratamento de dados sensíveis" (BARBOSA; LOPES, 2021, p. 37).

proteção aos dados sensíveis pode ser utilizada para salvaguardar outros direitos, tais como o respeito à igualdade material e, por fim, à própria personalidade. Contudo, tais objetivos em proteger os dados sensíveis não aparecem na conceituação dada pelas legislações supramencionas em que elas se limitam a condicionar os dados sensíveis "com base no seu conteúdo informativo" (KORKMAZ, 2019, p. 44).

Embora tais objetivos não apareçam nos conceitos normativos, não há dúvidas do grau altamente discriminatório que tais dados possuem, caso conhecidos. Sobre o assunto, Rodotà (2008, p. 106) exemplifica que o conhecimento sobre a infecção de uma pessoa com o vírus HIV pode causar inúmeras segregações sociais, podendo se manifestar em forma de demissão ou não admissão quando esse dado é conhecido por empregadores, ou, se o dado for conhecido por uma seguradora, pode gerar a negativa de estipular um contrato de seguro. Igualmente, a utilização de uma informação relativa à saúde debilitada de uma pessoa para analisar um perfil de crédito poderia ser utilizada para definir uma taxa de juros e desse modo inviabilizar o acesso dessa pessoa "ao crédito, repercutindo no impedimento ou na dificuldade de acesso a bens e serviços, inclusive referentes à própria saúde" (KORKMAZ, 2019, p. 48). Tais hipóteses já ocorreram de modo semelhante na prática. Mulholland (2018, p. 174) cita que seguradoras coletaram dados públicos relacionados a vítimas de violência doméstica e passaram a sugerir que "mulheres vítimas de violência doméstica não poderiam contratar seguros de vida, saúde e invalidez". Em outro exemplo, bancos, caso tomassem conhecimento de que uma pessoa havia tido um derrame, passavam a exigir a quitação dos empréstimos realizados.

Desta forma, podemos concluir que a proteção dos dados sensíveis evita possíveis danos a direitos fundamentais, determinados pela qualidade e pela natureza dessa categoria de dados pessoais (MULHOLLAND, 2018, p. 162). De fato, a tutela de dados sensíveis proporciona exercer "o direito à saúde, à liberdade de expressão e de comunicação, à liberdade religiosa, bem como a liberdade de associação, na medida em que, resguardando essas informações, resguarda a pessoa para se desenvolver livremente". Por tais razões necessita de uma proteção mais robusta e diferenciada (KORKMAZ, 2019, p. 49).

No tocante à classificação de alguns dados pessoais como sensíveis, Doneda (2006, p. 162) apresenta algumas críticas doutrinárias realizadas a essa diferenciação. A primeira delas gira em torno do argumento de que é impossível antever o resultado do tratamento de um dado, seja sensível ou não. Assim, dados não considerados sensíveis, a depender do tipo de tratamento empregado, podem indicar fatos sobre a personalidade da pessoa, o que pode

dar ensejo a tratamentos discriminatórios. “Tal argumento leva, em síntese, a concluir que um dado, em si, não é perigoso ou discriminatório – mas o uso que dele se faz pode sê-lo”. Isto porque a nova realidade tecnológica possibilitou o tratamento e cruzamento de uma imensidão de dados pessoais, emergindo bancos de dados que traçam o perfil dos indivíduos, e em razão dessa nova realidade Rodotà (2008, p. 84) argumenta que essa diferenciação perdeu significado.

> Seja porque dados pessoais, aparentemente não “sensíveis”, podem se tornar sensíveis se contribuem para a elaboração de um perfil, seja porque a própria esfera individual pode ser prejudicada quando se pertence a um grupo do qual tenha sido traçado um perfil com conotações negativas.

Por este ângulo, Korkmaz (2019, p. 49) também realiza algumas críticas à categoria dos dados sensíveis. Primeiramente, que qualquer tratamento de dados pessoais pode acarretar em consequências discriminatórias. Ademais, tanto dados pessoais sensíveis como não sensíveis podem ser tratados e gerar um efeito discriminatório, mas que, ao contrário, atenda a um propósito legítimo. Deste modo, a sensibilidade dos dados deveria ser analisada dentro de um contexto de como os dados serão e são usados, “sob o argumento de que uma abordagem abstrata não seria suficiente para assinalar a potencialidade lesiva de um tratamento de dados”. Mendes (2008, p. 64) filia-se a essa ideia. Para a autora, mais importante que classificar um dado *a priori* como sensível é visualizar o tipo de tratamento que é dado para os dados pessoais, se esse tratamento tem o condão de transformar os dados em dados sensíveis. “Trata-se, na realidade, de um tratamento sensível dos dados, que é capaz de transformar dados inofensivos em informações potencialmente discriminatórias”.

A noção de tratamento sensível dos dados é importante, pois é preciso considerar os dados pessoais de acordo com o contexto em que eles serão utilizados. O conceito diferenciado dos dados pessoais sensíveis “atende a uma necessidade de estabelecer uma área na qual a probabilidade de utilização discriminatória da informação é potencialmente maior”, porém não quer dizer que eles não poderão ser utilizados, nem que não existirão situações em que a “utilização destes dados se preste a fins legítimos e lícitos”. Ademais, setores fundamentais necessitam desses dados pessoais sensíveis – por exemplo, a pesquisa científica ou atividade médica (DONEDA, 2006, p. 163).

Os dados sensíveis possuem subespécies – os dados “pertinentes à saúde, raça, crença religiosa, opção sexual, dados genéticos, histórico médico, entre outros” (SANTOS et.

al, 2012, p. 273). Assim, podemos retirar que os dados relativos à saúde "estão inseridos na concepção de dados sensíveis, isto é, dados pessoais que se referem a aspectos mais íntimos da vida do indivíduo, tais como origem étnica ou racial, convicções políticas, religiosas ou filosóficas, vida sexual, etc." (BARAÚNA JR., 2019, p. 81). A inserção dos dados de saúde dentro da categoria de dados sensíveis se dá pois tais dados estão diretamente "ligados com a personalidade de seu titular e aptos a fundamentar a atuação discriminatória por quem os utiliza, gerando impactos inestimáveis" (CURY, 2021, p. 202). Desta forma, os dados médicos, bem como os dados genéticos, podem ser considerados sensíveis por excelência (SCHAEFER, 2010, p. 62), pois guardam em seu conteúdo um caráter personalíssimo (BARBOSA; LOPES, 2021, p. 37).

Diferentemente de outros dados sensíveis, tais como a crença religiosa ou a opinião política, que dizem respeito a escolhas da pessoa e são, muitas vezes, divulgadas ao público, os dados pessoais sensíveis referentes à saúde, genética e biometria "não dizem respeito propriamente a escolhas que devem ser tuteladas", mas sim à própria pessoa dentro de aspectos ligados à sua intimidade (KORKMAZ, 2019, p. 44).

Segundo Kapla (2016, p. 316), são os dados que dizem respeito à existência tanto física quanto simbólica de uma pessoa. A rigor, são informações da pessoa relativas ao seu corpo físico, ou quanto a aspectos psicológicos. São dados que apresentam as vulnerabilidades da pessoa doente, e, desta forma "propiciam uma espécie de radiografia de uma área muito íntima" de seu titular (SARLET; MOLINARO, 2019, p. 186). O grau de sensibilidade dessas informações, se não forem utilizadas dentro de balizas éticas, pode acarretar graves prejuízos aos titulares, pois possuem um alto potencial discriminatório e estigmatizante.

Por dados de saúde, podemos entender os dados pessoais sensíveis "capazes de revelar o estado (passado, presente e/ou futuro) de saúde física ou psíquica de seu titular, bem como, cuja divulgação possa fazer surgir uma condição físico-psíquica capaz de conduzir à discriminação ou causar prejuízo ao seu titular" (SCHAEFER, 2010, p. 49-50). Neste sentido, é importante pontuar que o Regulamento Geral de Proteção de Dados Europeu inovou sendo a primeira legislação que traz uma definição para dados de saúde (BARBOSA; LOPES, 2021, p. 38).

De acordo com o Considerando 35 do RGPD, "deverão ser considerados dados pessoais relativos à saúde todos os dados relativos ao estado de saúde de um titular de dados que revelem informações sobre a sua saúde física ou mental no passado, no presente ou no

futuro". Nesse sentido, o texto do Considerando 35 explica que inclui no conceito de dados de saúde

> [...] informações sobre a pessoa singular recolhidas durante a inscrição para a prestação de serviços de saúde, ou durante essa prestação, conforme referido na Diretiva 2011/24/UE do Parlamento Europeu e do Conselho (9), a essa pessoa singular; qualquer número, símbolo ou sinal particular atribuído a uma pessoa singular para a identificar de forma inequívoca para fins de cuidados de saúde; as informações obtidas a partir de análises ou exames de uma parte do corpo ou de uma substância corporal, incluindo a partir de dados genéticos e amostras biológicas; e quaisquer informações sobre, por exemplo, uma doença, deficiência, um risco de doença, historial clínico, tratamento clínico ou estado fisiológico ou biomédico do titular de dados, independentemente da sua fonte, por exemplo, um médico ou outro profissional de saúde, um hospital, um dispositivo médico ou um teste de diagnóstico in vitro.

Ademais, o Regulamento, em seu artigo 4º, 15, prevê a definição de dados de saúde como "dados pessoais relacionados com a saúde física ou mental de uma pessoa singular, incluindo a prestação de serviços de saúde, que revelem informações sobre o seu estado de saúde". No mesmo artigo foi referenciada a definição de uma subcategoria dos dados de saúde (BARBOSA; LOPES, 2021, p. 38), os dados genéticos, como sendo

> [...] dados pessoais relativos às características genéticas, hereditárias ou adquiridas, de uma pessoa singular que deem informações únicas sobre a fisiologia ou a saúde dessa pessoa singular e que resulta designadamente de uma análise de uma amostra biológica proveniente da pessoa singular em causa.

Os dados genéticos também "definem características relevantes e únicas não só dos indivíduos, como também de seus ascendentes e descendentes", podendo inclusive ser classificados para além de um dado referente à saúde, destacando-se como uma categoria própria, pois definem "o ser humano como espécie, descrevendo os laços comuns da humanidade" (NAVES; GOITÁ, 2017, p. 70). Contudo, tais dados são capazes de revelar o estado de saúde de seu titular, de modo que podem ser enquadrados dentro da categoria de dados de saúde, mesmo com algumas especificidades.

Para Schaefer (2010, p. 47), dados médicos, dados clínicos ou dados de saúde podem ser tratados indistintamente. A mencionada autora propõe uma divisão dos dados médicos em dois elementos: o elemento material e o imaterial. O primeiro diz respeito ao meio físico que dá suporte a informações, como os exames ou as amostras biológicas; por outro lado, o elemento imaterial é constituído pelo agrupamento de informações colhidas, em suma, da

“histórica clínica do paciente e de documentos médicos diversos e que podem assumir diferentes funções – inclusive política e econômica – dependendo do destino que pretende dar a eles”. Percebe-se que os elementos que dizem respeito aos dados de saúde abarcam uma gama de situações, possuindo uma concepção ampla. Inclusive a tentativa de conceituar os dados médicos ou de saúde apenas possui utilidades para fins didáticos, “pois incapaz de enumerar exaustivamente o que se pretende por dados médicos (ou referentes à saúde), já que demasiadamente ampla” (SCHAEFER, 2010, p. 50).

A título de exemplo, Palhares (2021, p. 303) escreve:

> Dados relacionados à saúde, não se trata apenas de dados que claramente são de saúde, como o resultado de um exame de sangue ou os contidos num prontuário médico, mas também qualquer informação relacionada a uma pessoa natural, identificada ou identificável, que permita fazer uma inferência sobre aspectos relacionados à sua saúde, a exemplo de uma fotografia sua acamado em um leito hospitalar, ou de um pedido de refeição especial à companhia aérea por conta de uma restrição alimentar.

Em vista disso, os dados de saúde podem sofrer uma espécie de alargamento. Por tal razão, é necessário analisar o contexto em que se encontra determinado dado pessoal. Aliás, há quem defenda que, praticamente, todos os dados têm potencial de se tornarem dados de saúde. De acordo com Kaplan (2020, p. 9), vários profissionais de marketing, empresas de mídia social bem como agregadores de dados afirmam que quase todos os dados podem ter implicação na área da saúde, e são vendidos como tais há anos. Interações sociais, compras e outras transações on-line ou presencialmente, rastreadores da web, rastreadores de localização via telefone celular, dispositivos vestíveis de condicionamento físico, registro de hospitais estaduais, registro de imóveis, reclamações de seguro, dispositivos conectados à internet das coisas, todos os ambientes fornecem dados que podem ser relacionados com a saúde de alguém. Identifica-se com tal afirmação que os dados médicos detêm um valor inclusive monetário e que desperta interesses de diversos setores, tais como políticos e do setor privado, “grandes laboratórios farmacêuticos, como também são cobiçados pelas empresas informáticas, pela indústria alimentícia, pelas empresas que produzem produtos agropecuários e pelas seguradoras e planos de saúde” (SCHAEFER, 2010, p. 160).

Apenas a título ilustrativo, Cohen et al. (2018, p. 1) afirmam que todos os aspectos da nossa vida trazem questões relevantes para a definição da saúde de uma pessoa. Deste modo, pode-se coletar dados de saúde com base em hábitos de compras, pesquisas no Google,

dados FitBit[65]... De acordo com o relatório da Casa Branca *Big Data: Seizing Opportunities and Preserving Values*, de 2014, existe uma poderosa conexão entre estilo de vida e resultados de saúde, de forma que se pode afirmar que o Big Data revolucionou e expandiu o significado de dados de saúde (KAPLAN, 2020, p. 9).

Nesse sentido, estudos têm mostrado que dados coletados de smartphones podem ser úteis para detectar sintomas de depressão, por meio da captura da geolocalização e o tempo de utilização dos aparelhos telefônicos e, potencialmente, com mais precisão quando comparados com os questionários padrões (COHEN et al., 2018, p. 3). Por tal razão, a legislação brasileira, ao contrário do realizado pelo RGPD, não conceituou dados de saúde, visando a não restringi-los, pois, conforme mencionado, dados sensíveis, incluídos os dados de saúde, podem ser obtidos de informações que não revelam maiores qualidades. Nessa orientação é a Nota Técnica nº 3/2019/GEPIN/DIRAD-DIDES/DIDES da ANS (2019, p. 6):

> Apesar de didática, a distinção de dados pessoais sensíveis dos não sensíveis está cada vez mais menos clara em razão dos avanços na tecnologia de comunicação e informação. A coleta massiva de dados pessoais e os grandes avanços no processamento, cruzamento e análise de grandes conjuntos de dados têm permitido a inferência de informações pessoais sensíveis a partir de dados aparentemente não relacionados. O histórico de navegação e de pesquisas na Internet e curtidas em publicações nas redes sociais, por exemplo, podem indicar se uma mulher está grávida ou se uma pessoa está doente.

Assim, considerando que dados sociais, tais como escolhas de estilo de vida, profissão e influências culturais podem ter impactos na saúde do indivíduo, bem como seus hábitos alimentares ou habitação, "é possível, em princípio, avaliar todos esses dados como relevantes para a saúde, engendrando um conjunto que tende a permanecer em ritmo de crescimento vertiginoso" (SARLET; MOLINARO, 2019, p. 186). Logo, em muitos casos não será possível definir no instante da coleta dos dados como sendo dados pessoais sensíveis e/ou de dados relevantes para saúde. Para tanto, o contexto de utilização dos dados será capaz de definir se sensível ou não, devendo ser norteada pela finalidade empregada no uso dos dados.

---

65 Segundo a descrição do produto na loja do GooglePlay, o FitBit é "o principal app do mundo para monitorar sua atividade durante dia, seus treinos, seu sono e muito mais. Use o app individualmente para monitorar atividades básicas e corridas em seu celular ou conecte-se a um dos diversos trackers de atividade da Fitbit e à Balança Inteligente com Wi-Fi Aria para obter informações completas sobre sua saúde, incluindo contagem de passos, distância, calorias queimadas, sono, peso, entre outros". O aplicativo está sincronizado com dispositivos vestíveis como um relógio que consegue monitorar número de passos, calorias gastas, ritmo de corrida, dentre outas funcionalidades.

Tais cuidados são importantes pois, como verificado, os dados pessoais de saúde possuem um potencial discriminatório, bem como uma forte carga íntima. Por conseguinte, podemos dizer que os dados pessoais de saúde trazem em seu conteúdo aspectos da privacidade da pessoa? Uma vez que "é notável que o setor da saúde lida com informações extremamente pessoais e privadas, muitas vezes apenas partilhadas em confidência com os profissionais de saúde" (SOUSA, 2017, p. 12).

De acordo com Rodotà (2008, p. 248), os dados pessoais de saúde "referem à nua condição humana, colhem a pessoa nos momentos de maior fragilidade, revelam a fraqueza do corpo". Tal afirmação demonstra o grau de sensibilidade que os dados de saúde possuem, bem como o seu vínculo com assuntos privados. Tais dados, em muitos casos, chamam a proteção da privacidade, pois não há intenção – ao menos levando em consideração o agir do "homem médio" – de que tais informações venham a público ou saiam do contexto médico ou de cuidados com a saúde. Os dados de saúde, em sua maioria, são compartilhados dentro de uma lógica de confiança e de lealdade. Dentro do entendimento de que as informações apenas serão utilizadas para os fins de cuidado, em caso de divulgação da maioria desses dados a pessoa teria a sua personalidade desnudada, a privacidade violada, abatendo a integridade moral do sujeito (FERRAZ JR., 1993, p. 448-9).

O senso comum entende as informações de saúde como relacionadas com os recantos mais privados das pessoas (COSTA, 2021, p. 89), ou, como preferem Barbosa e Lopes (2021, p. 56-7), são os dados "que se enraízam no último reduto da vida privada de cada um de nós e que por esse motivo se consideram dados sensíveis e personalíssimos". Exatamente porque a pessoa, quando procura atendimento médico, se encontra fragilizada pela sua situação, acometida por uma enfermidade, um sofrimento, e na busca pela cura ou pela diminuição de sua dor, revela informações íntimas relativas a si, bem como a sua família (SCHAEFER, 2010, p. 52).

Essa vulnerabilidade especial, constituída por dor e angústia, ou medos sobre sua saúde e vida, leva à anamnese das informações aos profissionais da saúde sobre aspectos relacionados com a sua existência, tanto física como simbólica. E não é porque foi relatado que elas deixaram de ser privadas, até porque as pessoas tendem a dar grande importância para informações íntimas sobre si mesmas e seus corpos (KAPLAN, 2016, p. 316). Além do que, considerando que os dados de saúde estão diretamente relacionados com informações do plano privado da pessoa, de acordo com Cancelier (2017, p. 120), uma vez ocorrida a sua violação e perdida a qualidade de privado do conteúdo , "não há mais como devolvê-la a esse

plano; do mesmo modo, quando uma informação que não deveria ser compartilhada é divulgada, é impossível reverter o movimento, sobretudo quando se faz uso de ferramentas digitais". Desta forma, "o dano causado ao indivíduo e o desrespeito pelo seu direito à privacidade nunca mais será reposto" (SOUSA, 2017, p. 16).

Consequentemente, como forma de resguardar a privacidade do paciente, surge o dever de sigilo profissional no manuseio dos dados pessoais de saúde (SCHAEFER, 2010, p. 219). O reconhecimento da confidencialidade é um direito do paciente, sendo benéfico para este, para os médicos e para a sociedade como um todo (KAPLAN, 2016, p. 313), pois assegura que "os dados clínicos não saiam do âmbito de controle de seu titular, impedindo, dessa forma, que sejam utilizados como meio a permitir autoritário controle social, econômico e/ou político" (SCHAEFER, 2010, p. 220)[66]. Ademais, assegurar o sigilo das informações acaba dando maior tranquilidade para o paciente falar a verdade e descrever todos os detalhes de suas dores, sintomas, medos e aflições, permitindo ao profissional da saúde chegar a um diagnóstico mais assertivo. O paciente precisa confiar no médico e muito dessa confiança advém do fato de existir um compromisso do profissional de saúde em manter confidenciais as informações narradas em uma consulta ou na coleta de seus dados clínicos (SCHAEFER, 2010, p. 136).

O dever de sigilo que existe nas relações médicas, inicialmente, foi pensado dentro de uma preocupação puramente ética. A primeira formulação remonta ao século VI-V a.C., feita por Hipócrates, considerado pai da medicina ocidental, em um trecho de seu famoso juramento: "Àquilo que no exercício ou fora do exercício da profissão e no convívio da sociedade eu tiver visto ou ouvido, que não seja preciso divulgar, eu conservarei inteiramente secreto". Contudo, somente em meados do século XX que o sigilo profissional ganha contornos jurídicos, tendo como marco a sentença proferida pela Parlamento de Paris, em 13 de julho de 1573, "que condenou um farmacêutico por quebra de sigilo profissional quando

66 Nesse sentido, o Código de Ética Médica (Resolução nº 1.638, de 10 de julho de 2002) preceitua que os prontuários médicos são de propriedade dos pacientes e a guarda deve ser da instituição de saúde. As informações contidas no prontuário médico são sigilosas e pertencem ao paciente, que pode solicitar cópias a qualquer momento. Em suma, o prontuário médico contém "o registro da situação de saúde do paciente, a história da família, da saúde e de vida dos pacientes anotado pelos profissionais de saúde, particularmente pelo médico responsável pelas condutas e pela prescrição, além de reunir outros documentos, tais como diagnósticos, sob a forma de laudos, imagens ou dados, prognósticos, planos de cuidados, resultados de exames, consultas realizadas por diferentes profissionais etc." (SARLET; FERNANDES; RUARO, 2021, p. 493).

em um processo de cobrança de honorários pronunciou a doença que acometia seu cliente" (SCHAEFER, 2010, p. 99).

O juramento foi atualizado, em 1948, pela Convenção de Genebra, referenciada como um dos documentos principais da Ética Médica. No tocante à confidencialidade, o juramento passou a dispor: "*Mesmo após a morte do doente respeitarei os segredos que me tiver confiado*" (SANDOVAL, 2019, sem página). Apesar da redação aberta, desde a aprovação do texto da convenção, "todos os código deontológicos destinados à profissão médica passaram a trazer previsões com relação ao sigilo profissional" (SCHAEFER, 2010, p. 100).

Tal dever de sigilo entre o médico e o paciente é previsto no Código de Ética Médica brasileiro (Resolução CFM nº 1.931/2009), estabelecendo que o dever de guardar sigilo das informações obtidas em virtude da profissão é um dos princípios fundamentais previstos no código. Ademais, possui um capítulo específico para tratar sobre o sigilo profissional[67]. Além do Código de Ética Médica, há outros diplomas deontológicos que tratam sobre o sigilo profissional na área da saúde, por exemplo, o Código de Ética dos Profissionais de

---

67 Capítulo 1 – Princípios fundamentais.
"XI - O médico guardará sigilo a respeito das informações de que detenha conhecimento no desempenho de suas funções, com exceção dos casos previstos em lei" (CONSELHO FEDRAL DE MEDICINA, 2010, p. 31).
Capítulo IX – Sigilo Profissional.
É vedado ao médico:
"Art. 73. Revelar fato de que tenha conhecimento em virtude do exercício de sua profissão, salvo por motivo justo, dever legal ou consentimento, por escrito, do paciente.
Parágrafo único. Permanece essa proibição: a) mesmo que o fato seja de conhecimento público ou o paciente tenha falecido; b) quando de seu depoimento como testemunha. Nessa hipótese, o médico comparecerá perante a autoridade e declarará seu impedimento; c) na investigação de suspeita de crime o médico estará impedido de revelar segredo que possa expor o paciente a processo penal.
Art. 74. Revelar sigilo profissional relacionado a paciente menor de idade, inclusive a seus pais ou representantes legais, desde que o menor tenha capacidade de discernimento, salvo quando a não revelação possa acarretar dano ao paciente.
Art. 75. Fazer referência a casos clínicos identificáveis, exibir pacientes ou seus retratos em anúncios profissionais ou na divulgação de assuntos médicos, em meios de comunicação em geral, mesmo com autorização do paciente.
Art. 76. Revelar informações confidenciais obtidas quando do exame médico de trabalhadores, inclusive por exigência dos dirigentes de empresas ou de instituições, salvo se o silêncio puser em risco a saúde dos empregados ou da comunidade.
Art. 77. Prestar informações a empresas seguradoras sobre as circunstâncias da morte do paciente sob seus cuidados, além das contidas na declaração de óbito, salvo por expresso consentimento do seu representante legal.
Art. 78. Deixar de orientar seus auxiliares e alunos a respeitar o sigilo profissional e zelar para que seja por eles mantido.
Art. 79. Deixar de guardar o sigilo profissional na cobrança de honorários por meio judicial ou extrajudicial" (CONSELHO FEDRAL DE MEDICINA, 2010, p. 44).

Enfermagem[68], o Código de Ética da Fisioterapia, que prevê em seu art. 9º, inciso IV, o dever de "manter segredo sobre fato sigiloso de que tenha conhecimento em razão de sua atividade profissional e exigir o mesmo comportamento do pessoal sob sua direção, salvo situações previstas em lei" (BARRETO JR., 2019, p. 303)[69].

Nesse sentido, cabe destacar que o dever de guardar sigilo profissional transpassa os deveres da ética determinados pelas mencionadas resoluções, sendo protegido juridicamente pela Constituição Federal, em seu art. 5º, X. A sua violação é tipificada como crime, arts. 153 e 154 do Código Penal (MENDES, 2008, p. 66). É mister lembrar que seu dever de guarda também pode advir de disposição contratual[70] (SCHAEFER, 2010, p. 105-6).

A garantia do sigilo é fundamental para o cuidado médico e preserva a personalidade da pessoa vulnerável, em virtude de seu estado de saúde, garantindo que as suas confissões se manterão fora do conhecimento público (BARAÚNA JR., 2019, p. 80). Portanto, pode-se afirmar que a confidencialidade possui três funções:

> promover a harmonia social protegendo a confiança que informa as relações sociais e contratuais, tutelar o direito à saúde e proteger e promover a dignidade da pessoa humana evitando o desenvolvimento de sistemas classificatórios e excludentes baseados em informações médicas (SCHAEFER, 2010, p. 160).

Por conseguinte, o segredo traz confiança à relação entre o profissional da saúde e o paciente (SCHAEFER, 2010, p. 134). A confiança entre o médio e o paciente, o enfermeiro e o paciente, psicólogo e paciente é primordial para o tratamento de saúde, pois sem confiança muitas pessoas evitariam buscar auxílio e/ou esconderiam informações sobre suas mentes e corpos durante uma consulta (PEEL, 2013, p. 2013). A perda dessa confiança pode ter resultados consideráveis na prestação de serviços de saúde, atingindo o sistema de cuidados como um todo, além dos danos causados na vida do paciente em particular, que não terá a

---

68 Art. 52 Manter sigilo sobre fato de que tenha conhecimento em razão da atividade profissional, exceto nos casos previstos na legislação ou por determinação judicial, ou com o consentimento escrito da pessoa envolvida ou de seu representante ou responsável legal. (CONSELHO FEDERAL DE ENFERMAGEM, 2017, sem página).

69 Inclusive, com o intuito de proteger o sigilo profissional o Código Civil afirma que não existe obrigatoriedade de depor sobre fato a cujo respeito em virtude da profissão deva guardar segredo (Art. 229, I, Código Civil).

70 Pode-se imaginar a situação em que profissionais da saúde, por exemplo médicos, para além das obrigações legais, ao serem contratados assinem um termo de confidencialidade no tocante a as informações sensíveis que tiver acesso em razão das atividades que desempenha. A figura do Termo de Confidencialidade, ou *Non Disclosure Agreement* – NDA é conhecido do meio empresarial como um contrato visando manter dados confidenciais e pode ser levado para áreas que trabalhem com dados sensíveis, com o proposito de trazer mais segurança.

melhor solução para a sua enfermidade (SOUSA, 2017, p. 17). De acordo com Mendes (2008, p. 65), a "privacidade na área médica tem uma enorme relevância na sociedade, na medida em que o paciente relata os sintomas da sua doença a um médico, em que ele confia, com finalidade de receber um diagnóstico e um tratamento adequado".

Assim, não resta dúvida de que a relação entre o paciente e o profissional da saúde está baseada entre os pilares éticos da confiança, transparência e fidelidade. Dentro dessa relação, o médico, respeitando a autonomia do paciente, retribui a confiança nele posta buscando achar o melhor diagnóstico, tratamento ou cura para a moléstia apresentada, assegurando a intimidade dos dados coletados em razão de seu ofício, bem como protegendo a integridade física de seu paciente. Por outro lado, "o paciente responde à lealdade do médico revelando-lhe o que for necessário ao seu diagnóstico e tratamento, cumprindo as determinações terapêuticas e, até mesmo, lutando por sua cura" (SCHAEFER, 2010, p. 143).

Ante o exposto, observa-se que há uma perceptível conexão entre a privacidade e a confidencialidade nas relações de saúde. "A confidencialidade garante a não exposição dos dados ou informações que firam a privacidade dos pacientes ou usuários" do sistema de saúde (BARRETO JR., 2019, p. 303). Nessa perspectiva, os dados de saúde, na maioria das vezes, estão diretamente relacionados com assuntos privados, chamando para si a proteção inerente aos dados pessoais sensíveis, mas também a proteção à privacidade do seu titular. Por tal razão, é vital na relação médico-paciente que se mantenha preservada a privacidade do enfermo, que "aspectos de sua vida privada não saiam da esfera íntima em que estes se desenvolvem, que não se divulguem sem sua autorização" (SCHAEFER, 2010, p. 131).

A Sociedade da Informação, com a informatização de todos os assuntos da vida, trouxe alterações também para dentro da área médica e de cuidados com a saúde. Hodiernamente, os arquivos médicos tornaram-se digitais, as terapias podem ser realizadas a distância, aplicativos prometem prevenir doenças[71]. Nesse novo contexto, houve um aumento da possibilidade "da coleta, do armazenamento e da cessão das informações do paciente". Tais mudanças aumentaram a preocupação com a privacidade das pessoas, uma vez que tais dados, como mencionado, são sensíveis, se encontram dentro da esfera íntima das pessoas, e a

71 Aplicativos e dispositivos móveis estão disponíveis no mercado digital prometendo aos consumidores benesses como parar de fumar, monitorar a fertilidade, controlar o apetite, fazer mais exercícios, dormir melhor, como também monitorar a pressão arterial, estresse e níveis de hidratação. Assim, tais aplicativos são capazes de fazer as pessoas e algumas empresas nos conhecerem melhor (IGO, 2018, p. 359).

"sua circulação na sociedade pode acarretar graves danos a seu titular" (MENDES, 2008, p. 65).

Conforme visto, há uma tentativa por parte da doutrina de dar aos danos pessoais caráter patrimonial, e com os dados de saúde não é diferente. Assim, há quem defenda que os dados pessoais de saúde possuam a qualidade de bem patrimonial, presumindo-se que quem os detém possui autorização para vendê-los. No entanto, este trabalho filia-se ao entendimento de que dados pessoais não são uma espécie de direito de propriedade, justamente porque estão diretamente ligados com a personalidade da pessoa. No caso dos dados de saúde, a sensibilidade inerente a eles não pode corresponder com práticas mercantis (KAPLAN, 2016, p. 323). Exatamente porque os dados de saúde são elementos essenciais da pessoa (e da vida privada), pertencentes ao "estatuto jurídico do corpo humano", considerados elementos da personalidade, e como tais devem ser protegidos (SCHAEFER, 2010, p. 229).

Como bem observado por Santos et al. (2012, p. 277), a coleta dos dados de saúde possui inúmeros riscos para a privacidade, a dignidade da pessoa humana, pois aumenta as chances de ruptura da confidencialidade depositada, assim como possibilita uma estigmatização social se os dados forem utilizados para fins ilegítimos. A confecção de perfis clínicos de um indivíduo seria capaz de ser determinante em relações contratuais ou trabalhistas, podendo levar à marginalização de grupos de pessoas, discriminação e exclusão social. Todavia, isso não significa que dados de saúde não trafeguem, muitas vezes, em prol de objetivos positivos para o seu titular ou para a coletividade (SCHAEFER, 2010, p. 183)[72].

72 Por tais razões, legislações como a Lei nº 11.903/2009 é vista com desconfiança. A legislação em comento "propõe o rastreamento da produção e consumo de medicamentos em território nacional por meio do Sistema Nacional de Controle de Medicamentos" (SCHAEFER, 2010, p. 156). Contudo, a legislação "não deixa claro seus objetivos, não indica quais serão os mecanismos técnicos e administrativos de segurança que garantirão (durante o tratamento de dados considerados sensíveis), a integridade, a autenticidade, a qualidade e o sigilo das informações captadas de receituários médicos" (SCHAEFER, 2010, p. 158). Sabe-se que por detrás da legislação, além do interesse de vigilância do Estado sobre a saúde dos brasileiros, existem interesses de ordem econômica. O Brasil é o oitavo maior mercado de produtos farmacêuticos do mundo, sendo eleito um dos mercados mais atrativos da América Latina (SANTOS, et. al, 2012, p. 280). Assim empresas visando adentrar no mercado precisam encontrar formas de chegar aos consumidores, o que fomenta iniciativas como as da Lei nº 11.903/2009 que possibilitam a construção de banco de dados populacional para práticas de marketing podendo direcionar propagandas incentivando "novos e nem sempre sadios hábitos de consumo de medicamentos" (SCHAEFER, 2010, p. 159). No entanto, as empresas farmacêuticas utilizam de inúmeras estratégicas para angariar dados dos consumidores, uma delas é os programas de descontos para clientes registrados que leva os consumidores fornecerem dados capazes de revelar informações sensíveis (SANTOS, et. al, 2012, p. 280). Ademais, segundo Schaefer (2010, p. 135), antes de 2009 as empresas farmacêuticas já coletavam dados de saúde constante em receituários médicos brasileiros, estimasse que 15% dos dados de 35 milhões de receituários foram coletados, sem consentimento, para fins não bem definidos.

Assim, com o intuito de evitar abusos e que não haja uma quebra na confiança existente entre médico e paciente, e garantir a dignidade, uma parte da doutrina defende que o titular dos dados de saúde deve consentir antes da dissociação desses dados ou dar acesso a terceiros (pesquisadores e/ou empresas farmacêuticas) aos seus dados pessoais de saúde. Sem querer esgotar a matéria referente ao consentimento, é importante destacar que o consentimento do titular dos dados deve ser livre, inequívoco, específico e expresso. Desta forma, entende-se que o consentimento deve ser informado, baseado em valores éticos e legais, em que a pessoa detém autonomia e liberdade para consentir, estando distante de um consentimento meramente formal. Assim, o direito-dever de informar deve ser capaz de dar subsídios para o titular dos dados de saúde para dar início a um "processo de tomada de decisão no que tange ao fluxo de seus dados. A prestação de uma informação clara, adequada e suficiente é o portal de entrada para tanto" (BIONI; LUCIANO, 2021, p. 153). Exige-se, dessa forma, que exista um efetivo diálogo entre os profissionais da saúde e o paciente que proporcione uma compreensão exata sobre como os seus dados serão utilizados (SCHAEFER, 2010, p. 176).

Por não se tratar de uma mera formalidade ou faculdade do médico, o método como esse consentimento será colhido é de suma importância, devendo ser claro para o titular dos dados como eles serão utilizados e para quais finalidades. Prevalece a relação de confiança existente entre as partes, por isso há a necessidade de transparência no tratamento de dados[73], para permitir que se mantenha uma relação sincera e sem danos, "eliminando-se qualquer tipo de opacidade e obscuridade com relação ao trânsito dos dados pessoais" (BIONI; LUCIANO, 2021, p. 154).

Ademais, "para que a autorização seja válida, é necessário que seja livre" (SCHAEFER, 2010, p. 181). Por consentimento livre entende-se o ato de vontade realizado sem coações, de qualquer tipo, "que remete à ideia de uma ação espontânea, que não seja objeto de pressão" (BIONI; LUCIANO, 2021, p. 154). O consentimento também deve ser "inequívoco", ou seja, a finalidade deve estar clara. Logo, a finalidade do uso dos dados pessoais não pode ser ambígua ou genérica. Percebe-se que essa espécie de consentimento encontra forte relação com o princípio da finalidade, que dispõe que o tratamento de dados

73 Inclusive, a Lei Geral de Proteção de Dados conceitua transparência como sendo "uma garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial". Ademais, o art. 6º, VI faz referência à transparência como um princípio para o tratamento de dados pessoais.

pessoais deve ser "para propósitos legítimos, específicos, explícitos" (art. 6º, I, LGPD). Assim, não será permitido um consentimento sem delimitar "um direcionamento, já que não se consente no vazio e de forma genérica" (BIONI; LUCIANO, 2021, p. 154), devendo ser específico, destacado e para finalidades específicas[74] ou expressas.

Todos esses atributos do consentimento são necessários não apenas dentro de ideais éticos, mas também como valores jurídicos pautados em deveres de lealdade, transparência, fidelidade, confiança, veracidade, "todos corolários da boa-fé que informa indubitavelmente relações sociais e jurídicas" (SCHAEFER, 2010, p. 181). Ademais, no tocante ao consentimento do titular dos dados de saúde, dados sensíveis que, conforme visto, possuem uma forte carga privada e um potencial risco de discriminação, razão pela qual "o consentimento do titular dos dados pessoais não deve ser um recurso para legitimar os mais abusivos e invasivos tipos de tratamentos de dados pessoais, coisificando-o" (BIONI, 2020, p. 202).

Ao se proteger os dados de saúde, protege-se o titular de tratamentos discriminatórios, assim como a sua privacidade e ao fim a sua personalidade de modo integral – garantindo a dignidade da pessoa. Logo, por se tratar de uma proteção à personalidade, existem limites impostos à autonomia privada, conforme preceitos estabelecidos no art. 11 do Código Civil brasileiro, que dispõe: "Com exceção dos casos previstos em lei, os direitos da personalidade são intransmissíveis e irrenunciáveis, não podendo o seu exercício sofrer limitação voluntária". Não obstante, apesar de em uma primeira leitura parecer que o citado artigo veda qualquer possibilidade de disponibilidade dos direitos da personalidade, a doutrina entende que a regra pode ser relativizada quando em prol do interesse social. De modo que alguns direitos da personalidade poderão, por exemplo, ser objeto de contrato de concessão ou de licença (DINIZ, 2012, p. 120).

Há uma indisponibilidade relativa dos direitos da personalidade. Porém, o titular estaria impedido de dispor desses direitos permanentemente ou totalmente. Busca-se com

---

74 Sobre o termo que parece redundante, Bioni (2020, p. 189) explica que na redação original do projeto de lei da LGPD estava previsto que para o tratamento de dados sensíveis se necessitaria de uma camada a mais. Essa camada adicional estava visando que o tratamento precisaria ser para finalidades expressas. Contudo, com a tramitação e as mudanças ocorridas durante as discussões legislativas, o texto passou para "finalidades específicas". Levando em consideração que o consentimento já deve ser específico, parece ter ocorrido uma redundância. "Diante desse cenário, o desafio interpretativo é extrair qual seria a 'camada adicional de proteção' conferida por esse consentimento especial". A saída apontada pelo autor seria entender o trecho como um "vetor para que haja mais *assertividade* do titular com relação a esse movimentos 'específicos' de seus dados".

esses impedimentos resguardar a estrutura física, psíquica e intelectual da pessoa humana. De modo que a esfera de autonomia do titular dos dados pessoais de saúde está restrita a atos que não venham a ferir a sua dignidade (FARIAS; ROSENVALD, 2014, p. 173). Nesse sentido, como bem pontua Bioni (2020, p. 206), a autonomia privada não é um paradigma normativo absoluto, e quando estamos diante de dados pessoais de saúde precisa haver o cuidado para que o consentimento não se transforme numa "armadilha a esconder um território informacional que lhe seja destrutivo" (BIONI, 2020, p. 206).

Não obstante, existem exceções à regra do consentimento para o tratamento de dados de saúde e em que devem ser consideradas. Situações como exigências legais ou requerimentos judiciais[75], urgências ou emergências clínicas, estudos sobre doenças ou saúde pública, situações em que o direito do titular de dados pessoais é sobrepesado com outros valores também caros à sociedade (SCHAEFER, 2010, p. 182). Desta forma, haverá momentos em que o consentimento será limitado, mas mesmo nessas situações deverá existir um fluxo informacional adequado, que não quebre as legítimas expectativas do titular dos dados pessoais (BIONI, 2020, p. 195).

A relação médico e paciente ocorre dentro de um contexto de confiança e lealdade, e, deste modo, a troca de informações se dá dentro de um fluxo informacional guiado por considerações políticas e morais, que, segundo o entendimento do "homem médio", determinará ser este contexto apropriado ou não. Assim, considerando os atores (profissional de saúde e paciente), os tipos de dados pessoais (em sua maioria, dados de saúde) e como eles são disseminados, é possível determinar qual o contexto da troca de informações – e, deste modo, conseguir verificar quais as legítimas expectativas no tocante ao fluxo informacional e à privacidade. Primeiramente, podemos analisar o fluxo interno: com base nos atores, consegue-se verificar o vínculo existente entre eles, e, conforme apurado, é um vínculo de confiança e lealdade, bem como é possível perceber qual esfera em que eles se encontram – uma esfera dentro dos limites da privacidade. Posteriormente, podemos analisar o fluxo externo, sobre a disseminação dessa informação obtida, momento em que questionamos quem são as pessoas que podem ter acesso às informações colhidas. Desta forma, devem-se indagar

75 Nesse sentido a "Portaria 1.271/2014, do Ministério da Saúde, que define a lista nacional de notificação compulsória de doenças, agravos e eventos de saúde pública nos serviços de saúde públicos e privados em todo o território nacional, nos termos do anexo, e dá outras providências, que em seu art. 3º prevê, como obrigatória, a notificação compulsória" (BARRETO JR., 2019, p. 305). Bem como existe a exigência legal prevista no art. 269 do Código Penal que tipifica como crime deixar o médico de comunicar à autoridade pública doença cuja notificação é compulsória.

quais as legítimas expectativas criadas quando do compartilhamento dos dados pessoais de saúde. Nesse sentido, não fere essa expectativa se o médico troca informações do estado de saúde com sua equipe médica. Por outro lado, não soa adequado que o médico compartilhe essas informações com empresas de recrutamento e seleção (BIONI, 2020, p. 197-201).

À vista disso, o sigilo médico não será absoluto – assim como nenhum direito o é. Sabe-se que os dados de saúde trazem muitos benefícios para o próprio titular, como para a pesquisa e saúde pública (KAPLAN, 2020, p. 5). A informação é tão importante para o paciente como o é para a medicina, para a política e para a economia. É por meio dessas informações que se transmite conhecimento, trocam-se experiências, encontram-se novas soluções, analisam-se epidemias e se buscam meios para controlá-las. São bases para a formulação de diagnósticos, bem como possibilitam análises para alcançar políticas públicas de saúde mais eficazes (SANTOS et al., 2012, p. 279).

A medicina tornou-se mais complexa, os tratamentos passaram a contar com várias especialidades médicas, fato que impõe um compartilhamento entre mais atores dos dados clínicos do paciente na busca do melhor tratamento, limitando o sigilo das informações. Da mesma forma, existe o compartilhamento entre os médicos e outros profissionais da saúde – tais como os enfermeiros, os técnicos de enfermagem, farmacêuticos que atuam na realização de exames, psicólogos, nutricionistas, fisioterapeutas e assistentes sociais. Igualmente, outros profissionais não relacionados com o cuidado direto do paciente têm acesso às informações de saúde, por exemplo, secretárias, recepcionistas, pessoas de departamentos administrativos, membros de ouvidorias, auditores (BARAÚNA JR., 2019, p. 89). Assim, "o cotidiano dos serviços de saúde revela, portanto, que é impraticável conceber o funcionamento de toda a sua estrutura sem que informações de pacientes sejam acessadas por outros profissionais não médicos" (BARAÚNA JR., 2019, p. 90)[76].

Não obstante existir um maior resguardo e até certa confidencialidade no tocante aos dados pessoais de saúde, não parece existir ofensa à integridade contextual caso haja um compartilhamento entre profissionais da saúde com o objetivo de ampliar o diagnóstico ou tratamento necessários. Do mesmo modo, não parece haver violação à integridade contextual

76 Nesse sentido, o Código de Ética Médica, reconhecendo que não há como prestar cuidados de saúde sem compartilhar dados dos pacientes com outros profissionais, prevê em seu art. 78 que ao médico é vedado "deixar de orientar seus auxiliares e alunos a respeitar o sigilo profissional e zelar para que seja por eles mantido". Para Baraúna Jr. (2019, p. 93), "trata-se de norma que estabelece como pressuposto intrínseco a possibilidade de acesso às informações de saúde de pacientes por profissionais não médicos e prevê a responsabilidade do médico por manter o sigilo das informações".

a troca de informações para criação do cadastro ou registo do paciente por parte da secretaria da clínica ou do hospital. Nesse exemplo, é fácil perceber que a integridade contextual está relacionada ao princípio da finalidade do tratamento dos dados pessoais, que deve ser sempre observada. Entretanto, não atende ao princípio da finalidade, há quebra de confiança e, consequentemente, "uma quebra dessa integridade contextual" caso se verifique a distribuição desses mesmos dados com o objetivo de obter vantagens econômicas, se esta "não ocorrer em benefício dos interesses do titular dos dados" (MENDES; FONSECA, 2021, p. 84).

A ideia da análise da integridade contextual se faz necessária em qualquer espécie de tratamento de dados pessoais. No entanto, no tocante aos dados pessoais de saúde, tal análise deve ser mais acurada, pois, com base nela, conseguiremos avaliar se as informações ali divulgadas, dentro de uma concepção pautada no senso comum, estariam dentro da concepção de privadas – devendo ter uma limitação no fluxo desses dados. Bem como entender até onde vai o limite desse contexto privado e quais ações extrapolariam a confiança depositada. Em suma, a maioria das informações foi passada visando a cuidados na saúde do titular dos dados pessoais. Contudo, nem todos os dados de saúde estarão dentro da esfera dita como privada (que possui como consequência interromper/barrar o fluxo da informação para fora do contexto privado). Alguns dados ditos de saúde, apesar de sensíveis, não estão limitados pelo manto da privacidade, e dessa forma poderão fluir para além dos limites da esfera privada. Da mesma forma, existem dados de saúde que possuem conteúdo inerente à privacidade que poderão sair do domínio privado tendo por base o bem comum, interesse público[77] e necessidades coletivas, dentro da proporcionalidade com fundamento na ponderação de direitos fundamentais. Mais uma vez, a análise da integridade contextual será de grande valia, auxiliando no juízo ponderativo e fixar os limites do fluxo das informações pessoais de saúde.

No entanto, a proteção de dados exige formas de circulação controlada, e no tocante aos dados sensíveis há maior rigidez no procedimento que permite a sua circulação. E isto se faz necessário pois a proteção dos dados de saúde é muito mais do que simplesmente um problema de ordem jurídica ou médica. O tratamento adequado aos dados de saúde tem impactos no âmbito da ética e em toda a sociedade (KAPLAN; MONTEIRO, 2021). Haverá situações em que a dimensão coletiva permite o fluxo de dados pessoais, equilibrados com o

77 O interesse público pode ser localizado dentro do princípio administrativo de supremacia do interesse público ou, simplesmente, princípio do interesse público, que "significa que os interesses da coletividade são mais importantes que os interesses individuais". Tal ideia seria "inerente a qualquer grupo social: os interesses do grupo devem prevalecer sobre os dos indivíduos que o compõem. Essa é uma condição para a própria subsistência do grupo social" (MAZZA, 2016, p. 123).

desenvolvimento humano e aperfeiçoamento social, que, como visto, deverá estar limitado a um fim determinado, "que indubitavelmente estará limitado pela dignidade da pessoa humana" (SCHAEFER, 2010, p. 53).

Tais preocupações são necessárias pois se deve levar em consideração que existem forças do mercado e interesses de poder quando estamos trabalhando com dados de saúde, e por tais razões precisa-se analisar se, realmente, estamos em face de fundamentos de bem comum ou em face de "disfarces para angariar lucro". Isto porque dados médicos detêm um valor inclusive monetário e que desperta interesses de diversos setores[78].

Na Sociedade da Informação, os dados sensíveis de saúde tecnológica passaram a ser utilizados como "insumo para o desenvolvimento de atividades empresariais das mais diversas áreas". No entanto, não podemos deixar de considerar o caráter existencial que possuem os dados pessoais, em especial os dados sensíveis, que revelam aspectos íntimos da pessoa, bem como possuem um potencial de discriminação elevado quando utilizados de forma indevida (MAGRANI, 2019, p. 12).

Tentaremos descrever como funciona essa nova economia movida a dados pessoais, focalizando na utilização dos dados de saúde, que têm o condão de melhorar e muito a saúde das pessoas, sem desconsiderar os riscos inerentes a sua utilização. Por fim, iremos descrever esse mercado, altamente lucrativo, envolvendo os dados de saúde.

3.3 ECONOMIA DE DADOS GERAL

Segundo Castells (2020, p. 75) vivemos um novo sistema econômico e tecnológico que pode ser definido como "capitalismo informacional". Pela primeira vez o mundo é capitalista ou dependente de sua ligação às redes globais, porém não é o mesmo capitalismo de outrora – o capitalismo clássico (*laissez-faire*) ou o capitalismo keynesiano. O sistema capitalista sofreu um importante processo de reestruturação a partir da década de 1980 e o desenvolvimento e as manifestações das novas tecnologias da informação foram essenciais no processo desse novo sistema econômico organizado em torno de "redes globais de capital,

78 Ademais, importante mencionar que os dados de saúde podem ser utilizados por governos como uma nova forma de vigilância, em que ela deixar de ser uma vigilância "sobre a pele" para ser uma vigilância "sob a pele", ou seja, "a nova forma de controle social não consiste meramente em câmeras, mas pela obtenção de dados biológicos, como temperatura, pressão e histórico de saúde" (FACHINETTI, 2020, p. 493).

gerenciamento e informação cujo acesso a *know-how* tecnológico é importantíssimo para a produtividade e competividade" (CASTELLS, 2020, p. 550). Nesta perspectiva,

> a sociedade em rede, em suas várias expressões institucionais, por enquanto é uma sociedade capitalista. [...] Mas esse tipo de capitalismo é profundamente diferente de seus predecessores históricos. Tem duas características distintas fundamentais: é global e está estruturado, em grande medida, em uma rede de fluxos financeiros (CASTELLS, 2020, p. 555).

Para Boff (2018, p. 12), com a revolução da informação, o sistema econômico continua capitalista, porém ele foi reestruturado como consequência da flexibilidade e da descentralização das empresas, do aumento da concorrência entre os países, da diversificação das relações de trabalho, do fortalecimento do mercado financeiro e do desfazimento por parte dos Estados da lógica do "estado-de-bem-estar-social" motivado pelo fracasso da União Soviética.

A informação é um novo ativo econômico, e muito valioso, fato que leva Lyotard (2009, p. 5) a acreditar que, da mesma forma que os estados-nação disputaram pela exploração das matérias-primas e mão de obra barata, é provável que os estados da atualidade disputem pelo domínio das informações, tendo em vista as possibilidades existentes tanto para as estratégias industriais e comerciais quanto para estratégias militares e políticas.

De acordo com Cohen (2016, p. 371), esse novo sistema econômico pode ser denominado como "economia da informação", que consiste em um modelo, derivado da era industrial, de produção em massa direcionado para o desenvolvimento de bens intelectuais, tais como informativos, serviços, produção e distribuição de tecnologia de informação para os consumidores e empresas prestadoras de serviço. Além dos novos bens de produção, a economia da informação revoluciona a indústria tradicional, que passa a se utilizar da tecnologia da informação para gestão e controle da produção industrial. Assim, a base da nova economia é o crescimento da produtividade proveniente "da capacidade de se usar a nova tecnologia da informação para alimentar um sistema de produção fundamentado nos conhecimentos" (CASTELLS, 2020, p. 210).

Em apertada síntese, Boff (2018, p. 16) descreve a nova economia como uma economia informacional e global:

> É informacional porque a produtividade e a competitividade de unidades ou agentes nessa economia (sejam empresas, regiões ou nações) dependem basicamente de sua capacidade de gerar, processar e aplicar de forma eficiente a informação baseada em

> conhecimentos. É global porque as principais atividades produtivas, o consumo e a circulação, assim como seus componentes (capital, trabalho, matéria-prima, administração, informação, tecnologia e mercados) estão organizados em escala global, diretamente ou mediante uma rede de conexões entre agentes econômicos. É informacional e global porque, sob novas condições históricas, a produtividade é gerada, e a concorrência é feita em uma rede global de integração. E ela surgiu no último quartel do século XX porque a Revolução da Tecnologia da Informação fornece a base material indispensável para esta nova economia.

Schaefer (2010, p. 130) descreve a Sociedade da Informação como uma sociedade essencialmente capitalista, em que a principal matéria-prima passa a ser a informação, visto que a informação satisfaz os desejos das pessoas e das empresas por meio da geração de conhecimentos que são empregados em atividades econômicas, "na definição da qualidade de vida e nas práticas culturais". A matéria-prima desse conhecimento, a informação, passa a ser adquirida, armazenada, processada, distribuída e disseminada para os mais diversos fins, graças à adesão da tecnologia "em todas as esferas da atividade humana".

Conforme exposto, a vida passou a ser on-line e a utilização de aplicativos de todo tipo possibilitou a coleta de inúmeras informações pessoais. Com tais dados, foi possível empreender de forma mais eficiente no mercado comercial. Assim, os dados pessoais passam a ser entendidos como matéria-prima importante dentro de uma economia capitalista – remodelada pelos avanços das tecnologias de comunicação e inovação, destacando-se os dados pessoais como meio de auxiliar na acumulação e geração de riquezas (BIONI, 2020, p. 11).

Em razão desse novo mercado, Lyon (1994, p. 37) fala que a Sociedade da Informação é também a Era da Mercantilização da Informação, pois dados, incluindo dados pessoais, são vendidos em um mercado próprio. Além dos antigos métodos de monitoramento dos funcionários no sistema econômico anterior, para controlar a jornada de trabalho e a produtividade, a Era da Mercantilização da Informação vai além e monitora também os consumidores. O mercado se especializou para analisar e direcionar o consumo, por meio de técnicas computacionais de enorme poder e sofisticação que avaliam o mercado interno e o global. Esse crescimento da produtividade com base em redes globalizadas, de acordo com Castells (2020, p. 211), é liderado pelo setor da tecnologia da informação, cada vez mais estruturado em torno da internet, que transformou-se em matéria-prima para toda uma economia, bem como impulsionou o mercado financeiro "global eletronicamente conectado". As informações passaram a ser "a fonte suprema dos investimentos".

Além do mais, a nova economia também pode ser entendida como uma economia de serviços, não mais uma economia de produtos. Para Rodotà (2008, p. 100), a sociedade hoje é uma "sociedade dos serviços", que está altamente associada à economia de dados, pois para prestar os serviços os fornecedores passam a captar uma gama relevante de dados pessoais. Os serviços atuais diferenciam-se dos serviços da Era Moderna, pois agora eles são prestados por meio da rede – o que facilita a interconexão entre bancos de dados e a disseminação das informações coletadas globalmente. Passam a ser "a mola propulsora da economia, citando-se, a título de exemplo, os setores bancários, securitário, educacional, de assistência médica e de consultoria jurídica/legal" (BIONI, 2020, p. 3).

Todas essas mudanças, principalmente a revolução digital, acarretaram uma enorme concentração de poder e riqueza. Estamos diante de um "sistema econômico apoiado inteiramente na coleta, na armazenagem e na análise de dados pessoais" (ZANATTA; ABROMAVAY, 2019, p. 431). Logo, podemos dizer que existe a formação de um novo campo da microeconomia, a microeconomia da interceptação de dados[79].

> A obtenção de dados resulta de um conjunto de estratégias de captura e de agrupamentos específicos das informações. Além disso, à interceptação e coleta desses dados somam-se as possibilidades de cruzamento com dados obtidos por sensores e dispositivos que permitem registrar lugares, períodos e atividades realizadas pelos indivíduos. Interceptação é um termo que envolve também as atividades de intrusão em computadores a fim de analisar arquivos armazenados ou acompanhar a navegação pessoal, de desenvolvimento de robôs para coleta de dados de caixas postais e dispositivos de conversação privada, de rastreamento das pegadas digitais, do envio de cookies e pixels (pequenos arquivos que permitem identificar os computadores nas redes), mas também de processamento e análise dos dados captados e cruzados com outras bases de dados, bem como as técnicas preditivas que se expandem com o *big data* (SILVEIRA, 2017, p. 59).

Desta forma, a evolução digital que ocorreu com os avanços significativos na tecnologia de informação e comunicação, em particular com o surgimento da internet, conforme visto, tornou possível uma coleta em massa de informações pessoais, bem como seu armazenamento, pois trouxe aplicações interativas com os usuários (blogs, redes sociais, etc.) que necessitam de informações pessoais para funcionarem e, consequentemente, transformaram os mesmos em produtores de dados pessoais, e não meros consumidores (ACQUISTI et al., 2016, p. 3).

---

[79] Segundo Silveira (2017, p. 59), a Teoria Econômica possui uma série de divisões. A microeconomia ou teoria de preços é uma parte da Teoria Econômica que volta a sua atenção para os consumidores, firmas, mercados específicos.

Assim, pode-se dizer que os dados e a evolução tecnológica agregaram ao sistema capitalista três novas características:

> a) os próprios objetos materiais convertem-se em formas de captar e transmitir dados. Isso vai do televisor doméstico que responde a comando de voz ao automóvel autônomo. [...]
> b) publicidade de precisão, ou seja, a capacidade de dirigir mensagens apoiadas no conhecimento do perfil exato dos consumidores a partir das informações que a "fusão de dados" permite obter (Wu, 2016; Zuckerberg, 2019), somada ao fato da comodificação da vida cotidiana e das ações individuais e relacionais que podem ser registradas como dados pessoais (Morozov, 2018; Zuboff, 2019).
> c) capacidade de antecipar os comportamentos dos cidadãos e planejar as atividades econômicas a partir daí (ZANATTA, ABROMAVAY, 2019, p. 432).

Tais características trazem benefícios para os titulares dos dados pessoais, tecnologias mais cômodas e direcionamento de produtos que atendam a suas necessidades e interesses, como também beneficiam os detentores dos dados, que conseguem fazer uma publicidade mais assertiva e melhorar seus serviços de acordo com o seu público consumidor. Por tal razão, dados pessoais como atributos e traços individuais que incluem idade, sexo, renda, preferências, comentários realizados, cliques em sites e fotos postadas em redes sociais têm valor econômico e são cada vez mais usados como negócios ativos que podem ser usados para direcionar serviços ou ofertas, direcionar publicidade, melhorar produtos, dentre outras funções comerciais (ACQUISTI et al., 2016, p. 3-4).

Dentre os benefícios listados, encontramos a publicidade direcionada, que pode ser entendida, segundo Bioni (2020, p. 15), como "uma prática que procura personalizar, ainda que parcialmente, a comunicação social, correlacionando-a a um determinado fato que incrementa a possibilidade de êxito da indução ao consumo"[80]. A publicidade depende do rastreamento das informações deixadas pelos usuários por toda a web enquanto navegam. Tais

[80] Bioni (2020, p. 15-16) continua sua explicação subdividindo a publicidade direcionada em três subcategorias, que são espécies do gênero publicidade direcionada. São elas: a publicidade direcionada contextual, a publicidade direcionada segmentada e a publicidade direcionada comportamental. Entende-se por publicidade direcionada comportamental aquela que "correlaciona a temática de um determinado ambiente (aspecto objetivo), seja ele o conteúdo de um determinado caderno de um jornal impresso (off-line) ou de um website (on-line), ao objeto anunciado. Contextualiza-se, pois, a abordagem ao potencial consumidor, levando-se em conta o meio no qual é promovido o bem de consumo. Ao passo que a publicidade segmentada se foca no aspecto subjetivo, isto é, no próprio público-alvo do bem ofertado. Não importa propriamente o conteúdo do ambiente em que será direcionada a publicidade, mas o público que a ele tem acesso. Se o bem de consumo direciona-se ao público feminino de meia-idade, adolescentes ou pessoas idosas, a abordagem será, então, realizada em ambientes onde a audiência de tal público seja predominante", e, por fim, a "chamada publicidade comportamental on-line, que é outra espécie da publicidade direcionada. Esta última prática publicitária permitiu uma personalização maior do contato entre compradores e vendedores".

informações, juntamente com auxílio da tecnologia, dão subsídios para desenvolver perfis de usuários ou tipos de usuários a fim de inferir interesses e preferências. Essa segmentação dos usuários de acordo com interesses e preferências torna possível direcionar anúncios seletivos para cada "tipo" de usuário.

Além de capturar o fluxo de informações deixadas pelos usuários, também se analisa como os mesmos reagiram aos anúncios apresentados, criando subsídios para aproximações futuras. Nesse novo modelo de abordagem comercial há um alto grau de abrangência, sendo tudo facilmente registrado e correlacionado. Diferentemente do comportamento off-line, em que profissionais do marketing apenas tomavam conhecimento dos dados quando o usuário realizava uma ação, tais como uma compra e uma venda ou a abertura de um cadastro em algum estabelecimento. O comportamento virtual dos usuários gera dados mesmo sem que realizem ações nos estabelecimentos comerciais, pois as tecnologias conseguem captar todas as ações facilmente. A título de exemplo, é possível registrar os sites que o usuário olhou e por quanto tempo olhou, se a compra foi ou não finalizada, bem como inferir os assuntos que lhe interessam (BAROCAS; NISSENBAUM, 2009, p. 1-3).

Os dados são o novo petróleo, são valiosos, mas há algo a mais. Para Viktor Mayer-Schönbergerm[81], os dados não são apenas um produto ou um recurso com o qual transacionamos. Eles são mais que um ativo econômico valioso: ditam as regras do mercado, mudam a forma como ele opera. E isso é muito importante, pois reformula a economia, tornando-a muito mais eficiente e produzindo resultados mais sustentáveis. Isto porque os dados conseguem unir compradores e vendedores com muito mais precisão que outrora. A disponibilidade dos dados permite que as melhores decisões sejam tomadas e, consequentemente, traz resultados mais assertivos e eficientes, quando comparada às decisões tomadas sem acesso a informação.

Assim, coadunamos com Silveira et al. (2016, p. 129) quando afirmam que o mercado de dados pessoais torna-se mais importante a cada dia "e pode ser entendido como as interações econômicas voltadas à compra e venda das informações relativas a uma pessoa identificada ou identificável, direta ou indiretamente". As necessidades dos agentes envolvidos dentro da economia (usuários finais, instituições públicas e empresas) são a base desse novo modelo econômico.

[81] Vídeo no YouTube: https://www.youtube.com/watch?v=u4gzCpd3hJw. Acesso em: 20 mar. 2021.

A coleta dos dados pessoais passou a se dar de forma massiva, tendo como principal aliado as novas tecnologias, principalmente a internet, que tornou possível um novo modelo de negócio, o *zero-price advertisement business model*. Nesse modelo, o consumidor não paga em dinheiro pela utilização de um serviço on-line ou bem de consumo – a contraprestação se dá mediante a possibilidade da coleta dos dados pessoais que serão vendidos para a publicidade direcionada – o que criou uma nova economia, a economia de dados (BIONI, 2020, p. 42). As informações fornecidas pelos usuários desses serviços são tais, em quantidade e qualidade, que proporcionam inúmeros usos secundários, em especial a comercialização dos dados para agências de publicidade, utilizados para obtenção de resultados com base em estatística, análises de preferências, perfis de consumo individual ou familiar.

Os serviços "gratuitos" e as tecnologias interativas fizeram surgir uma nova mercadoria: a informação, que é mais que um bem ou um recurso – é um produto com valor econômico (RODOTÀ, 2008, p. 46). "Navegando" pela internet, ou olhando as opções existentes nas lojas de aplicativos para *tablets* e celulares, é fácil constatar que a maioria dos serviços oferecidos é gratuita[82], ou seja, não existindo uma contraprestação em dinheiro para o seu uso. As pessoas acabam fornecendo seus dados pessoais em troca de publicidade direcionada, ou outros fins, ao passo que os consumidores dos serviços também são produtos comercializados na nova economia[83] (BIONI, 2020, p. 22). Logo, podemos afirmar que os dados pessoais "gerados pelas identidades e comportamentos, dos indivíduos e suas ações em redes digitais, são a moeda paga pelo uso gratuito de plataformas, sites e serviços online" (SILVEIRA et al., 2016, p. 219)[84].

---

[82] Bioni (2020, p. 24) destaca que existem serviços que são pagos, versões "premium", que são "versões diferenciadas do mesmo produto", e no entanto, mesmo nessas versões, a lógica do mercado de dados permanece, os dados pessoais são contabilizar "para rentabilizar mais ainda esses negócios".

[83] Tal afirmação já foi realizada por Bauman (2008). Tal autor fala que estamos inseridos numa pós-modernidade, e essa pós-modernidade possui como característica a liquidez, fluidez e volatilidade. "Na vida líquida, a distinção entre consumidores e objetos de consumo é frequentemente momentânea, efêmera – e sempre condicional. Podemos dizer que a regra aqui é a reversão de papéis, embora mesmo essa afirmação distorça a realidade da vida líquida, na qual os dois papéis se interligam, se misturam e se fundem". Nessa sociedade, também entendida como sociedade de consumidores, "ninguém pode deixar de ser um objeto de consumo" (BAUMAN, 2008, p. 18).

[84] Os serviços de informação, tais como Google, Facebook e Apple, estão estruturados dentro de um sistema integrado que fornece aos usuários uma ampla variedade de serviços e permite, simultaneamente, a coleta de dados pessoais e o controle do mercado publicitário. A maioria desses serviços é fornecida sem contraprestação financeira, mas, conforme mencionado, isso não significa gratuidade (COHEN, 2016, p. 377). Uma das primeiras empresas a utilizar de forma mais "intensa" dos dados pessoais foi a MySpace. A companhia revelou que "não recorreria apenas aos dados pessoais que compunham os perfis dos seus usuários, mas, também, a

Por isso, Rodotà (2008, p. 111) adverte sobre a importância de se enxergar o contexto em que se estabelecem os relacionamentos entre as pessoas e as organizações, e buscar compreender quem é o indivíduo que está se formando nesse novo modelo comercial. Hodiernamente, as pessoas utilizam inúmeros serviços que demandam, para sua utilização, disponibilizar dados pessoais, direta ou indiretamente, bem como a própria interação em rede depende do fornecimento de dados pessoais e aspectos da privacidade, o que muitas vezes é realizado sem a devida crítica.

Na verdade, toda ação cotidiana na sociedade da informação envolve o fornecimento de dados pessoais, desde transações bancárias com cartão de crédito em que as pessoas cedem dados pessoais às instituições financeiras, ou quando decidem participar de uma rede social, cedendo dados pessoais para poder usar gratuitamente a plataforma, ou quando utilizam um aplicativo de transporte, ou em casos menos perceptíveis como realizar uma consulta rápida na internet, ao fazer uma ligação, ao solicitar auxílio-doença, ao escolher livros na biblioteca, ou ao cruzar fronteiras em viagens internacionais, em todas essas hipóteses existe troca de dados pessoais, realizados por computadores que registram todas as ações.

Os computadores e seus sistemas de comunicação conectados por meio de rede, agora, são capazes de intervir em todos esses tipos de relacionamentos (LYON, 1994, p. 3). Dardot e Laval (2017, p. 175), nesse sentido, mencionam a possibilidade da construção de um "Comum do Conhecimento", onde usuários construiriam e alimentariam gigantescas bases de dados de forma voluntária, bases essas exploradas comercialmente pela iniciativa privada e sem retorno direto ao fornecedor dessas informações. Fato que leva Lyon (1994, s. p.) a afirmar na introdução de seu livro que entre os impactos mais visíveis que as novas tecnologias trouxeram para a sociedade está a economia de dados, pois para o autor parece

---

eventuais informações garimpadas nos relatos sobre gostos e hábitos de consumo que cada um manifestava" (SIBILIA, 2016, p. 34). Deste modo, a empresa classificou milhares de usuários dentro de dez categorias diferentes, para que cada pessoa tivesse uma publicidade direcionada aos seus interesses de consumo. O Fecebook também utilizou estratégia semelhante, buscando potencializar a publicidade e aumentar a margem de lucro, e assim nasceu o projeto denominado "o Santo Graal da Publicidade", em que prometia transformar cada usuário da rede social num "eficaz instrumento de marketing para dezenas de companhias que vendem produtos e serviços na internet" (SIBILIA, 2016, p. 35). O mencionado projeto, basicamente, consistia no monitoramento de transações comerciais feitas pelos usuários do Facebook, jogando luz sobre o movimento dos usuários – comportamento geral na internet, tais como sites visitados ou compras realizadas –, diminuindo o foco apenas em comentários negativos ou positivos. Nesse novo modelo, a ideia era de uma publicidade sutil, os anúncios dirigidos surgem de modo não intrusivo. A ideia era que a mensagem publicitária "se instale nas conversas", conforme exposto por Mark Zuckerberg, o que de certo modo acabou levantando dúvidas sobre a privacidade das conversas entre os membros do Facebook. As informações coletadas dos usuários e oferecidas por eles sem nenhum tipo de questionamento são o principal ativo do Facebook, e são exploradas pela empresa para "extrair todo o seu valor em termos de mercado" (SIBILIA, 2016, p. 34-36).

estar socialmente difundida a coleta de informações pessoais para serem armazenadas, combinadas, recuperadas, processadas, comercializadas e mapeadas por meio de poderosos bancos de dados eletrônicos.

Neste contexto de dependência tecnológica, juntamente com o impulso realizado pela nova economia de dados, as informações on-line e off-line estão interligadas, pois "desde que a internet se tornou mais integrada com o mundo real, dados on-line e off-line se misturam facilmente" (BOFF, 2018, p. 118). Compras realizadas fisicamente podem ser cruzadas com dados de compras realizadas pela internet, como através de cartões de fidelização de supermercados ou farmácias. Como exemplo dessa nova abordagem comercial, podemos citar a rede de supermercados Sainsbury's, que ganhou o prêmio de *Mobile and Messaging* no *Marketing Week Masters Awards,* pois passou a utilizar dados de localização de smartphones para mostrar ofertas personalizadas nos celulares dos clientes, tanto na loja física como nos arredores dela. A mesma estratégia também é adotada por empresas de vestuário como a Nike, que possui um esquema de fidelidade, o Nike+*,* e um aplicativo de personalização de produtos, o NikeID, que também coleta dados pessoais dos seus usuários[85]. Outro exemplo é a rede britânica de supermercados Tesco, que passou a comercializar a sua base de dados, denominada Crucible*,* para outras empresas, de diferentes ramos do mercado – tais como Sky (televisão por assinatura), Gillette (barbeadores e produtos cosméticos) e Orange (provedores de televisão e internet) (AMARAL, 2019). Sobre esse fenômeno, Rodotà (2008, p. 112) analisa que a coleta de dados realizada é utilizada para organização das empresas, finalidades estatísticas, entender o perfil dos consumidores, bem como esses dados podem ser comercializados ou cedidos a terceiros[86].

---

[85] A Nike utiliza o sistema Zodiac, que, com base nos detalhes de cada consumidor (residência, renda, estilo de vida, etc.), passou a criar perfis inteligentes, classificando os clientes por grupos de modo a segmentar os dados dos clientes por categorias (AMARAL, 2019).

[86] "Se, por exemplo, considerarmos a maioria dos programas com os quais são administradas as relações entre vendedores e compradores, entre fornecedores e usuários de serviços, entre gestores e usuários de sites da Internet, veremos que, em um número relevante de casos, são produzidos os assim chamados *transactional data* ou *telecommunications-related personal information* (TRPI), ou seja, informações geradas a partir do próprio fato de que entre determinados indivíduos ocorreu uma relação contratual que permite ao vendedor ou ao fornecedor de serviços adquirir automaticamente uma série de informações sobre o usuário, e que dizem respeito à sua identificação, aos horários e locais de utilização do serviço, às suas escolhas (e, portanto, suas preferências), às formas de pagamento preferidas, e assim por diante. Estes dados não somente podem ser consultados sempre que o gestor do sistema considerar oportuno, com finalidades estatísticas, para planejar campanhas publicitárias, para traçar perfis dos usuários, como também podem ser cedidos a terceiros" (RODOTÀ, 2008, p. 111-112).

A segmentação dos usuários é possível graças a tecnologias de rastreamento que estão espalhadas por um rede complexa. Segundo Igo (2018, p. 355), dentro dos cinquenta maiores sites dos Estados Unidos existe uma média de sessenta e quatro dispositivos de rastreamento instalados em seus sistemas, possibilitando a essas empresas o mapeamento em tempo real de seus usuários[87], utilizando informações referentes a localização, renda, interesses comerciais e até questões de saúde – toda essa coleta de dados se dá de modo sutil, sendo difícil para o usuário médio perceber a intrusão[88].

Essa coleta e estocagem de dados pessoais é um fenômeno recente, que iniciou em meados dos anos de 1970, juntamente com a entrada da Sociedade da Informação. Antes o armazenamento dos dados pessoais pelo setor privado era pontual e eventual. Porém, atualmente os bancos de dados aumentam numa velocidade exponencial, tanto no setor público como no setor privado, estando conectados em redes, o que permite o cruzamento de vários bancos de dados, "constituindo uma *Personal Information Economy* – ramo bastante lucrativo de trocas informacionais. Além disso, essa massa de dados circula por uma rede descentralizada e com finalidades as mais distintas" (BRUNO, 2013, p. 150)[89].

---

[87] A tecnologia de análise de dados utiliza inúmeros métodos para chegar a essas classificações, que "vão desde o rastreamento de cliques e a mensuração do tempo dedicado a cada página até a captura automatizada do que é teclado ao visitar um determinado site" (BRUNO, 2013, p. 145). Um exemplo de como a classificação dos usuários pode ser eficaz com base em rastros on-line é o caso Target. A equipe de análise de dados dessa empresa varejista americana conseguiu traçar o perfil de consumidoras grávidas com base na lista de produtos. A análise pretendia ser tão eficaz que, além de prever o estado de gravidez, informava qual o provável período para, com base nessas informações, direcionar a publicidade correta para essas consumidoras. A eficácia da tecnologia foi comprovada por um pai furioso que se dirigiu à Target exigindo que a mesma parasse de encaminhar propagandas à sua filha adolescente referentes a gravidez, pois com essa atitude poderia incentivar a sua jovem filha a engravidar. No entanto, passado um tempo, o pai da jovem liga para a loja pedindo desculpas, porque, posteriormente, foi informado de que sua filha estava de fato grávida. A Target, por meio da tecnologia de análise de dados, soube antes mesmo do próprio pai da jovem sobre seu estado de gravidez (BIONI, 2020, p. 37). Em sentido semelhante, Lima (2018) afirma que "diferentes tecnologias podem agora rastrear o histórico de visitas dos usuários (incluindo links para sites anteriores e posteriores), quais informações eles acessam e recuperam, quanto tempo gastam em um determinado artigo, o que compram (e onde e quando o compram), que anúncios visualizam e por quanto tempo, quais dados pessoais (incluindo dados financeiros) eles inserem em formulários da web, que software estão usando, quais e-mails recebem, abrem (incluindo quando e onde é acessado) e para quem é encaminhado. Jornais on-line, por exemplo, agora podem obter facilmente registros dos interesses políticos ou outros de seus leitores, e livrarias on-line podem obter registros de quais livros seus clientes visualizaram ou compraram (em qualquer tópico, incluindo saúde, finanças, etc.)" (LIMA, 2018, p. 130).

[88] Esse mapeamento e criação de perfis é possível analisando as pesquisas realizadas na internet, compras e postagens em redes sociais, formando um enorme banco de dados que, cruzando informações, é capaz de traçar um perfil pessoal dos usuários ou grupos de usuários, vinculando-os, inclusive, a doenças psicológicas ou médicas, pessoas vítimas de abuso sexual, compradores impulsivos, ou possibilidade de gravidez (BRUNO, 2013, p. 145).

[89] Isto apenas tornou-se possível graças ao desenvolvimento de tecnologias baseadas em microeletrônica que possibilitaram uma expansão da capacidade de armazenamento de informações e processamento de dados, além de tornar muito mais simples a recuperação de dados (LYON, 1994, p. 83). Uma das diferenças marcantes que a informatização permitiu dar ao tratamento de dados pessoais pode ser visualizada tanto num aspecto

Por conseguinte, tornou-se fácil obter uma imagem detalhada da vida cotidiana dos usuários e consumidores de serviços e produtos. A capacidade de vigilância foi aumentada pelo uso de novas tecnologias quando comparada àquela do tempo em que a coleta e análise se davam de modo manual. Agora dados referentes a questões como situação financeira, registros de saúde, preferências do consumidor, transações de telefone, elegibilidade de bem-estar, residência, nacionalidade e formação étnica, experiência educacional e atividades criminais estão prontamente disponíveis para os mais diversos usos. Além disso, os registros duram mais tempo e podem ser recuperados e comparados com outros registros de modo rápido e simples. Inclusive, tais bancos de dados não precisam nem ser da mesma instituição ou geograficamente próximos[90] (LYON, 1994, p. 83).

Big data é "um termo em evolução que descreve qualquer quantidade volumosa de dados estruturados, semiestruturados ou não estruturados que podem ser explorados para se obterem informações" (MAGRANI, 2019, p. 15). Segundo Bioni (2020, p. 34), *big data* geralmente é associado a três "Vs": volume, velocidade e variedade[91].

A tecnologia do *big data* permite que um enorme volume de dados seja estruturado e analisado para as mais diversas finalidades. Uma das grandes diferenças dessa tecnologia: os dados não precisam estar previamente estruturados para serem tratados. Os dados não precisam estar separados em entidades e atributos para se conseguir os resultados desejados – a linguagem no *big data* é não estrutural, os dados não estão estruturados em tabelas e são

---

quantitativo quanto num aspecto qualitativo. O primeiro aspecto é demonstrado pela facilidade e rapidez de processar uma gama imensa de dados em um período de tempo extremamente curto, e o outro aspecto é a possibilidade de adotar refinadas metodologias de tratamento de dados, tais como novos métodos, algoritmos e técnicas, que obtêm resultados mais assertivos para os mais diversos fins, e consequentemente mais valiosos. Tais aspectos, o volume de dados tratados e a qualidade desse tratamento, representam a base técnica que potencialmente pode ser utilizada a qualquer coleta de dados pessoais (DONEDA, 2006, p. 172).

[90] Um exemplo do cruzamento de dados de segmentos bem diferenciados é o caso da sorveteria Farrell's, nos EUA. A Farrell's Ice Cream Parlor tinha uma promoção em que seus consumidores, no dia de seu aniversário, tinham direito a um sundae de graça. Esses dados com nome e data de aniversário foram posteriormente vendidos para uma empresa de marketing que acabou revendendo-os para o Departamento de Defesa dos EUA. Outro exemplo de cruzamento de dados pode ser a comparação dos registros dos funcionários da American Civil Service Commission, agência federal do governo americano que foi criada para selecionar os funcionários do governo por mérito, com funcionários que recebiam os benefícios a fim de erradicar as fraudes. No mesmo sentido, o Departamento de Seguro de Saúde dos EUA estava combinando arquivos para verificar se nenhum médico vinculado aos planos de saúde Medicare ou Medicaid estava cobrando em dobro. Comparar arquivos em uma escala tão grande claramente só é possível usando computadores. Portanto, tais investigações são tecnologicamente facilitadas. Mas, uma vez iniciada, a correspondência por computador tem implicações enormes. Qualquer um pode ser pego na rede do computador e pode ser considerado culpado até que se prove sua inocência (LYON, 1994, p. 10).

[91] "Volume e variedade, porque ele excede a capacidade das tecnologias 'tradicionais' de processamento, conseguindo organizar quantidades antes inimagináveis – dos bits aos yottabytes – e em diversos formatos – e.g., textos, fotos etc. – e, tudo, em alta velocidade" (BIONI, 2020, p. 35).

registrados separadamente[92]. O grande "avanço" dessa metodologia é justamente a desnecessidade de estruturação dos dados, o que faz com que consiga trabalhar com velocidade, com um volume alto e variado de dados, pois a etapa de estruturação onera e demanda esforços por parte de quem trabalha com as análises de dados. De acordo com Boff (2018, p. 204), os dados podem ser divididos em três classificações no que se refere à estruturação: estruturados, não estruturados e semiestruturados[93].

Com o *big data* os dados podem ser analisados em toda a sua extensão, não sendo necessário separar em amostras – antes a necessidade surgia em razão do tempo para organizar as informações e para estruturar um volume elevado de dados. Agora, todos os dados podem ser relacionados com diversos fatores distintos para encontrar padrões e prever comportamentos, tudo isso em um curto intervalo de tempo. No entanto, tal metodologia não analisa as causas do evento, apenas a probabilidade dele vir a acontecer – "não se está preocupado com as análises das razões que geram uma cadeia de eventos, mas, tão somente,

---

[92] A diferença entre dados relacionais e não relacionais – ou SQL (*structured query language*) e NoSQL (*not only structured query language*) é que os dados não relacionais não estão estruturados. "Os dados relacionais são definidos no nível básico por uma série de entidades tabela que contêm colunas e linhas, ligadas a outra entidades de mesa por atributos comuns. Assim, por exemplo, como o proprietário de um pequeno negócio online você pode ter uma banco de dados SQL por trás de seu site com uma mesa de gravação de nome e endereço de e-mail de seus clientes. Outra tabela pode gravar os seus nomes de produtos e preços. A terceira tabela pode ligar os dois, registrando os clientes que compraram produtos, com informações adicionais, com a data da compra e se ou não qualquer desconto foi aplicado. Os dados não relacionais, no entanto, não são (em geral) armazenados nas tabelas. Muitas vezes chamados de 'dados não estruturados' esses dados consistem de registros separados com atributos que variam, muitas vezes por registro". [...] O próprio vocábulo induz a essa compreensão quanto à desnecessidade da estruturação prévia dos dados para trabalhá-los. As iniciais No (NoSQL) significam "*not only*", ou seja, não apenas SQL, fazendo alusão, justamente, à analise de dados não estruturados que o sistema SQL – dos bancos de dados tradicionais – não é capaz de trabalhar" (BIONI, 2020, p. 35).

[93] "**Estruturados**: são os dados que são facilmente organizados, armazenados e transferidos por meio de um modelo de dados definido, por exemplo, números e textos que nomeiam as variáveis como atributos, em tabelas ou em bancos de dados relacionais: nome, data de nascimento, CPF, endereço, entre outros. Os dados estruturados podem ser processados, pesquisados, consultados, combinados e analisados por diferentes métodos e algoritmos computacionais e, ainda, podem ser visualizados por meio de tabelas, quadros, gráficos, mapas, infográficos, entre outros. Dados estruturados são hierarquicamente estruturados e apresentam menor flexibilidade no que se refere ao formato (por exemplo, no atributo do CPF somente podem ser armazenados valores numéricos compatíveis com as regras de verificação de um CPF válido); **Não estruturados**: são os dados que não são facilmente acessados ou analisados pelos computadores de maneira automática. Podem se apresentar por conteúdos complexos, tais como imagens, vídeos, postagens (posts ou tweets), sem apresentar uma estrutura lógica previamente definida ou esperada. Ao se pensar em um arquivo de dados, tem-se na prática um conjunto não estruturado de dados, visto que o arquivo pode armazenar qualquer formato de dados; **Semiestruturados:** são os dados que possuem uma estruturação fraca e não podem ser organizados por meio de modelos de dados relacionais, por exemplo, em bancos de dados convencionais. Apresentam estrutura irregular, implicitamente definida e não fixa. Como exemplo deste tipo de estrutura pode-se citar o padrão XML (*Extensible Markup Language*), o qual permite de maneira flexível descrever dados e criar formatos de informação para compartilhar dados eletronicamente por meio da Internet, bem como em redes corporativas (intranet)" (BOFF, 2018, p. 205).

com o seu desencadeamento" (BIONI, 2020, p. 36). Logo, não estamos diante de um sistema inteligente.

Em sentido semelhante, Boff (2018, p. 217-218) afirma que o poder do *big data* é a possibilidade de tratar e analisar dados semiestruturados e não estruturados derivados de diferentes lugares, tipos, formatos, estruturas e fontes, além da capacidade de operar com um enorme volume de dados preservando a veracidade e a autenticidade dos dados. Dessa forma, passa a ser interessante coletar o máximo possível de dados, pois mais cruzamentos podem ser realizados e infinitos fins e previsões podem ser feitas. Por tal razão as informações pessoais são constantemente rastreadas, coletadas, arquivadas, copiadas, manipuladas, transferidas e expostas.

O *big data* começou a ser utilizado em diversos tipos de previsão, chegando a antecipar crises financeiras. Inclusive o Facebook chegou a afirmar que conseguiria prever fins de relacionamentos amorosos com base nos posts dos seus usuários. Igo (2018, p. 357) vê com preocupação os poderes do *big data*, pois para ela os destinos das pessoas estão sendo moldados por fórmulas matemáticas de difícil compreensão que são utilizadas diariamente para influenciar decisões em todas as esferas da vida, ao passo que essas mesmas pessoas desconhecem ou conhecem pouco sobre como essas grandes empresas usam desse conhecimento coletado. Conhecimento que adentra nas minúcias da vida desses indivíduos, conhecendo-os mais que eles mesmos, para ao fim serem utilizados com o objetivo de classificação e avaliação por diversos atores (agências de financiamento, governos, agências comerciais, seguros de saúde, departamentos de RH de empresas).

Obviamente que apenas um amontoado de informações não teria valor algum, mas sim a transformação da informação em conhecimento que depois é aplicado no mercado de diversas formas (BIONI, 2020, p. 10) Neste sentido, é o "conhecimento que permite uma tomada de decisão para agregação de valor" (BOFF, 2018, p. 200). A técnica utilizada para transformar dados em informações denomina-se mineração de dados. Com base nessa técnica é possível retirar conhecimento e determinar padrões[94].

[94] Também comumente apresentada em seu nome em inglês, *data mining*. Segundo Doneda (2006, p. 176), o método consiste "na busca de correlações, recorrências, formas, tendências e padrões significativos a partir de uma quantidade muito grande de dados, com o auxílio de instrumentos estatísticos e matemáticos". Logo, é possível transformar amontoados de dados brutos e não organizados em informações definidas e organizadas para fins definidos e a possibilidade de obter tais informações úteis cresce à medida que cresce a quantidade de dados em estado bruto disponíveis para a mineração (DONEDA, 2006, p. 176-177).

Segundo Bioni (2020, p. 37), basicamente, a mineração de dados corresponde a um procedimento "automatizado de processamento de grandes volumes de dados que possui como principal função a extração de padrões e regras de correlação entre elementos". Como resultado desse processamento, dependendo do tipo de regras utilizadas chegamos a determinados padrões. Ainda de acordo com Bioni (2020, p. 37), a regra mais empregada é o *profiling*[95], que, por meio de um mecanismo de associação, cria regras (similaridade, vizinhança, afinidade) entre dois dados, no mínimo. Feita a associação e criado o padrão, a máquina passa a ter a faculdade de distinguir pessoas ou grupos, ou seja, criam-se perfis que visam a "determinar indicadores de características e/ou padrões que são relacionados à ocorrência de certos comportamentos" e inferir a sua recorrência no futuro (BRUNO, 2013, p. 158). Bioni (2020, p. 37) enumera exemplos de padrões de comportamento que podem ser auferidos futuramente utilizando bases de dados. São eles:

> i) um provável surto de gripe, com base nos termos agregados de pesquisa de um buscador;
> ii) o risco de um tomador de crédito ser inadimplente para calibrar a taxa de juros ;
> iii) segurados que tendem a ter maiores riscos de problemas de saúde para daí aumentar o pagamento do prêmio (BIONI, 2020, p. 37).

Nesse sentido, o perfil[96] visa a representar a probabilidade de ocorrência de um fator, ou seja, "preferências potenciais de consumo, valor econômico potencial, tendências e inclinações comportamentais, capacidades profissionais, doenças virtuais" (BRUNO, 2013, p. 162). Como explicado, com o *big data* não é mais necessário fazer análises por amostragem, podendo-se considerar todos os dados coletados. Por isso, com a mineração dos dados chega-se a perfis específicos – isso não significa que se faça referência a uma pessoa específica, mas sim visa-se à análise de relações entre pessoas (interpessoal), ou, como prefere Bruno (2013, p. 160), "perfis são microrregularidades dos nichos, tribos, grupos". O principal objetivo é categorizar as condutas, buscando prever acontecimentos futuros previstos dentro de um

[95] Doneda (2006, p. 173) explica que essa técnica de criação de perfis utiliza tanto informações disponibilizadas pelas pessoas ou que são colhidos de outras bases de dados. Os perfis criados podem ser de indivíduos ou mesmo de grupos de pessoas. "Nela, os dados pessoais são tratados, com o auxílio de métodos estatísticos, técnicas de inteligência artificial e outras mais, com o fim de obter uma 'metainformação', que consiste numa síntese dos hábitos, preferências pessoais e outros registros da vida desta pessoa" (DONEDA, 2006, p. 173). Ademais, o resultado dessa análise pode ser utilizado para diversos fins, como prever comportamentos ou tendências para o futuro, sendo aplicada em vários segmentos, tais como: envio de mensagens publicitárias para pessoas mais suscetíveis em gostar do produto/serviço, bem como controle alfandegário, criando grupos que poderiam ser perigosos para a nação.

[96] Entende-se por perfil "um padrão de ocorrência de certo fator (comportamento, interesse, patologia, traços psicológicos) num dado conjunto de variáveis" (BRUNO, 2013, p. 160).

quadro de variáveis, pois a mineração de dados não deixa de funcionar dentro de uma lógica de triagem algorítmica (BRUNO, 2013, p. 172-174).

A tecnologia da informação tornou possível agregar e comparar dados de toda natureza – dados que estavam espalhados pelas inúmeras interações em sociedade e muitas vezes esquecidos. Agora torna-se concebível reuni-los em um único lugar e manipulá-los em novas configurações, sendo possível realizar comparações e identificações de todos os tipos de perfis de pessoas e/ou populações, graças à junção entre técnicas estatísticas e tecnologia computacional (LYON, 1994, p. 84).

De acordo com Bioni (2020, p. 42), esse mesmo avanço da tecnologia permitiu a criação de perfis cada vez mais invasivos sobre as pessoas, pois passou a controlar os comportamentos psicológicos e emocionais dos indivíduos para correlacioná-los a padrões que podem ser utilizados para levar ao consumo. Tais conhecimentos possuem valor monetário. Os dados brutos são a matéria-prima desse sistema, e também são elementos de valor, por possibilitar o processamento e a geração de informações, as quais "pode[m] ser continuamente processadas em conjunto com novos dados ou informações a ponto de se estabelecer um ciclo a partir de, sobre e com a informação" (BOFF, 2018, p. 179). Informação gera mais informação, e a sociedade vai sendo moldada de acordo com o conjunto informacional que é criado e a todo momento aperfeiçoado, indexado, agrupado e organizado de acordo com prioridades não tão claras.

Contudo, mede-se o valor da informação de acordo com a sua possibilidade de se transformar em conhecimento. Os dados coletados precisam ter sentido para auxiliar nas necessidades das empresas e organizações. Neste sentido, entra a mineração de dados, que, segundo Boff (2018, p. 196), é confundida por muitos autores com a Descoberta do Conhecimento ou Extração do Conhecimento (também conhecido como KDD – *knowledge-discovery in databases*). Porém, a mineração de dados é uma etapa (importante) do processo da Descoberta do Conhecimento. Pode-se dizer que se trata de um ramo da computação que visa a automatizar a exploração de grandes bases de dados e reconhecer padrões através da modelagem de fenômenos do mundo real. Esse processo é composto por uma série de etapas: a) criação da base de dados; b) amostragem; c) pré-processamento; d) extração de características; e) construção do modelo; f) avaliação do modelo; g) visualização; e h) resultados (*score*). A mineração de dados cuidaria das etapas da amostragem (b) até a visualização (g). A diferença principal é que a Descoberta do Conhecimento engloba o

ordenamento dos resultados, "sob critério de ordenação, crescente, decrescente, do mais relevante para o menos relevante, entre outros" (BOFF, 2018, p. 199). Ademais, a Descoberta do Conhecimento permite retornar às etapas anteriores para obter uma maior interação ou poder validar as hipóteses que apareceram ao longo da análise dos dados, firmando o conhecimento adquirido (BOFF, 2018, p. 197).

O produto almejado no processo de Descoberta do Conhecimento é uma informação significativa no processo de tomada de decisão, podendo ser utilizada em diversas áreas[97]. Toda essa sistemática trabalha para a geração de riquezas. Dados pessoais e não pessoais são utilizados na engrenagem econômica e graças à Descoberta do Conhecimento e do *big data* de forma muito mais escalável (BIONI, 2020, p. 12). As novas tecnologias passaram a rastrear os movimentos dos indivíduos, principalmente on-line[98], e, desta forma, a compreender os interesses dos usuários e direciona-los a uma publicidade mais assertiva[99]. A assertividade é possível graças ao processo realizado por algoritmos nos websites e nas plataformas on-line que, com base no perfil do usuário, elegem conteúdos que se encaixem em suas preferências, causando um efeito de filtro bolha, uma vez que limitam o conteúdo que é mostrado aos usuários. Trata-se de um dos mais relevantes processos de modulação. "Para modular as

---

[97] a) relacionamento com os clientes: os sistemas baseados em Descoberta do Conhecimento podem responder desde quem são os melhores clientes até quais clientes provavelmente encerrarão o relacionamento com a loja virtual;
b) apoio à tomada de decisão: aplica-se a quase todas as áreas, desde a medicina ao marketing; e
c) sistemas de recomendação: classificam os objetos de acordo com os perfis de usuário. Os objetos podem ser, por exemplo, produtos como na loja virtual ou documentos a serem apontados por mecanismos de busca.
[...] Bem como sistemas de Descoberta do Conhecimento e Mineração de Dados podem auxiliar aos médicos terem uma segunda opinião, visto que métodos computacionais podem procurar padrões em bancos de dados médicos (sintomas, doenças, casos raros, entre outros) e fornecer indicações para o diagnóstico (BOFF, 2018, p. 198-199).

[98] Nesse quesito, destacam-se os cookies, que são necessários para a visualização das páginas da internet. Os cookies nada mais são que informações enviadas pelo site ao navegador web que ele espera receber de volta a cada página aberta. "Eles são usados para manter sessões ativas, por exemplo. Sem cookies, seria bastante difícil ficar 'logado' em um site, porque o site não ia saber que você é a mesma pessoa que digitou a senha com sucesso. Quando o navegador envia de volta o cookie do site, a página consegue associar aquele cookie ao usuário" (ROHR, 2021). Contudo, os cookies também podem ser utilizados para rastrear os usuários: são os chamados "*web beacons*". Eles cedem informações sobre as visitas realizadas, e isto inclui todos os sites que possuem tal sistema, conseguindo um vasto histórico do usuário na web.

[99] "Por meio do registro da navegação dos usuários cria-se um rico retrato das suas preferências, personalizando-se o anúncio publicitário. A abordagem publicitária passa a ser atrelada com precisão ao perfil do potencial consumidor. Sabe-se o que ele está lendo, quais os tipos de websites acessados, enfim, tudo aquilo em que a pessoa está efetivamente interessada e, em última análise, o que ela está mais suscetível a consumir com base nesse perfil comportamental" (BIONI, 2020, p. 17).

escolhas, é preciso selecionar e agrupar os indivíduos em conjuntos, conforme os perfis de consumo e de comportamento"[100] (SILVEIRA et al., 2016, p. 221).

Conforme todo o exposto, é possível dividir o mercado de dados em camadas. Silveira et al. (2016, p. 223) resumiram o complexo mercado de dados dividindo-o em quatro camadas: a primeira é a de coleta e armazenamento de dados. Nessa camada estão as plataformas de relacionamento (Instagram, Facebook, etc.), os demais sites, os mecanismos de busca (Google, Bing, etc.) e de rastreamento de navegação, os sensores, as antenas de celulares, dentre tantas outras formas de coletas de dados. A segunda camada é a de processamento e mineração de dados, que, conforme visto, envolve o tratamento e a reunião dos dados coletados e armazenados, cruzando com outros dados de fontes diversas ou não com o intuito de aprimorar e enriquecer um perfil, criar segmentos mais detalhados, por meio do uso de linguagens artificiais. Os chamados *brokers* atuam nessa camada como agentes que se dedicam à compilação e venda dessas informações. Na terceira camada é executada a análise e formação das amostras, local em que se encontram os departamentos de marketing

[100] As redes sociais trabalham com algoritmos invisíveis que determinam o que aparecera para cada usuário em suas telas. São os chamados *curation algorithms*. Logo, mesmo uma pessoa com várias conexões em comum tem o seu *feed* diferente de seus amigos, pois o algoritmo mapeia as preferências dos usuários, colocando-os em bolhas para melhorar a publicidade e fazer com que as pessoas gastem mais tempo nas redes, uma vez que apenas aparecem assuntos e temas que lhes interessam. Existem algumas iniciativas para melhor entender o funcionamento dos *curation algorithms*, e uma delas é o Istawareness, que promete entender melhor esse algoritmo do Instagram. Buscando entender como funciona a o algoritmo do Instagram, foi utilizado o Istawareness disponível no site instawareness.ugent.be, que faz uma comparação do *feed* do aplicativo Instagram com e sem os *curation algorithms.* No caso, foi utilizado a conta do Instagram de titularidade da presente autora, Camila Kohn. De cada 50 postagens no *feed* da conta sob analise no Instagram, apenas uma aparecia sem o algoritmo, ou seja, que apareceu por ordem cronológica de postagem. Isto significa que de 50 postagens apenas uma não foi ocultada pelo algoritmo. Por exemplo, o algoritmo do Instagram mostrou uma postagem de uma página de perfil que estaria 1.105 posições abaixo no lugar de um perfil de humor, se fosse considerada a ordem cronológica de postagem. O algoritmo também faz uma classificação dos perfis que ele entende como aqueles com que o usuário possui mais afinidade dentre aqueles que escolheu seguir. Sobre a ferramenta, utilizando minha conta pessoa, foi espantoso perceber que as postagens do perfil de um deputado foram classificadas como o perfil de mais afinidade. Realmente, é pouco provável que ele seria o escolhido (se me fosse dada essa oportunidade) como meu conteúdo favorito ou algo que gostaria de ver com frequência. Sobre esse fenômeno, não podemos deixar de mencionar que os *curation algorithms* criam o efeito filtro bolha, que tem preocupado estudiosos sobre a democracia, uma vez que muitos autores enxergam nesses mecanismos uma das causas do aumento da polarização ideológica no consumo das mídias on-line, pois os usuários seriam colocados em câmaras de ecos de suas próprias crenças (SPOHR, 2017, p. 150). Em sentido semelhante, Barocas e Nissenbaum (2009, p. 3) veem com preocupação a segmentação e as postagens em ordem diferente de informações e anúncios, pois tais arquiteturas podem ameaçar a autonomia individual, visto que terceiros montam ambientes capazes de limitar as escolhas dos indivíduos, diminuindo sua real liberdade. A objeção das autoras está na interferência indevida na construção das identidades humanas. As pessoas devem possuir a prerrogativa de selecionar os produtos, localidades ou serviços dentro de todo o universo possível de escolhas, e não ter essa liberdade tolhida por meio de um algoritmo que segmentou essa pessoa para um determinado grupo em que serão apresentadas opções de conteúdo e produtos com as quais a princípio ela teria mais afinidade, inferidas com base no seu comportamento passado e interações on-line.

de empresas e plataformas que vendem o serviço de localização de públicos segmentados e audiências semelhantes (*look alikes*). Na terceira camada também estão presentes empresas que realizam análises de audiência na internet, grau de sucesso das publicidades direcionadas, dentre outras atividades envolvendo conversão em vendas e dados. Por fim, a quarta camada é a da modulação. Aqui estão agrupados serviços de oferta de produtos e serviços com base na segmentação dos perfis de acordo com as divisões encontradas na fase de mineração de dados. Nessa camada, encontram-se os dispositivos de filtro, os *curation algorithms*, ou algoritmos de controle de visualização e a formação de bolhas de usuários/consumidores. É nessa fase final que as empresas fazem a publicidade direta com os usuários das redes. Aqui também está incluída a atividade de venda final dos produtos julgados apropriados para determinado perfil de pessoa (SILVEIRA et al., 2016, p. 223-224).

No entanto, o sistema não sobrevive apenas com a coleta intrusiva ou discreta dos dados. Na realidade, a maioria das informações é cedida espontaneamente pelas pessoas e vai além das fornecidas para utilizar os serviços. As pessoas expõem suas vidas e informações até pouco tempo tidas como privadas nesses novos espaços, possibilitando a criação de perfis cada vez mais fidedignos da realidade. Desde 1990, estudiosos sobre proteção de dados e privacidade viam com preocupação a criação e o desenvolvimento acelerado do modelo de negócio *zero-price advertisement*, em que os usuários negociam sua privacidade e seus dados por conta própria (IGO, 2018, p. 354). Dito em outros termos,

> concretamente, isso significa que a contrapartida necessária para se obter um bem ou um serviço não limita mais à soma de dinheiro solicitada, mas é necessariamente acompanhada por uma cessão de informações. Nessa troca, então, não é mais somente o patrimônio de uma pessoa que está envolvido. A pessoa é obrigada a expor seu próprio eu, sua própria persona, com consequências que vão além da simples operação econômica e criam uma espécie de posse permanente da pessoa por parte de quem detém as informações a seu respeito (RODOTÀ, 2008, p. 113).

A Sociedade da Informação pode ser entendida como tela gigante em que se confessam segredos e intimidades privadas. Experiências íntimas são pronunciadas em público, tornando a discrição em espetáculo e convertendo o sigilo embaraçador em exaltação (BAUMAN, 2012, p. 51). Fenômeno que Igo (2018, p. 354) denomina de Era da Confissão 2.0, nitidamente perceptível nas redes sociais, que tiveram o condão de transformar o corriqueiro em extraordinário. As pessoas, no afã de se tornarem celebridades, ou apenas serem vistas, divulgam voluntariamente aspectos de sua vida privada (BAUMAN, 2011, p. 41). Assim, com o rastreamento on-line associado à cessão voluntária das mais diversas

informações, torna-se possível conhecer os desejos das pessoas por meio de plataformas que as mesmas utilizam para compartilhar suas histórias pessoais, hábitos, preferências e movimentos (IGO, 2018, p. 354)[101]. Nesta perspectiva, "materializa-se assim a imagem do 'homem de vidro', o verdadeiro cidadão desse novo mundo" (RODOTÀ, 2008, p. 113)[102].

O montante de dados coletados, armazenados e analisados é gigantesco, trazendo à tona outro lado desse mercado de dados, que Zanatta e Abromavay (2019, p. 424) chamam "economia da atenção, cujo domínio é exercido por gigantes como Alphabet (Google), Alibaba, Amazon, Apple, Microsoft, Facebook e Twitter". Tal economia também pode ser relacionada com uma economia do vício, pois a arquitetura dos aplicativos é pensada com o intuito de prender a atenção das pessoas, utilizando de gatilhos psíquicos, pois, quanto mais tempo se gasta nas redes, mais dados são coletados e mais publicidade é direcionada aos seus usuários (ZANATTA; ABROMAVAY, 2019, p. 429). Os vícios nas redes vão além da necessidade de existir, conforme exposto por Bauman (2011, p. 28)[103], mas também estão baseados em designs viciantes, repletos de inúmeros pequenos eventos inesperados, o que

---

[101] A exposição na rede não vem apenas através de textos, mas também por imagens. Praticamente todos os computadores do mercado vêm com uma câmera embutida, assim como os aparelhos celulares também vêm equipados com câmeras. As pessoas passaram a tirar fotos de si mesmas, as famosas selfies. As imagens de si mesmo foram as que mais foram produzidas e exibidas em todo o planeta em 2013. As fotos instantâneas tiradas da própria face e postadas em redes sociais facilitaram a difusão do fenômeno de visibilidade e conexão com as outras pessoas (SIBILIA, 2016, p. 21).

[102] Apenas para exemplificar, em 2019, foram gerados 2,5 quintilhões de bytes por dia, o que equivale, aproximadamente, a dois milhões e meio de terabytes de dados por dia. "Cada fração destes dados pode ser associada a uma pessoa, acumulada, ressignificada e reutilizada" (DAINEZI, 2019, p. 22-23). Segundo Boff (2018, p. 131), a humanidade está mergulhada num universo digital, e este dobrará de tamanho a cada dois anos. A autora entende por universo digital todos os dados digitais criados, replicados e consumidos, desde os vídeos compartilhados no YouTube, imagens e filmes digitais nas TVs de alta definição, as músicas tocadas nas plataformas de streaming, tais como Spotify, os dados bancários nos aplicativos de internet banking e em caixas automáticos, as mensagens de voz, texto e imagens transmitidas pelos aplicativos de conversa, como Telegram, WhatsApp, Facebook, dentre outros, que se transformaram no meio de comunicação mais comum da atualidade. Neste sentido, o volume de dados em formato digital gerado e armazenado vem crescendo exponencialmente com a evolução das tecnologias de informação e comunicação (TICs) aplicadas nas mais diversas áreas e organizações. Gantz e Reinsel (2012, p. 1) estudaram o crescimento do volume de informações no planeta, apontando que, de 2005 a 2020, o volume de dados digitais crescerá em um fator igual a 300, ou seja, passará de 130 hexabytes para 40 mil hexabytes ou 40 trilhões de gigabytes. Isto representa 5.200 gigabytes para cada homem, mulher ou criança em 2020 (BOFF, 2018, p. 131).

[103] Para Bauman (2011, p. 28), um dos principais atrativos do Twitter seria a prova de existência, pois quanto mais pessoas podem ver o indivíduo, maior o seu convencimento de que está no mundo. Em tal plataforma as pessoas respondem em tempo real à pergunta: "O que está acontecendo?", que não pode exceder 140 caracteres (BAUMAN, 2011, p. 27). As respostas giram em torno de situações banais, como "relatar a que horas costumam dormir, tomar banho ou café da manhã, falar sobre o tempo, o trânsito, a novela ou difundir certas notícias jornalísticas. Com essas práticas, em pouco tempo o Twitter adquiriu credibilidade no que se relaciona à informação que circula no ambiente, e muitos perceberam que o software possibilitava em tempo real entender e compartilhar os acontecimentos da vida pessoal, cultural e social do planeta" (SANTANA; COUTO, 2012, p. 34).

gera produção de dopamina (hormônio da felicidade) e pode levar ao vício. Esse ecossistema econômico e social está levando as pessoas a abdicarem de direitos fundamentais em troca de benefícios e sensações de satisfação momentâneas (MASSIS, 2020). A lógica atual dita que para pertencer e existir em sociedade é necessário ceder e produzir dados sobre si, como bem exposto por Dainezi (2019, p. 28) de maneira coercitivamente livre.

Aliada a uma arquitetura viciante, conforme detalhado no item 2.1, a tecnologia tornou-se onipresente na Sociedade da Informação, adentrando em todos os espaços e momentos, nas casas e ambientes de convívio social, no trabalho, nos momentos de lazer, no quotidiano como um todo. A computação ubíqua fez com que as pessoas não percebessem a sua presença, isso porque "toda a área de computação estará agregada às estruturas básicas e fundamentais da vida do ser humano" (BOFF, 2018, p. 134)[104].

A coleta e o uso, cada vez maior, das informações pessoais sem a devida conscientização das pessoas pode levar a um abismo entre os dados e informações conscientemente fornecidas e a real utilidade desses dados após a sua conversão em informação-resultado. Ficam obscuros quais os reais objetivos após as técnicas de tratamento dos dados pessoais. Não há clareza sobre como esses dados serão, realmente, utilizados e qual o potencial risco que eles representam à vida das pessoas. Essa falta de clareza e controle dos dados pessoais leva Doneda (2006, p. 181) a afirmar que a falta de controle e consciência do uso dos dados pessoais "produz como efeito a perda de controle da pessoa sobre o que se sabe em relação a si mesma – o que, em última análise" pode levar a uma diminuição da "própria liberdade".

É indiscutível o valor desse enorme banco de dados[105] que pode ser associado à maneira renovada com que os profissionais do marketing, bem como seguradoras (inclusive de saúde) ou agências de proteção ao crédito, conseguem visualizar as ações dos seus

---

[104] Ademais, a computação ubíqua está diretamente ligada com a computação pervasiva, que "implica no uso de sistemas computacionais com sensores e atuadores, que podem estar conectados em rede, podem ter diversas interfaces e estar presentes em qualquer tipo de objeto" (MURINA et al., 2021, p. 1), distribuídos de modo perceptível ou imperceptível. Em resumo, de acordo com Dainezi (2019, p. 23), podemos afirmar que o mercado de dados está organizado em quatro camadas que se misturam e ligam de acordo com o modelo empresarial das organizações que se relacionam no mercado: "A primeira é a de coleta e armazenamento de dados; a segunda pode ser denominada de processamento e mineração de dados; a terceira é a análise e formação de amostras; por fim, a quarta é a de modulação".

[105] Dentre os modelos de negócio mais rentáveis pode-se vislumbrar as redes sociais, que são embasadas dentro de conceitos como visibilidade, vigilância, identidade e indexação (TEFFÉ; MORAES, 2017, p. 122). Neste contexto, Bezerra (2018, p. 26) ilustra que no espaço virtual circulam imagens, sons e textos de cunho pessoal, em muitos casos, sem a consciência dos titulares desses dados sobre os usos que podem ser feitos dessas informações.

consumidores, havendo a possibilidade de definir padrões precisos e prever comportamentos derivados de um vasto estoque de informações de todas as áreas da vida (informações médicas, financeiras, genéticas e de localização).

No entanto, esses dados, quando empregados de formas diferentes, têm o condão de causar danos reais a pessoas reais e definidas (IGO, 2018 p. 355). Não sem razão Rodotà (2008, p. 99) alerta para os problemas que podem advir da monetização das informações pessoais, que fomenta a criação de enormes bancos de dados sobre tudo e sobre todos ao passo que dá muito poder para aqueles que os detêm, tanto entes públicos como privados, possibilitando um invasivo controle social.

3.4 UTILIZAÇÃO DE DADOS NA SAÚDE

O setor da saúde[106] sempre precisou ter conhecimento de dados pessoais e dados pessoais sensíveis referentes à saúde, uma vez que não há como pensar em assistência à saúde sem ter acesso aos dados da pessoa. Da mesma forma, necessita-se de dados para a investigação de novas soluções de saúde, tais como novos medicamentos, dispositivos médicos, melhores tratamentos, e diagnósticos mais assertivos (BARBOSA; LOPES, 2021, p. 57). As aplicações dos dados de saúde são diversas, e esse número continua a crescer dia após dia. Dados de saúde podem ser utilizados desde a melhoria de um serviço de saúde, do ponto de vista administrativo, até mesmo para a construção e/ou aperfeiçoamento de um protocolo clínico que visa ao diagnóstico de uma doença (PINOCHET et. al, 2014, p. 12). São inúmeras as melhorias e os avanços que se podem obter no setor da saúde com auxílio dos dados e da tecnologia, que incluem de tudo, "desde sites que fornecem informações sobre doenças para aplicativos de saúde móvel e robótica de saúde doméstica" (TSCHIDER, 2019, p. 1.508).

O modelo de cuidado de saúde está sofrendo uma transformação e os dados nesse segmento serão de suma importância para os avanços no setor. Lottenberg et al. (2019, p. 11) afirmam que a saúde esta numa nova era. Para os autores, na Quarta Revolução Industrial, em que haverá mais consultas remotas que presenciais – a exemplo da operadora de saúde estadunidense Kaiser Permanente –, governos estão passando a fomentar a inovação e a

[106] Setor de saúde é uma área complexa, envolvendo inúmeros profissionais que atuam direta e indiretamente na promoção da saúde. "Inclui provedores, pagadores e beneficiários de serviços de saúde, mas inclui, igualmente, autoridades públicas, grupos de interesse e pesquisadores com vínculo direto com a prática clínica" (SARLET; MOLINARO, 2019, p. 189).

tecnologia na saúde, e gigantes no mercado da tecnologia, como Google, Amazon e Apple, estão começando a acenar grande interesse no setor médico e de cuidados de saúde.

De acordo com Comitre (2021, s. p.), no último evento promovido pela Apple, a empresa, novamente, demonstrou seu interesse pelo setor de saúde. Foram apresentadas novidades para o setor como "hardwares para monitorar dados de saúde, até atualizações no aplicativo Saúde e no HealthKit, com melhorias para integração de terceiros ou novas formas de compartilhamento de dados com usuários".

Outro gigante de tecnologia, o Google, em 2019, comprou a Fitbit, o que indicou que a empresa também tem interesse nesse setor. Inclusive, o Google vem coletando "dados médicos de milhões de americanos desde 2018 e sem o seu consentimento", juntamente com a empresa Ascension, que possui uma cadeia de hospitais nos Estados Unidos. O projeto de coleta de dados médicos do Google, denominado Projeto Nightingale, já coletou dados de saúde advindos de "resultados de exames de laboratório, diagnósticos médicos, registros hospitalares" além de dados pessoais "normais" como nomes e datas de nascimento de pacientes. O Projeto Nightingale, segundo a empresa, estaria de acordo com a lei federal de saúde dos Estados Unidos, pois a Lei de Portabilidade e Prestação de Contas do Seguro de Saúde (ou HIPAA) permite o compartilhamento de dados de saúde sem o consentimento dos pacientes, desde que relacionados à prestação de serviço de saúde. Assim, como o projeto da Google com a Ascension visa a "migrar sua infraestrutura para a nuvem, a integração com a G Suite e permitir que os médicos melhorem o atendimento ao paciente, fornecendo-lhes ferramentas melhores", isto seria para fins de melhorar a saúde, logo dentro da lei (ROSOLEN, 2019, s. p.).

A Apple, por outro lado, está investindo fortemente em segurança e privacidade de dados, e na área de saúde, a empresa está seguindo a mesma linha. No último evento da empresa, apresentou a possibilidade de integração de softwares de prontuários eletrônicos, porém sempre dando ao usuário a escolha do que compartilhar ou não e com quem. Há uma grande expectativa para o futuro da utilização dos aparelhos vestíveis, tais como o Apple Watch, e que possam ser usados mais incisivamente no setor da saúde, passando a permitir medição de temperatura e glicemia (COMITRE, 2021, s. p.). Ademais, a Apple já havia anunciado que auxiliaria em três novos estudos médicos. O primeiro deles é um estudo envolvendo saúde da mulher. Desde 2014 a empresa utiliza recursos para avaliar a saúde da mulher. O objetivo é identificar pacientes que possuem risco para doenças comuns, tais como síndrome do ovário policístico, bem com outras condições, como infertilidade ou osteoporose.

O estudo é uma parceria da Apple com a T. H. Chan School of Public Health de Harvard e o Instituto Nacional de Ciência da Saúde Ambiental. Outro estudo em parceria com a Universidade de Michigan envolve audição. Busca-se verificar "como a exposição sonora afeta a audição ao longo do tempo". E por fim, o terceiro estudo analisa como o ritmo de caminhadas e passos está diretamente relacionado com a saúde do coração e qualidade de vida (FARR, 2019, s. p.).

Todas essas inovações, dentre outras, necessitam de dados. E falar de dados dentro do setor da saúde é basicamente falar de dados sensíveis, em sua maioria, o que torna o setor da saúde completamente diferente de outros ramos da economia. Para se tratar um paciente é necessário possuir informações sobre ele, e informações sensíveis. Por tal razão o sigilo médico sempre foi tão valorizado, quase como um dogma da profissão. Na área da saúde, o compartilhamento de dados tem consequências diretas nas vidas das pessoas. O "atendimento assistencial tem impacto por toda a vida", e os dados são muito importantes para a pessoa e para uma coletividade que pode se aproveitar dos resultados positivos de um tratamento para outros casos similares (KIATAKE, 2021, p. 329).

Sempre foi necessário coletar dados de saúde do paciente. Porém, com a tecnologia, essa necessidade aumentou. Segundo Naes (2020, p. 5), a tecnologia no setor da saúde é entendida como "uma ferramenta para auxiliar as atividades humanas, tais como computação de dados, a qualidade e a velocidade dos processos de trabalho e seus resultados". Dentro do setor, a utilização do termo eHealth é como um guarda-chuva que abarca as ferramentas tecnológicas em saúde, que incluem coleta, processamento e compartilhamento de dados dentro de uma organização de saúde, que incorporam essas informações em diferentes níveis e sistemas. Envolvendo sistemas administrativos, radiologia, informação farmacêutica, telemedicina e sistemas de informação hospitalar, mesmo com diferenças, esses sistemas têm por finalidade última auxiliar nos cuidados de saúde para os pacientes (NAES, 2020, p. 6).

O mais antigo e, ainda, um dos mais importantes documentos para compreender a saúde de um paciente é o prontuário médico. O termo prontuário "deriva do latim *promptuarium*, que significa lugar onde se guardam ou depositam as coisas de que se pode necessitar a qualquer instante" (BARAÚNA JR, 2019, p. 45). Do significado da expressão, dá para se ter uma ideia da necessidade desse documento, onde estão localizadas todas as informações dos pacientes, de forma individualizada, relativas ao seu estado de saúde gerado ao longo da sua vida (BARAÚNA JR, 2019, p. 47). Neste sentido, percebe-se que os dados de

saúde do paciente, transcritos no prontuário do paciente pelo médico, são algo de longa data. Nesse documento o médico descreve a anamnese, o exame físico, exames laboratoriais e/ou de imagem, hipóteses de diagnósticos, conduta, evolução do tratamento, bem como outras informações que visam ao diagnostico e tratamento de uma determinada moléstia. Todos esses conjuntos de dados e informações são essenciais para o trabalho do médico, e por meio deles é possível desenvolver o raciocínio clínico acerca de um determinado caso. Ademais, essas informações são importantes para outros profissionais, ao lerem o prontuário do paciente, entenderem o contexto clínico em que o paciente se encontra e não precisarem "iniciar do zero" toda vez. Logo, o prontuário médico tem a função de fazer o registro clínico do paciente para fins de diagnóstico e tratamento, bem como transmitir de forma segura e acessível as informações para os múltiplos profissionais, autorizados, envolvidos no cuidado do paciente (PINOCHET et al., 2014, p. 15).

Além de auxiliar no tratamento do próprio paciente, os dados de saúde, podem ajudar toda a coletividade. Sabe-se que os dados em saúde, bem como a ciência por detrás de sua análise e interpretação, também servem para responder a uma das perguntas mais fundamentais na ciência médica: como sabemos o que funciona? (KESSLER, 2018). Esses dados são utilizados em estudos para comprovar a eficácia dos tratamentos e medicamentos, o que faz com que algumas particularidades sejam excluídas do resultado total. Basicamente, hoje as decisões estão baseadas em uma média. E essa média nem sempre é compatível com todos os pacientes, uma vez que muitos ocupam posições de extremidade na curva gaussiana. Por exemplo, hoje, um médico, objetivando tratar um paciente que se queixa de febre, pode prescrever 500 mg de paracetamol de 6 em 6 h. Isso é um padrão que foi encontrado por meio de uma média. Mas, certamente, uma pessoa de 100 kg com o metabolismo rápido poderá não apresentar o mesmo resultado de uma pessoa de 50 kg com o metabolismo lento. Com o avanço da tecnologia da coleta e interpretação de dados de saúde, poderemos chegar em um mundo onde a posologia será personalizada para cada paciente. Contudo, para que isso seja possível, será necessário cada vez mais coleta e tratamento de dados de saúde para que a máquina seja capaz de prever os melhores diagnósticos, os melhores remédios, as pré-disposições e como dar mecanismos para prevenir doenças e fazer com que os pacientes sejam saudáveis e não doentes. O futuro da medicina une tecnologia e prevenção de doenças, não apenas a cura de enfermidades. A tendência é de humanização das relações médicas, enxergando o paciente como um ser único e individual.

Todavia, para que a medicina avance para esse estágio, serão necessários dados para que possam ser implementados avanços na área da saúde. Dentre os mais festejados, o desenvolvimento da Inteligência Artificial – IA no setor da saúde, que seria capaz de auxiliar os profissionais na elucidação de diagnósticos. Porém, para que as máquinas tenham um grau elevado de assertividade, elas precisam ser treinadas. Em outras palavras, é preciso ensinar as máquinas. E esse ensinamento ocorre pela absorção de dados gerados a partir de consultas, resultados de exames laboratoriais e de imagem, tratamentos, anotações médicas, gravações eletrônicas de dispositivos médicos, bem como outros dados de saúde. A máquina aprende a partir de casos semelhantes, fazendo associações com casos semelhantes, e quanto mais dados forem fornecidos, melhor será o "aprendizado" e maior será a sua funcionalidade (LOTTENBERG et al., 2019, p. 35).

Neste sentido, a IBM, por meio da análise preditiva, desenvolveu um modelo para prever sepse[107], popularmente conhecida como infecção generalizada. Em parceria com a Geisinger Health System, a empresa conseguiu avançar nos resultados, chegando em um modelo que consegue prever e, por consequência, prevenir a doença. O modelo foi construído com dados de pacientes internados e os dados enviados para seguradoras – os códigos de cobrança que os profissionais e serviços de saúde enviam para as companhias de seguro, por exemplo. O objetivo foi identificar os pacientes que possuem maior risco de desenvolver a sepse. Assim é possível priorizar o atendimento e evitar internações arriscadas (CLEMENTE, 2021, s. p.).

No exemplo acima, o modelo preditivo é construído com auxílio de inteligência artificial, que tem encontrado diversas funcionalidades no setor de saúde, tanto para estabelecer e/ou aperfeiçoar políticas públicas sanitárias quanto para diagnóstico e terapia individuais. A inteligência artificial pode ser utilizada, como visto, em sistemas de apoio à decisão clínica. Esses sistemas usam dados de saúde para auxiliar os médicos na tomada de decisão clínica, seja sobre um diagnóstico, seja sobre um tratamento. Este ramo tecnológico da medicina, que utiliza inteligência artificial e aprendizado de máquina (*machine learning*), permite que o sistema aprenda com experiências anteriores e utilize da imensa base de dados (*big data*) para reconhecer padrões. Esses sistemas de inteligência artificial baseados em

[107] Segundo o site da IBM, a sepse é uma doença com taxa de mortalidade elevada (25 e 50%), e, além de ameaçar a vida das pessoas internadas, os custos dispendidos por conta da complicação viram em torno dos US$ 27 bilhões por ano. Para piorar o cenário, a Covid-19, dentre outras infecções, pode acarretar a sepse e sobrecarregar ainda mais as UTIs (CLEMENTE, 2021, s. p.).

metodologias de aprendizado de máquinas dependem intensivamente de dados de saúde para a acurácia e eficiência de suas informações. Quanto mais dados, mais eficiente e preciso o sistema consegue ser, o que explica o porquê dos dados de saúde serem tão valiosos dentro deste contexto (NAES, 2020, p. 7). Outra aplicação da inteligência artificial seria a utilização de *chatbots*[108] para orientar a população, como, por exemplo, com informações sobre o horário de funcionamento de postos de saúde, detalhes sobre campanhas de vacinação, esclarecimentos sobre *fake news* associada à área de saúde, entre outras aplicações para o público em geral (MARANHÃO; ALMADA, 2021, p. 359). Dentre os benefícios dos *chatbots*, o relatório do Fórum Econômico Mundial (2020b, p. 11) listou cinco: 1) a possibilidade do acesso à informações de saúde em qualquer hora e lugar; 2) com apenas um *chatbot* podem ser atendidos milhares de clientes; 3) rápida implementação; possibilidade de reaproveitamento do sistema para outros usos de saúde pública e/ou emergências; 4) respostas mais rápidas e de modo mais intuitivo que outras opções digitais; e 5) geração automática de grande quantidade de dados para uso ou treinamento futuro.

Outra utilização benéfica de dados de saúde é a sua utilização para definição de políticas sanitárias e para a pesquisa (SCHAEFER, 2010, p. 56). Por exemplo, se um médico de família e comunidade que trabalha em uma unidade básica de saúde começa a atender vários pacientes de uma mesma região com gastroenterite viral aguda, as entidades políticas no âmbito da secretaria municipal de saúde, com acesso a esses dados, podem propor intervenções públicas para reverter esse cenário, como: melhorar o saneamento básico daquela região ou conscientização sobre a importância de lavar bem os alimentos e as mãos antes das refeições. Outro exemplo de como os dados de saúde podem ser utilizados para auxiliar em programas de saúde é o programa londrino Whole System Integrated Care (WSIC), que junta informações da saúde e da assistência social por meio de um software que "transforma essas informações soltas em conhecimento para dar suporte" nas tomadas de decisão. O programa de computador consegue identificar as pessoas na região que se encontram em situação de maior vulnerabilidade ou que precisam de internação

[108] "Um chatbot é um programa de IA projetado para conversar de maneira natural com as pessoas via interfaces de voz ou mensagens de texto. Chatbots são normalmente encontrados em sites, aplicativos ou mensagens instantâneas". São também conhecidos como agentes conversacionais, em que, geralmente, são pré-carregados com um conjunto de regras ou pré-treinados usando dados para poder ter uma conversa significativa com o usuário em tempo real e para fornecer serviços úteis no processo (WORLD ECONOMIC FORUM, 2020b, p. 6-7).

(LOTTENBERG et al., 2019, p. 76). Neste sentido, a inteligência artificial aliada às novas tecnologias ligadas

> [...] com grandes bancos de informação médica, permitem conhecer as principais causas de morbidade e fornecer informações que contribuam para a elaboração de políticas para prevenção e acompanhamento desses casos. Além disso, possibilitam identificar os estratos populacionais que mais demandam o sistema de saúde, os custos gerados, e traçar estratégias para atendê-los de forma mais eficiente (LOTTENBERG et al., 2019, p. 39).

Todavia, se a inteligência artificial aprende com exemplos, e não com regras pré-programadas, para o sucesso dessa revolução tecnológica será necessário coletar e armazenar muitos dados. Assim, para as abordagens de aprendizado de máquina fornecerem informações precisas, precisa haver uma base com muitos dados de modo estruturado. Um exemplo de base que deteria uma enorme gama de informações seriam os prontuários médicos eletrônicos, unificados (SARLET et al., 2021, p. 498). O prontuário digital unificado é uma inovação que veio para revolucionar a forma com que o profissional de saúde registra o atendimento, com uma perspectiva de poupar do paciente o tempo de ter que relatar a sua moléstia e sua história clínica inúmeras vezes para cada novo profissional da saúde que lhe atende, e poupá-lo de levar uma pasta cheia de exames antigos para cada nova consulta médica, preservá-lo de fazer exames redundantes e ainda facilitar o acesso dessas informações para conhecimento próprio. Além dessas vantagens para os pacientes, o prontuário unificado, apoiado por um sistema de dados e algoritmos de inteligência artificial, também poupa o tempo do médico na coleta de dados da anamnese, auxilia no diagnóstico e propõe a melhor conduta com base no desfecho de milhares de casos semelhantes (LOTTENBERG et al., 2019, p. 17).

Além da coleta dos dados pelos prontuários médicos, esses mesmos dados podem ser captados em resultados de exames de sangue e nos laudos dos exames de imagem. Com o avanço da tecnologia da internet das coisas (IoT – *Internet of Things*), os dados de saúde poderão, como já o são, coletados de diversos objetos físicos, muitos deles que compõem o vestuário. São os chamados *wearables.* Atividades corporais de todos os tipos (frequência cardíaca, temperatura, qualidade do sono, percurso de caminhada, percurso de ciclismo) são coletadas, armazenadas e enviadas para bancos de dados de saúde por meio desses dispositivos. Por exemplo, já existem relógios que registram a frequência cardíaca, a saturação de oxigênio, as horas de sono, o deslocamento, o número de passos, e que podem juntar informações que complementam o exame físico do médico em consultório. A chamada

hipertensão do jaleco branco (que é o aumento pressórico do paciente quando em ambiente hospitalar) é uma das possibilidades práticas que os dispositivos móveis têm em elucidar sobre um diagnóstico, já que ele consegue coletar dados de saúde do paciente em um contexto fora do meio hospitalar/ambulatorial. A essas pequenas informações, referentes à coleta de dados personalizadas de um indivíduo, chama-se *small data*. A *small data* avalia dados históricos de um indivíduo, enquanto que a *big data* avalia um grande volume de dados para descobrir padrões (KANNAN, 2019). Diferentemente do *big data*, os *small data* não são utilizados na busca por padrões, e sim nos modos eficazes para um paciente em específico. Com a expansão dos smartphones, aplicativos de saúde e dispositivos, agora estão disponíveis para ajudar consumidores a se conhecerem melhor, bem como a incentivar seus usuários a realizar feitos como parar de fumar, lembrar de beber água, dormir melhor, controlar o estresse, monitorar a fertilidade (IGO, 2018, p. 359).

O uso da Internet das Coisas possibilitaria esse tipo de coleta, uma vez que todas as coisas, desde celulares e relógios inteligentes até geladeiras e automóveis, estariam conectadas à internet. E os dados que essas "coisas" conseguem captar estão em constante e rápida expansão – para compartilhar, armazenar, analisar e processar um volume grande de dados e gerarem novas informações. Quanto mais dispositivos estiverem conectados, maiores as informações e mais dados podem ser produzidos (e mais invasivas se tornam essas tecnologias) (MAGRANI, 2019, p. 15). O uso dessas tecnologias é encarado com entusiasmo em vários setores, e na saúde não é diferente. Segundo o Ministério da Saúde (2020, p. 106), "o futuro da saúde passa pela capacidade de armazenamento, processamento, organização, gestão e utilização desses conjuntos de dados oriundos das mais diversas fontes", e com base nessa coleta de dados os gestores e profissionais da saúde estarão munidos de informações para soluções avançadas no setor. Ademais, Tschider (2019, p. 1.508) comenta que o setor da saúde passou a chamar a internet das coisas de *Internet of Health Things* (IoHT). Seria uma espécie de variação da internet das coisas para a tecnologia que conecta dispositivos físicos, como dispositivos médicos, abrangendo o mercado de dispositivos relacionados à saúde envolvendo dispositivos médicos conectados e dispositivos de autocuidado em saúde.

Neste sentido, a junção da internet das coisas, aplicativos móveis e o prontuário eletrônico podem possibilitar uma rede de apoio em cuidados preventivos em grande escala, como cuidados de enfermagem e colaboração entre médicos de diferentes áreas de atuação e especialidades (NAES, 2020, p. 6). Em igual sentido, Lottenberg et al. (2019, p. 39) percebem que a associação da internet das coisas com a inteligência artificial irá permitir uma

"expressiva melhoria de qualidade na jornada de cuidado do paciente e na construção de soluções mais eficientes e inovadoras"[109]. Assim,

> no que afeta os cuidados de saúde, o uso de big data inaugura oportunidades para tratamentos personalizados, incrementando a eficácia, a acurácia e a eficiência. O uso de grandes quantidades de dados possibilita uma melhor estratificação dos pacientes, de modo que, por exemplo, os efeitos colaterais são reduzidos e as tentativas terapêuticas fúteis podem ser evitadas. A coleta e a análise de dados relacionados à saúde abrem definitivamente novos potenciais no que se refere à medicina preditiva (SARLET; MOLINARO, 2019, p. 189).

Os dados de saúde também são necessários para possibilitar a prática da telessaúde. Telessaúde é um termo amplo que descreve atividades que envolvem a área da saúde que são realizadas a distância por intermédio de tecnologias digitais. Segundo Schaefer (2010, p. 205) essa é a "área da telemática em saúde que engloba todas as ações da medicina a distância voltada à coletividade, promovendo a prevenção de doenças, a educação e a coleta de dados de grupos determinados". Dentro da telessaúde temos a telemedicina, que restringe um pouco mais esse conceito para descrever a troca de dados e informações de saúde a distância. As formas mais populares de telemedicina são a teleconsulta e as teleconferências (NAES, 2020, p. 5). As teleconsultas, além das consultas prestadas por médicos a distância para resolver problemas simples de saúde cuja falta do exame físico não irá comprometer a qualidade do serviço nem a assertividade do diagnóstico, também podem ser extrapoladas pela troca de dados (mensagens de texto, imagens, áudios) entre profissionais da saúde para esclarecimento de dúvidas (LOTTENBERG et al., 2019, p. 40). A telemedicina, apesar de parecer uma novidade, ocorria e ocorre informalmente há tempo, quando os profissionais da saúde esclareciam dúvidas e prescreviam cuidados por meio de plataformas digitais como WhatsApp[110], Messenger e Facetime, celular ou e-mail. "Nesses dispositivos é grande o

---

[109] Dentre os exemplos, existe a possibilidade de "marcapasso cardíaco monitorado remotamente, pâncreas artificial que monitora a glicose no sangue e fornece insulina, implantes cerebrais para tratar os sintomas de Parkinson e Alzheimer, próteses com software conectado aos ossos". Ademais, existem estudos de pílulas inteligentes, cápsulas "com sensores que percorrem o organismo em busca de sinais fora do padrão (anomalias), capazes de detectar desde doenças benignas até câncer". Todas essas tecnologias são capazes de gerar ainda mais dados sobre a saúde das pessoas que podem ser utilizados em novas pesquisas para achar outros benefícios (KAUFMAN, 2021, s. p.).

[110] Inclusive, o CFM, em 2017, divulgou o Parecer nº 14/2017, que permite o uso de tecnologias como o WhatsApp em que prevê que ao médico é permitido o uso de aplicativos de conversas "para comunicação entre médicos e seus pacientes, bem como entre médicos e médicos, em caráter privativo, para enviar dados ou tirar dúvidas, bem como em grupos fechados de especialistas ou do corpo clínico de uma instituição ou cátedra, com a ressalva de que todas as informações passadas têm absoluto caráter confidencial e não podem extrapolar os

tráfego de imagens de problemas de pele, dúvidas sobre exames, orientações sobre como tomar os remédios ou como seguir o tratamento, dieta, exercícios" (LOTTENBERG et al., 2019, p. 111). Em 2020, por conta da pandemia do novo coronavírus, o Conselho Federal de Medicina (CFM) reconheceu em caráter provisório a possibilidade de atendimento médico a distância durante o combate à Covid-19 (Lei nº 13.989/2020)[111]. Essa medida abriu espaço para a ascensão da prática médica por dispositivos digitais, que aumenta a formação de dados de saúde digitais. Esse tipo de serviço de saúde ajuda a aliviar a pressão em hospitais e prevenir a propagação de doenças infectocontagiosas, uma vez que pacientes com condições latentes e leves podem ser consultados no conforto de casa.

A informatização do prontuário médico traz benefícios imensuráveis para a medicina, como descrito e exemplificado anteriormente; entretanto, também é inegável que os dados de saúde movimentam um mercado bilionário que pode se utilizar da pessoa como instrumento para ganhar mais dinheiro. Com a consolidação da quarta revolução industrial e a expansão de tecnologias como *big data*, *wearables*, inteligência artificial, o corpo humano poderá ser enxergado como um conjunto de números e informações (SCHAEFER, 2010, p. 59). Dentro dessa perspectiva, a tendência atual é compreender o corpo humano como um grande arquivo de dados, uma grande fonte de informações e recursos para o mercado.

O mercado de dados pessoais "tem se tornado cada vez mais relevante na era informacional e pode ser entendido como as interações econômicas voltadas à compra e venda das informações relativas a uma pessoa identificada ou identificável" (SOUZA et al., 2017, p. 263). Os dados nesse sistema podem ser entendidos como uma forma de capital, além de uma simples mercadoria. Sua coleta é necessária para "a concorrência entre os grupos capitalistas, têm sua coleta impulsionada pelo ciclo perpétuo de acumulação de capital". Sendo que os dados são extremamente lucrativos e podem ser utilizados para os mais diversos fins. E assim como o capital, nem todos os dados são iguais, ou possuem as mesmas finalidades, razão pela qual existem dados com valores diferentes (SILVEIRA; SOUZA, 2020, p. 21).

---

limites do próprio grupo, nem tampouco podem circular em grupos recreativos, mesmo que compostos só por médicos".

[111] Art. 1º Esta Lei autoriza o uso da telemedicina enquanto durar a crise ocasionada pelo coronavírus (SARS-CoV-2). Art. 2º Durante a crise ocasionada pelo coronavírus (SARS-CoV-2), fica autorizado, em caráter emergencial, o uso da telemedicina. Art. 3º Entende-se por telemedicina, entre outros, o exercício da medicina mediado por tecnologias para fins de assistência, pesquisa, prevenção de doenças e lesões e promoção de saúde. Art. 4º O médico deverá informar ao paciente todas as limitações inerentes ao uso da telemedicina, tendo em vista a impossibilidade de realização de exame físico durante a consulta. Art. 5º A prestação de serviço de telemedicina seguirá os padrões normativos e éticos usuais do atendimento presencial, inclusive em relação à contraprestação financeira pelo serviço prestado, não cabendo ao poder público custear ou pagar por tais atividades quando não for exclusivamente serviço prestado ao Sistema Único de Saúde (SUS).

Na área da saúde, como visto, os dados têm diversos fins. “Os dados são normalmente utilizados para melhor servir os clientes, melhorar a eficiência das transações e a qualidade dos produtos, bem como para identificar as macrotendências” (SOUZA et al., 2017, p. 267-269). Sabe-se que dados pessoais, na era da informação, têm importante valor econômico. Os dados pessoais são o substrato para a análise comportamental de hábitos de vida, hábitos de consumo, bem como diversas outras informações, de uma população. Permitindo a análise de padrões, preferências, consumo, dentre outros. Esses dados permitem, por exemplo, uma empresa fazer propaganda direcionada ao público que tem maior probabilidade de comprar determinado produto. No entanto, quando estamos diante de dados de saúde, em que se consegue extrair minúcias sobre as pessoas, seus comportamentos e pré-disposições, estes dados possuem um valor bem diferenciado. Dados pessoais são valiosos, mas dados pessoais de saúde são ainda mais valiosos, devido ao grau de sensibilidade das informações que eles contêm e suas potenciais aplicações práticas. Tanto é verdade que, em 2017, na 47ª edição anual do Fórum Econômico Mundial, realizado em Davos, na Suíça, os dados de saúde foram um dos tópicos debatidos (BUSINESS, 2017). O próprio criador do Fórum Econômico Mundial, o prestigiado economista alemão Klaus Schwab, aborda o processo de digitalização da medicina e da saúde como um dos pilares que compõem a chamada “quarta revolução industrial”, assunto esmiuçado pelo intelectual em livro homônimo escrito em 2016. Segundo o autor, a quarta revolução industrial é caracterizada por “adesão a inovações tecnológicas nos campos da conectividade, informação e controle de dados aplicados à produção de bens e serviços e com impacto econômico, social e político”. Tecnologias com caráter disruptivo, como inteligência artificial (IA), análise massiva de dados (*big data*), computação quântica, robótica, biologia sintética, realidade aumentada, nanotecnologia, impressão 3D e suas aplicações, internet das coisas, entre outras (LOTTENBERG et al., 2019, p. 15).

Dentre os ganhos que se esperam com a utilização da internet das coisas no setor da saúde, há a projeção de que esse setor será o terceiro mais impactado no mundo, com ganho econômico de US$ 0,2 trilhão a US$ 1,5 trilhão. No Brasil, a internet das coisas no setor da saúde poderá gerar até 2025 um ganho de US$ 5 bilhões a US$ 39 bilhões (LOTTENBERG et al., 2019, p. 38). E de acordo com o exposto, a internet das coisas e a inteligência artificial precisam de dados para operar, e os dados de saúde são o combustível que move esse processo. Dados de saúde, que compõem a *big data*, são o substrato para os algoritmos usados

na inteligência artificial, que são aplicados na área médica para orientação sobre tomada de decisão, também são úteis nas pesquisas farmacêuticas para a comercialização e/ou investigação de um novo fármaco, na análise de rendimento de um estabelecimento de saúde, nos estudos epidemiológicos, entre outras diversas possibilidades elucidadas anteriormente. Neste sentido, Tschider (2020, p. 442) afirma, categoricamente, que sem esses dados os sistemas de inteligência artificial em saúde falham, sendo os dados de saúde "absolutamente essenciais". O mercado de saúde é vasto e lucrativo, as inovações no setor envolvem alguns milhares de dólares, em 2017 havia "mais de 165 mil aplicativos disponíveis para celulares, onde as soluções envolvendo saúde no ambiente digital". Juntos os aplicativos movimentaram "quatro bilhões de dólares, somente na primeira metade do ano de 2017" (BARRETO JR., 2019, p. 302).

Assim, pode-se concluir que estamos diante de um setor extremamente lucrativo e os dados de saúde, necessários para que essa engrenagem continue girando, são tão valiosos quanto. Inclusive, os dados de saúde podem ser utilizados para outros fins e vendidos com outras finalidades que vão além do cuidado ou tratamentos inovadores. De acordo com uma pesquisa realizada pela Frost&Sullivan, intitulada "Global State of Digital Trust Survey and Index 2018", 43% dos líderes de negócios digitais vendiam dados pessoais. De acordo com o relatório, "tem-se que o setor da saúde é o segundo maior destino de venda de dados". As razões das vendas não ficaram claras. As únicas informações disponíveis são a alta lucratividade do setor de saúde, em especial o farmacêutico, que, somente no Brasil, em 2018, chegou a ter um fluxo de "quase R$ 120 bilhões, correspondendo a um crescimento de 11,89% em comparação com o ano antecedente, e chegando a ter uma projeção de crescimento até 2023 para R$ 175 bilhões" (SILVA, 2020, p. 30-31).

Segundo Kfouri Neto et al. (2020, p. 163), em 2008, ocorreu um incidente nos Estados Unidos "em que os dados de prescrição médica estavam sendo utilizados no mercado de seguros individuais, pois as farmácias repassavam a relação de compras de remédios às seguradoras". Com base nessa troca de informação entre as empresas de milhões de pedidos de medicamentos, que provavelmente não se deu de modo gratuito, as empresas de seguro de saúde passaram a alterar suas políticas, "a fim de excluir da cobertura algumas doenças e impor cobranças mais altas do prêmio a determinadas pessoas". A alteração na política dos planos de saúde significa evitar pessoas com grandes chances de utilizar altas taxas médicas. Assim, as seguradoras que tinham informações que possam excluir os "limões podres" para ficar apenas com as "cerejas saudáveis" conseguem uma taxa de lucro muito maior, pois

segundo Souza et al. (2017, p. 268), “um por cento dos doentes representa mais de um quinto dos custos de cuidados com saúde e cinco por cento representam quase metade dos custos”. Juntando essa informação com o crescimento do setor farmacêutico e a alta venda de dados de saúde, tudo indica que é um mercado muito lucrativo possuir os subsídios necessários para antever as “demandas farmacológicas de consumidores e oferta-las explorando ao máximo todo seu potencial econômico” (SILVA, 2020, p. 31)[112].

Desta forma, levando em consideração a alta lucratividade do setor, bem como a quantidade de dados de saúde dos pacientes disponíveis para certos atores do ramo, sem haver uma clareza em como esses dados são utilizados pode-se levar à conclusão de que há um mercado de troca de informações, extremamente desvantajoso para o titular dos dados, em dados colhidos de “entradas em hospitais, clínicas e farmácias”, utilizados para extração de “dados sensíveis sem que nem ao menos os pacientes saibam que estão sendo extraídos, muito menos autorizando suas extrações”. A atividade de compra e venda de informações, apesar de obscura, não é totalmente velada. Por exemplo, a “empresa IMS Health, a qual abriu seu capital em 2014, e tem como seu objetivo social a compra e venda de informações sobre a saúde dos pacientes”, deixando disponível em seu website que possui informações médicas de “85% de todas as receitas médicas prescritas no mundo” (SILVA, 2020, p. 31).

Ademais, além da coleta que pode existir com base nas prescrições médicas ou a lista de compras realizadas em uma farmácia, aplicativos de e-Health ou e-Saúde, para conseguirem funcionar e beneficiar os usuários, precisam coletar e processar dados, e no caso dados sensíveis de saúde, possibilitando a formação de bancos de dados dessas informações coletadas de seus usuários. Logo, tais dados podem ser tratados pelos aplicativos ou serem comercializados com outras empresas, “como é feito hoje em dia no mercado, sem o consentimento dos donos desses dados” (BARRETO JUNIOR, 2019, p. 297). Os aplicativos que prometem uma melhora na saúde e nos hábitos de seus usuários, mesmo sem a utilização de equipamentos vestíveis, conseguem monitorar, coletar e analisar dados de saúde, tais como qualidade de sono ou mesmo consumo de bebidas alcoólicas (SOUZA et al., 2017, p. 267).

[112] Apenas para adiantar uma discussão que será mais bem analisada no item 4.3, “ironicamente, esse tipo de dado foi originalmente reunido para ajudar os pacientes em situações de atendimento de emergência – para garantir o acesso a um registro de seus medicamentos. Mas quando esse plano fracassou, as ordens foram silenciosamente reelaboradas como um meio de discriminar os doentes” (SOUZA et al., 2017, p. 268).

> Monitorando em quais horários do dia, em quais dias da semana e em que lugar uma pessoa desbloqueia seu celular é possível identificar seu padrão de sono, ou mesmo o seu consumo de álcool. Ao identificar uma diminuição das horas de sono às sextas-feiras e na contagem de passos no dia seguinte, por exemplo, é possível detectar um hábito semanal de frequentar festas (SOUZA et al., 2017, p. 267).

A existência de um mercado de dados de saúde é inegável e não há margem para dúvidas de que esses dados valem muito dinheiro também. Porém, também são inegáveis os riscos e os abusos que essas informações podem acarretar para o titular dos dados de saúde. Desde negativas de planos de saúde, ou empréstimos negados, ou dispensa de emprego. Segundo Kaplan (2016, p. 321), nos Estados Unidos, empresas costumam verificar o MIB (*Medical Information Bureau*) de seus candidatos a empregos. Perfis de saúde são os mais vendidos para agências de crédito. Os dados de saúde são muito valiosos. Dentre a gama de possibilidades, podemos imaginar que fornecedores de produtos de saúde poderiam identificar populações para tratamentos, ou para marketing farmacêutico. Inclusive, em 2011, a Suprema Corte dos Estados Unidos analisou um caso envolvendo compra de prescrições médicas para marketing de farmácias. Caso semelhante ocorreu no Reino Unido, em 2000, em que a Souce Informatics, uma subsidiária da IMS Health Inc.[113], queria vender para farmácias os dados de prescrições médicas. No caso UK Souce, a Corte deu permissão para a venda dos dados sem permissão dos pacientes, pois eles estariam anônimos – logo, não seriam dados pessoais de saúde, mantendo a privacidade das pessoas. A solução nos Estados Unidos adotada por sua Suprema Corte deu-se de modo semelhante, derrubando a Lei de Vermont que restringia a venda de dados de prescrições médicas, com base na liberdade de expressão, pois, segundo a Corte, os dados farmacêuticos das prescrições seriam discursos e por estarem anônimos não haveria dados para a privacidade. Apesar de serem dados anônimos, é relevante salientar, os registros médicos contêm informações genéticas, biométricas, dados que não se alteram no tempo, sendo sempre dados que irão fazer referência a uma pessoa. Ademais, registros médicos, também, contêm dados sobre comportamento social, tais como tabagismo, uso de álcool, emprego, nível educacional, etnia, hábitos de saúde que podem ser facilmente

[113] O site da IMS Health afirma que a empresa é líder mundial em informações, serviços e tecnologias dedicados a melhorar a performance dos cuidados em saúde. Operando em mais de 100 países, processando mais de 45 bilhões de transações em serviço de saúde anualmente, organiza informações de 100 mil fornecedores e atende mais de 5 mil clientes de saúde em todo o mundo. Ao longo da década de 1980, a IMS Health desenvolveu um serviço on-line para relatar as vendas de produtos farmacêuticos e comprou a colaboração de companhias envolvidas nesse ramo. Em 1989, a empresa estava fornecendo uma ferramenta de base de dados para laptop com a finalidade de gerenciar as vendas farmacêuticas nos Estados Unidos e na Europa (KAPLAN, 2015, p. 256-257).

cruzados com enormes bancos de dados de terceiros, o que facilita a reidentificação das pessoas com outros dados dispersos, conforme já analisado.

Apesar das boas intenções, o aumento no uso das tecnologias na área da saúde para os fins mais nobres também está possibilitando o seu uso para um mercado preocupado apenas com o lucro. Informações pessoais privadas possuem valor comercial que pode reduzir atritos no mercado e facilitar as transações (ACQUISTI et al., 2016, p. 42). Porém, também podem ser utilizadas para discriminar pessoas e aumentar estigma social (ACQUISTI et al., 2016, p. 4). "Esse ambiente, por sua fluidez, incerteza e fugacidade, pode fragilizar os controles quanto às garantias à privacidade, à não discriminação, ao controle de informações, ao respeito, à autodeterminação e, especialmente, ao compartilhamento dos dados pessoais" (SARLET et al., 2021, p. 499). E ao que tudo indica, "o mercado de dados dará maior poder às corporações do que aos cidadãos em relação às trocas que realizam (SILVEIRA et al., 2016, p. 228). E considerando todo o ecossistema de saúde[114] e toda a gama de informação que pode ser dele retirada para, posteriormente, ser transformada em capital na nova economia, urge a necessidade de um sistema protetivo para os pacientes, titulares dos dados de saúde, em que a personalidade da pessoa humana se sobressalte em relação ao lucro e ao capital, pois, como bem observado por Frazão (2020, p. 108), direitos fundamentais são deontológicos e vinculantes e, deste modo, não estão sujeitos, exclusivamente, a relações de custo-benefício, bem como inovação e desenvolvimento econômico não são valores absolutos, não podendo ser perseguidos "de forma irrestrita e à custa do sacrifício das situações existenciais mais elementares dos titulares de dados".

4 PROTEÇÃO DA PRIVACIDADE E DADOS PESSOAIS

4.1 PRIVACIDADE NO ORDENAMENTO JURÍDICO BRASILEIRO

Conforme visto no capítulo anterior, o fluxo de informações é necessário para a economia e para o progresso em diversas áreas, inclusive na área da saúde humana. Assim, o fluxo de informação alimenta a economia moderna, alimenta as pesquisas e aumenta o conhecimento, traz eficiência para os processos, diminui gastos, quebra barreiras físicas. O fluxo de informação pode ser considerado um exercício de liberdade. E nessa perspectiva, as

[114] O sistema de saúde é muito vasto, "há todo um ecossistema interligado, que vai da clínica médica ao hospital, perpassa o laboratório, a farmácia, o próprio paciente e os agentes de saúde, bem como toda a esfera pública – como o Sistema Único de Saúde (SUS)" (PINHEIRO, 2019, s. p.).

leis que visam a regular, ou mesmo impedir, esse fluxo de informações – como leis que protegem a privacidade – podem parecer leis contra o progresso ou até mesmo leis de censura (OHM, 2010, p. 1.736).

No entanto, a privacidade, conforme visto, possui uma importante função "para a formação do ser humano" (CANCELIER, 2017, p. 121). Após os horrores da Segunda Guerra Mundial, "a comunidade internacional passa a demonstrar constante preocupação com a proteção relacionada à vida privada, o que levou ao reconhecimento do direito no art. 12 da DUDH[115]", Declaração Universal dos Direitos Humanos de 1948 (CRISTO et al., 2020, p. 371-372). Isto porque muitas violações e atrocidades ocorreram no período anterior e durante a guerra. Dentre os exemplos envolvendo privacidade e dados pessoais, o governo de Hitler utilizou de registros públicos, tais como os censos dos países, para encontrar os judeus. O exemplo trágico demonstra como a falta de privacidade, em casos extremos, pode matar, pois, graças a políticas de privacidade francesas, "onde o censo não coletou informações sobre religião por motivos de privacidade", os nazistas conseguiram localizar apenas 25% da população de judeus. No entanto, em países em que o censo coletava muitas informações e com muito detalhes sobre a vida da população, a exemplo da Holanda, os nazistas conseguiram localizar cerca de 75% da população judia, levando ao genocídio desse povo (VALASCO, 2020, s. p.). "Em seguida, na Convenção para a Proteção dos Direitos do Homem e das Liberdades Fundamentais (1950), novamente o direito à privacidade teve papel de destaque, dentro do art. 8º[116] (CRISTO et al., 2020, p. 372).

Dentro do cenário brasileiro, o direito à privacidade não foi uma invenção do constitucionalista de 1988. As Cartas Constitucionais anteriores previam a inviolabilidade da correspondência e da moradia/residência, e em 1967 a privacidade, formalmente, foi ampliada para abarcar as comunicações telegráficas e telefônicas (MARINELI, 2017, p. 93). No entanto, foi apenas com a Constituição de 1988 que o direito à privacidade restou efetivamente "tutelado pela ordem constitucional como direito fundamental (inciso X do art.

---

[115] Ninguém será sujeito à interferência em sua vida privada, em sua família, em seu lar ou em sua correspondência nem a ataque à sua honra e reputação. Todo ser humano tem direito à proteção da lei contra tais interferências ou ataques.

[116] Direito ao respeito pela vida privada e familiar. 1. Qualquer pessoa tem direito ao respeito da sua vida privada e familiar, do seu domicílio e da sua correspondência. 2. Não pode haver ingerência da autoridade pública no exercício deste direito senão quando essa ingerência estiver prevista na lei e constituir uma providência que, numa sociedade democrática, seja necessária para a segurança nacional, para a segurança pública, para o bem-estar económico do país, a defesa da ordem e a prevenção das infracções penais, a protecção da saúde ou da moral, ou a protecção dos direitos e das liberdades de terceiros.

5º) e manteve a tutela da inviolabilidade da moradia e o sigilo de correspondência nos incisos XI e XIII do mesmo artigo" (CRISTO et al., 2020, p. 378).

A Constituição de 1988 deu maior ênfase e importância ao direito à privacidade, destacando a vida privada e a intimidade como direitos fundamentais, dispondo que: "são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação". Posteriormente, o Código Civil de 2002 (Lei n. 10.406) fez menção à vida privada e à intimidade em seu artigo 21, inscrito dentre os direitos da personalidade, com redação muito semelhante à da Constituição Federal. Por tal razão, pode-se dizer que o "direito à privacidade no ordenamento brasileiro possui uma 'dupla-titulação'", sendo considerada tanto um direito fundamental como um direito da personalidade (CANCELIER, 2017, p. 106).

Expliquemos brevemente as diferenças existentes entre os direitos de personalidade e os direitos fundamentais. Alguns autores, como Schreiber (2013, p. 13), defendem que a diferença entre os dois termos existe apenas em relação ao âmbito de proteção. E que os direitos fundamentais seriam os direitos positivados nas Constituições nacionais; ao passo que os direitos da personalidade apontariam para os atributos e necessidades humanas que carecem de uma proteção especial no campo das relações privadas, e por isso presente nas legislações civis. Tanto os direitos fundamentais como os direitos da personalidade poderiam ser traduzidos em direitos humanos, porém estes últimos estariam inseridos em proteções internacionais[117]. Em sentido semelhante Bittar (2015, p. 61) percebe que existe uma inclinação dos direitos fundamentais advirem dos direitos humanos, e estes por sua vez se traduzirem em direitos da personalidade, completando-se, de modo cada vez mais amplo, em busca da proteção de valores inerentes da pessoa humana. No entanto, o referido autor entende que os direitos fundamentais estão diretamente relacionados como uma oposição ao Estado, protegendo a pessoa humana, mais vulnerável, em face do Poder Público. Os direitos da personalidade, por outro lado, protegem o titular das relações particulares. Todavia, apesar das diferentes perspectivas, todos tratam do mesmo fenômeno, a tutela da dignidade humana.

[117] Para Bittar (2015, p. 57-58), os direitos humanos não necessitam de positivação, eles persistem, em face da noção transcendente da natureza humana. "Os direitos humanos subsistem por si, porque inerentes à natureza humana e, em comparação com as liberdades públicas, encontram-se em plano superior. Em outras palavras, esses direitos pairam acima do ordenamento positivo e do próprio Estado, pois encontram a sua raiz no direito natural". Logo, "direitos humanos são direitos ainda não positivados, quando são positivados erige para o plano e direitos fundamentais. A técnica retira-os do direito natural e insere-os nos textos do direito positivo" (BITTAR, 2015, p. 57).

A entrada dos direitos de personalidade nas codificações civis muito se deu após os horrores vivenciados nas Guerras Mundiais, em especial na Segunda Guerra, em que todas as barbaridades dos regimes nazifascistas estavam abarcadas nas legislações positivadas, emergindo a necessidade de resgatar[118] "a ideia da prometida universalidade de direitos do homem proposta pelo jusnaturalismo" (BIONI, 2020, p. 49). De acordo com Doneda (2005, p. 76), passou-se a buscar os direitos da personalidade como um "meio de tutela de um mínimo essencial, a salvaguarda de um espaço privado que proporcionasse condições ao pleno desenvolvimento da pessoa". Derivados do princípio constitucional da dignidade humana que passou a se fazer presente nas Constituições[119], "reposicionando o ser humano no centro" das relações jurídicas e devendo ser protegido em sua integridade (BIONI, 2020, p. 49).

Neste sentido, a personalidade é definida como "a qualidade de ser pessoa", qualidade que é inata ao ser humano, em função de sua exclusiva estrutura física, mental e moral (VIEIRA, 2007, p. 38). Os direitos da personalidade são "[...] direitos essenciais ao desenvolvimento da pessoa humana [...]. Destinam-se a resguardar a eminente dignidade da pessoa humana, preservando-a dos atentados que pode sofrer por parte dos outros indivíduos" (GOMES, 1996, p. 130, apud DONEDA, 2005, p. 77). Assim, Vasconselos (2014, p. 6) afirma que o direito da personalidade é uma exigência da dignidade humana.

A dignidade humana, valor tão caro, é a "qualidade tida como inerente a todo e qualquer humano, sendo frequentemente apresentada como o valor próprio que identifica o ser humano como tal" (SCHREIBER, 2013, p. 6). A dignidade da pessoa humana se manifesta na autonomia da pessoa de ser senhora de si mesma, possuindo valor espiritual e moral inerente, sendo detentora de sua consciente, livre e responsável escolha da própria vida (VIEIRA, 2007, p. 39).

---

[118] Fala-se em resgatar, pois, com a "dessacralização da ciência jurídica, emerge, ao mesmo tempo, o racionalismo na cena jurídica: o jusracionalismo". Fala-se em dessacralização, pois, segundo Doneda (2005, p. 73), o cristianismo exaltava o indivíduo como um ente único, à imagem e semelhança de Deus. O direito passou ser visto como uma ciência, e como tal deveria ser lógica e exata, passando a construir conceitos abstratos para compor um sistema "ordenado lógico-fechado. Os seus enunciados deveriam fornecer premissas com a exatidão da ciência matemática" (BIONI, 2020, p. 47). Perdurou por muito tempo a ideia de que a proteção à personalidade, como tutela da pessoa humana, não haveria guarida dentro do sistema lógico normativo vigente. As teorias negativistas, que possuem como autores mais lembrados Savigy e Iellinek, afirmavam que "a personalidade, identificando-se com a titularidade de direitos, não poderia, ao mesmo tempo, ser considerada como objeto deles. Tratar-se-ia de contradição lógica" (TEPEDINO, s. d., p. 5). Assim, nesse período, "a pessoa humana perdeu espaço em detrimento das abstrações do positivismo e da excessiva preocupação do direito com aspectos patrimoniais" (BIONI, 2020, p. 48).

[119] A Constituição de Weimar, de 1919, foi "a primeira das chamadas 'longas constituições', ciente de sua posição no vértice normativo e forjada neste espírito" (DONEDA, 2005, p. 76), prevendo em seu texto a dignidade da pessoa humana, mesmo antes da Segunda Guerra Mundial. Contudo, foi após esse período que o conceito proliferou para mais constituições no globo (BIONI, 2020, p. 48).

A dignidade da pessoa humana, nos moldes em que hoje a concebemos, deve-se muito à influência da obra de Immanuel Kant (DONEDA, 2006, p. 72). Para entender a dignidade em Kant, é necessário revisitar a segunda formulação do imperativo categórico, onde se lê: "age de tal maneira que tomes a humanidade, tanto em tua pessoa, quanto na pessoa de qualquer outro, sempre ao mesmo tempo como fim, nunca meramente como meio" (GMS, AA, 04: 429, apud GRANATO, 2014, p. 625). Este imperativo passou a ganhar força dentro da ciência jurídica, clamando pela existência de um direto da personalidade, como "direito da pessoa ser o seu próprio fim, afirmar-se e desenvolver-se como fim de si mesma" (NEUNER, 1866, p. 16 apud DONEDA, 2006, p. 73). Resumidamente, a dignidade humana pode ser entendida como o valor-síntese que reúne as esferas essenciais de desenvolvimento e realização da pessoa humana, sendo incorporada nos ordenamentos jurídicos visando a "proteger a condição humana, em seus mais genuínos aspectos e manifestações, tomando a pessoa 'sempre como um fim e nunca como um meio'" (SCHREIBER, 2013, p. 8).

O aumento da percepção de que o direito deveria proteger também a pessoa humana e sua dignidade, potencializado pela Declaração de Direitos Universais das Nações Unidas, passou a ingressar na ordem constitucional de inúmeros países. E esse fenômeno atinge o direito privado, fenômeno que ficou conhecido como despatrimonialização do direito civil (BIONI, 2020, p. 49). Neste novo contexto, o Código Civil não poderia mais se apresentar como um documento voltado apenas para questões patrimoniais, dentro de uma formulação rigorosa em: "direito objectivo, direito subjectivo e a sua divisão, negócio jurídico, a declaração de vontade, o contrato bilateral, o dever de prestação, a impossibilidade de prestação, etc." (WIACKER, 2004, apud BIONI, 2020, p. 47). Por consequência, o direito civil teve suas bases modificadas, não mais tratando apenas de aspectos patrimoniais da vida em sociedade, para tutelar, também, a pessoa humana em um sentido mais amplo. Sob essa nova dogmática, insurge o direito da personalidade, possuindo uma forte vocação para ser um centro de irradiação desse novo modo de entender o direito (DONEDA, 2006, p. 79).

No Brasil, segundo Bioni (2020, p. 50), a ruptura com a lógica patrimonialista deu-se com a codificação civilista[120] encabeçada por Orlando Gomes. O Código Civil anterior, de

120 Apenas para contextualizar, sabe-se que o direito privado é o ramo do direito "tendente a reger as relações humanas. Enfim, é o direito comum a todas as pessoas, disciplinando o seu modo de ser e de agir. É, pois, o direito da vida do homem. Desde atos simples e banais, como dar esmola, até situações jurídicas mais complexas, como o casamento ou a compra e venda de um imóvel, o Direito Civil está presente" (CHAVES; ROSENVALD, 2015, p. 21).

1916, “inspirado no liberalismo econômico, tinha preocupação obsessiva pela proteção patrimonial”, em que a pessoa era deixada para segundo plano. Com os novos paradigmas de valorização do homem, o direito civil precisava sistematizar as relações privadas protegendo a pessoa humana (CHAVES; ROSENVALD, 2015, p. 21). Assim, o novo Código Civil brasileiro foi pensado com o intuito de humanizar as relações privadas e para isso seria imprescindível “dispensar maior proteção à pessoa”. Foi com esse propósito que Gomes em “seu projeto de Código Civil enumerou os direitos da personalidade, por exemplo, o direito ao nome, à imagem, à liberdade, à honra, à integridade física e, por fim, os direitos autorais” (BIONI, 2020, p. 50). Contudo, apesar da apresentação do anteprojeto de código civil, pelo professor Orlando Gomes, em 1963[121], apenas em 2002 o novo Código Civil foi aprovado, sendo nítida a influência do professor baiano. A necessidade de um novo texto civil adveio com a promulgação da Constituição de 1988, que passou a evidenciar “valores fundamentais aclamados como garantias e direitos fundamentais do cidadão”. O direito civil não poderia mais relaxar a proteção de valores axiológicos da Constituição fundada “na dignidade humana (art. 1º, III), solidariedade social (art. 3º, III) e na igualdade substancial (arts. 3º e 5º)” (CHAVES; ROSENVALD, 2015, p. 38).

A dignidade da pessoa humana é “verdadeira valor-fonte que conforma e inspira todo o ordenamento constitucional vigente” (GRANATO, 2014, p. 624). Esse ponto de atenção que abre a Constituição Federal irradia para todas as legislações infraconstitucionais, e isso inclui todo o direito civil. A essa visão constitucional é possível apresentar a personalidade como um dos princípios basilares do direito civil, em que o ser humano é colocado como figura central no direito civil contemporâneo. Os direitos da personalidade devém uma cláusula geral de proteção de tutela e proteção da pessoa humana “ou de um sistema geral de tutela à pessoa” (BIONI, 2020, p. 51). São direitos que visam a proteger a pessoa, considerada em suas diversas concepções (físico, psíquico, intelectual...), estão a serviço da pessoa humana “tomada em si mesma e em suas necessárias projeções sociais”, e são direitos essenciais ao desenvolvimento da pessoa humana, que derivam da máxima do dever de preservar a dignidade da pessoa humana (CHAVES; ROSENVALD, 2015, p. 139). Não

121 Apesar das bem-vindas e necessárias alterações trazidas pelo professor Orlando Gomes, é necessário relembrar que o projeto de Código Civil foi redigido no auge da ditadura militar, o que acaba levando ao seu texto valores desse período histórico. Assim, a leitura do Código deve ser realizada sempre com olhares críticos e que tragam a norma para os dias atuais, em que o direito civil sirva de instrumento para concretizar valores fundamentais, que a norma seja interpretada com o intuito de “defender e proteger a vida humana em sua integralidade, contemporâneo com a sociedade que lhe incumbe pacificar” (CHAVES; ROSENVALD, 2015, p. 41).

sendo direitos presentes em um rol estanque, mas mutáveis, de acordo com as mudanças e novas necessidades humanas, de modo a sempre garantir os instrumentos necessários para que

> todo ser racional exista como um fim em si mesmo, não meramente como um meio para o uso discricionário dessa ou daquela vontade, mas sim tem de ser considerado em todas as suas ações, tanto as dirigidas a si mesmo quanto a outros seres racionais, sempre [e] ao mesmo tempo como fim (GMS, AA 04: 427f. 32-11 apud GRANATO, 2014, p. 632-633).

Conforme salientado por Bioni (2020, p. 52), os direitos da personalidade devem ser sempre cultivados e percebidos dentro da realidade em que o homem está inserido, ou seja, dentro da Sociedade da Informação. Neste sentido, é relevante a consolidação do Enunciado 274 da Jornada de Direito Civil, que dispõe: "Os direitos da personalidade, regulados de maneira não exaustiva pelo Código Civil, são expressões da cláusula geral da pessoa humana, contida no art. 1º, III, da Constituição (princípio da dignidade humana)". Deste modo, urgem novos valores que necessitam de igual e forte proteção, uma vez que "os direitos da personalidade recaem sobre aspectos indissociáveis de seu titular" (DONEDA, 2006, p. 82). Possuindo, como principais características, as de serem

> [...] personalíssimos (exaurem-se na própria pessoa, embora os herdeiros em alguns casos sejam legitimados por lei para sua defesa); gerais (concedidos a todos); inatos ou originários (adquiridos automaticamente com o nascimento); necessários (indispensáveis ao desenvolvimento da personalidade humana); vitalícios, perenes ou perpétuos (perduram por toda a vida e em alguns casos têm eficácia post mortem, como em questões nas quais se empresta defesa aos familiares, cite-se o caso de lesão à honra do morto); impenhoráveis (não se admite que a penhora ou qualquer outro ato de alienação incida sobre eles); absolutos (oponíveis erga omnes); indisponíveis (estão fora do comércio); irrenunciáveis (não podem ser renunciados); imprescritíveis (o transcurso do tempo e o eventual desinteresse do titular em nada afetam a existência e a possibilidade de gozá-los); inexpropriáveis (não podem ser destacados da pessoa humana); extrapatrimoniais (não são computáveis na aferição da situação econômica de seu titular, apesar de poderem trazer alguma utilidade financeira como, por exemplo, mediante exploração da própria imagem) [...] (VIEIRA, 2007, p. 38).

Nesse sentido, o fim último dos direitos da personalidade é tutelar a dignidade da pessoa humana, e "a dignidade da pessoa exige que lhe seja reconhecido um espaço de privacidade em que possa estar à vontade, ao abrigo da curiosidade dos outros". (VASCONSELOS, 2014, p. 79). Logo, a privacidade deve ser protegida, tanto que o é, sendo reconhecida, conforme visto, como um direito fundamental e de personalidade, estando prevista na Constituição Federal e no Código Civil de 2002 (CANCELIER, 2017, p. 105).

A privacidade deve ser protegida, pois é por meio dela que a pessoa consegue explorar livremente o seu íntimo, sem se preocupar com julgamentos externos, exercendo o seu direito de autodeterminação (VIEIRA, 2007, p. 20). Ao proteger a privacidade tutela-se juntamente a personalidade humana, valor tão caro ao nosso ordenamento, razão pela qual se pode afirmar sem medo que "a privacidade é componente essencial à formação da pessoa, indispensável à construção do indivíduo e de suas fronteiras com os demais" (CANCELIER, 2017, p. 105).

No entanto, apesar do termo "privacidade" não aparecer na legislação supracitada, o legislador brasileiro utilizou os termos *vida privada* e *intimidade* para fazer referência à privacidade, estando os dois termos abarcados dentro do conceito de privacidade. Logo, a privacidade está protegida pela legislação brasileira. A intimidade, na visão de Caio Mário da Silva Pereira (2011, p. 217), possui um caráter dúplice: o direito de estar só, de não se comunicar; e conjuntamente de não ser incomodado por outra pessoa, como também pela autoridade pública, salvo se por alguma necessidade de ordem pública. Para este autor, a intimidade está relacionada com o poder de escolher com quem conviver e se aproximar. Diniz (2012, p. 150) parte da concepção de que privacidade não se confunde com intimidade. No entanto, pode ocorrer de a intimidade estar incluída na privacidade. Ela entende que a intimidade diz respeito a aspectos internos do viver da pessoa, tais como relacionamentos amorosos, situações de pudor ou o segredo pessoal. Lafer (1997, p. 239) compreende o direito à intimidade como um direito a ser deixado só e de ver excluídos do conhecimento de terceiros aspectos de sua vida que dizem respeito a sua esfera privada. Doneda (2006, p. 109) apresenta um conceito de intimidade relacionado com a ideia de eventos mais particulares e pessoais, dentro de uma atmosfera de confiança, aproximando-se do direito de ser deixado em paz. Cancelier (2017, p. 87) conclui que há várias possibilidades de compreensão do objeto do direto à intimidade. Contudo, não vislumbra uma diferenciação relevante entre os termos privacidade e intimidade, pois entende que a intimidade está inserida dentro da privacidade.

Por outro lado, a vida privada, compreendida como outro braço da privacidade, "visa resguardar o direito das pessoas de intromissão indevida em seu lar, em sua família, em sua correspondência, em sua economia" (GONÇALVES, 2012, p. 195). Doneda (2006, p. 109) enxerga na vida privada a distinção entre as coisas da vida pública e da vida privada, no estabelecimento de limites, numa lógica de exclusão. Cancelier (2017, p. 91) expõe varias definições de vida privada, chegando à conclusão de que vida privada relaciona-se à proteção de um contexto – ela seria um dado bruto não trabalhado quando comparada à intimidade. A

vida privada seria o espaço que a pessoa tem para expor a intimidade, entendida aqui como uma expressão do sujeito.

A privacidade, direito de personalidade, está prevista no Código Civil em seu artigo 21, conhecido como cláusula geral da proteção à privacidade, que dispõe que: "A vida privada da pessoa natural é inviolável, e o juiz, a requerimento do interessado, adotará as providências necessárias para impedir ou fazer cessar ato contrário a esta norma". Percebe-se da redação do artigo 21 que a privacidade é reconhecida como um direito autônomo. "Assim, é possível afrontar a privacidade de uma pessoa sem qualquer violação de sua honra ou de sua imagem" (CHAVES; ROSENVALD, 2015, p. 217)[122].

O artigo 21 do Código Civil, além de dar à privacidade o *status* de direto autônomo, confere a ela uma proteção antes de ocorrer o dano, ou seja, "para impedir" ato que ponha em risco a vida privada da pessoa humana. Sendo possível ajuizar uma ação protetiva, autorizando ao Poder Judiciário, explicitamente, a impedir um prejuízo ou mesmo a detectar, preventivamente, um dano à intimidade ou à vida privada de alguém, contanto que verificada a verossimilhança de agressão ao direito num futuro imediato (CACHAPUZ, 2006, p. 213-214). Em caso de lesão à privacidade (art. 21 do CC/02), caberá tutela inibitória[123] para prevenir a prática de atos ilícitos, mas se o dano já foi consolidado é possível propor ação civil de indenização.

A razão da previsão de uma tutela inibitória ao direito à privacidade se justifica pois, após a sua violação, não há como reverter, depois de o privado se tornar público não há como realizar o movimento contrário. Dessa forma, devido à "irreversibilidade da violação que os acometem, necessitam de uma tutela que intervenha nos limites das possibilidades humanas, antes da violação do direito ou logo depois, a fim de impedir a sua ocorrência e/ou continuação" (CARDORIN, 2012, p. 8). Mesmo existindo a previsão constitucional em seu artigo 5º, XXXV, de que "a lei não excluirá da apreciação do Poder Judiciário lesão ou ameaça a direito", deixando evidente que a "ameaça" também é causa para clamar tutela jurisdicional em favor de todos os direitos fundamentais, o legislador infraconstitucional

122 Um caso que ilustra bem a categoria de direito autônomo foi julgado pelo Superior Tribunal de Justiça, que reconheceu a violação da privacidade "por conta da afirmação contida em uma biografia de que o saudoso jogador de futebol Garrincha teria um órgão genital avantajado. Apesar da inexistência de afronta à imagem ou à honra, foi reconhecida a violação de sua privacidade e determinada a reparação do dano (STJ, REsp. 521.697/RJ, Rel. Min. César Ásfor Rocha, j. 16.2.2006, DJU 20.3.2006, p. 276)" (CHAVES; ROSENVALD, 2015, p. 217).

123 "A tutela inibitória é essencialmente preventiva, pois é sempre voltada para o futuro, destinando-se a impedir a prática de um ilícito, sua repetição ou continuação" (MARINONI, 2016, p. 289).

fortaleceu a possibilidade em razão da natureza do direito envolvido, em que a tutela ressarcitória não tem o condão de, efetivamente, reparar o dano. Exatamente, porque o direito à privacidade é direito da personalidade, distante da lógica patrimonial, e por tal razão os meios de proteção precisam estar de acordo com a natureza do direito material sob tutela. Em igual sentido, Marinoni (2016, p. 490) afirma que "a instituição de direitos que não podem ser tutelados através da técnica ressarcitória faz surgir, por consequência lógica, o direito a uma tutela que seja capaz de evitar a violação do direito material". Obviamente, nos casos em que a violação já tenha ocorrido, caberá uma ação de indenização referente aos danos morais sofridos pela pessoa que teve a sua privacidade devassada.

Desta forma, não restam dúvidas de que a norma em comento protege a privacidade das situações e que é provável a ocorrência da sua violação, devendo haver prioridade em prevenir a ocorrência de um dano, razão pelo qual o juiz deverá adotar "as providências necessárias para impedir ato contrario à inviolabilidade da privacidade" (CANCELIER, 2017, p. 120). Isto porque, de acordo com Cachapuz (2006, p. 214-215), o Código Civil deu a possibilidade de se entrar com uma "ação protetiva não orientada exclusivamente pela ideia de indenizabilidade, e sim por um conceito de prevenção à própria esfera de privacidade". Ademais, a proteção à privacidade também pode ser percebida em outros dispositivos da legislação brasileira[124].

Percebe-se que o direito de privacidade no ordenamento brasileiro tutela a privacidade em situações específicas, conforme podemos analisar na legislação esparsa. Como também destinou-se um local de destaque a esse direito por meio de cláusulas gerais. O direito à privacidade está presente em nossa Constituição, reconhecida como direito fundamental, uma vez que o valor da privacidade é essencial à concretização da individualidade e da liberdade, tutelando assim a dignidade humana. A privacidade é direito

[124] O próprio Código Civil, em seu artigo 1.513, protege o direito de família como expressão de uma vida privada familiar. Marineli (2017, p. 94-95) destaca alguns dispositivos que tratam do assunto em nosso ordenamento: o Estatuto da Criança e do Adolescente, Lei 8.069 de 1990, estabelece em seu artigo 100, inciso X, respeito pela intimidade, direito à imagem e reserva da vida privada. O Estatuto da Ordem dos Advogados do Brasil estabelece a inviolabilidade do local, dos instrumentos de trabalho e das correspondências (art. 7º, inciso III) e o sigilo profissional (art. 7º, inciso XIX). A Lei 9.296/1996 regulamenta as interceptações telefônicas, assim como a 9.472 de 1997 estabelece a inviolabilidade dos segredos de comunicação (artigo 3º, inciso V) e respeito à privacidade nos documentos de cobrança e na utilização de dados pessoais pelas prestadoras de serviço (art. 3º, inciso IX). Por fim, cabe menção ao Código de Processo Civil de 2015, que desobriga as partes e testemunhas a depor quando devem guardar sigilo (338, inciso II e 448, inciso II), assim como também desobriga as partes e terceiros a exibir em juízo coisa ou documento concernente à intimidade da família ou protegida por segredo (art. 404, incisos I e IV).

da personalidade, conforme expresso pelo nosso Código Civil, em que se afirma que a privacidade da pessoa é inviolável, e se ocorrer dano a esse direito é assegurado indenização. Apesar dessa garantia, precisamos ter em mente que o dano à privacidade é irreversível. Esta informação jamais voltará a ser privada, ainda mais em um mundo altamente informatizado em que as informações são repassadas em uma velocidade extremamente alta. De modo que os esforços devem ser maiores no sentido de evitar a ocorrência de um dano à privacidade.

4.2 PROTEÇÃO DE DADOS

A primeira fase da conceituação jurídica de dados pessoais está muito relacionada com o surgimento dos bancos de dados, pois as legislações buscavam proteger as pessoas da atuação existente com base nesses bancos de dados potencializada com novos aparatos tecnológicos. Neste contexto, entendia-se por bancos de dados, segundo Doneda (2006, p. 158), "um conjunto de informações organizadas segundo uma determinada lógica", que poderia ser governado com ou sem o artifício da informática. Obviamente, um banco de dados informatizado possui uma eficácia de tratamento dos dados muito superior que um banco de dados tratado de modo manual, pois pode armazenar um volume extremamente vasto de informações, bem como pode processá-las, agregá-las e combiná-las de incontáveis formas em um espaço de tempo muito reduzido quando comparado com idêntica operação realizada manualmente.

Logo, tendo em vista as novas potencialidades e os riscos que a operação de tratamento automatizada de dados poderia causar, parte da doutrina jurídica voltou-se primeiramente para eles, criando normas e regulamentos exclusivos para bancos de dados. Porém, posteriormente, o conceito de bancos de dados perdeu a centralidade com o aprimoramento das tecnologias e "lançaram luz sobre a necessidade de compreender diretamente os dados pessoais na regulação da matéria, em situações nas quais estes não estão vinculados a um banco de dados" (DONEDA, 2006, p. 158).

A segunda fase das leis de proteção de dados pessoais começou a surgir no final dos anos 1970, tendo como marco a lei francesa de proteção de dados pessoais de 1978. Essa fase tem como característica diferenciadora o modo como as leis eram estruturadas. A proteção partia de uma liberdade negativa do cidadão em decidir pela possibilidade ou não de utilização de seus dados pessoais. Neste sentido, "criou-se um sistema que fornece

instrumentos para o cidadão identificar o uso indevido de suas informações pessoais e propor a sua tutela". No entanto, tal liberdade da pessoa escolher sobre a utilização ou não de seus dados pessoais acarretou problemas, pois, frequentemente, implicava na segregação da pessoa em algum aspecto da vida social, ou outra espécie de prejuízo, sendo uma liberdade "que de fato poderia ser usufruída somente por eremitas" (DONEDA, 2006, p. 210).

Posteriormente, a terceira fase de leis de proteção de dados pessoais teve consciência de que o exercício puramente individual dessa liberdade de escolher na utilização dos dados pessoais ou não poderia causar outros prejuízos às pessoas. Passaram a abranger em seus textos garantias para efetivamente assegurar essa liberdade de escolha, ou seja, o pleno exercício da autodeterminação informativa. Estas leis buscaram "levar em consideração o contexto no qual [são] solicitado[s]" os dados pessoais, considerando também a existência de bancos de dados interligados. O marco destas leis de terceira geração é a decisão do Tribunal Constitucional Alemão, no julgamento da Lei do Recenseamento de População, Profissão, Moradia e Trabalho, de 25 de março de 1982, que, em apertada síntese, deliberou que a pessoa tem o direito ao controle sobre o fluxo de suas informações privadas. Tendo em vista que as práticas de processamento de dados pessoais caracterizam uma preocupante "ameaça à personalidade do indivíduo, na medida em que possibilita o armazenamento ilimitado de dados, bem como permite a sua combinação de modo a formar um retrato completo da pessoa sem a sua participação ou conhecimento" (MENDES, 2008, p. 31-32).

Posteriormente, surgiram as leis de quarta geração, que podem ser consideradas as leis hoje vigentes. Essas leis buscam preencher a lacuna da proteção de dados focada no indivíduo. Conforme explicado por Doneda (2006, p. 211), as prerrogativas de autodeterminação informativa apenas eram efetivamente usufruídas por uma minoria privilegiada. Por tal razão, as leis de proteção de dados de quarta geração buscam dar instrumentos para um "padrão coletivo de proteção". Dentre essas leis, existe o reconhecimento de desequilíbrio entre as pessoas e as entidades que coletam e processam dados pessoais, não sendo possível resolver apenas com o instituto da autodeterminação informativa. Na verdade, pode-se dizer que há uma redução na função da autodeterminação informativa por existir "dados pessoais que necessitam de uma proteção no seu mais alto grau, que não pode ser obtida exclusivamente de uma decisão individual". Por fim, outra característica é a existência de autoridades independentes para fiscalização e aplicação da lei

de proteção de dados pessoais[125], havendo normas diferenciadas para cada setor (saúde, financeiro, créditos de consumo, dentre outros), visando a "uma maior eficácia dos princípios presentes nas leis de proteção de dados em situações que apresentam suas próprias particularidades" (DONEDA, 2006, p. 212-213).

A lei de proteção de dados brasileira, conhecida como Lei Geral de Proteção de Dados (LGPD), encontra-se dentro da quarta geração de leis de proteção de dados. Apesar da aprovação tardia, o Brasil se insere dentro dos países que detêm uma normativa de proteção de dados, mas para chegar nesse *status* muito chão precisou ser percorrido. Apesar da lei de proteção de dados ser aprovada apenas no ano de 2018, não é correto afirmar que o Brasil estava numa situação de completa desproteção em relação aos dados pessoais. Existiam leis esparsas de caráter público e privado que asseguravam algum grau de proteção aos dados pessoais (OLIVEIRA; LOPES, 2020, p. 80).

Neste sentido, Cots e Oliveira (2019, p. 27-42) destacam algumas legislações que ilustram que havia um sistema esparso de proteção de dados pessoais. Assim, a Constituição Federal de 1988 que previu o instituto do *habeas data* em seu artigo 5º, LXXII[126], como uma ferramenta para retificação dos dados. O Código de Defesa do Consumidor (Lei n. 8.078/1990) em seu artigo 43[127] disciplina a criação de banco de dados dos consumidores, bem como prevê o direito do consumidor ao acesso aos dados que lhe digam respeito. Dentro

125 "A institucionalização da proteção de dados na figura de uma autoridade ou de um conselho foi o caminho trilhado pela maioria dos países, além de ser medida fundamental para o funcionamento de muitos mecanismos de proteção estabelecidos na própria lei" (OLIVEIRA; LOPES, 2020, p. 80).

126 "LXXII - conceder-se-á 'habeas-data': a) para assegurar o conhecimento de informações relativas à pessoa do impetrante, constantes de registros ou bancos de dados de entidades governamentais ou de caráter público; b) para a retificação de dados, quando não se prefira fazê-lo por processo sigiloso, judicial ou administrativo; [...]".

127 Art. 43. O consumidor, sem prejuízo do disposto no art. 86, terá acesso às informações existentes em cadastros, fichas, registros e dados pessoais e de consumo arquivados sobre ele, bem como sobre as suas respectivas fontes. § 1º Os cadastros e dados de consumidores devem ser objetivos, claros, verdadeiros e em linguagem de fácil compreensão, não podendo conter informações negativas referentes a período superior a cinco anos. § 2º A abertura de cadastro, ficha, registro e dados pessoais e de consumo deverá ser comunicada por escrito ao consumidor, quando não solicitada por ele. § 3º O consumidor, sempre que encontrar inexatidão nos seus dados e cadastros, poderá exigir sua imediata correção, devendo o arquivista, no prazo de cinco dias úteis, comunicar a alteração aos eventuais destinatários das informações incorretas. § 4º Os bancos de dados e cadastros relativos a consumidores, os serviços de proteção ao crédito e congêneres são considerados entidades de caráter público.§ 5º Consumada a prescrição relativa à cobrança de débitos do consumidor, não serão fornecidas, pelos respectivos Sistemas de Proteção ao Crédito, quaisquer informações que possam impedir ou dificultar novo acesso ao crédito junto aos fornecedores. § 6º Todas as informações de que trata o caput deste artigo devem ser disponibilizadas em formatos acessíveis, inclusive para a pessoa com deficiência, mediante solicitação do consumidor.

da esfera de proteção do consumidor, destaca-se a Portaria nº 5/2012 da SDE/MJ[128], que considera abusivas as cláusulas contratuais que autorizam o envio de dados pessoais sem o consentimento prévio do consumidor. O Decreto 6.523/2008 regulamentou o SAC, estabelecendo como sigilosos os dados das pessoas que utilizam esse expediente. Em 2011, a Lei 12.414 disciplinou o cadastro positivo, que trata da regulamentação da formação e consulta em bancos de dados com informações para criação de histórico de crédito, e também reconheceu direito aos titulares dos dados em que o uso dos dados pessoais deve estar atrelado a determinada finalidade. Recentemente, o Decreto 7.962/2013 regulamentou o comércio eletrônico, determinando que o fornecedor deverá utilizar mecanismos que garantam a segurança para os pagamentos e para os tratamentos de dados pessoais do consumidor.

Os autores também trazem como exemplo de legislações anteriores a Lei Geral de Telecomunicações, que prevê em seu artigo 3º, IX[129], que os usuários possuem direito ao resguardo de sua privacidade e proteção aos seus dados pessoais. A Lei do *Habeas Data*, que regulamentou o instituto, previsto na Constituição, para retificação dos dados[130]. A Lei Complementar 105/2001, que trata do sigilo das operações de instituições financeiras, sendo que as instituições deverão conservar o sigilo em suas operações ativas e passivas e serviços prestados. No âmbito da administração, o Decreto 6.135/2007, que dispõe sobre o Cadastro Único para Programas Sociais do Governo Federal, prevê a possibilidade de utilização dos dados pessoais, bem como prevê responsabilidades pelo uso dos dados[131]. O Decreto

---

128 Art. 1º Considerar abusiva, nos contratos de fornecimento de produtos e serviços, a cláusula que: I - autorize o envio do nome do consumidor, e/ou seus garantes, a bancos de dados e cadastros de consumidores, sem comprovada notificação prévia; II - imponha ao consumidor, nos contratos de adesão, a obrigação de manifestar-se contra a transferência, onerosa ou não, para terceiros, dos dados cadastrais confiados ao fornecedor; III - autorize o fornecedor a investigar a vida privada do consumidor;

129 Art. 3º O usuário de serviços de telecomunicações tem direito: IX - ao respeito de sua privacidade nos documentos de cobrança e na utilização de seus dados pessoais pela prestadora do serviço;

130 Art. 7º Conceder-se-á *habeas data*: I - para assegurar o conhecimento de informações relativas à pessoa do impetrante, constantes de registro ou banco de dados de entidades governamentais ou de caráter público; II - para a retificação de dados, quando não se prefira fazê-lo por processo sigiloso, judicial ou administrativo; III - para a anotação nos assentamentos do interessado, de contestação ou explicação sobre dado verdadeiro mas justificável e que esteja sob pendência judicial ou amigável.

131 Art. 8º Os dados de identificação das famílias do CadÚnico são sigilosos e somente poderão ser utilizados para as seguintes finalidades: I - formulação e gestão de políticas públicas; e II - realização de estudos e pesquisas. § 1º São vedadas a cessão e a utilização dos dados do CadÚnico com o objetivo de contatar as famílias para qualquer outro fim que não aqueles indicados neste artigo. § 2º A União, os Estados, os Municípios e o Distrito Federal poderão utilizar suas respectivas bases para formulação e gestão de políticas públicas no âmbito de sua jurisdição. § 3º O Ministério do Desenvolvimento Social e Combate à Fome poderá ceder a base de dados nacional do CadÚnico para sua utilização, por órgãos do Poder Executivo Federal, em políticas públicas que não tenham o CadÚnico como instrumento de seleção de beneficiários.§ 4º Os dados a que se refere este artigo somente poderão ser cedidos a terceiros, para as finalidades mencionadas no **caput**, pelos órgãos gestores do CadÚnico no âmbito da União, do Distrito Federal e dos Municípios.§ 5º A utilização

6.425/2008, que assegura sigilo e proteção dos dados pessoais apurados no censo de educação, vedando a utilização desses dados para outros fins que não os previstos na legislação educacional. Outro importante instrumento normativo foi a Lei de Acesso à Informação, Lei 12.527/2011, que disciplina que o tratamento de dados pessoais deve ser realizado de forma transparente e com respeito à privacidade, regulamentando como deve ser realizado o tratamento dos dados pessoais dentro do seu escopo de aplicação[132]. Ademais, esta norma define dados pessoais, bem como informação, e diferencia informações comuns de informações pessoais[133].

Havia regulamentação para dados de saúde, presente na Resolução CFM 1.821/2007[134], que disciplina o prontuário eletrônico e a proteção de dados médicos. Na esfera

---

dos dados a que se refere o **caput** será pautada pelo respeito à dignidade do cidadão e à sua privacidade.§ 6º A utilização indevida dos dados disponibilizados acarretará a aplicação de sanção civil e penal na forma da lei.

132 Art. 4º Para os efeitos desta Lei, considera-se: I - informação: dados, processados ou não, que podem ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato; II - documento: unidade de registro de informações, qualquer que seja o suporte ou formato; III - informação sigilosa: aquela submetida temporariamente à restrição de acesso público em razão de sua imprescindibilidade para a segurança da sociedade e do Estado; IV - informação pessoal: aquela relacionada à pessoa natural identificada ou identificável; V - tratamento da informação: conjunto de ações referentes à produção, recepção, classificação, utilização, acesso, reprodução, transporte, transmissão, distribuição, arquivamento, armazenamento, eliminação, avaliação, destinação ou controle da informação; VI - disponibilidade: qualidade da informação que pode ser conhecida e utilizada por indivíduos, equipamentos ou sistemas autorizados; VII - autenticidade: qualidade da informação que tenha sido produzida, expedida, recebida ou modificada por determinado indivíduo, equipamento ou sistema; VIII - integridade: qualidade da informação não modificada, inclusive quanto à origem, trânsito e destino; IX - primariedade: qualidade da informação coletada na fonte, com o máximo de detalhamento possível, sem modificações.

133 Art. 31. O tratamento das informações pessoais deve ser feito de forma transparente e com respeito à intimidade, vida privada, honra e imagem das pessoas, bem como às liberdades e garantias individuais. § 1º As informações pessoais, a que se refere este artigo, relativas à intimidade, vida privada, honra e imagem: I - terão seu acesso restrito, independentemente de classificação de sigilo e pelo prazo máximo de 100 (cem) anos a contar da sua data de produção, a agentes públicos legalmente autorizados e à pessoa a que elas se referirem; e II - poderão ter autorizada sua divulgação ou acesso por terceiros diante de previsão legal ou consentimento expresso da pessoa a que elas se referirem. § 2º Aquele que obtiver acesso às informações de que trata este artigo será responsabilizado por seu uso indevido. § 3º O consentimento referido no inciso II do § 1º não será exigido quando as informações forem necessárias: I - à prevenção e diagnóstico médico, quando a pessoa estiver física ou legalmente incapaz, e para utilização única e exclusivamente para o tratamento médico; II - à realização de estatísticas e pesquisas científicas de evidente interesse público ou geral, previstos em lei, sendo vedada a identificação da pessoa a que as informações se referirem; III - ao cumprimento de ordem judicial; IV - à defesa de direitos humanos; ou V - à proteção do interesse público e geral preponderante.§ 4º A restrição de acesso à informação relativa à vida privada, honra e imagem de pessoa não poderá ser invocada com o intuito de prejudicar processo de apuração de irregularidades em que o titular das informações estiver envolvido, bem como em ações voltadas para a recuperação de fatos históricos de maior relevância.

134 Art. 2º Autorizar a digitalização dos prontuários dos pacientes, desde que o modo de armazenamento dos documentos digitalizados obedeça a norma específica de digitalização contida nos parágrafos abaixo e, após análise obrigatória da Comissão de Revisão de Prontuários, as normas da Comissão Permanente de Avaliação de Documentos da unidade médico-hospitalar geradora do arquivo. § 1º Os métodos de digitalização devem reproduzir todas as informações dos documentos originais. § 2º Os arquivos digitais oriundos da digitalização dos documentos do prontuário dos pacientes deverão ser controlados por sistema especializado (Gerenciamento eletrônico de documentos - GED), que possua, minimamente, as seguintes características: a) Capacidade de

penal, a Lei 9.983/2000[135], que trata do crime de inserção de dados falsos em sistemas de informação da administração pública, bem como a Lei 12.737/2012, que disciplina o crime de invasão de dispositivos informáticos[136].

Por fim, importante diploma aprovado antes da Lei Geral de Proteção de Dados foi o Marco Civil da Internet (Lei 12.965) e o Decreto 8.771/2016, que o regulamenta. Segundo Leonardi (2020, p. 218), o Marco Civil da Internet veio normatizar a economia digital e as atividades realizadas no ambiente virtual, estabelecendo regras e princípios. Dentre os dispositivos dessa lei, muitos foram voltados para a proteção da privacidade e a proteção de dados pessoais dos usuários da internet, destacando-se o art. 7º, que prevê que a intimidade e a vida privada são invioláveis, bem como o sigilo do fluxo de suas comunicações pela internet, e o sigilo de suas comunicações privadas armazenadas, salvo por ordem judicial. Vedação do fornecimento a terceiros de seus dados pessoais, inclusive registros de conexão, e de acesso a aplicações de internet, salvo mediante consentimento livre, expresso e informado ou nas hipóteses previstas em lei. O usuário da internet tem direito a informações claras e completas sobre coleta, uso, armazenamento, tratamento e proteção de seus dados pessoais, que somente poderão ser utilizados para finalidades que tenham a sua coleta justificada, não sejam vedadas pela legislação e estejam especificadas nos contratos de prestação de serviços ou em termos de uso de aplicações de internet.

---

utilizar base de dados adequada para o armazenamento dos arquivos digitalizados; b) Método de indexação que permita criar um arquivamento organizado, possibilitando a pesquisa de maneira simples e eficiente; c) Obediência aos requisitos do "Nível de garantia de segurança 2 (NGS2)", estabelecidos no Manual de Certificação para Sistemas de Registro Eletrônico em Saúde;

135 "Art. 313-A. Inserir ou facilitar, o funcionário autorizado, a inserção de dados falsos, alterar ou excluir indevidamente dados corretos nos sistemas informatizados ou bancos de dados da Administração Pública com o fim de obter vantagem indevida para si ou para outrem ou para causar dano: Pena – reclusão, de 2 (dois) a 12 (doze) anos, e multa."

136 "Art. 154-A. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita: Pena - detenção, de 3 (três) meses a 1 (um) ano, e multa. § 1º Na mesma pena incorre quem produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no caput . § 2º Aumenta-se a pena de um sexto a um terço se da invasão resulta prejuízo econômico. § 3º Se da invasão resultar a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas, assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido: Pena - reclusão, de 6 (seis) meses a 2 (dois) anos, e multa, se a conduta não constitui crime mais grave. § 4º Na hipótese do § 3º, aumenta-se a pena de um a dois terços se houver divulgação, comercialização ou transmissão a terceiro, a qualquer título, dos dados ou informações obtidos. § 5º Aumenta-se a pena de um terço à metade se o crime for praticado contra: I - Presidente da República, governadores e prefeitos; II - Presidente do Supremo Tribunal Federal; III - Presidente da Câmara dos Deputados, do Senado Federal, de Assembleia Legislativa de Estado, da Câmara Legislativa do Distrito Federal ou de Câmara Municipal; ou IV - dirigente máximo da administração direta e indireta federal, estadual, municipal ou do Distrito Federal."

Por fim, em relação à proteção de dados pessoais, dispõe o usuário da internet de direito à exclusão definitiva dos dados pessoais que tiver fornecido a determinada aplicação de internet, a seu requerimento, ao término da relação entre as partes, quando não houver outras ressalvas na lei. Apesar das grandes contribuições que o Marco Civil trouxe sobre a matéria de proteção de dados, o seu alcance apenas abarcava os dados que estavam no mundo virtual, existindo a necessidade de uma legislação geral de proteção de dados pessoais no Brasil, uma das razões pelas quais existia um movimento pela aprovação de uma lei com essa característica.

Neste sentido, o tema da proteção de dados não é uma novidade. Existiram vários projetos de leis envolvendo a matéria. Inclusive, no ano de 2010, foi realizada uma audiência pública sobre anteprojeto de lei de dados pessoais, promovida pelo Ministério da Justiça. Nesse período já existia a preocupação de proteger as informações pessoais e o entendimento de que os dados pessoais configuram a pessoa humana. De acordo com publicação do Idec (2010, s. p.), existia uma preocupação com a formação de perfil e o cruzamento de dados, bem como o entendimento de que existiriam dados sensíveis, passíveis de gerar discriminação, que deveriam possuir um resguardo maior da legislação. No ano seguinte, foi apresentado o primeiro projeto de lei, PL nº 4060, sobre proteção de dados pessoais, porém a matéria ainda não estava madura o suficiente (IDEC, 2021).

Em 2013, o mundo é assolado com o escândalo de programa de espionagem dos Estados Unidos delatado por Edward Snowden[137], fato que impulsionou o mundo a rever suas políticas e legislações de proteção de dados. No Brasil, o escândalo influenciou o debate sobre cibersegurança e impulsionou a aprovação do Marco Civil da Internet, de modo célere e um pouco atropelado, deixando algumas discussões para o futuro. Nesse sentido, apesar de a legislação referente ao Marco Civil da Internet ter incluído regras sobre proteção de dados pessoais e privacidade (IDEC, 2021), ainda existiam algumas lacunas. Isso pode ser

137 Em junho de 2013, segundo Bruno (2013, p. 10), foi revelado ao mundo pelo ex-assistente técnico da CIA Edward Snowden um gigantesco aparato de vigilância e espionagem de dados digitais. Os documentos vazados demonstraram a existência de um programa de espionagem denominado Prism, que permitia que a NSA tivesse acesso direito a servidores de grandes empresas da Internet, permitindo a coleta de diversos tipos de materiais como transferência de arquivos, conteúdo de e-mails, chats, histórico de internet, conseguindo assim monitorar usuários da internet em escala global, permitindo rastrear a comunicação de qualquer pessoa sem nenhuma forma de controle prévio. Com base nos documentos apresentados por Snowden foi possível constatar que o 2,3 bilhões de telefonemas e mensagens de e-mail foram espionados. Além de cidadãos comuns, o programa americano espionou a alta cúpula de governos, entre eles do Brasil e da Alemanha (CANCELIER, 2017, p. 47-50).

percebido, por exemplo, na previsão do art. 3º da lei que disciplina o uso da internet no Brasil. Um dos princípios que devem ser observados é a proteção de dados, na forma da lei. Contudo, na época em que o texto foi aprovado, não existia uma legislação específica para a proteção de dados pessoais.

Em 18 de março de 2018, outro escândalo assombra o mundo e coloca em xeque o próprio jogo democrático. Revelações de violações de dados envolvendo a empresa de marketing Cambridge Analytica demonstraram que foram utilizadas mais de 50 milhões de informações de pessoas, sem consentimento, para realizar propaganda política segmentada (BBC, 2018). Tal fato aumenta a preocupação dos países com a proteção de dados pessoais. "O caso foi emblemático para alertar sobre riscos de manipulação e violações aos direitos digitais e impulsionar a aprovação" de uma lei geral de proteção de dados nacional (IDEC, 2021, s. p.). Importante mencionar que nesse mesmo ano, no dia 13 de abril de 2018, o governo brasileiro torna público o seu desejo de ingressar na Organização para Cooperação e Desenvolvimento Socioeconômico (OCDE), que possui como uma de suas exigências de boas práticas que seus membros possuam "regulamentação de uso de dados pessoais, assim como um órgão supervisor independente e autônomo" (DATAPRIVACY, 2021, s. p.).

Outro elemento importante para a aprovação da Lei Geral de Proteção de Dados no Brasil foi a entrada em vigor do Regulamento Geral de Proteção de Dados (GDPR – *General Data Protection Regulation*) da União Europeia. A regulamentação europeia forçou multinacionais a se adequarem a uma nova legislação de proteção de dados, e no Brasil urgia a necessidade de uma lei para trazer uma maior segurança jurídica, fato que fez com que grande parte do setor empresarial entendesse que era melhor a criação de uma lei nacional mais próxima do modelo europeu (DATAPRIVACY, 2021).

Por fim, para fechar a "conjunção astral" – nas palavras de Doneda – que possibilitou a aprovação de uma lei geral de proteção de dados no Brasil, havia o desejo do governo brasileiro em aprovar a nova Lei do Cadastro Positivo (DATAPRIVACY, 2021, s. p.). No entanto, como não existia uma lei de proteção de dados, a sociedade civil tinha forte oposição à aprovação de um projeto de lei que ampliava a análise de dados financeiros de consumidores brasileiros sem nenhum tipo de resguardo legislativo (IDEC, 2021).

Essas razões levaram o presidente da Câmara à época, Rodrigo Maia, a pressionar pela aprovação da Lei Geral de Proteção de Dados. Neste sentido, o deputado Orlando Gomes, entendendo a necessidade de tal legislação, convocou uma reunião com todos os setores envolvidos no debate, e posteriormente foi criada uma comissão para a discussão da

lei. Interessante foi a metodologia utilizada na confecção do projeto da Lei Geral de Proteção de Dados. Foram realizadas reuniões com os diferentes atores envolvidos no debate (sociedade civil, academia, setor empresarial, privado, financeiro, dentre outros) para discutir artigo por artigo, cada ponto do projeto, um por um. A ideia era tentar conseguir um consenso sobre o texto final com todos os interessados. Foram realizadas quatro reuniões lideradas pelo deputado Orlando Gomes, em que a máxima geral foi no sentido de que "se ninguém ficou 100% satisfeito, então trata-se da melhor versão possível", exatamente porque a negociação foi feita de forma aberta em que todos os lados tiveram a oportunidade de discutir o texto (DATAPRIVACY, 2021).

Em 29 de maio de 2018, o PL 4.060, que tratava da matéria de proteção de dados, foi aprovado por unanimidade no plenário da Câmara dos Deputados (IDEC, 2021). "Na discussão do Senado, diversos setores da iniciativa privada que não haviam participado da discussão até então tentam – sem sucesso – modificar o teor da Lei", dentre os quais o setor da saúde suplementar (DATAPRIVACY, 2021, s. p.). Em 14 de agosto de 2018, o presidente Michel Temer sanciona a Lei n. 13.709, a Lei Geral de Proteção de Dados (LGPD), porém com vetos importantes: a criação da Autoridade Nacional de Proteção de Dados, algumas regras sobre o tratamento de dados pelo Poder Público e algumas sanções mais rígidas, como a suspensão de atividade (IDEC, 2021).

Por conta do veto presidencial em relação à Autoridade Nacional de Proteção de Dados, existia a necessidade da sua criação. Nesse sentido, foi proposta a Medida Provisória 869/2018, porém a Autoridade criada não detinha a autonomia e a independência necessárias, de acordo com os padrões internacionais. Bem como trouxe outras modificações que trabalharemos melhor no item 4.3. O deputado Orlando Gomes foi designado relator da MP 869/2018, no entanto o desenho político havia se alterado – após as eleições de 2018 houve uma renovação recorde de parlamentares, "o equilíbrio de forças pendeu para o setor privado e a aliança entre as partes interessadas vista durante a discussão da LGPD não se repetiu". A MP 869/2018 foi convertida na Lei 13.853/2019, que alterou alguns dispositivos da Lei n. 13.709/2018, no dia 8 de julho de 2019 (DATAPRIVACY, 2021, s. p.).

A Lei Geral de Proteção de Dados buscou "sistematizar a problemática relacionada ao tratamento de dados pessoais e proporcionar um eixo em torno do qual a disciplina passa a se estruturar". Contudo, essa tarefa não se cumpre apenas com "a absorção de elementos anteriores presentes em nosso ordenamento" (DONEDA, 2021, p. 18). O objetivo da

mencionada legislação pode ser vislumbrado já em seu primeiro artigo, que dispõe possuir "o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural", no tocante ao tratamento de dados pessoais, não fazendo restrição em relação aos meios empregados, por pessoa natural ou pessoa jurídica de direito público ou privado.

Neste sentido, começa a legislação invocando valores já bem consolidados na legislação brasileira, porém a lei traz diversos elementos novos ao ordenamento jurídico brasileiro, passa a integrar institutos próprios da proteção de dados pessoais, princípios de proteção de dados pessoais capazes de valer em uma imensidão de atividades, tanto públicas como privadas, bem como trouxe direitos aos titulares de dados, que levam em consideração regras de prestação e demonstração de contas, ou seja, passa-se a dar enfoque ao risco das atividades desenvolvidas (DONEDA, 2021, p. 18).

Conforme já analisado, a LGPD conceituou dado pessoal como "informação relacionada a pessoa natural identificada ou identificável" (art. 5º, I). Percebe-se que o legislador considerou que todo dado pessoal deve ser considerado importante, inclusive dados públicos ou que se tornaram públicos pelos titulares[138].

O conceito amplo leva em consideração a realidade da sociedade hodierna e a capacidade de cruzamento e organização de dados, que pode resultar em informações bem específicas sobre seus titulares, inclusive sensíveis – que, de acordo com a LGPD, são dados pessoais relativos à qualidade "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" (art. 5º, II).

Ademais, o legislador, entendendo a dinamicidade e a rapidez com que as sociedades e as tecnologias se transformam, ao desenhar a LGPD, fê-la baseada em princípios, conceitos abertos, cláusulas gerais, *standards* de comportamento, pois, ao invés de um texto muito denso, se buscou uma redação que pode ser adaptada ao caso concreto, "à situação específica de cada agente de tratamento e dos riscos dos respectivos tratamentos". Assim, pode-se dizer que a LGPD é uma lei fundamentalmente principiológica (FRAZÃO, 2020, p. 115).

---

138 Apesar de um tratamento diferenciado, os dados em questão estão sob a proteção da LGPD, neste sentido: art. 7º, § 3º O tratamento de dados pessoais cujo acesso é público deve considerar a finalidade, a boa-fé e o interesse público que justificaram sua disponibilização.

Tal concepção é imprescindível, uma vez que a proteção de dados pessoais ao fim visa a proteger o titular dos dados pessoais, resguardando a sua dignidade humana. Isto pode ser verificado no art. 2º da LGPD, que, dentre seus fundamentos, traz o respeito à privacidade (art. 2º, I); a autodeterminação informativa (art. 2º, II); a liberdade, de expressão, de expressão, de informação, de comunicação e de opinião (art. 2º, III); a inviolabilidade da intimidade, da honra e da imagem (art. 2º, IV); e os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais. Percebe-se que é possível extrair importantes manifestações da dignidade da pessoa humana (art. 2º, VII).

No art. 6º da mencionada lei está elencado um rol de princípios que devem ser utilizados para o tratamento de dados pessoais, ou seja, devem ser respeitados os princípios da finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação, responsabilização e prestação de contas. Dentro desse arcabouço normativo, retira-se que a interpretação da norma deve se basear na dignidade do titular de dados. A LGPD destaca-se pela proteção jurídica à personalidade humana, concebida como valor em face das ameaças, maleáveis e dinâmicas que cada contexto social lhe opõe. Essas características são possíveis pela escolha de trazer uma base principiológica e termos abertos (KONDER, 2020, p. 442-443). A escolha do legislador foi evitar o ancilosamento prematuro da nova normativa. Outrossim, importante mencionar que tais princípios não estão indicados apenas no art. 6º da lei, mas ao longo dos dispositivos da LGPD (OLIVEIRA; LOPES, 2020, p. 81).

O primeiro princípio elencado no rol do art. 6º diz respeito à exigência de que seja observada a ligação entre o tratamento dos dados pessoais e a finalidade informada. O princípio da finalidade exige que, para a realização do tratamento de dados pessoais, necessita-se ter finalidades legítimas, específicas, explícitas e informadas ao titular dos dados, e é vedado o tratamento posterior dos dados de modo incompatível com essas finalidades. Nesse sentido, o princípio da finalidade tem estreita correlação com os princípios da adequação e da necessidade (OLIVEIRA; LOPES, 2020, p. 73).

Por necessidade, entende-se que os dados pessoais devem ser armazenados e tratados somente durante o lapso temporal necessário para as finalidades para as quais foram coletados, ao passo que passado esse período deve haver medidas efetivas “para destruição dos bancos de dados gerados no período caso não tenham uma finalidade legítima para

manutenção posterior" (FACHINETTI, 2020, p. 500). Neste sentido, o princípio da necessidade (art. 6º, III) prevê "limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com a abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados". Tal princípio, também, pode ser retirado no § 1º do art. 10[139], no art. 16[140] e no art. 18, VI[141], uma vez que neles há previsão de restrição da coleta de dados "ao estritamente necessário para cumprir a finalidade informada, assim como estabelecem a eliminação dos dados mediante requisição do titular ou quando cessado o tratamento, ou seja, quando eles deixam de ser necessários" (OLIVEIRA; LOPES, 2020, p. 74).

A previsão busca evitar uma coleta de dados exagerada, sendo permitido apenas o tratamento dos dados necessários. São dispensados os dados pessoais excessivos ou desnecessários (COTS; OLIVEIRA, 2019, p. 81). Por outro lado, o princípio da adequação (art. 6º, II) busca evitar desvirtuação entre as finalidades informadas e o tratamento efetivamente realizado. "A diferença entre este princípio e o da finalidade está no fato de que, enquanto o último se preocupa na regularidade da finalidade em si, o segundo aborda o procedimento realizado para chegar à finalidade pretendida" (COTS; OLIVEIRA, 2019, p. 80).

O princípio do livre acesso (art. 6º, IV) dispõe sobre a "garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e duração do tratamento, bem como a integralidade dos dados pessoais". Diz respeito ao direito do titular dos dados de solicitar a correção dos seus dados pessoais quando incorretos "ou revisão de decisões subsidiadas em procedimentos exclusivamente automatizados sobre seus dados" (OLIVEIRA; LOPES, 2020, p. 75). O art. 9º da LPGD positivou expressamente o princípio do livre acesso, dispondo que o titular dos dados pessoais possui a prerrogativa "ao acesso facilitado às informações sobre o tratamento de seus dados, que deverão ser disponibilizadas de forma clara, adequada e ostensiva acerca

---

139 § 1º Quando o tratamento for baseado no legítimo interesse do controlador, somente os dados pessoais estritamente necessários para a finalidade pretendida poderão ser tratados.

140 Art. 16. Os dados pessoais serão eliminados após o término de seu tratamento, no âmbito e nos limites técnicos das atividades, autorizada a conservação para as seguintes finalidades: I - cumprimento de obrigação legal ou regulatória pelo controlador; II - estudo por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais; III - transferência a terceiro, desde que respeitados os requisitos de tratamento de dados dispostos nesta Lei; ou IV - uso exclusivo do controlador, vedado seu acesso por terceiro, e desde que anonimizados os dados.

141 Art. 18. O titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição: [...] VI - eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no art. 16 desta Lei;

de, entre outras características previstas em regulamentação para o atendimento do princípio do livre acesso".

O princípio seguinte, denominado princípio da qualidade dos dados (art. 6º, V), garante aos titulares que seus dados pessoais serão objetivos, claros, relevantes, exatos e atualizados. De acordo com Oliveira e Lopes (2020, p. 75), a essência desse princípio encontra-se no art. 18, III da LPGD, que dispõe que é um direito do titular dos dados a requisição da correção de dados incompletos, inexatos ou desatualizados. Tal princípio tem relação com o próximo, o princípio da transparência, o qual visa a garantir informações claras, precisas e facilmente acessíveis aos titulares dos dados pessoais sobre quais dados estão sendo tratados e por quem. Assim, além do tratamento de dados ser realizado de modo ético e seguro, deve ser garantido "que os indivíduos tenham ciência do tratamento que poderá ser realizado com seus dados (mesmo que posteriormente sejam anonimizados)", sendo imprescindível esclarecer aos usuários de todo e qualquer uso de seus dados pessoais (FACHINETTI, 2020, p. 500). A transparência, para Frazão (2020, p. 105), inclui a necessidade de explicações dentro dos julgamentos realizados pelos algoritmos, pois deve ser possível fiscalizar se as informações estão sendo utilizadas dento de parâmetros justos de modo a evitar discriminações e outras injustiças.

A não discriminação, prevista como princípio no inciso IX do art. 6º, veda o tratamento de dados para fins ilícitos ou abusivos. Apesar de não ser um princípio novo do ordenamento jurídico brasileiro, a LGPD deu enfoque quando apresenta uma característica diferenciada de dados pessoais, os chamados dados pessoais sensíveis. Conforme já analisado, ela elenca identificadores pessoais que podem levar à discriminação de um indivíduo (OLIVEIRA; LOPES, 2020, p. 79).

Os princípios da prevenção (art. 6º, VII) e da segurança (art. 6º, VIII) dizem respeito à adoção e utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão e/ou prevenir a ocorrência de danos ao titular dos dados em virtude do seu tratamento. E neste sentido, o art. 46 da LGPD prevê que ao tratar dados pessoais devem ser observadas "medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito". De igual modo, o art. 47 da LGPD dispõe que deve-se garantir a segurança das informações,

mesmo após o término do tratamento dos dados. Por fim, o princípio da responsabilização e prestação de contas (art. 6º, X) aduz que o agente que trata os dados pessoais deve demonstrar a adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados. Ademais, o art. 42 da lei responsabiliza o controlador ou o operador que, em virtude da atividade de tratamento de dados, causar dano em violação ou desrespeito à legislação de proteção de dados.

De acordo com o art. 1º da LGPD, a pessoa natural ou jurídica que tratar dados pessoais precisará observar o disposto nesta lei. Logo, para o tratamento lícito de dados pessoais, é necessária a utilização de uma base legal como fundamento da atividade. Logo, apenas não será necessária a identificação de uma base legal nos casos de exclusão, previstos em seu no art. 4º da LGPD[142]. Assim, não sendo uma das hipóteses que comportam a exclusão da legislação de proteção de dados, deve ser utilizada uma das bases de tratamento (art. 7º ou art. 11 da LGPD) para que não haja ocorrência de atividade ilegítima ou ilícita (VIOLA; TEFFÉ, 2021, p. 118).

Segundo o art. 7º, apenas poderá ser realizado o tratamento de dados pessoais nas hipóteses:

> I - mediante o fornecimento de consentimento pelo titular; II - para o cumprimento de obrigação legal ou regulatória pelo controlador; III - pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei; IV - para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais; V - quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados; VI - para o exercício regular de direitos em processo judicial, administrativo ou arbitral, esse último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem); VII - para a proteção da vida ou da

142 Art. 4º Esta Lei não se aplica ao tratamento de dados pessoais: I - realizado por pessoa natural para fins exclusivamente particulares e não econômicos; II - realizado para fins exclusivamente: a) jornalístico e artísticos; ou b) acadêmicos, aplicando-se a esta hipótese os arts. 7º e 11 desta Lei; III - realizado para fins exclusivos de: a) segurança pública; b) defesa nacional; c) segurança do Estado; ou d) atividades de investigação e repressão de infrações penais; ou IV - provenientes de fora do território nacional e que não sejam objeto de comunicação, uso compartilhado de dados com agentes de tratamento brasileiros ou 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. § 1º O tratamento de dados pessoais previsto no inciso III será regido por legislação específica, que deverá prever medidas proporcionais e estritamente necessárias ao atendimento do interesse público, observados o devido processo legal, os princípios gerais de proteção e os direitos do titular previstos nesta Lei.

> incolumidade física do titular ou de terceiro; VIII - para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; X - para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente.

Segundo Cots e Oliveira (2019, p. 82), o tratamento de dados pode se utilizar de uma ou mais de uma base legal. Admite-se que o rol do art. 7º, assim como do art. 11 da LGPD são taxativos, em que algumas hipóteses de tratamento possuem interpretação mais aberta e com certo grau de subjetividade. Por exemplo, a base legal do legítimo interesse (VIOLA; TEFFÉ, 2021, p. 119).

A primeira base legal é a do consentimento do titular dos dados, e deverá ocorrer, como regra, de acordo com o previsto no art. 7º, I. Por consentimento, a LGPD em seu art. 5º, XII, conceitua como sendo "manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada". Nesse sentido, dispõe o art. 8º da LGPD que o consentimento deve ser fornecido por escrito ou por outro meio que demonstre a manifestação de vontade do titular. A base do consentimento tem especial importância, pois a base principiológica está voltada para a proteção da dignidade da pessoa humana, de modo que a pessoa deve poder ter maior controle sobre o fluxo de seus dados pessoais.

O cenário tecnológico hodierno, como demonstrado, está pautado numa economia de dados do novo capitalismo de vigilância, em que a coleta em massa de dados pessoais e sua comercialização fazem parte de negócios muito rentáveis. Por tais razões, o consentimento deve ocorrer de maneira restritiva, sendo vedado ao agente de tratamento expandir a autorização concedida para além daqueles pactuados, por tempo alargado ou para fins diferentes. Tal vedação está prevista no § 4º, art. 8º, que dispõe que "o consentimento deverá referir-se a finalidades determinadas, e as autorizações genéricas para tratamento de dados pessoais serão nulas". O consentimento poderá ser revogado a qualquer momento mediante expressão do titular dos dados, gratuitamente, e de modo fácil, bem como o uso dos dados pessoais para outra finalidade não compatíveis com o consentimento original necessitará de novo consentimento (VIOLA; TEFFÉ; 2021, p. 121). O consentimento pode ser dispensado nos casos em que os dados pessoais tornem-se públicos por manifestação do titular. No entanto, as demais disposições e os princípios da lei de proteção de dados deverão incidir nos dados, mesmo que públicos.

A base legal prevista no art. 7º, II permite o tratamento de dados pessoais sem o consentimento do titular para cumprimento de obrigação legal ou regulatória pelo controlador (art. 7º, II), Cots e Oliveira (2019, p. 83) exemplificam os casos de tratamento de dados pessoais de empregados, dados do consumidor para emissão de nota fiscal ou envio de mercadoria, para pagamento de serviços pessoa física, guarda e registro de acesso à internet, nos termos do Marco Civil da Internet, dente outros.

O inciso III do art. 7º faz referência à base legal de execução de obras públicas, "pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres". Pode-se traçar um paralelo entre essa base legal e o requisito previsto no art. 23 da LGPD, em que o tratamento de dados pessoais realizado pelas pessoas jurídicas de direito público precisa seguir os parâmetros do direito administrativo. Assim, o tratamento de dados deverá observar a finalidade pública, na persecução do interesse público, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público, desde que:

> I) sejam informadas as hipóteses em que, no exercício de suas competências, realizam o tratamento de dados pessoais, fornecendo informações claras e atualizadas sobre a previsão legal, a finalidade, os procedimentos e as práticas utilizadas para a execução dessas atividades, em veículos de fácil acesso, preferencialmente em seus sítios eletrônicos; II) seja indicado um encarregado quando realizarem operações de tratamento de dados pessoais.

A próxima base legal faz referência à realização de estudos por órgão de pesquisa, que, de acordo com a LGPD, é

> órgão ou entidade da administração pública direta ou indireta ou pessoa jurídica de direito privado sem fins lucrativos legalmente constituída sob as leis brasileiras, com sede e foro no País, que inclua em sua missão institucional ou em seu objetivo social ou estatutário a pesquisa básica ou aplicada de caráter histórico, científico, tecnológico ou estatístico.

No entanto, ainda deve-se observar os ditames da LGPD, não sendo possível se utilizar de tal base legal se a pesquisa não necessita da utilização de dados pessoais, ou se dados são coletados sem observar a finalidade ou a necessidade (COTS; OLIVEIRA, 2019, p. 84) Ademais, o legislador teve o cuidado de acrescentar que, nos casos em que seja possível, os dados pessoais devem ser anonimizados. A pesquisa possui padrões éticos e normativas próprias que deverão ser observadas ao longo do estudo, e dentre eles podemos citar

aprovação do Sistema CEP/Conep para todas as pesquisas que envolvem seres humanos (DONEDA et al., 2020, p. 528). Vale destacar que, por força do art. 13 da LGPD, nos estudos em saúde pública existe a previsão que os dados pessoas deverão ser tratados dentro do órgão de pesquisa, respeitar as finalidade especifica de realização de estudo e pesquisa e, sempre que possível, a anonimização ou pseudonimização dos dados.

Outra hipótese legal para tratamento de dados pessoais é a execução de contrato ou procedimentos preliminares à sua formação. O agente de tratamento de dados poderá tratar dados pessoais para a contratação. Nesse caso basta apenas o titular dos dados ser uma das partes da avença ou estar em negociação contratual. Apesar de a hipótese se assemelhar com o consentimento, a diferença consiste no fato de que, caso o titular dos dados deseje revogar o seu consentimento, apenas terá seus dados excluídos após a execução do contrato (VIOLA; TEFFÉ, 2021, p. 135-136).

Em seguida, autoriza-se o tratamento de dados pessoais para o exercício regular de direitos em processo judicial, administrativo ou arbitral. “Há, aqui, base legal ampla que autoriza o uso de dados pessoais em processo para garantir o direito de produção de provas de uma parte contra a outra” (VIOLA; TEFFÉ, 2021, p. 136).

No inciso VII do art. 7º há a possibilidade de tratamento de dados pessoais para a proteção da vida ou da incolumidade física do titular ou de terceiro. A proteção deve ser a um dano concreto, não podendo ser alegado em situações gerais e genéricas. A pandemia da Covid-19 pode ser considerada um exemplo, tendo em vista a necessidade de garantir a proteção à vida, porém, mesmo nas situações excepcionais, conforme já mencionado, os tratamentos de dados devem ser realizados com base nos princípios da lei de proteção de dados, que ao fim visam a garantir a tutela da pessoa na sociedade da informação.

Desdobramento da hipótese anterior, o inciso seguinte prevê a possibilidade de tratamento de dados para a tutela da saúde, desde que em procedimento realizado por profissional da saúde, serviços de saúde ou autoridade sanitária (art. 7º, VIII). O tratamento apenas poderá ocorrer por profissionais de saúde, na visão de Cots e Oliveira (2019, p. 88). Não se inserem nesta hipótese empresas do ramo da saúde. Ademais, os dados devem ser utilizados em razão da profissão, fora do âmbito profissional ou por outro motivo que não de tutela à saúde. Tal base legal não pode ser utilizada por desviar a intenção do legislador.

Essa base legal sofreu alteração pela Lei 13.853/2019, que no item 4.3 vamos trabalhar com mais detalhes. No entanto, por ora é importante registrar que foi acrescentada a expressão “serviços de saúde”, podendo causar certa insegurança jurídica. “Isso porque, anteriormente, o legislador tinha o cuidado em não permitir o tratamento de dados pessoais sob o manto da tutela da saúde a entidades privadas, com ou sem objetivo de lucro” (COTS; OLIVEIRA, 2019, p. 89). Com a alteração, alguns doutrinadores passaram a questionar o alcance da norma, se no caso poderá ser tratado dados de saúde na operalização dos serviços de saúde.. No caso, fica a dúvida se é obrigatório ser realizado por profissional da saúde. O problema aqui é o fato de que esses outros profissionais não estão subordinados a rigorosos códigos de ética, diferentemente dos médicos, enfermeiros, dentistas, psicólogos, dentre outros.

A base do legítimo interesse (art. 7º, IX), uma base legal dotada de certa subjetividade, que, segundo Viola e Teffé (2021, p. 127), “visa possibilitar tratamento de dados importantes, vinculados ao escopo de atividades praticadas pelo controlador, e que encontrem justificativa legítima”. Na aplicação dessa base legal não devem ser esquecidos os princípios de proteção de dados pessoais, quais sejam: finalidade, necessidade e a proporcionalidade da utilização dos dados.

Dentre os exemplos para a utilização do legítimo interesse apresentado pelo *Central for Information Policy Leadership* está a utilização do legítimo interesse para: 1) detecção de fraude e prevenção ao crime, como de lavagem de dinheiro; 2) conformidade com a lei estrangeira; 3) observação a padrões da empresa; 4) informações, sistema, rede e segurança cibernética; 5) processamento de dados de emprego, que não se enquadram dentro do contrato de emprego, mas são necessárias para o operacional, administrativo, RH, fins de recrutamento; 6) operações gerais e *due dilience*, para operações do dia a dia, gestão do negócio e planos de crescimento estratégico; 7) desenvolvimento e aprimoramento de produtos; e para 8) comunicação, marketing e inteligência (CENTRAL OF INFORMATION POLICY LEADERSHIP, 2017, s. p.).

Apesar dos exemplos, como mencionado, sempre se precisará considerar os demais princípios e objetivos da lei de proteção de dados, uma vez que tratamentos invasivos, inesperados ou genéricos não serão considerados lícitos.

A base legal do legítimo interesse não foi disponibilizada para o tratamento de dados sensíveis, porém o rol do art. 11 da LGPD, que trata das bases legais para o tratamento de dados sensíveis, previu “a possibilidade de tratamento para a garantia da prevenção à fraude e

à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, e o exercício regular de direitos em contratos" (VIOLA; TEFFÉ, 2021, p. 129).

Por fim, para a proteção do crédito (art. 7º, X). O Código de Defesa do Consumidor em seu art. 43 já previa a possibilidade de formação de bancos de dados dos consumidores com o fim de proteger o crédito. O objetivo desse tipo de regulação encontra-se em possibilitar uma ampliação na concessão de crédito, mitigar os riscos e impulsionar o mercado de consumo (VIOLA; TEFFÉ, 2021, p. 137).

A Lei Geral de Proteção de Dados inovou com a diferenciação do tratamento de certas categorias de dados pessoais, criando uma separação entre os dados pessoais e os dados pessoais sensíveis. Nesse sentido, considerou-se que "se o tratamento de qualquer dado pessoal tem potencial de atingir o seu titular, alguns dados apresentam potencial de dano qualificado no que tange à pessoa humana". Visto o grau de importância que alguns dados possuem, o legislador acertou em criar bases legais próprias, mais restritivas, a essa nova categoria normativa (KONDER, 2020, p. 442). A proteção mais rígida se justifica, pois, segundo Viola e Teffé (2021, p. 139), estamos diante de dados que concentram o "núcleo duro" da privacidade, em razão da natureza das informações que podem deles derivar.

Comparando os artigos 7º (tratamento de dados pessoais) e 11 (tratamento de dados pessoais sensíveis), retira-se a repetição de diversas regras. Em ambos os dispositivos o legislador elegeu o consentimento como base legal para justificar o tratamento de dados pessoais, mas também especificou outras hipóteses de tratamento. Dentre as bases que são excluídas no caso do tratamento de dados sensíveis, elenca-se: o legítimo interesse do controlador ou de terceiro, bem como para proteção ao crédito (VIOLA; TEFFÉ, 2021, p. 141).

De acordo com o art. 11 da LGPD, estará legitimado o tratamento de dados sensíveis, sem o consentimento do titular, para: a) cumprimento de obrigação legal ou regulatória pelo controlador; b) tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos; c) realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis; d) exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral; e) proteção da vida ou da incolumidade física do titular ou de terceiro; f) tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; ou g) garantia da prevenção à fraude e à

segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no art. 9º desta lei e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais.

Assim, no que pese o art. 11, II, b trazer a hipótese de dispensa de consentimento para tratamento de dados sensíveis voltados à execução de políticas públicas, no tocante aos dados sensíveis somente serão legítimos os tratamentos que tiverem respaldo na lei. Hipótese que difere do art. 7º, III, que prevê a dispensa no consentimento para tratamento de dados pessoais voltados à execução de políticas públicas respaldadas em contratos (KONDER, 2020, p. 453).

Segundo Viola e Teffé (2020, p. 141), no lugar da base legal do legítimo interesse, o art. 11 da LGPD permite a utilização de dados sensíveis para prevenção de fraudes e garantir a segurança do titular, como exemplo a utilização de dados biométricos por instituições bancárias ou empregadores para evitar fraudes.

No tocante à base legal do consentimento, existem algumas diferenças entre as hipóteses de tratamento comuns e as dos dados sensíveis. No artigo 11 parece que o legislador conferiu uma camada de proteção a mais para os dados sensíveis ao prever que o consentimento do titular precisa ser "'de forma específica e destacada, para finalidades específicas', ou seja, impondo restrição formal quanto ao consentimento" (KONDER, 2020, p. 453).

A utilização desses dados para fins econômicos é vedada, exceto quando for necessária para a prestação de serviços de saúde, de assistência farmacêutica ou mesmo de assistência à saúde, para possibilitar a portabilidade requerida pelo titular ou quando suplementar ou para transações financeiras e administrativas resultantes do uso e da prestação dos referidos serviços (KONDER, 2020, p. 454). A vedação de uso de dados sensíveis para fins econômicos sofreu alterações, alargando demasiadamente as exceções, tema de análise do item seguinte.

4.3 O ART. 11 § 4º DA LEI GERAL DE PROTEÇÃO DE DADOS

Neste item vamos focar especificamente no § 4º do artigo 11 da LGPD, para posteriormente analisar se, ao permitir o compartilhamento de dados pessoais sensíveis de saúde, sem o consentimento do titular, com o intuito de obter vantagem econômica, respeita o

viés protetivo da legislação de proteção de dados, bem como a privacidade da pessoa humana – que no fim irá se refletir em sua dignidade.

Antes de adentrar na redação atual do § 4º do artigo 11, é importante trazer a discussão de que esse dispositivo legal sofreu alterações em seu texto pela Medida Provisória nº 869/2018. Quando a Lei Geral de Proteção de Dados (Lei nº 13.709, de 14 de agosto de 2018) foi inicialmente sancionada, a redação do aludido parágrafo era a seguinte:

> § 4º É vedada a comunicação ou o uso compartilhado entre controladores de dados pessoais sensíveis referentes à saúde com o objetivo de obter vantagem econômica, exceto nos casos de portabilidade de dados quando consentido pelo titular.

Assim, como bem pontua Palhares (2021, p. 304), inicialmente, não existia previsão no texto da LGPD da possibilidade de "comunicação ou compartilhamento de dados de saúde para fins de obtenção de vantagem econômica, salvo nos casos em que o titular exercesse seu direito de portabilidade". O texto original da LGPD não previa em seu texto uma possibilidade de compartilhamento de dados de saúde com objetivo de obter vantagem econômica, salvo quando o titular dos dados consentia para fins de portabilidade.

Tal redação mais restritiva em relação às hipóteses de tratamento de dados de saúde visando a vantagens econômicas foi incluída originalmente no texto normativo com o objetivo de impedir "o tratamento de dados sensíveis que tragam prejuízo ou desvantagem ao titular, como poderia acontecer, por exemplo, com troca de informações entre operadoras de planos de saúde" (COTS; OLIVEIRA, 2019, p. 113).

No entanto, no apagar das luzes do governo de Michel Temer, foi expedida a Medida Provisória nº 869, com o intuito de criar a Autoridade Nacional de Proteção de Dados (ANPD). Porém, o seu texto trouxe outras modificações à LGPD, dentre elas o § 4º do artigo 11 (DALLARI, 2019, s. p.), passando a prever:

> § 4º É vedada a comunicação ou o uso compartilhado entre controladores de dados pessoais sensíveis referentes à saúde com objetivo de obter vantagem econômica, exceto nas hipóteses de:
> I - portabilidade de dados quando consentido pelo titular;
> II - necessidade de comunicação para a adequada prestação de serviços de saúde suplementar.

Percebe-se que foi incluída no texto legal mais uma exceção, além da portabilidade já prevista anteriormente, expandindo a possibilidade de compartilhamento de dados de saúde

para obter vantagem econômica. Sendo possível para as hipóteses de necessidade de comunicação para a adequada prestação de serviços de saúde suplementar (PALHARES, 2021, p. 304).

A Medida Provisória nº 869, "que dispôs sobre a criação da ANPD, bem como alterou a redação de alguns dos dispositivos da norma" (DALLARI; MARTINS, 2021, p. 119), trouxe uma redação mais flexível para a lei de proteção de dados. No entanto, durante as discussões no Congresso Nacional, a Medida Provisória passa por novas alterações para chegar ao texto atual do § 4º do artigo 11 da LGPD:

> § 4º É vedada a comunicação ou o uso compartilhado entre controladores de dados pessoais sensíveis referentes à saúde com objetivo de obter vantagem econômica, exceto nas hipóteses relativas a prestação de serviços de saúde, de assistência farmacêutica e de assistência à saúde, desde que observado o § 5º deste artigo, incluídos os serviços auxiliares de diagnose e terapia, em benefício dos interesses dos titulares de dados, e para permitir:
> I - a portabilidade de dados quando solicitada pelo titular; ou
> II - as transações financeiras e administrativas resultantes do uso e da prestação dos serviços de que trata este parágrafo.

Foi também acrescentado o § 5º, que prevê a vedação "às operadoras de planos privados de assistência à saúde o tratamento de dados de saúde para a prática de seleção de riscos na contratação de qualquer modalidade, assim como na contratação e exclusão de beneficiários". Tais redações foram, posteriormente, convertidas na Lei nº 13.853, de 2019.

Assim como a Lei Geral de Proteção de Dados, a Medida Provisória 869/2018, quando passou pela apreciação do Legislativo, contou com participação da população. No dia 17 de abril de 2019 ocorreu a 4ª Audiência Pública relacionada à MP 869/2018, cuja pauta foi: "compartilhamento e proteção de dados na saúde e na pesquisa científica". Foram realizadas duas rodadas de discussão com a sociedade civil, momento em que foram apresentados argumentos contra e a favor à mudança do texto normativo. A discussão que se deu na Audiência Pública elucida as questões que estavam em jogo na alteração do § 4º do artigo 11. Deste modo, passasse a elencar os argumentos favoráveis às mudanças.

Segundo o diretor-adjunto da Diretoria de Desenvolvimento Setorial da Agência Nacional de Saúde Suplementar (ANS), Daniel Meirelles Fernandes Pereira, na saúde suplementar existe a necessidade de "comunicação dos dados de usuários para, por exemplo, controle e reembolso". Outro parecer a favor da mudança foi do representante da Confederação das Santas Casas e Hospitais Filantrópicos, Ronaldo Lemos, para quem a mudança é necessária, pois "o tratamento de dados reduz déficits e custos na saúde, combate a

falta de acesso, confere maior agilidade e se ‘externaliza’, por exemplo, na criação de ecossistemas de *startups* que se utilizam de Inteligência Artificial”. Para o presidente da Câmara Jurídica da Associação Brasileira de Medicina Diagnóstica e diretor jurídico do Grupo Das, Fabio Cunha, a mudança é benéfica, pois os dados de saúde são necessários ao “atendimento, tratamento rápido, humanizado e eficaz”, bem como o tratamento de dados de saúde e sua unificação trazem benéficos coletivos, uma vez que promovem a eficiência, melhorando o sistema de saúde suplementar, o que por sua vez tem como consequência diminuir a demanda pelo Sistema Único de Saúde. Fabio Cunha enfatizou que “o setor é contrário à comercialização desses dados”, bem como todos os compartilhamentos são realizados com base no sigilo, que sempre existiu no setor de saúde. Por fim, Glauce Karina de Jesus Madureira Carvalhal, superintendente jurídica da Confederação Nacional das Empresas de Seguros Gerais, Previdência Privada e Vida, Saúde Suplementar e Capitalização – CNSEG, defendeu a mudança que torna viável a prática dos seguros de saúde, pois “comunicação entre profissionais é essencial para diversas atividades como o pagamento de honorários e o reembolso, para aumentar a segurança das transações e evitar fraudes, sempre no interesse dos pacientes, hipóteses que acontecem no dia a dia das seguradoras de saúde” (BRASIL, 2019, p. 40-42).

Por outro lado, o diretor executivo da Sociedade Brasileira de Informática em Saúde, Marcelo Silva, se manifestou contrário à mudança, levando em consideração que o texto ficaria muito aberto e não seguiria os princípios protetivos da LGPD. No mesmo sentido advogou Dennys Antonialli, diretor presidente do Centro de Pesquisa Independente em Direito e Tecnologia – InternetLab. Em sua visão a redação da MP nº 869/2018 traz prejuízos aos usuários dos dados, uma vez que isso permitiria que as “farmácias, laboratórios e outros poderiam utilizar desses dados para calcular valores de planos de saúde, por meio de utilização de algoritmos. Ademais, alertou que o termo *benefício ao usuário* poderia comportar várias interpretações, dentre elas a alegação de que, ao analisar os dados de saúde, uma pessoa que o algoritmo considera saudável conseguiria planos mais vantajosos (o que seria um benefício), mas tal ação acarretaria um malefício para outros usuários. Para Raquel Lima de Saraiva, presidente do Instituto de Pesquisa em Direito e Tecnologia do Recife – IP.Rec – e integrante da coalizão Direitos na Rede, a alteração permitiria aumentos abusivos e negativas de tratamento sob uma alegada *adequada prestação*, sem existirem parâmetros para

definir o que seria uma adequada prestação. “A flexibilização seria uma externalidade negativa na contramão do espírito protetivo da LGPD” (BRASIL, 2019, p. 42).

Das discussões realizadas na audiência pública, colhem-se os dois lados da moeda de se permitir utilizar dados, em especial os sensíveis, com finalidades econômicas. De um lado, “a importância do uso das informações para otimizar processos de produção e reduzir custos, e, por outro lado, os efeitos distributivos que tenderiam a reduzir o benefício dos consumidores por meio de precificação seletiva” (COSTA, 2021, p. 100). Do outro lado, o receio que existe com o tratamento de dados sensíveis com a finalidade de obter vantagem econômica, uma vez que os dados sensíveis de saúde estão muito próximos de questões privadas, e tal permissivo legal pode acabar violando a privacidade dos seus titulares na busca por mais lucro no setor da saúde.

De acordo com Dallari (2019, s. p.), após três reuniões deliberativas, no dia 7 de maio de 2019 o relatório da Comissão Mista da MP 869/2018, de lavra do deputado Orlando Silva, foi aprovado, por unanimidade, pelo colegiado, e seguiu para o Plenário da Câmara dos Deputados (casa iniciadora), sendo aprovada a Medida Provisória nº 869, de 2018, na forma do Projeto de Lei de Conversão nº 7, de 2019, que se transformou na Lei nº 13.853, de 2019, alterando o conteúdo normativo na LGPD, deixando-a menos rígida em alguns pontos envolvendo pesquisa científica com fins exclusivamente acadêmicos, bem como aumentando as bases legais para tratamento de dados de saúde sem o consentimento do titular (DALLARI, MARTINS, 2021, p. 120). A ampliação das hipóteses de autorização para a comunicação ou os usos de dados, segundo Lemos et al. (2018, p. 5), trouxe resultados positivos, pois o texto original era muito restritivo e “poderia resultar na precarização da prestação de certos serviços relacionados à saúde, como aqueles oferecidos por planos de saúde, hospitais e clínicas médicas”.

Nesse sentido, extrai-se do relatório do deputado Orlando Silva as razões da alteração realizada pela MP nº 869, que inclui uma nova possibilidade de comunicação de dados de saúde. Acolhendo a emenda 96, permite que o compartilhamento desses dados se dê apenas em “benefício dos interesses do titular”, bem como a emenda 121, que troca “serviços de saúde suplementar” para “prestação de serviços à saúde e de apoio à assistência à saúde”. Segundo o relatório, a primeira redação da lei visava a proteger os pacientes da exposição de seus dados sensíveis, sem o seu consentimento, buscando evitar que, em razão de sua vulnerabilidade, tivessem sua intimidade devassada, evitando também possíveis discriminações. No entanto, segundo o deputado, as discussões que ocorreram nas audiências

públicas deixaram claro que os agentes do setor não têm a intenção de comercializar "dados de saúde para fins diversos e não relacionados com o atendimento que está sendo prestado a pacientes". E que os dados de saúde são necessários para a prestação de serviços de saúde. Apesar de reconhecer que a coleta de dados poderia gerar perfil de consumidores e que esses dados poderiam ser utilizados em malefício dos pacientes, o autor do relatório observa que os dados de saúde são necessários para a prestação do serviço e "ao atendimento médico moderno, rápido, eficiente e seguro" (BRASIL, 2019, p. 67-69).

Por tais razões, o relator concluiu, na parte referente ao compartilhamento de dados de saúde, que "a flexibilização proposta tanto pela MP quanto pelas emendas 96 e 121 são pertinentes no sentido de acatar a real necessidade de comunicação desse tipo de dados entre as empresas". Contudo, com o objetivo de proteger o titular dos dados de saúde, foi determinado que, nas "hipóteses relativas a prestação de serviços de saúde, incluídos os serviços auxiliares de diagnose e terapia", poderá haver comunicação de dados referentes à saúde quando em benefício dos titulares e para "transações financeiras e administrativas resultantes do uso e prestação dos serviços contratados". Por condicionar apenas aos serviços contratados, entende o relator que não há permissão para utilização dos dados sem o consentimento do titular para fins não contratados, tais como "cadastros em farmácias ou laboratórios para a obtenção de descontos". Ademais, buscaram deixar claro que "a exceção para se tratar dados de saúde sem consentimento poderá ser realizada por toda a cadeia do setor de saúde, valendo-nos para isso da inclusão da definição constante na Lei Orgânica da Saúde (Lei nº 8.080/90), 'serviços de saúde[143]'". Todavia, o tratamento e o compartilhamento de dados sem consentimento do titular dos dados de saúde, na visão do relator, apenas poderá ocorrer nos casos para a tutela da saúde, ou seja, quando o tratamento dos dados beneficiar o paciente titular (BRASIL, 2019, p. 69).

---

143 O relatório faz referência à Lei Complementar nº 141/12, que estabelece critérios para os serviços públicos de saúde e nomenclatura consagrada pelo Ministério da Saúde, a exemplo da Portaria 403/07. Nesse sentido, dispõe o Art. 2º da mencionada Lei Complementar: "Para fins de apuração da aplicação dos recursos mínimos estabelecidos nesta Lei Complementar, considerar-se-ão como despesas com ações e serviços públicos de saúde aquelas voltadas para a promoção, proteção e recuperação da saúde que atendam, simultaneamente, aos princípios estatuídos no art. 7º da Lei nº 8.080, de 19 de setembro de 1990, e às seguintes diretrizes: I - sejam destinadas às ações e serviços públicos de saúde de acesso universal, igualitário e gratuito; II - estejam em conformidade com objetivos e metas explicitados nos Planos de Saúde de cada ente da Federação; e III - sejam de responsabilidade específica do setor da saúde, não se aplicando a despesas relacionadas a outras políticas públicas que atuam sobre determinantes sociais e econômicos, ainda que incidentes sobre as condições de saúde da população. Parágrafo único. Além de atender aos critérios estabelecidos no caput, as despesas com ações e serviços públicos de saúde realizadas pela União, pelos Estados, pelo Distrito Federal e pelos Municípios deverão ser financiadas com recursos movimentados por meio dos respectivos fundos de saúde.

Apesar das explicações dadas no relatório redigido pelo deputado Orlando Silva, o § 4º do artigo 11 da LGPD não ficou com uma redação tão clara no tocante aos limites do compartilhamento, uma vez que os termos utilizados são demasiadamente abertos, permitindo outras interpretações. Passemos à análise da redação final do § 4º do artigo 11 da LGPD. Para essa análise, iremos destacar os termos que consideramos abertos na redação do parágrafo, atribuindo a eles possíveis significados, com base na doutrina, na própria Lei Geral de Dados Pessoais, na legislação brasileira esparsa sobre o tema, bem como normativas de agências reguladoras.

Nesse sentido, dispõe o § 4º do artigo 11:

> § 4º É vedada **a comunicação ou o uso compartilhado** entre **controladores** de dados pessoais sensíveis referentes à saúde com objetivo de obter **vantagem econômica**, exceto nas hipóteses relativas a **prestação de serviços de saúde**, de **assistência farmacêutica** e de **assistência à saúde**, desde que observado **o § 5º deste artigo**, incluídos os **serviços auxiliares de diagnose e terapia**, em **benefício dos interesses dos titulares de dados,** e para permitir:
> I - a **portabilidade de dados** quando solicitada pelo titular; ou
> II - as transações financeiras e administrativas resultantes do uso e da prestação dos serviços de que trata este parágrafo.

Assim, o parágrafo veda a **comunicação ou o uso compartilhado** entre os controladores de dados pessoais sensíveis referentes à saúde com objetivo de obter vantagem econômica. Conforme visto no item 4.3, a Lei Geral de Proteção de Dados trouxe em seu artigo 5º uma série de definições, dentre elas a de **uso compartilhado de dados**, que define como

> comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicos no cumprimento de suas competências legais, ou entre esses e entes privados, reciprocamente, com autorização específica, para uma ou mais modalidades de tratamento permitidas por esses entes públicos, ou entre entes privados.

Dentre as definições previstas no parágrafo 5º da LGPD, não há uma definição específica para **comunicação**, mas retira-se que a comunicação está abarcada dentro do conceito do uso compartilhado de dados pessoais, bem como a comunicação está contida dentro do conceito de tratamento de dados pessoais, que, conforme o Art. 5º, X da LGPD,

> é toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão,

> distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, **comunicação**, transferência, difusão ou extração;

Logo, de acordo com o exposto, o Art. 6º da LGPD[144] condiciona que todo tratamento de dados pessoais precisa observar a boa-fé e os princípios da finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação, responsabilização e prestação de contas (*accountability*). Assim, a comunicação e o uso compartilhado de dados, por serem espécies de tratamento de dados pessoais, precisam seguir esses princípios, bem como deve ser levado em consideração que em qualquer hipótese de tratamento de dados pessoais deve-se atentar para os fundamentos da lei previstos no artigo 2º da LGPD[145].

A exceção da comunicação ou o uso compartilhado de dados de saúde se dá entre **controladores de dados pessoais sensíveis** com objetivo de obter vantagem econômica. Conforme visto, a LGPD define controlador (art. 5º, VI) como sendo a "pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais". Então, controlador é quem detém o poder de decisão sobre os dados pessoais.

---

144 Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios: I - finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades; II - adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento; III - necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados; IV - livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais; V - qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento; VI - transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial; VII - segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão; VIII - prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais; IX - não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos; X - responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

145 Art. 2º A disciplina da proteção de dados pessoais tem como fundamentos: I - o respeito à privacidade; II - a autodeterminação informativa; III - a liberdade de expressão, de informação, de comunicação e de opinião; IV - a inviolabilidade da intimidade, da honra e da imagem; V - o desenvolvimento econômico e tecnológico e a inovação; VI - a livre iniciativa, a livre concorrência e a defesa do consumidor; e VII - os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.

A Agência Nacional de Proteção de Dados disponibilizou um Guia Orientativo para definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado, em que define controlador como:

> o agente responsável por tomar as principais decisões referentes ao tratamento de dados pessoais e por definir a finalidade deste tratamento. Entre essas decisões, incluem-se as instruções fornecidas a operadores contratados para a realização de um determinado tratamento de dados pessoais (ANPD, 2021, p. 7).

O guia também disponibilizou exemplos de controladores, alertando que a "identificação do controlador deve partir do conceito legal e dos parâmetros auxiliares indicados neste Guia" (ANPD, 2021, p. 7). O controlador, pessoa física ou jurídica, é "o responsável pelas principais decisões referentes ao tratamento de dados pessoais" e tal definição vai depender do contexto (ANPD, 2021, p. 10). Para ajudar na elucidação do conceito, o guia apresenta os seguintes exemplos:

> **Exemplo 1 - Médica profissional liberal**: Uma médica, profissional liberal, armazena os prontuários e os demais dados pessoais de seus pacientes no computador de seu consultório. A médica, pessoa natural, é a controladora dos dados pessoais.
> **Exemplo 2 - Médica empregada de um hospital**: Uma médica é empregada de um hospital, constituído sob a forma de associação civil sem fins lucrativos. Nessa condição, atua como principal representante do hospital junto a um serviço de armazenamento de dados de pacientes em nuvem, inclusive assinando os contratos correspondentes. O hospital, isto é, a associação civil, pessoa jurídica de direito privado, é o controlador na hipótese. A médica, por atuar sob o poder diretivo da organização, não se caracteriza como agente de tratamento.
> **Exemplo 3 - Órgão público contratante de um serviço de inteligência artificial**: Um órgão público, vinculado à União, contrata uma solução de inteligência artificial fornecida por uma sociedade empresária com a finalidade específica de realizar o tratamento automatizado de decisões com base em um banco de dados gerido pelo órgão. Seguindo as instruções fornecidas pelo gestor público responsável e estabelecidas em contrato, a sociedade empresária realiza as operações necessárias para viabilizar o tratamento dos dados em questão. A União, pessoa jurídica de direito público, é a controladora na hipótese. Não obstante, o órgão público responsável detém obrigações legais específicas em face dos titulares e da ANPD, conforme previsto na LGPD. A sociedade empresária é a operadora, uma vez que realiza o tratamento dos dados conforme as instruções fornecidas pelo controlador. Por fim, o gestor público responsável, por atuar como servidor público subordinado à União, não se caracteriza como agente de tratamento (ANPD, 2021, p. 12).

Nesse sentido, percebe-se que o controlador é a pessoa, física ou jurídica, que toma as principais decisões a respeito do tratamento dos dados pessoais. Dentro do contexto envolvendo dados de saúde, a controladora pode ser um hospital, o médico, operadoras de

plano de saúde. No entanto, a definição vai precisar ser analisada com base no contexto fático[146].

Continuando a análise do parágrafo 4º, a legislação permitiu aos controladores compartilharem o uso e a comunicação de dados de saúde com objetivo de obter vantagem econômica nas hipóteses relativas à prestação de serviços de saúde, de assistência farmacêutica e de assistência à saúde, incluídos os serviços auxiliares de diagnose e terapia, em benefício dos interesses dos titulares de dados. Porém, que sentido quis o legislador dar para **obter vantagem econômica**?

Segundo Costa (2021, p. 100-101) o termo vantagem econômica deve ser interpretado de modo restritivo, sendo "situações em que as vantagens informativas possibilitam efeitos distributivos, com a transferência de vantagens dos consumidores para os fornecedores, não abrangendo hipóteses de vantagens resultantes da maior eficiência produtiva". Isto porque os fins econômicos devem ser realizados sempre em benefício do titular, sendo expressamente vedado seleção de riscos em cálculo de plano de saúde (SAAVEDRA; GARCIA, 2020, p. 113).

Para Cots e Oliveira (2019, p. 113), as condições que permitem o tratamento de dados de saúde para obter vantagem econômica parecem contraditórias quando o próprio parágrafo condiciona que precisa se dar em benefício dos interesses dos titulares dos dados. "Em outras palavras, se a comunicação ou compartilhamento de dados pessoais sensíveis pretende a vantagem econômica para os controladores, como poderia se dar em benefício do titular?" Para os mencionados autores, as mudanças legislativas não deveriam ter sido aprovadas para permitir a obtenção de vantagem econômica, ou, no caso, de alterar a legislação que a permissão para a obtenção de uma vantagem econômica indireta, como a redução dos custos entre o compartilhamento de dados entre o laboratório e o hospital. Outro exemplo seria o "redimensionamento de rede assistencial baseado no número de usuários de uma determinada região. Em ambos os exemplos haveria vantagem econômica que não ensejaria prejuízo ao titular".

146 Ademais, apesar da LGPD não fazer referência, podem existir situações de controladoria conjunta, em que há "dois ou mais controladores das finalidades e dos elementos essenciais para a realização do tratamento de dados pessoais, por meio de acordo que estabeleça as respectivas responsabilidades quanto ao cumprimento da LGPD". Nesse caso, a responsabilidade dos controladores será solidária, com base no artigo 42, § 1º, II, da LGPD (ANPD, 2021, p. 12).

Contudo, o que significaria **benefício ao titular dos dados** que permitiria o uso compartilhado e a comunicação de dados pessoais referentes à saúde, aspecto "de suma importância, pois não é incomum a verificação de dados de saúde compartilhados, para fins lucrativos, com empresas seguradoras de saúde e/ou farmácias com informações sobre o perfil de saúde do usuário" (ROSA et al., 2021, p. 283).

Ao contrário de Cots e Oliveira (2019, p. 111), que defendem ser antagônica a busca por vantagem econômica e benefícios ao titular, Palhares (2021, p. 307) afirma que "a subjetividade da concepção do que seria um benefício aos interesses dos titulares" possibilita reflexões sobre circunstâncias em que o tratamento dos dados seria possível, por ser benigno ao titular dos dados, e simultaneamente possibilitar que os controladores aufiram proveito econômico. Assim, o autor se vale do exemplo comum de compartilhar informações com farmácias visando a obter um desconto. Importante mencionar que tal exemplo apareceu no Relatório da Comissão Mista destinada a emitir parecer sobre a MP 869/2018 como sendo uma hipótese que estaria proibida (BRASIL, 2018, p. 69)[147], o que demonstra que o entendimento não está longe de estar pacificado. Porém, voltemos ao exemplo elaborado por Palhares (2021, p. 307-308):

> O exemplo rotineiro das farmácias traria algumas possibilidade, a exemplo das seguintes hipóteses: (i) ao compartilhar informações sobre seu plano de saúde com uma farmácia, o titular pode receber um desconto em determinados medicamentos (um benefício em seu interesse financeiro), ao mesmo tempo que está compartilhando a informação com o plano de saúde, que poderia usar esses dados para a obtenção de vantagens econômicas, e, sem esse compartilhamento entre farmácia e plano de saúde, não seria possível dar o desconto no medicamento ao titular; (ii) ao compartilhar os remédios que são comprados pelo titular com hospitais da região, a farmácia recebe uma compensação financeira por essa informação, que é utilizada pelos hospitais para criar um cadastro em prol do melhor atendimento ao titular, com registros sobre seus medicamentos de uso frequente, o que pode ser extremamente benefício em casos que o titular seja levado inconsciente ao hospital e não possa indicar qual remédio toma todos os dias, dado que pode ser essencial para o seu tratamento.

Contudo, Palhares (2021, p. 308) reconhece que determinar de fato o que seria um interesse do titular é controverso, mesmo naqueles casos em que existem ganhos diretos, como no exemplo de aquisição com descontos em farmácias. A dificuldade de avaliar se

147 "[...] Nas "hipóteses relativas a prestação de serviços de saúde, incluídos os serviços auxiliares de diagnose e terapia", poderá haver comunicação de dados referentes à saúde quando em benefício dos titulares e para "transações financeiras e administrativas resultantes do uso e prestação dos serviços contratados". Dessa forma, cadastros em farmácias ou laboratórios para a obtenção de descontos ou o repasse de dados para outros fins não contratados estariam proibidos (BRASIL, 2018, p. 69).

realmente se trata de um beneficio fica mais complexa quando são colocados outros fatores em análise.

Sabe-se que o setor farmacêutico possui várias regulamentações, dentre elas a Lei nº 10.742 de 06 de outubro de 2003. A mencionada lei cria a Câmara de Regulação de Mercado de Medicamentos – CMED[148] –, que é o órgão interministerial responsável pela regulação econômica do mercado de medicamentos no Brasil, definindo os limites para preços de medicamentos de acordo com o art. 4º da Lei nº 10.742/2003[149].

Destarte, o preço dos medicamentos no Brasil é tabelado de modo que exista um limite de preços que pode ser praticado pelas farmácias e drogarias, sendo vedado cobrar valores além do permitido pela tabela. Apesar da boa intenção do legislador, pesquisa elaborada pelo Instituto Brasileiro de Defesa do Consumidor (Idec) demonstrou que o "preço teto definido pela CMED é muito elevado e descolado da realidade dos preços praticados em compras públicas e privadas, o que acaba por permitir aumentos abruptos e abusivos" (PL nº 5.591, 2021, p. 6)[150]. Inclusive, a tabela pode ser utilizada como meio para apoiar a

148 Art. 5º Fica criada a Câmara de Regulação do Mercado de Medicamentos - CMED, do Conselho de Governo, que tem por objetivos a adoção, implementação e coordenação de atividades relativas à regulação econômica do mercado de medicamentos, voltados a promover a assistência farmacêutica à população, por meio de mecanismos que estimulem a oferta de medicamentos e a competitividade do setor.

149 Art. 4º As empresas produtoras de medicamentos deverão observar, para o ajuste e determinação de seus preços, as regras definidas nesta Lei, a partir de sua publicação, ficando vedado qualquer ajuste em desacordo com esta Lei. § 1º O ajuste de preços de medicamentos será baseado em modelo de teto de preços calculado com base em um índice, em um fator de produtividade e em um fator de ajuste de preços relativos intra-setor e entre setores. § 2º O índice utilizado, para fins do ajuste previsto no § 1º, é o Índice Nacional de Preços ao Consumidor Amplo - IPCA, calculado pelo Instituto Brasileiro de Geografia e Estatística - IBGE. § 3º O fator de produtividade, expresso em percentual, é o mecanismo que permite repassar aos consumidores, por meio dos preços dos medicamentos, projeções de ganhos de produtividade das empresas produtoras de medicamentos. § 4º O fator de ajuste de preços relativos, expresso em percentual, é composto de duas parcelas: I - a parcela do fator de ajuste de preços relativos intra-setor, que será calculada com base no poder de mercado, que é determinado, entre outros, pelo poder de monopólio ou oligopólio, na assimetria de informação e nas barreiras à entrada; e II - a parcela do fator de ajuste de preços relativos entre setores, que será calculada com base na variação dos custos dos insumos, desde que tais custos não sejam recuperados pelo cômputo do índice previsto no § 2º deste artigo. § 5º Compete à Câmara de Regulação do Mercado de Medicamentos - CMED, criada pelo art. 5º desta Lei, propor critérios de composição dos fatores a que se refere o § 1º, bem como o grau de desagregação de tais fatores, seja por produto, por mercado relevante ou por grupos de mercados relevantes, a serem reguladas até 31 de dezembro de 2003, na forma do art. 84 da Constituição Federal.

150 "Projeto de Lei do Senador Fabiano Contarato (Rede/ES) visa alterar a Lei nº 10.742, de 6 de outubro de 2003, que define normas de regulação para o setor farmacêutico, cria a Câmara de Regulação do Mercado de Medicamentos - CMED e altera a Lei nº 6.360, de 23 de setembro de 1976, e dá outras providências, para dispor sobre ajuste positivo e negativo de preços, competência e composição da CMED, e critérios para definição de preços de entrada dos medicamentos; e a Lei nº 6.360, de 23 de setembro de 1976, que dispõe sobre a Vigilância Sanitária a que ficam sujeitos os Medicamentos, as Drogas, os Insumos Farmacêuticos e Correlatos, Cosméticos, Saneantes e Outros Produtos, e dá outras Providências, para incluir informações para fins de registro de medicamentos" (PL 5.591, 2020, p. 1).

precificação de medicamentos, bem como há a possibilidade de ser utilizada para estratégias promocionais – assim, o preço máximo seria o preço de partida da promoção.

> Considere um medicamento que tem como Preço Máximo ao Consumidor o valor de R$ 120,00: 'X medicamento: de R$ 120,00 por R$ 99,00. Promoção válida até a data X'. O preço se torna atrativo ao cliente, tem uma excelente margem para venda e ainda ativa o gatilho da urgência, pois a promoção tem um prazo estipulado para acabar. Essas estratégias podem ser utilizadas tanto nos medicamentos isentos de prescrição médica (MIP ou OTC) quando com correlatos, vitaminas, e produtos de higiene pessoal, perfumaria e cosméticos (HPC). Nas seções de vitaminas e HPC é possível até fazer promoções para a venda de kits (TABELA... 2021).

Pesquisa realizada pelo Idec concluiu que a tabela elaborada pela CMED não condiz com a realidade do mercado, "o que cria um vácuo que pode ser permissivamente aproveitado pelas empresas", razão pela qual existem diferenças de preços consideráveis praticadas entre diferentes estabelecimentos, como também "a concessão de descontos robustos pelas redes varejistas ou laboratórios" (IDEC, 2021, p. 3-9). Apenas para exemplificar, no caso do medicamento Liraglutina, do laboratório Norkisk, com preço máximo definido na tabela CMED em R$ 860,12, de acordo com a pesquisa o valor do produto encontrado na internet ficava na média de R$ 694,99. Porém, se fosse realizado um cadastro junto ao laboratório, o que envolve o fornecimento de dados pessoais, o valor médio do medicamento baixava para R$ 590,03. "A distância entre o preço cobrado ao consumidor e o teto da CMED aumentou de -23,76% para -45,78%" (IDEC, 2021, p. 8).

Considerando a tabela da CMED e a utilização do preço máximo por ela estabelecido, que segundo pesquisa do Idec está além do valor padrão de mercado, o titular dos dados, ao cedê-los buscando uma vantagem econômica, realmente foi beneficiado? Ou na verdade o titular dos dados é vítima de uma prática abusiva do mercado farmacêutico, que, além de faturar com a venda do medicamento, ganha com a obtenção dos dados de saúde do usuário consumidor[151]?

---

151 Sobre o tema, a prática rotineira de pedir os CPFs dos consumidores das farmácias é realizada ainda sem muita clareza sobre como esses dados são processados, quais as finalidades e para onde vão. Inclusive, em 2018, o Ministério Público do Distrito Federal iniciou uma investigação para descobrir o que as farmácias fazem com os dados sensíveis dos clientes. De acordo com o promotor do caso, Frederico Meinberg, "existe uma verdadeira obsessão das farmácias em dar desconto. E no capitalismo, não existe obsessão de graça. Há um interesse por trás". Se esses dados são repassados para terceiros, o titular ao final pode sofrer prejuízos, desde seguros de saúde com preços diferentes, negativas de empréstimo ou negativas de contratações trabalhistas (GABRIEL LUIZ, 2018). Ademais, Joyce Souza relata no podcast do DataPrivacyBrasil que em sua pesquisa de mestrado constatou que as farmácias trocavam dados com RHs de empresas conveniadas às farmácias em modelos de descontos, o que poderia ao longo prazo causar discriminação com demissões com base na saúde do empregado, pois, se a empresa sabe que determinado funcionário está passando a tomar

Assim, percebe-se que o critério em benefício dos interesses dos titulares é um conceito demasiadamente aberto e subjetivo, podendo haver vários entendimentos sobre a sua definição, gerando uma complexidade interpretativa que ficou a cargo dos próprios controladores de dados, que, "nas circunstâncias determinadas pelo § 4º, buscam obtenção de uma vantagem econômica, seja direta, seja indireta" (PALHARES, 2021, p. 307).

Ainda no tocante à expressão **em benefício dos interesses dos titulares de dados**, esta abarcaria situações em que o titular dos dados não fosse beneficiado diretamente, mas indiretamente numa avaliação mais genérica, levando em consideração a coletividade e o bem comum. Assim, se um nosocômio vende informações para uma indústria farmacêutica sobre medicamentos ministrados para pacientes com, por exemplo, Covid-19, o titular desses dados de saúde teria algum benefício? Observando a hipótese do ponto de vista restrito apenas ao titular, a resposta tende a ser negativa. Porém, considerando toda a coletividade, e supondo que a indústria farmacêutica em posse das informações as aplicará como subsídios para criar novos medicamentou ou vacinas para o mercado, "e que os novos medicamentos ou vacinas podem salvar a vida de milhares de pessoas, conceitualmente seria razoável alegrar a existência de um benefício em interesse do titular, ainda que não seja um benefício direto". Deste modo, admissível considerar benefícios indiretos aos titulares dos dados de saúde, principalmente nos casos envolvendo o progresso em medicamentos, serviços e produtos na área da saúde em que toda a sociedade, inclusive os titulares, seriam beneficiados com esse desenvolvimento. No entanto, esse tipo de argumentação flexibiliza ainda mais as "restrições à comunicação ou ao compartilhamento de dados de saúde com o objetivo de obtenção de vantagem econômica pelos controladores" (PALHARES, 2021, p. 308).

Obviamente, não estamos defendendo uma paralisia total nos dados de saúde. Até porque os dados de saúde "trafegam e precisam trafegar dentro de uma cadeia de modo a

---

determinado medicamento que indica que ele pode desenvolver uma doença que o afaste do trabalho, ou que começou a fazer uso de antidepressivos, ou uma empregada que sempre utilizava remédios contraceptivos e deixa de comprar pode levar os empregadores a tomarem atitudes discriminatórias como demissão para não ter as "despesas" da licença-maternidade, e a empregada dificilmente saberá os reais motivos que levaram a sua demissão. Levando em consideração essas preocupações, o estado de São Paulo sancionou em 1º de dezembro de 2020 a Lei nº 17.301, de autoria do deputado Alex de Madureira (PSD), que proíbe às farmácias e drogarias "exigir o Cadastro de Pessoas Físicas – CPF do consumidor, no ato da compra, sem informar de forma adequada e clara sobre a abertura de cadastro ou registro de dados pessoais e de consumo, que condiciona a concessão de determinadas promoções". Tendo como justificativa "coibir essa prática abusiva ao consumidor, que de boa-fé acaba passando seus dados pessoais, sem informar de forma adequada e clara sobre a abertura de cadastro ou registro de dados pessoais e de consumo, que condicionam a concessão de determinadas promoções" (PROJETO DE LEI Nº 1.212/2019, SÃO PAULO).

garantir a melhor assistência do paciente e do titular dos dados" (DALLARI; MARTINS, 2021, p. 121). Há a necessidade dos dados serem acessados pelos profissionais de saúde, por exemplo, após a realização de exames de sangue ou de imagem por determinado laboratório com o objetivo de evitar desperdício de tempo e dinheiro com a repetição desnecessária de exames, ou mesmo buscando evitar a repetição de exames que podem trazer malefícios (tais como o PET scan, em que é utilizada uma substância radiativa), em tais situações, sempre, buscando o bem-estar do paciente. Ademais, dados de saúde, por vezes, precisam ser acessados por operadoras de planos de saúde em situações tais como reembolso ou autorização de procedimentos (DALLARI; MARTINS, 2021, p. 121).

Há casos em que o "compartilhamento e a comunicação de dados de saúde podem trazer – e, efetivamente, trarão – benefícios relevantes" mesmo em situações em que "os controladores o tenham feito em razão de vantagens econômicas" (PALHARES, 2021, p. 309). O problema não é obter a vantagem econômica, mas ela ser o norte da ação dos controladores no tratamento dos dados, em detrimento de aspectos da personalidade do titular dos dados, que nesse caso não teria consentido com o uso compartilhado e a comunicação. No entanto, segundo Dallari e Martins (2021, p. 121), o texto da LGPD é inequívoco no sentido de que o tratamento de dados de saúde sem consentimento do titular é a exceção, apenas foi previsto para "viabilizar o cruzamento de informações proporcionadas pelo tratamento desses dados poderá ser aplicada por toda a cadeia do setor de saúde, valendo-se para isso da definição constante na Lei Orgânica da Saúde (Lei nº 8.080/90)". Inclusive, Costa (2021, p. 101) advoga que as vedações previstas no artigo 11, § 4º da LGPD "não poderiam ser afastadas pela vontade dos titulares dos dados de saúde, ainda que por meio do consentimento expresso e informado". Ao que parece a intenção da norma foi proteger os titulares dos dados de abusos, restringindo hipóteses do consentimento dos titulares dos dados de saúde.

Assim, Dallari e Martins defendem que as alterações no texto da LGPD não permitem tratamentos que não sejam, exclusivamente, "para a tutela da saúde e para a proteção da vida ou da incolumidade física do titular ou de terceiros", ou seja, as hipóteses em que o titular dos dados de saúde não dará o seu consentimento apenas serão efetivas nos casos em que o tratamento dos dados visa ao "tratamento de saúde, ou continuidade de sua assistência, e desde que em benefício dos pacientes e titulares dos dados". Sendo proibido em quaisquer circunstâncias ação de seleção de riscos (DALLARI; MARTINS, 2021, p. 122). A permissão apenas poderá ser conferida para situações em benefício do titular dos dados, e que a alteração veio permitir ações que já ocorrem atualmente na prática dos serviços de saúde e

são indispensáveis para um bom tratamento[152]. Bem como o fluxo de dados pode gerar um tratamento mais eficiente, facilitado para os pacientes, melhorar o atendimento e barateá-lo. Assim como ocorre no Canadá, em que o Estado se empenhou em tornar a saúde digitalizada, aumentando a conectividade entre as ferramentas digitais de modo a "criar uma vinculação entre os dados capturados por um aplicativo de gerenciamento de medicamentos a serviço de uma instituição que faz diagnostico *online* com os serviços médicos baseados na internet e as farmácias *online*" (LOTTENBERG et al., 2019, p. 47). O compartilhamento de dados nesse exemplo beneficia os titulares, bem como traz vantagens econômicas aos atores envolvidos nas operações de tratamento de dados.

Ante o exposto, percebe-se que mensurar o significado de benefício aos titulares dos dados, bem como o alcance da vantagem econômica, não é uma tarefa simples. Palhares (2021, p. 309) propõe como solução o "balanceamento entre esses benefícios e as vantagens econômicas pretendidas pelos controladores, no sentido de se encontrar um meio-termo para essa equação". A ideia do autor seria contrapor os benefícios que seriam auferidos pelos titulares dos dados ou pela coletividade (se considerar a hipótese de benefício indireto) com interesses econômicos dos controladores dos dados. A solução proposta visa a equilibrar dois fundamentos presentes na LGPD: o do respeito à privacidade (art. 2º, I) e o do desenvolvimento econômico e tecnológico e a inovação (art. 2º, V).

Ademais, de acordo com as discussões que ocorreram na audiência pública, bem como analisando o novo texto normativo, pode-se concluir que a intenção do legislador era permitir o uso econômico dos dados em prol do titular, permitindo o funcionamento do setor de saúde, porém buscou um modo de evitar abusos e discriminações contra os titulares, em particular a possibilidade da "compra e venda mascarada de bases de dados com essas

152 "Alguns exemplos de compartilhamento já realizado hoje são: (a) reembolso: o médico precisa compartilhar dados de saúde para a operadora para reembolso de honorários; (b) autorização de procedimentos: requer-se a apresentação de laudo de exames anteriores para autorização, como Pet CT; (c) obrigação de apresentação de prontuário para fins de auditoria in loco; (d) Obrigação do preenchimento da declaração de saúde (doenças pré-existentes) nos processos de adesão aos planos de saúde; (e) o profissional de saúde precisa compartilhar dado com outro centro de saúde de diferente especialidade para discutir diagnóstico; (e) o profissional de saúde contratado pelo laboratório precisa compartilhar para informar resultado de diagnóstico; (f) no caso de políticas públicas, o monitoramento controla epidemias, cria e promove prevenção da saúde; (g) o compartilhamento evita gastos desnecessários como a repetição de exames e diagnósticos já realizados em outro estabelecimento; (h) evita e combate fraudes; (i) incentiva o investimento em segurança como certificação e criptografia; (j) o compartilhamento e a unificação de dados favoreceriam a eficiência e que o aumento do sistema de saúde suplementar desafogaria o Sistema Único de Saúde" (DALLARI, 2019, s. p.).

informações sensíveis e a discriminação na formação de preços de planos de saúde em razão dos conhecimentos obtidos por meio desses dados" (PALHARES, 2021, p. 309).

Tal temor fez com que o legislador condicionasse que as exceções ao uso compartilhado e a comunicação entre controladores de dados pessoais de saúde com objetivo de obter vantagem, previstas no § 4º do artigo 11 da LGPD, observassem o disposto no § 5º do mesmo artigo, que prevê uma vedação "às operadoras de planos privados de assistência à saúde o tratamento de dados de saúde para a prática de seleção de risco na contratação de qualquer modalidade, assim como na contratação e exclusão de benefícios"[153].

De acordo com a Lei nº 9.656, de 3 de junho de 1998, considera-se:

> I - Plano Privado de Assistência à Saúde: prestação continuada de serviços ou cobertura de custos assistenciais a preço pré ou pós-estabelecido, por prazo indeterminado, com a finalidade de garantir, sem limite financeiro, a assistência à saúde, pela faculdade de acesso e atendimento por profissionais ou serviços de saúde, livremente escolhidos, integrantes ou não de rede credenciada, contratada ou referenciada, visando a assistência médica, hospitalar e odontológica, a ser paga integral ou parcialmente às expensas da operadora contratada, mediante reembolso ou pagamento direto ao prestador, por conta e ordem do consumidor;
> II - Operadora de Plano de Assistência à Saúde: pessoa jurídica constituída sob a modalidade de sociedade civil ou comercial, cooperativa, ou entidade de autogestão, que opere produto, serviço ou contrato de que trata o inciso I deste artigo (Art. 1º da Lei nº 9.656/1998).

Retira-se que a Operadora de Plano de Assistência à Saúde é pessoa jurídica, obrigatoriamente registrada na Agência Nacional de Saúde Suplementar – ANS, "que opera ou comercializa planos privados de assistência à saúde". Do outro lado da relação, os contratantes dos planos de saúde ou de seguros podem ser pessoas físicas ou jurídicas, porém a pessoa física será a beneficiária do contrato que utilizará os serviços de saúde previstos no contrato. "Nesses modelos de negócio, os valores das mensalidades são calculados conforme o risco do beneficiário" (FAVERO, 2021, p. 172).

Como os preços das mensalidades dos seguros são calculados com base no risco, ou seja, na probabilidade do segurado vir a utilizar o plano, entende-se por que os dados de saúde

153 Sobre esse ponto, vale a pena fazer uma breve alusão à Constituição Federal em seu artigo 196, que reza que "a saúde é direito de todos e dever do Estado, garantido mediante políticas sociais e econômicas que visem à redução do risco de doença e de outros agravos e ao acesso universal e igualitário às ações e serviços para sua promoção, proteção e recuperação". Apesar de ser um dever do Estado, o artigo 199 da Carta Maior possibilita à iniciativa privada a livre assistência à saúde, "de forma complementar ao Sistema Único de Saúde. Assim, o sistema de saúde brasileiro pode ser acessado pelo cidadão por meio de dois subsistemas: o SUS [...] e o Sistema de Saúde privado, que pode ser exercido por "meio de contratação de planos privados de saúde, assistência junto a operadora de plano de saúde (Sistema de Saúde Suplementar)", bem como por meio de contratação direta com os profissionais de serviço de saúde privados (FAVERO, 2021, p. 171).

são tão importantes para esses negócios. As operadoras de planos de saúde analisaram o perfil da pessoa que pretende contratar um plano de saúde ou um seguro de saúde e fizeram uma estimativa do tamanho do risco que essa pessoa representa. Logo, se as operadoras tiverem muitas informações sobre a saúde das pessoas, elas conseguirão melhor mensurar o risco, o que pode acarretar discriminação. Foi com o intuito de evitar essa prática que a alteração na LGPD trouxe a redação do § 5º, que inclusive, segundo o Relatório da MP nº 869/2018, teve como inspiração a súmula 27/5 da ANS, que dispõe:

> É **vedada a prática de seleção de riscos** pelas operadoras de planos de saúde na contratação de qualquer modalidade de plano privado de assistência à saúde. Nas contratações de planos coletivo empresarial ou coletivo por adesão, a vedação se aplica tanto à totalidade do grupo quanto a um ou alguns de seus membros. **A vedação se aplica à contratação e exclusão de beneficiários.**

Uma primeira leitura, tanto da súmula 27/5 da ANS quanto do § 5º do art. 11 da LGPD, poderia suscitar o entendimento de que há uma vedação na utilização de dados de saúde para a subscrição de seguros saúde. No entanto, segundo o Guia de Boas Práticas na CNseg (2019, p. 14), o § 5º do art. 11 da LGPD deve ser lido conjuntamente com a Lei nº 9.656/98, em que existe uma proibição de seleção de riscos e a exclusão indiscriminada de usuários pela não renovação ou rompimento do contrato. Todavia, a Lei nº 9.656/98 também prevê

> a possibilidade de precificação e de análise de riscos para fins de subscrição ao admitir que, na presença de doença preexistente, deverá ser ofertada ao proponente a cobertura parcial temporária ou o agravo do prêmio durante o período no qual seria aplicável a cobertura parcial temporária. Portanto, é nessa linha que deve ser interpretado esse dispositivo da LGPD (CNSeg, 2019, p. 14).

Assim, a mitigação de risco é permitida com base na coleta de dados para aplicar carência, cobertura parcial e agravo, de modo que as operadoras de plano de saúde podem elaborar "estudos populacionais, avaliando o comportamento de carteiras para o fim de aplicar uma precificação justa e adequada para cada grupo, coletivamente considerado" (VICENTE, 2019, s. p.). A vedação estaria nas hipóteses de seleção de pessoas específicas, bem como exclusão de usuários, negativa de contratação ou outras condutas discriminatórias com base no risco. Ademais, previsão semelhante está descrita no art. 16 da Resolução Normativa nº 195, de 14 de julho de 2009, da ANS: "Para vínculo de beneficiários aos planos privados de

assistência à saúde coletivos por adesão ou empresarial não serão permitidas quaisquer outras exigências que não as necessárias para ingressar na pessoa jurídica contratante". Logo, a proibição de utilizar dados pessoais sensíveis para permitir, negar ou excluir determinada pessoa da carteira de segurados não é nova para o setor.

Continuando a análise do parágrafo 4º do artigo 11 da LGPD, a exceção da vedação à comunicação ou o uso compartilhado entre controladores de dados pessoais sensíveis referentes à saúde com objetivo de obter vantagem econômica se dá nas hipóteses relativas: 1) prestação de serviços de saúde, 2) de assistência farmacêutica, e 3) de assistência à saúde, incluídos os serviços auxiliares de diagnose e terapia. Esses são extremamente amplos, possuindo inúmeros modos de interpretá-los e, consequentemente, "permitindo a comunicação e o compartilhamento de dados de saúde em maior número de casos" quando comparado com a redação original da lei, e inclusive, da própria redação original da MP 869, que apenas possibilitava a exceção para a prestação de serviços de saúde suplementar (PALHARES, 2021, p. 306).

A **prestação de serviços de saúde** pode ser considerada, dentre os três conceitos sob análise, um dos mais amplos. Isto porque a saúde, de acordo com o art. 196 da Constituição Federal, é um direito de todos e dever do Estado, que deve garantir "políticas sociais e econômicas que visem à redução do risco de doenças e de outros agravos e ao acesso universal e igualitário às ações e serviços para sua promoção, proteção e recuperação". O texto constitucional, tendo em vista esse dever do Estado, já estabelece em seu artigo 198 a organização do Sistema Único de Saúde – SUS, que detém a competência para

> I - controlar e fiscalizar procedimentos, produtos e substâncias de interesse para a saúde e participar da produção de medicamentos, equipamentos, imunobiológicos, hemoderivados e outros insumos;
> II - executar as ações de vigilância sanitária e epidemiológica, bem como as de saúde do trabalhador;
> III - ordenar a formação de recursos humanos na área de saúde;
> IV - participar da formulação da política e da execução das ações de saneamento básico;
> V - incrementar em sua área de atuação o desenvolvimento científico e tecnológico;
> VI - fiscalizar e inspecionar alimentos, compreendido o controle de seu teor nutricional, bem como bebidas e águas para consumo humano;
> VII - participar do controle e fiscalização da produção, transporte, guarda e utilização de substâncias e produtos psicoativos, tóxicos e radioativos;
> VIII - colaborar na proteção do meio ambiente, nele compreendido o do trabalho (Art. 200, CF/88).

Percebe-se que o SUS possui um leque amplo de competências e todas envolvem direta ou indiretamente a promoção da saúde[154]. Descendo ao nível infraconstitucional, a Lei nº 8.080, de 19 de setembro de 1990, "regula, em todo o território nacional, as ações e serviços de saúde, executadas isolada ou conjuntamente, em caráter permanente ou eventual, por pessoas naturais ou jurídicas de direito Público ou privado" (art. 1º da Lei 8.080/2019). Ou seja, a referida lei regula todos os serviços de saúde no território nacional, não estando restrita apenas ao Poder Público.

O artigo 3º da Lei nº 8.080/1990, ou Lei Orgânica da Saúde, reza que são determinantes ou condicionantes da saúde, entre outros, "a alimentação, a moradia, o saneamento básico, o meio ambiente, o trabalho, a renda, a educação, a atividade física, o transporte, o lazer, o acesso aos bens e serviços essenciais". Desta forma, ações que promovem saúde "se destinam a garantir às pessoas e à coletividade condições de bem-estar, físico, mental e social" (Parágrafo Único, Art. 3º, da Lei Orgânica da Saúde). Estão incluídas no campo de atuação do SUS, que presta ações e serviços de saúde: I – a execução de ações: a) de vigilância sanitária, b) de vigilância epidemiológica; c) de saúde do trabalhador, e d) de assistência terapêutica integral, inclusive farmacêutica. Sobre esse campo de atuação, entende-se por vigilância em saúde:

> Conjunto de práticas contínuas e articuladas voltadas para o conhecimento, a previsão, a prevenção e o enfrentamento de problemas de saúde da população de um território determinado relativos a fatores de risco, atuais e potenciais, a acidentes, a incapacidades, a doenças e a agravos à saúde. Notas: i) Inclui, além da vigilância epidemiológica das doenças transmissíveis, a promoção da saúde, a vigilância de agravos (violências e acidentes) e doenças não transmissíveis, a vigilância em saúde ambiental, a vigilância da saúde do trabalhador e a vigilância das situações de saúde. ii) Por meio da vigilância em saúde, é possível monitorar e analisar o perfil das doenças e agravos e de seus fatores determinantes e condicionantes, bem como detectar mudanças nas suas tendências no tempo, no espaço geográfico e em grupos populacionais, contribuindo, também, para o planejamento de ações na área de saúde" (MINISTÉRIO DA SAÚDE, 2013, p. 35).

Também estão incluídas no campo de atuação do SUS:

---

154 "Promoção da saúde, fem. Uma das estratégias de produção de saúde que, articulada às demais estratégias e políticas do Sistema Único de Saúde, contribui para a construção de ações transversais que possibilitem atender às necessidades sociais em saúde. Notas: i) A promoção da saúde é uma das prioridades do Pacto pela Vida para a construção de uma abordagem integral do processo saúde-doença e tem como foco o enfrentamento dos problemas de saúde baseado no reconhecimento dos determinantes sociais da saúde na sua produção. ii) A promoção da saúde deve dialogar com as diversas áreas do setor sanitário, com outros setores do governo e com a sociedade, para que sejam partícipes no cuidado com a vida, compondo redes de compromisso e corresponsabilidade" (MINISTÉRIO DA SAÚDE, 2013, p. 29).

> II - a participação na formulação da política e na execução de ações de saneamento básico; III - a ordenação da formação de recursos humanos na área de saúde; IV - a vigilância nutricional e a orientação alimentar; V - a colaboração na proteção do meio ambiente, nele compreendido o do trabalho; VI - a formulação da política de medicamentos, equipamentos, imunobiológicos e outros insumos de interesse para a saúde e a participação na sua produção; VII - o controle e a fiscalização de serviços, produtos e substâncias de interesse para a saúde; VIII - a fiscalização e a inspeção de alimentos, água e bebidas para consumo humano; IX - a participação no controle e na fiscalização da produção, transporte, guarda e utilização de substâncias e produtos psicoativos, tóxicos e radioativos; X - o incremento, em sua área de atuação, do desenvolvimento científico e tecnológico; XI - a formulação e execução da política de sangue e seus derivados (art. 6º da Lei Orgânica da Saúde).

A Lei Orgânica da Saúde não traz uma definição de serviços de saúde, apenas aponta quais são as determinantes ou condicionantes para a existência da saúde, e dentro desse universo quais são os campos de atuação do SUS. Na busca por um conceito de serviços de saúde, retira-se da Resolução de Diretoria Colegiada – RDC nº 63, de 25 de novembro de 2011, da Anvisa que serviços de saúde são "estabelecimentos de saúde destinados a prestar assistência à população na prevenção de doenças, no tratamento, recuperação e na reabilitação de pacientes". Por sua vez, o Conselho Federal de Farmácia (2016, p. 48) entende que "serviços de saúde são aqueles que lidam com a prevenção, o diagnóstico e o tratamento de doenças e de outras condições, bem como a promoção, manutenção e recuperação da saúde". Por essa razão o Conselho entende que os serviços farmacêuticos são considerados serviços de saúde, pois alcançam uma série de ações coordenadas em um processo de trabalho, "que visa a contribuir para prevenção de doenças, a promoção, a proteção e a recuperação de saúde, e para a melhoria da qualidade de vida das pessoas" (CONSELHO FEDERAL DE FARMÁCIA, 2016, p. 48).

Ademais, a Anvisa (2021, s. p.) também regulamenta os serviços de interesse à saúde, que "são atividades que englobam serviços de assistência ao cidadão, fora do contexto hospitalar ou clínico, que possam alterar ou influenciar o seu estado de saúde". São exemplos, segunda a própria Anvisa, salões e centros de estética, estúdios de tatuagem, creches, asilos, academias de ginástica, comunidades terapêuticas e cemitérios. Nesse quesito, os serviços de interesse à saúde estariam abarcados dentro de uma espécie de serviço de saúde que foram executados pelo legislador no art. 11 § 4º da LGPD? Dois asilos de idosos poderiam se valer dessa base legal para compartilhar dados pessoais sensíveis referentes à saúde, com finalidade lucrativa, ainda que seja no interesse do paciente? Da análise do § 4º, Favero (2021, p. 186) entende que não, e realmente, se fosse a vontade do legislador, ele teria especificado que a

exceção também abrangeria os serviços de interesse à saúde. Porém, não podemos deixar de salientar que existe o risco de uma interpretação mais abrangente, razão pela qual a Agência Nacional de Proteção de Dados editou regulamento definindo o escopo de alcance da expressão "Serviços de Saúde".

No tocante à expressão **assistência farmacêutica**, a Lei nº 13.021/2014, que dispõe sobre o exercício e a fiscalização das atividades farmacêuticas, prevê em seu artigo 2º que:

> Entende-se por assistência farmacêutica o conjunto de ações e de serviços que visem a assegurar a assistência terapêutica integral e a promoção, a proteção e a recuperação da saúde nos estabelecimentos públicos e privados que desempenhem atividades farmacêuticas, tendo o medicamento como insumo essencial e visando ao seu acesso e ao seu uso racional.

Sendo a farmácia designada como uma unidade de prestação de assistência farmacêutica, bem como também presta um serviço de assistência à saúde e orientação para conservação da saúde e à higiene individual ou coletiva, "na qual se processe a manipulação e/ou dispensação de medicamentos magistrais, oficinais, farmacopeicos ou industrializados, cosméticos, insumos farmacêuticos, produtos farmacêuticos e correlatos" (art. 3º da Lei nº 13.021/2014).

Ademais, a Resolução nº 228, de 06 de maio de 2004, do Conselho Nacional de Saúde, que aprovou a Política Nacional de Assistência Farmacêutica (PNAF), define assistência farmacêutica como

> um conjunto de ações voltadas à promoção, proteção e recuperação da saúde, tanto individual como coletiva, tendo o medicamento como insumo essencial e visando ao acesso e ao seu uso racional. Este conjunto envolve a pesquisa, o desenvolvimento e a produção de medicamentos e insumos, bem como a sua seleção, programação, aquisição, distribuição, dispensação, garantia da qualidade dos produtos e serviços, acompanhamento e avaliação de sua utilização, na perspectiva da obtenção de resultados concretos e da melhoria da qualidade de vida da população; (art. 1º, III, Resolução nº 338, de 06 de maio de 2004, Conselho Nacional de Saúde).

Conforme se retira da Lei nº 13.021/2014, a assistência farmacêutica encontra-se englobada dentro da expressão **assistência à saúde**, que, de acordo com a Lei Orgânica da Saúde em seu artigo 53-A, são as atividades "desenvolvidas pelos laboratórios de genética humana, produção e fornecimento de medicamentos e produtos para saúde, laboratórios de análises clínicas, anatomia patológica e de diagnóstico por imagem". O mesmo dispositivo

afirma que a assistência à saúde pode se dar pela "participação direta ou indireta de empresas ou de capitais estrangeiros".

Ademais, o Glossário Temático de Promoção da Saúde, promovido pelo Ministério da Saúde (2013, p. 16-17), trata como sinônimos as expressões "assistência em saúde" e "atenção à saúde". Por "atenção em saúde" consideram-se as "ações que envolvem o cuidado com a saúde do ser humano, incluindo ações de proteção, prevenção, recuperação e tratamento de doenças e de promoção da saúde". O Glossário também define o significado de "atenção básica à saúde", que seria uma espécie da "atenção à saúde", compreendida como "conjunto de ações de saúde, no âmbito individual e coletivo, que abrangem a promoção e a proteção da saúde, a prevenção de agravos, o diagnóstico, o tratamento, a reabilitação e a manutenção da saúde" (MINISTÉRIO DA SAÚDE, 2013, p. 17).

Levando-se em consideração apenas a palavra saúde, percebe-se o quão abrangente é, também, a assistência à saúde. Razão pela qual Palhares (2021, p. 311) afirma que as "alterações ao texto da LGPD acabaram sendo, com outros dispositivos da legislação, redigidas de forma aberta, com conceitos amplos e subjetivos, que dão margem a interpretações diversas e antagônicas, com potencial de trazer insegurança jurídica". Mesmo utilizando-se de conceitos legais é difícil descrever um rol, objetivo, com todas as atividades que podem ser abarcadas tanto em serviços de saúde como em assistência à saúde.

Por fim, foram incluídos na exceção no § 4º do artigo 11 os **serviços auxiliares de diagnose e terapia**. De acordo com o Ministério da Saúde (2013, p. 24-25), atividades de apoio diagnóstico e terapêutico, como o próprio nome sugere, são ações que visam a investigar qual o acometimento do paciente, e possibilitar a melhor terapia para aquele caso concreto. Englobam diversas atividades, tais como:

> laboratórios de análises clínicas, anatomia patologia, radiologia, endoscopia, fisioterapia, provas funcionais, hemoterapias, traçados diagnósticos (EEG, ECG) e os atendimentos individuais e em grupos realizados pelas diversas categorias profissionais nas unidades de saúde (MINISTÉRIO DA SAÚDE, 2013, p. 24-25).

Porém, também podem ser lembrados como serviços de apoio diagnóstico os estudos de imagem, os exames de sangue ou urina. Por outro lado, há os serviços de apoio terapêutico, que são definidos pelo Hospital Santa Rita (2019, sem página) como abordagens para melhorar o estado de saúde dos pacientes, visando a curar e minimizar os sintomas. São exemplo: "as ações de diálise/hemodiálise; fisioterapia; hemoterapia; litotripsia extracorpórea;

nutrição enteral e parenteral; além das abordagens em oncologia; quimioterapia e radioterapia". Além dos conselhos de saúde e educação, como "assistência para aprender a lidar com uma doença crônica" (NETINBAG)[155].

Feita essa digressão, as *healthtechs* se enquadrariam como serviços auxiliares de saúde? Conforme analisado, as *healthtechs* são empresas que "pretendem unir tecnologia, dados e conhecimentos médicos para, em última instância, melhorar as condições de vida das pessoas" (SOFTPLAN, 2021). Essas empresas atuam em assuntos diversos como "*devices* médicos, telemedicina, *wearables*, gestão do paciente e prontuário médico, entre vários outros" (CARMEN, 2021, sem página). Sendo assim, a grande maioria delas auxilia a prestação do serviço de saúde diretamente tanto no diagnóstico como na terapia. Inclusive, a realidade atual caminha para a imprescindibilidade da utilização dos recursos tecnológicos e informativos para a prestação de um serviço de saúde de qualidade, eficaz, eficiente e célere (SCHAEFER, 2010, p. 55).

Sendo assim, as *healthtechs* podem usar e compartilham dados sensíveis referentes à saúde com objetivo de obter vantagem econômica, desde que em benefício dos interesses dos titulares. Porém, como visto, as *healthtechs* possuem diferentes tipos de estrutura e de negócios. Assim, será que os dados de saúde podem circular em todos os ambientes dessas empresas? Até onde vai a prestação de serviços auxiliares de saúde, eles abarcam os desenvolvedores de aplicativos e/ou plataformas de saúde, quem faz a guarda dos dados de saúde (em que muitas vezes a nuvem está localizada fora do Brasil), segurança da informação, dentre outros atores envolvidos nesses sistemas de saúde – que até o momento não se encontra tão transparente para os pacientes, titulares dos dados de saúde e consumidores desses serviços. E nem mesmo é claro para os aplicadores do direito até onde vai a interpretação do próprio parágrafo 4º do artigo 11 da LGPD.

Apenas para ilustrar como a questão se torna problemática, no corrente ano, o grupo Raia Drogasil passou a requerer dados biométricos (dado sensível) aos seus clientes em troca de descontos nos medicamentos, além do CPF vinculado ao histórico de compras. Importante pontuar que integram o grupo Raia Drogasil, para além da Drogaria Raia e Drogasil, outros

155 O setor da saúde clássico é muito regulado e prevê sigilo em várias situações, inclusive, para prestação de serviços auxiliares de diagnose e terapia. A RDC nº 302/2005, da Anvisa, que regulamenta o funcionamento de laboratórios clínicos, prevê em seu artigo 5.1.4, b, que o responsável técnico do laboratório clínico tem a responsabilidade de planejar, implementar e garantir a qualidade dos processos, incluindo a proteção das informações confidenciais dos pacientes.

integrantes. O plano da rede é se transformar em uma nova farmácia agregando vários serviços em um único ponto, desde "prestação de serviços de saúde em loja, integrado com venda e serviços do site". Dentre os serviços de saúde está prevista a telemedicina, ou seja, consultas médicas remotas. O grupo, inclusive, em 2020, comprou a HealthBit, uma empresa "*healthtech* de *big data* voltada para redução de custos, melhoria de uso do plano de saúde e prevenção de casos graves de doenças", ou seja, é uma empresa voltada para mitigar riscos com planos de saúde e ajudar áreas de recursos humanos a economizarem (DIAS, 2021, sem página). Da leitura do parágrafo 4º do artigo 11 da LGPD podemos afirmar categoricamente que os integrantes do Grupo Raia Drogasil, mencionados, estão proibidos de compartilhar o uso e comunicar dados pessoais de saúde entre si com objetivo de obter vantagem econômica? O questionamento é complexo, pois todos os integrantes se enquadram dentro dos termos serviço de saúde, ou assistência farmacêutica, ou de assistência à saúde, e como visto o benefício ao titular dos dados também é um termo aberto. Nesse caso o titular ganhou uma vantagem econômica com um desconto no medicamento. Também é possível alegar que HealthBit beneficia a saúde do colaborador, pois, diminuindo o custo da saúde, ela viabiliza investimentos em saúde para os seus beneficiários, que se tornam mais eficientes e exatos, permitindo salvar mais vidas. O ponto é polêmico e, mais uma vez, a ANPD vai precisar se debruçar sobre a questão para determinar os limites dessa base de tratamento de dados pessoais sensíveis referentes à saúde.

Cots e Oliveira (2019, p. 114) levantam mais um ponto controverso do parágrafo 4º do artigo 11 da LGPD. Os autores questionam se há a necessidade de uma prévia relação jurídica entre todos os controladores envolvidos no tratamento dos dados pessoais de saúde e o titular, para prestação de serviços de saúde, assistência farmacêutica, assistência à saúde e os serviços auxiliares. Nesse sentido, os autores questionam a possibilidade, por exemplo, de uma operadora de plano de saúde compartilhar dados de saúde com outras operadoras com que o titular não tenha contrato ativo, por exemplo, uma operadora de plano odontológico da região do titular. Apesar de possuírem o entendimento de que tal hipótese não é viável aos olhos da legislação de compartilhamento de dados entre operadoras que o titular não possui um contrato ativo, uma vez, segundo os autores, ensejaria compartilhamento indiscriminado de dados pessoais sensíveis, sem finalidade demonstrada". De modo que a permissão do tratamento de dados de saúde necessita que os controladores de dados de saúde possuam prévia relação com o titular dos dados, caso contrário os controladores poderão se utilizar de outra base legal para o tratamento, "quando for necessário para a atuação para proteção da

vida ou da incolumidade física do titular ou do terceiro (art. 11, f)". Porém, a questão não é pacifica, os próprios autores admitem que a leitura do artigo pode suscitar outra interpretação, "em decorrência da referência ao § 5º, pois a vedação implementada por ele veda a seleção de riscos na contratação, ou seja, em momento anterior ao fechamento do contrato de prestação de serviços e do início da relação jurídica" (COTS; OLIVEIRA, 2019, p. 114).

Continuando na análise do artigo 11, § 4º, a permissão de portabilidade prevista no inciso I para comunicação e uso compartilhado entre controladores de dados pessoais sensíveis referentes à saúde, quando solicitada pelo titular. Tal previsão já estava presente no texto original da LGPD, com uma pequena, mas expressiva modificação. Originalmente, a portabilidade de dados entre as controladoras estava condicionada ao consentimento. Com a Lei 13.853/2019, restringiu-se a hipótese de portabilidade, pois, agora, está condicionada à solicitação do titular dos dados. Na solicitação, diferente do consentimento, precisa haver a iniciativa do titular de pedir a portabilidade. Segundo Costa (2021, p. 102), a alteração melhor protege os titulares de abusos, pois evita a portabilidade de dados "mediante mero consentimento".

Ademais, o inciso I apenas reafirma um dos direitos do titular de dado, previsto no artigo 18, V da LGPD, de requerer, em caso de seu interesse, a portabilidade dos dados a outro fornecedor de serviço ou produto. A portabilidade é realizada em benefício ao titular e se serve, mesmo que se houver vantagem econômica entre os controladores. Dentro dessa hipótese, como bem explicado por Cots e Oliveira (2019, p. 114), "o controlador anterior entregaria os dados pessoais necessários, mantendo em seu banco de dados apenas os dados pessoais necessários que se encaixassem em outra base legal do artigo 11".

Para terminar, o inciso II permite a comunicação ou o uso compartilhado entre controladores de dados pessoais sensíveis referentes à saúde com objetivo de obter vantagem econômica para permitir as transações financeiras e administrativas resultantes do uso e da prestação dos serviços de que trata este parágrafo. Ou seja, serviços de saúde, de assistência farmacêutica e de assistência à saúde, incluídos os serviços auxiliares de diagnose e terapia. Assim, a dispensa para permitir as transações financeiras e administrativas resultantes do uso e da prestação dos serviços que tenham ligação com a promoção da saúde do titular dos dados, não podendo haver compartilhamento para outras espécies de serviço mesmo que dentro de empresas de saúde. Nesse sentido, muito ilustrativo o exemplo de Dallari (2021, p. 123):

> Uma empresa que atua como instituição financeira pode contratar um serviço de telemedicina como forma eficiente e complementar a um plano de saúde, em benefício de seus colaboradores. Por outro lado, não pode solicitar relatório contendo dados pessoais sensíveis, relacionados aos atendimentos alegando que isso seria necessário para "viabilizar transações administrativas ou financeiras". Por mais que dito relatório fosse acessado somente pelo médico do trabalho, contratado, uma instituição financeira, nesse dado exemplo, não presta serviços de saúde ou assistência farmacêutica, tampouco de assistência à saúde, incluídos sérvios auxiliares de diagnose e terapia.

Ademais, o II em comento possui outro detalhe que pode passar despercebido numa primeira leitura. No caso do parágrafo 4º, o uso e o compartilhamento apenas poderão ocorrer entre controladores, ou seja, quem detém poder de decisão referente ao tratamento de dados, logo, os dois atores têm poder de decisão. Assim, o controlador que escolher compartilhar o dado com outro estará assumindo o risco pelas decisões tomadas pelo novo controlador, com base no artigo 42, inciso II, da LGPD. Mas, para além da possibilidade de uma responsabilização solidária, nos casos em que uma empresa médica transfere dados ao banco para registro de boleto, o banco é um controlador ou operador dos dados? Na visão de Cots e Oliveira (2019, p. 115) o banco é operador, bem como, nos casos envolvendo empresas de auditoria de contas médicas ou como prestadoras de serviços de eletrônicos de comunicação e informação. Se elas se comportam como operadoras, pois não detêm o poder de decisão, poderia haver a comunicação ou o uso compartilhado dos dados?

Voltando ao exemplo do compartilhamento com o banco para emissão de boleto, importante lembrar que o artigo 11, como um todo, faz referência a dados sensíveis, e o § 4º, mais especificamente, apenas a dados sensíveis referentes à saúde (COTS; OLIVEIRA, 2019, p. 115). Logo, deve-se se questionar se os dados sensíveis são, realmente, necessários para a finalidade almejada – respeitando o princípio da necessidade (art. 6º, III, LGPD). Aliás, tal princípio deve nortear qualquer tipo de tratamento de dados pessoais, porém, levando em consideração as especificidades dos dados de saúde, a atenção para as finalidades e a necessidade de tais dados nas operações e tratamentos deve ser analisada com maior atenção.

5 CONCLUSÃO

Com o avanço da tecnologia, o uso da internet assumiu um papel de destaque na organização dos sistemas que regem a sociedade. E junto com todos os benefícios que a internet trouxe, também vieram alguns riscos. Dentro desse contexto, torna-se imprescindível pensar na proteção da personalidade humana e na sensibilidade inerente a algumas categorias de dados pessoais. Os dados de saúde, pela proximidade com a privacidade e a potencialidade discriminatória, causam especial preocupação dentro desse mundo conectado. Em uma sociedade caracterizada pela informação, dados podem ser valiosos a diferentes setores da economia, podendo ser utilizados em prol do bem coletivo ou em benefício de poucos.

Dentro deste contexto, a presente pesquisa se propôs a responder ao seguinte problema: A alteração aprovada pelo Congresso Nacional no § 4º do art. 11 da LGPD pela Lei 13.853/19 pode ocasionar a violação da privacidade e dos dados relativos à saúde do titular dos dados pessoais tendo em conta a letra original do referido diploma legislativo?

O trabalho possuía como hipótese que a alteração do texto legislativo que passou a permitir o tratamento nas hipóteses relativas à prestação de serviços de saúde, de assistência farmacêutica e de assistência à saúde, incluídos os serviços auxiliares de diagnóstico e terapia – hipóteses que mostravam-se muito abertas –, possibilitou diversas interpretações que abarcam inúmeras atividades, colocando em risco a proteção à privacidade e aos dados pessoais da pessoa interessada. Assim, o objetivo geral da pesquisa era verificar se a alteração do art. 11, § 4º pode representar uma violação à privacidade e aos dados relativos à saúde do titular dos dados pessoais.

O primeiro capítulo possuía como objetivo específico contextualizar a Sociedade da Informação, para compreender a privacidade dentro deste contexto, bem como apresentar a privacidade, sua origem e seu conceito atual. Foi possível concluir que a arquitetura em redes, criada pelas novas tecnologias de informação, alterou a essência da sociedade. Com a popularização da internet e o uso cotidiano (quase obrigatório) de tecnologias ligadas à rede, o mundo on-line e off-line se misturam, as vidas normais passaram a ser compartilhadas para milhões. Nesse cenário, surgem questionamentos referentes à morte da privacidade na sociedade atual.

No entanto, as pessoas, ao viverem em sociedade, expõem pedaços de sua vida. Todavia, ainda há um espaço que é considerado íntimo, e que as pessoas querem manter longe de interferências alheias. Existem razões para defender a proteção da privacidade nos dias atuais, em que a sua violação não ocorre em virtude da devassa do lar, da violação de cartas, mas sim da coleta e uso indiscriminado de informações pessoais em transações abstratas.

As pessoas, realmente, expõem sua vida on-line, porém, ao divulgarem as informações, existe a consciência e seleção do que será postado ou não, logo há algo que se encontra numa esfera não pública. A privacidade não acabou. Concluímos que cada pessoa possui uma conotação para privacidade, faltando uma definição clara do conceito de privado, pois envolto nas subjetividades e sensibilidades de cada ser.

Assim, procurando um conceito uniforme de privacidade, foi utilizada a ficção jurídica do "homem médio", de modo que apenas seriam considerados danos à privacidade aquelas violações que a média da sociedade identifica como prejudicial. Assim, a privacidade protege informações que não gostaríamos de ver caírem no domínio público. É tudo aquilo que não deve ser objeto de informação ou curiosidade da sociedade moderna.

Comparamos os conceitos de proteção à privacidade e a proteção de dados pessoais. Averiguamos que são institutos que protegem coisas distintas. A privacidade visa a interromper/barrar o fluxo da informação, diferentemente da proteção de dados pessoais, que visa a controlar esse fluxo informacional, porém permitindo que ele flua. A proteção de dados está relacionada com controle informacional, é uma proteção procedimental. Proteção de dados diz respeito a diretrizes, os modos de tratamento, o processamento de dados, logo a proteção de dados permite o fluxo informacional. No entanto, esse fluxo deve ser regulado de modo a promover responsabilidades públicas significativas para os agentes que tratam dados pessoais. Por fim, percebeu-se que privacidade e dados pessoais, apesar de distintos em vários pontos, possuem algumas semelhanças, de modo que há uma zona de intersecção entre os conceitos de privacidade e dados pessoais.

No segundo capítulo buscou-se apresentar o conceito de proteção de dados pessoais e analisá-lo a partir do conceito de economia da informação. Dados pessoais podem ser conceituados como quaisquer informações relativas a uma pessoa física identificada ou identificável. São informações inerentes a cada ser humano e eles fazem parte da personalidade humana, como a representação direta da pessoa. Neste sentido, verificou-se que dados pessoais podem ser divididos em diferentes espécies, possuindo uma categoria especial, os dados sensíveis. A criação dessa categoria autônoma de dados pessoais está intimamente

ligada aos riscos que o armazenamento, tratamento, processamento e fluxo de certas informações pessoais poderiam causar à personalidade da pessoa humana, principalmente no tocante a práticas discriminatórias. Razões pelas quais os dados sensíveis necessitam de maior proteção e limites ao seu tratamento. Dados pessoais de saúde enquadram-se na classificação de dados sensíveis, justamente por conter um forte teor pessoal e pelo elevado risco que advém do seu tratamento; sua circulação discriminada pode acarretar graves danos a seus titulares, de forma que necessitam, portanto, de cuidados redobrados em sua proteção.

De fato, o entendimento de que as informações trocadas em momentos de fraqueza, enfermidade, sofrimento, na busca por uma cura ou diminuição de dor devem ser privadas é milenar. O dever de sigilo médico remonta a Hipócrates (460 a.C.), sendo fundamental preservar a personalidade da pessoa vulnerável, em virtude de seu estado de saúde, garantindo que as suas confissões se manterão fora do conhecimento público. Razão pela qual foi possível concluir que dados pessoais de saúde guardam uma estreita relação com questões da privacidade.

Para melhor compreender a proteção de dados pessoais, buscamos contextualizar a economia da informação, que possui como matéria-prima as informações. Os dados pessoais estão incluídos dentro de aspectos econômicos, sendo inúmeros os seus usos, em especial a comercialização dos dados para agências de publicidade, utilizados para obtenção de resultados com base em estatística, análises de preferências, perfis de consumo individual ou familiar. Bem como podem ser utilizados para pesquisas e inovações. Dentro desse aspecto, as inovações no setor da saúde são empolgantes. O futuro da medicina une tecnologia e prevenção de doenças, não apenas a cura de enfermidades. A tendência é de humanização das relações médicas, enxergando o paciente como um ser único e individual. Dentre os mais festejados, o desenvolvimento da Inteligência Artificial – IA – no setor da saúde, que seria capaz de auxiliar os profissionais na elucidação de diagnósticos. Esses sistemas de inteligência artificial baseados em metodologias de aprendizado de máquina dependem intensivamente de dados de saúde para a acurácia e eficiência de suas informações. Quanto mais dados, mais eficiente e preciso o sistema consegue ser, o que explica o porquê dos dados de saúde serem tão valiosos dentro deste contexto. Foi possível concluir que o valor dos dados de saúde está relacionado ao grau de sensibilidade das informações que eles contêm e suas potenciais aplicações práticas. Nesse sentido, levando em consideração a alta lucratividade do setor, bem como a quantidade de dados de saúde dos pacientes disponíveis para certos atores

do ramo, sem haver uma clareza em como esses dados são utilizados, pode-se levar à conclusão de que há um mercado de troca de informações, nem sempre vantajoso para o titular dos dados.

Por fim, o terceiro capítulo tinha como objetivo verificar se a alteração legislativa pode representar uma violação à privacidade e à proteção de dados. Para isso, foi analisada a proteção legislativa da privacidade e da proteção de dados pessoais no ordenamento jurídico brasileiro. A privacidade está tutelada no ordenamento pátrio como direito fundamental, prevista no art. 5º, inciso X da Constituição Federal. Bem como a privacidade é um direito da personalidade insculpida no art. 21 do Código Civil. Tal artigo, além de dar à privacidade o status de direito autônomo, confere a ela uma proteção antes de ocorrer o dano, ou seja, "para impedir" ato que ponha em risco a vida privada da pessoa humana. A razão da previsão de uma tutela inibitória ao direito à privacidade se justifica pois, após a sua violação, não há como reverter. Depois de o privado se tornar público não há como realizar o movimento contrário. A proteção de dados pessoais no Brasil ganhou ênfase com a aprovação da Lei Geral de Proteção de Dados Pessoais (Lei n. 13.709/2018). Constatou-se que a nova legislação possui como objetivo proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural (art. 1º, LGPD). Ademais, a legislação em comento possui uma forte carga principiológica, possibilitando a extração de importantes manifestações em prol da dignidade da pessoa humana.

Conforme constatado, a legislação passou a prever bases legais para o tratamento legítimo dos dados pessoais. A LGPD fez uma distinção entre as hipóteses que autorizam o tratamento de dados pessoais e dados pessoais sensíveis. As bases legais para o tratamento de dados sensíveis previstas no art. 11 da lei são mais restritivas quando comparadas às bases legais dos dados pessoais gerais. Constatou-se que a versão original da LGPD, aprovada em 14 de agosto de 2018, previa uma vedação ao tratamento de dados pessoais de saúde com objetivo de obter vantagem econômica, prevendo apenas uma exceção: nos casos de portabilidade de dados quando consentida pelo titular.

No entanto, o texto mais protetivo foi alterado para permitir o tratamento nas hipóteses relativas à prestação de serviços de saúde, de assistência farmacêutica e de assistência à saúde, incluídos os serviços auxiliares de diagnóstico e terapia. Hipóteses que, conforme analisado, são muito abertas, possibilitam um universo de interpretações e abarcam inúmeras atividades. De modo a deixar a pessoa humana descoberta, a LGPD trouxe uma hipótese de base legal para o tratamento de dados pessoais sensíveis que viola a privacidade

do titular ao retirar esses dados do contexto privado no qual os dados foram decididos, bem como vai de encontro com a lógica original da redação da legislação, ou seja, conferir uma camada protetiva maior ao tratamento de dados de saúde.

Assim, o objetivo geral deste trabalho foi atingido e a hipótese foi verificada, uma vez que foi possível constatar que a alteração no art. 11, § 4º, pela Lei n. 13.853/2019 cedeu às pressões do mercado e passou a permitir tratamento de dados de saúde com objetivo de obter vantagem econômica, exceto nas hipóteses relativas à prestação de serviços de saúde, de assistência farmacêutica e de assistência à saúde. A mudança causou sérios riscos à proteção da privacidade dos titulares dos dados de saúde, pois permite tratamentos de dados de saúde com objetivo de obter vantagem econômica para, praticamente, qualquer atividade.

REFERÊNCIAS

ACQUISTI, Alessandro; CURTIS, Taylor; LIAD, Wagman. The Economics of Privacy. **Journal of Economic Literature**, v. 54, n. 2, p. 442-92, June 2016.

AMARAL, Gisele. **Defesa da personalidade e o direito ao esquecimento**. 2019. 204 f. Dissertação (Mestrado) – Curso de Direito, Universidade de Lisboa, Lisboa/Portugal, 2019.

ANDRADE, Norberto Nuno Gomes de. Data Protection, Privacy and Identity: Distinguishing Concepts and Articulating Rights. In: FISCHER-HÜBNER, S. et al. (Ed.). **Privacy and Identity**. IFIP AICT, 2011. p. 90-107.

ANPD. **Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado**. Brasília: Autoridade Nacional de Proteção de Dados, 2021. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/2021.05.27GuiaAgentesdeTratamento_Final.pdf. Acesso em: 07 jul. 2021.

ANS. **Nota Técnica Nº 3/2019/Gepin/Dirad-Dides/Dides**. Brasília: Registro ANS: Dides, 2019. Disponível em: https://www.sbac.org.br/wp-content/uploads/2019/12/Nota-Te%CC%81cnica-sobre-LGPD.pdf. Acesso em: 06 jul. 2021.

BARAÚNA JR., Haroldo V. **Documentos médicos eletrônicos**: uma abordagem sobre seus efeitos jurídicos. Rio de Janeiro: Lumen Juris, 2019.

BARBOSA, Carla; LOPES, Dulce. RGPD: compartilhamento e tratamento de dados sensíveis na União Europeia – o caso particular da saúde. In: DALLARI, Analluza Bolivar; MONACO, Gustavo Ferraz de Campos (Coord.). **LGPD na saúde**. São Paulo: Revista dos Tribunais, 2021.

BAROCAS, Solon; NISSENBAUM, Helen F. On Notice: The Trouble with Notice and Consent (2009). **Proceedings of the Engaging Data Forum**: The First International Forum on the Application and Management of Personal Electronic Information, October 2009. Disponível em: https://ssrn.com/abstract=2567409. Acesso em: 06 jul. 2021.

BARRETO JR., Irineu Francisco; FAUSTINO, André. Aplicativos de serviços para saúde e proteção dos dados pessoais de usuários. **Revista Jurídica**, [s. l.], v. 1, n. 54, p. 292, 29 mar. 2019. Disponível em: http://dx.doi.org/10.21902/revistajur.2316-753x.v1i54.3311.

BAUMAN, Zygmunt. **44 cartas do mundo líquido moderno**. Tradução de Vera Pereira. Rio de Janeiro: Jorge Zahar, 2011.

BAUMAN, Zygmunt. **Vigilância líquida**: diálogos com David Lyon. Tradução de Carlos Alberto Medeiros. Rio de Janeiro: Jorge Zahar, 2012.

BBC. **Entenda o escândalo de uso político de dados que derrubou valor do Facebook e o colocou na mira de autoridades**. Disponível em: https://g1.globo.com/economia/tecnologia/noticia/entenda-o-escandalo-de-uso-politico-de-

dados-que-derrubou-valor-do-facebook-e-o-colocou-na-mira-de-autoridades.ghtml. Acesso em: 29 set. 2021.

BEZERRA, Arthur Coelho. Os reflexos do Grande Irmão no admirável espelho novo de Black Mirror. In: BRANCO, Sérgio; TEFFÉ, Chiara de (Org.). **Privacidade em perspectivas**. Rio de Janeiro: Lumen Juris, 2018.

BELLO, Cíntia Dal. Visibilidade, vigilância, identidade e indexação: a questão da privacidade nas redes socais digitais. **LOGOS 34** o Estatuto da Cibercultura no Brasil, v. 34, n. 1, p. 139-151, 2011.

BIONI, Bruno Ricardo. Inovar pela lei: a formação de uma cultura de proteção de dados a partir da nova legislação pode trazer valor agregado para as organizações. **GV-executivo**, v. 18, n. 4, p. 30-33, jul. 2019.

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

BIONI, Bruno Ricardo; LUCIANO, Maria. O consentimento como processo: em busca do consentimento válido. In: MENDES, Laura Schertel; DONEDA, Danilo; SARLET, Ingo Wolfgang; RODRIGUES JR., Otavio Luiz. **Tratado de proteção de dados pessoais**. Rio de Janeiro: Forense, 2021.

BITTAR, Carlos Alberto. **Os direitos da personalidade**. 8. ed. rev. São Paulo: Saraiva, 2015.

BOFF, Salete Oro. **Proteção de dados e privacidade**: do direito às novas tecnologias na sociedade da informação. Rio de Janeiro: Lumen Juris, 2018.

BRUNO, Fernanda. **Máquinas de ver, modos de ser**: vigilância, tecnologia e subjetividade. Porto Alegre: Sulina, 2013.

CACHAPUZ, Maria Cláudia. **Intimidade e vida privada no novo Código Civil brasileiro**: uma leitura orientada no Discurso Jurídico. Porto Alegre: Sergio Antonio Fabris, 2006.

CADORIN, Anelise Dell'Antonio. Tutela inibitória e os direitos à intimidade e à privacidade. In: CONGRESSO DE DIREITO DA UNIVERSIDADE FEDERAL DO ESTADO DE SANTA CATARINA, 7, 2012, Florianópolis. **Anais...** Florianópolis: UFSC, 2012. p. 1-20.

CANCELIER, Mikhail. **Infinito particular**: privacidade no século XXI e a manutenção do direito de estar só. Rio de Janeiro: Lumen Juris, 2017.

CARMEN, Gabriel del. 15 healthtechs que estão revolucionando a saúde para ficar de olho em 2021. **Forbes**. Disponível em: https://forbes.com.br/forbes-tech/2021/07/16-healthtechs-que-estao-revolucionando-a-saude-para-ficar-de-olho-em-2021. Acesso em: 06 jul. 2021.

CASTELLS, Manoel. **A sociedade em rede**. Tradução de Roneide Venancio Majer. 21. ed., rev. São Paulo: Paz e Terra, 2020.

CNSEG. **Guia de boas práticas do mercado segurador brasileiro sobre a proteção de dados pessoais**. 2019. Disponível em: https://cnseg.org.br/publicacoes/guia-de-boas-praticas-do-mercado-segurador-brasileiro-sobre-a-protecao-de-dados-pessoais.html. Acesso em: 18 ago. 2020.

COHEN, Glenn et al. Introduction. In: COHEN, Glenn et al. **Big Data, Health Law, And Bioethics**. Cambridge University Press, 2018.

COHEN, Julie E. The Regulatory State in the Information Age. **Theoretical Inquiries in Law,** [s. l.], v. 17, n. 2, p. 369-370, Jan. 1 2016. Disponível em: http://dx.doi.org/10.1515/til-2016-0015.

COMITRE, Gustavo. Amazon, Apple, Facebook, Google e Microsoft: a investida das Big Techs na Saúde. **MIT Technology Review**, 25 jun. 2021. Acesso em: 06 out. 2021.

CONSELHO FEDERAL DE MEDICINA. **Resolução CFM nº 1.931, de 17 de setembro de 2009**: Código de Ética Médica. Brasília: Conselho Federal de Medicina, 2010.

CORREIA, Victor. **Da privacidade**: significado e valor. Coimbra: Almedina, 2018.

COSTA, Jeferson Morais da; ROSA, Stefan de Oliveira. Lei Geral de Proteção de Dados aplicada à saúde. **Humanidades e Inovação**, Palmas, v. 8, n. 45, p. 137-143, set. 2020.

COSTA, José Augusto Fontoura. Tratamento de dados pessoais na LGPD: obrigações, limites e responsabilidades dos agentes. In: DALLARI, Analluza Bolivar; MONACO, Gustavo Ferraz de Campos (Coord.). **LGPD na saúde**. São Paulo: Revista dos Tribunais, 2021. p. 89-102.

COTS, Marcelo; OLIVEIRA, Ricardo. **Lei Geral de Proteção de Dados Pessoais comentada**. 3. ed. São Paulo: Revista dos Tribunais, 2019.

CRISTO, Camila Kohn de; COSTA, Mateus Stallivieri da; CRISTÓVAM, José Sérgio da Silva. Redescobrindo a declaração dos direitos de privacidade: mais de 70 anos e uma reflexão necessária. **Revista da Esmesc**, [s. l.], v. 27, n. 33, p. 365-388, 11 nov. 2020. Disponível em: http://dx.doi.org/10.14295/revistadaesmesc.v27i33.p365.

CURY, Alberto Rondina. Aspectos contratuais da saúde na LGPD: proteção de dados e contratos eletrônicos. In: DALLARI, Analluza Bolivar; MONACO, Gustavo Ferraz de Campos (Coord.). **LGPD na saúde**. São Paulo: Revista dos Tribunais, 2021. p. 192- 207.

DAINEZI, Gustavo Fernandes Americo. **Consumidores ou cidadãos?**: questões éticas nos discursos sobre a proteção de dados pessoais na cidade de São Paulo. 2019. 364 f. Dissertação (Mestrado) - Programa de Pós-graduação em Comunicação e Práticas de Consumo da ESPM-SP, São Paulo, 2019.

DALLARI, Analluza Bolivar; MARTINS, Amanda Cunha e Mello Smith. Proteção e compartilhamento de dados entre profissionais e estabelecimentos de saúde. In: DALLARI, Analluza Bolivar; MONACO, Gustavo Ferraz de Campos (Coord.). **LGPD na saúde**. São Paulo: Revista dos Tribunais, 2021. p. 117-134.

DALLARI, Analluza Bolivar. Proteção de dados na telemedicina. In: DALLARI, Analluza Bolivar; MONACO, Gustavo Ferraz de Campos (Coord.). **LGPD na saúde**. São Paulo: Revista dos Tribunais, 2021.

DATAPRIVACY. **Memória LGPD**. Disponível em: https://www.observatorioprivacidade.com.br/memoria/2018-uma-conjuncao-astral. Acesso em: 05 out. 2021.

DIAS, Tatiana. Não cadastre sua biometria na Droga Raia – e nem em qualquer farmácia: não é só pelo desconto: a rede usa seus dados de saúde para fazer negócios. **The Intercept**, 2021. Disponível em: https://theintercept.com/2021/07/05/nao-cadastre-biometria-na-droga-raia. Acesso em: 18 out. 2021.

DINIZ, Maria Helena. **Curso de direito civil brasileiro**: volume1: teoria geral do direito civil. 29. ed. São Paulo: Saraiva, 2012.

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

DONEDA, Danilo et al. Uso e proteção de dados nas relações de trabalho. In: MENDES, Laura Schertel; DONEDA, Danilo; SARLET, Ingo Wolfgang; RODRIGUES JR., Otavio Luiz. **Tratado de proteção de dados pessoais**. Rio de Janeiro: Forense, 2021.

DONEDA, Danilo. Os direitos da personalidade no código civil. **Revista da Faculdade de Direito de Campos**, [s. l.], v. 6, n. 6, p. 71-99, jun. 2005.

DONEDA, Danilo. Panorama histórico da proteção de dados pessoais. In: MENDES, Laura Schertel; DONEDA, Danilo; SARLET, Ingo Wolfgang; RODRIGUES JR., Otavio Luiz. **Tratado de proteção de dados pessoais**. Rio de Janeiro: Forense, 2021. p. 3-21.

FACHINETTI, Aline Fuke. Big data, pandemia e proteção de dados pessoais. In: PALHARES, Felipe. **Temas atuais de proteção de dados**. São Paulo: Revista dos Tribunais, 2020. p. 487-507.

FARIAS, Cristiano Chaves de; ROSENVALD, Nelson. **Curso de Direito Civil**: Parte Geral LINDB. 12. ed. Salvador: Juspodivm, 2014.

FARR, Christina. **Apple will oversee new medical studies focusing on women's health, hearing, and mobility.** 2019. Disponível em: https://www.cnbc.com/2019/09/10/apple-medical-studies-womens-health-hearing-mobility.html

FAVERO, Walquiria Nakano Eloy. Proteção e compartilhamento de dados na saúde suplementar. In: DALLARI, Analluza Bolivar; MONACO, Gustavo Ferraz de Campos (Coord.). **LGPD na saúde**. São Paulo: Revista dos Tribunais, 2021.

FERRAZ JR., Tercio Sampaio. **Introdução ao estudo do direito**: técnica, decisão, dominação. São Paulo: Atlas, 1993.

FORTES, Vinicius Borges. **Os direitos de privacidade de dados pessoais na internet**. Rio de Janeiro: Lumen Juris, 2016.

FRAZÃO, Ana. Objetivos e alcance da Lei Geral de Proteção de Dados. In: TEPEDINO, Gustavo; FRAZÃO, Ana; DONATO, Milena. **Lei Geral de Proteção de Dados Pessoais**: e suas repercussão no direito brasileiro. 2. ed. São Paulo: Revista dos Tribunais, 2020. p. 97-125.

GONÇALVES, Carlos Roberto. **Direito civil brasileiro**: volume 1: parte geral. 10. ed. São Paulo: Saraiva, 2012.

GRANATO, Marcelo de Azevedo. Quem habita a dignidade humana?: a fundamentação kantiana. **R. Fac. Dir. Univ. São Paulo**, São Paulo, v. 109, p. 623-639, dez. 2014.

HARTZOG, Woodrow. The Public Information Fallacy. **SSRN Electronic Journal**, [s. l.], p. 1-73, 2017. Disponível em: http://dx.doi.org/10.2139/ssrn.3084102.

HOSPITAL SANTA RITA. **Apoio terapêutico**: tratamento além da medicação. 2019. Disponível em: https://www.hospitalsantarita.com.br/br/blog/apoio-terapeutico-tratamento-alem-da-medicacao. Acesso em: 09 out. 2021.

IDEC. **Proteção de dados**: sorria, você está sendo monitorado. 2010. Disponível em: http://pensando.mj.gov.br/dadospessoais2011/protecao-de-dados-sorria-voce-esta-sendo-monitorado. Acesso em: 29 set. 2021.

IDEC. **Sancionada em agosto de 2018, a Lei Geral de Proteção de Dados Pessoais (LGPD) foi uma vitória da sociedade civil**. Disponível em: https://idec.org.br/dadospessoais/linha-do-tempo. Acesso em: 14 out. 2021.

IDEC. **Remédio a preço justo**: sumário executivo. 2021. Disponível em: https://idec.org.br/sites/default/files/21-05-27_-_sumario_executivo_-_pesquisa_de_medicamentos_1_1.pdf. Acesso em: 20 out. 2021.

IGO, Sarah E. **The Known Citizen**: A History of Privacy in Modern America. Cambridge: Harvard University Press, 2018.

KAPLAN, Bonnie. How Should Health Data Be Used?. **Cambridge Quarterly of Healthcare Ethics**, [s. l.], v. 25, n. 2, p. 312-329, Mar. 9 2016. Disponível em: http://dx.doi.org/10.1017/s0963180115000614.

KAPLAN, Bonnie; MONTEIRO, Artur Péricles Lima. PHI Protection Under Hippa: An Overall Analysis In: DALLARI, Analluza Bolivar; MONACO, Gustavo Ferraz de Campos (Coord.). **LGPD na saúde**. São Paulo: Revista dos Tribunais, 2021. p. 61-81.

KAPLAN, Bonnie. Seeing through health information technology: the need for transparency in software, algorithms, data privacy, and regulation. **Journal of Law and the Biosciences**, [s. l.], v. 7, n. 1, p. 1-18, Jan. 2020. Disponível em: http://dx.doi.org/10.1093/jlb/lsaa062.

KAPLAN, Bonnie. Selling Health Data. **Cambridge Quarterly of Healthcare Ethics**, [s. l.], v. 24, n. 3, p. 256-271, June 10 2015. Disponível em: http://dx.doi.org/10.1017/s0963180114000589.

KAUFMAN, Dora. Internet of Bodies: o corpo humano como plataforma tecnológica. **Época Negócios**, 2021. Disponível em: https://epocanegocios.globo.com/colunas/IAgora/noticia/2021/03/internet-bodies-o-corpo-humano-como-plataforma-tecnologica.html. Acesso em: 19 mar. 2021.

KESSLER, Greg. Technology and the future of language teaching. **Foreign Language Annals**, [s. l.], v. 51, n. 1, p. 205-218, Feb. 19 2018. Disponível em: http://dx.doi.org/10.1111/flan.12318.

KFOURI NETO, Miguel; SILVA, Rodrigo da Guia; NOGAROLI, Rafaella. Inteligência artificial e big data no diagnóstico e tratamento da covid-19 na América Latina: novos desafios à proteção de dados pessoais. **Direitos Fundamentais & Justiça**, Belo Horizonte, v. 14, n. 1, p. 149-178, nov. 2020.

KIATAKE, Luis Gustavo Gasparini. Sistemas de prontuário eletrônico e digitalização: impacto da LGPD. In: DALLARI, Analluza Bolivar; MONACO, Gustavo Ferraz de Campos (Coord.). **LGPD na saúde**. São Paulo: Revista dos Tribunais, 2021.

KONDER, Carlos Nelson. O tratamento de dados sensíveis à luz da Lei 13.709/2018. In: TEPEDINO, Gustavo; FRAZÃO, Ana; DONATO, Milena. **Lei Geral de Proteção de Dados Pessoais**: e suas repercussões no direito brasileiro. 2. ed. São Paulo: Revista dos Tribunais, 2020. p. 441-456.

KORKMAZ, Maria Regina Detoni Cavalcanti Rigolon. **Dados sensíveis na Lei Geral de Proteção de Dados Pessoais**: mecanismos de tutela para o livre desenvolvimento da personalidade. 2019. 119 f. Dissertação (Mestrado) – Curso de Direito, Universidade Federal de Juiz de Fora, Juiz de Fora, 2019.

LAFER, Celso. A reconstrução dos direitos humanos: a contribuição de Hannah Arendt. **Estudos Avançados**, v. 30, n. 11, p. 55-65, 1997. Disponível em: https://www.scielo.br/j/ea/a/9Sr35XjVCx9L7Ws7QypPMrG/?lang=pt&format=pdf. Acesso em: 11 out. 2021.

LEMOS, Ronaldo. **A vida em rede**. Campinas/SP: Papirus 7 Mares, 2014.

LEMOS, Ronaldo et al. A criação da Autoridade Nacional de Proteção de Dados pela MP nº 869/2018. **Jota**, 2018. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/a-criacao-da-autoridade-nacional-de-protecao-de-dados-pela-mp-no-869-2018-29122018. Acesso em: 20 out. 2021.

LEONARDI, Marcel. **Tutela e privacidade na internet**. São Paulo: Saraiva, 2011.

LEONARDI, Marcel. Aspectos controvertidos entre a Lei Geral de Proteção de Dados e o Marco Civil da Internet. In: PALHARES, Felipe. **Temas atuais de proteção de dados**. São Paulo: Revista dos Tribunais, 2020. p. 217-245.

LEONG, Hong Cheng. Da construção de um novo paradigma de culpa do legislador e o correspondente critério de juízo: uma problematização no âmbito da responsabilidade civil extracontratual do estado decorrente do exercício da função político-legislativa. **E-Pública**, [s. l], v. 4, n. 2, p. 291-325, nov. 2017. Disponível em: https://www.e-publica.pt/volumes/v4n2a13.html. Acesso em: 07 jul. 2021.

LESSIG, Lawrence. Privacy as Property. **Social Research**, v. 69, n. 1, p. 247-269, Spring 2002. Disponível em: http://www.jstor.org/stable/40971547. Acesso em: jul. 2021.

LÉVY, Pierre. **Cibercultura**. Tradução de Irineu da Costa. São Paulo: Editora 34, 2010.

LOTTENBERG, Claudio; SILVA, Patrícia Ellen da; KLAJNER, Sidney. **A revolução digital na saúde**: como a inteligência artificial e a internet das coisas tornam o cuidado mais humano, eficiente e sustentável. São Paulo: Editora dos Editores, 2019.

LYON, David. **The Electronic Eye**: The rise of surveillance society. Cambridge: Polity Press, 1994.

LYOTARD, Jean-François. **A condição pós-moderna**. 12. ed. Tradução de Ricardo Corrêa Barbosa. Rio de Janeiro: José Olympio, 2009.

MAGRANI, Eduardo. **Entre dados e robôs**: ética e privacidade na era da hiperconectividade. Porto Alegre: Arquipélago, 2019.

MARANHÃO, Juliano Souza de Albuquerque; ALMADA, Marco. Inteligência artificial no setor de saúde: ética e proteção de dados. In: DALLARI, Analluza Bolivar; MONACO, Gustavo Ferraz de Campos (Coord.). **LGPD na saúde**. São Paulo: Revista dos Tribunais, 2021.

MARINELI, Marcelo Romão. **Privacidade e redes sociais virtuais**: sob a égide da Lei nº 12.965/2014 – Marco Civil da Internet. Rio de Janeiro: Lumen Juris, 2017.

MASSIS, Diana. Somos cada vez menos felizes e produtivos porque estamos viciados na tecnologia. **BBC**, 2020. Disponível em: https://www.bbc.com/portuguese/geral-51409523. Acesso em: 08 abr. 2021.

MAZZA, Alexandre. **Manual de direito administrativo**. 6. ed. São Paulo: Saraiva, 2016.

MENDES, Laura Schertel. **Transparência e privacidade**: violação e proteção da informação pessoal na sociedade de consumo. 2008. 158 f. Dissertação (Mestrado) – Curso de Direito. Universidade de Brasília, Brasília, 2008.

MENDES, Laura Schertel; FONSECA, Gabriel Campos Soares. Proteção de dados para além do consentimento: tendências de materialização. In: DONEDA, Danilo et al. (Coord.). **Tratado de proteção de dados pessoais**. Rio de Janeiro: Forense, 2021.

MINISTÉRIO DA SAÚDE. Secretaria-Executiva. Departamento de Informática do SUS. **Estratégia de Saúde Digital para o Brasil 2020-2028**. Brasília: Ministério da Saúde, 2020. Disponível em: http://bvsms.saude.gov.br/bvs/publicacoes/estrategia_saude_digital_Brasil.pdf. Acesso em: 07 jul. 2021.

MINISTÉRIO DA SAÚDE. Secretaria-Executiva. Departamento de Informática do SUS. **Promoção da Saúde** Brasília: Ministério da Saúde, 2012. Disponível em: https://bvsms.saude.gov.br/bvs/publicacoes/glossario_tematico_promocao_saude.pdf. Acesso em: 07 jul. 2021.

MIRANDA, Leandro Alvarenga. **A proteção de dados pessoais e o paradigma da privacidade**. São Paulo: All Print, 2018.

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). **Revista de Direitos e Garantias Fundamentais**, [s. l.], v. 19, n. 3, p. 159-180, 29 dez. 2018. Disponível em: http://dx.doi.org/10.18759/rdgf.v19i3.1603.

MURIANA, Luã Marcelo et al. **Ambientes ubíquos e pervasivos em hospitais**: uma revisão sistemática de literatura focada em aspectos sociais, emocionais e enativos. São Paulo: Universidade Estadual de Campinas; Instituto de Computação, 2021.

NAESS, Per Sigve; CHRISTENSEN, Fredrik. **How the General Data Protection Regulation Affects Health Information System Innovation**: an explorative study of general data protection regulation challenges and benefits for health information system innovation initiatives. Agder: University of Agder, 2020.

NAVES, Bruno Torquato de Oliveira; GOITÁ, Sarah Rêgo. Direitos humanos, patrimônio genético e dados humanos: crítica à doutrina dos dados genéticos como interesse difuso. **Revista de Bioética y Derecho**, 2017. Disponível em: http://scielo.isciii.es/scielo.php?script=sci_arttext&pid=S1886-58872017000200006. Acesso em: 20 set. 2021.

NETINBAG.COM. **O que são serviços auxiliares?**. Disponível em: https://www.netinbag.com/pt/health/what-are-ancillary-services.html. Acesso em: 14 out. 2021.

NISSEMBAUM, Helen. **Privacy in context**: technology, policy, and the integrity of social life. Stanford: Stanford University Press, 2010.

O'NEILL, Patrick Howell. **Zuckerberg diz que "privacidade é o futuro", mas o Facebook vai continuar sendo o Facebook**. 2019. Disponível em: https://gizmodo.uol.com.br/facebook-privacidade-futuro-f8-2019/. Acesso em: 14 out. 2021.

OHM, Paul. Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization. **UCLA Law Review**, v. 57, p. 1701, Aug. 13 2009. Disponível em: https://ssrn.com/abstract=1450006.

OLIVEIRA, Marco Aurélio Bellizze; LOPES, Isabela Maria Pereira. Os princípios norteadores da proteção de dados pessoais no Brasil e sua otimização pela Lei 13.709/2018. In: TEPEDINO, Gustavo; FRAZÃO, Ana; DONATO, Milena. **Lei Geral de Proteção de Dados Pessoais**: e suas repercussões no direito brasileiro. 2. ed. São Paulo: Revista dos Tribunais, 2020. p. 53-81.

PALHARES, Felipe. Vantagem econômica no compartilhamento de dados de saúde: interpretação do artigo 11, parágrafo 4º da LGPD. In: DALLARI, Analluza Bolivar; MONACO, Gustavo Ferraz de Campos (Coord). **LGPD na saúde**. São Paulo: Revista dos Tribunais, 2021. p. 303-312.

PEEL, Deborah C. An Implementation Path to Meet Patients' Expectations and Rights to Privacy and Consent. In: KOONTZ, Linda. **Information Privacy in the Evolving Healthcare Environment**. Chicago: Himss, 2013. p. 89-115.

PERES-NETO, Luiz. Ética e privacidade: múltiplos olhares e partir do campo da comunicação. In: BRANCO, Sérgio; TEFFÉ, Chiara de (Org.). **Privacidade em perspectivas**. Rio de Janeiro: Lumen Juris, 2018.

PINHEIRO, Patricia Peck. **LGPD e saúde**: os fins justificam os meios?. 2019. Disponível em: https://www.serpro.gov.br/lgpd/noticias/2019/paciente-no-comando-lgpd-dados-sensiveis-saude. Acesso em: 06 jul. 2021.

PINOCHET, Luis Hernan Contreras; LOPES, Aline de Souza; SILVA, Jheniffer Sanches. Inovações e tendências aplicadas nas tecnologias de informação e comunicação na gestão da saúde. **Revista de Gestão em Sistemas de Saúde**, [s. l.], v. 3, n. 2, p. 11-29, 1 dez. 2014. Disponível em: http://dx.doi.org/10.5585/rgss.v3i2.88.privacy/Privacy_brand_warr2.html. Acesso em: 28 set. 2021.

REALE, Miguel. **O Estado democrático de direito e o conflito das ideologias**. 2. ed. São Paulo: Saraiva, 1998.

RODOTÀ, Stafano. **A vida privada na sociedade da vigilância**: a privacidade hoje. Tradução de Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008.

ROHNR, Altiers. Saiba como os "cookies" ou "web beacons" rastreiam você. **G1**, 2017. Disponível em: http://g1.globo.com/tecnologia/blog/seguranca-digital/post/saiba-como-os-cookies-ou-web-beacons-rastreiam-voce.html. Acesso em: 11 out. 2021.

ROSA, Helena Rinaldi et al. Bancos de dados de saúde e pesquisa: prós e contra da LGPD. In: DALLARI, Analluza Bolivar; MONACO, Gustavo Ferraz de Campos (Coord.). **LGPD na saúde**. São Paulo: Revista dos Tribunais, 2021. p. 279-288.

ROSOLEN, Fabio. Projeto Nightingale do Google coleta dados médicos de milhões de americanos. **Mundo Conectado**, 2019. Disponível em: https://mundoconectado.com.br/noticias/v/11117/projeto-nightingale-do-google-coleta-dados-medicos-de-milhoes-de-americanos. Acesso em: 06 out. 2021.

SAAVEDRA, Giovani Agostini; GARCIA, Lara Rocha. Privacidade e proteção de dados na área de saúde. In: POTIN, Andre et al. **Compliance na área da saúde**. Indaiatuba/SP: Foco, 2020.

SANDOVAL, Olívio Rocha Barros. **O Juramento de Hipócrates**. 2019. Disponível em: https://www.fmrp.usp.br/pb/arquivos/3652. Acesso em: 12 ago. 2021.

SANTOS, Aline Fernandes dos et al. Dados sensíveis na era da informação: análise dos programas de desconto de medicamentos no Brasil. In: SMOLARECK, Guilherme et al. **Coleção Jovem Jurista**. Rio de Janeiro: Escola de Direito FGV, 2012. p. 267-314.

SARLET, Gabriella Bezerra Sales; FERNADES, Márcia Santana; RUARO, Regina Linden. A proteção de dados no setor da saúde em face do sistema normativo brasileiro atual. In: MENDES, Laura Schertel et al. **Tratado de proteção de dados pessoais**. Rio de Janeiro: Forense, 2021. p. 485-507.

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

SARLET, Ingo Wolfgang. Fundamentos constitucionais: o direito fundamental à proteção de dados. In: DONEDA, Danilo et al. (Coord.). **Tratado de proteção de dados pessoais**. Rio de Janeiro: Forense, 2021.

SAWARIS, Adriana. **A tutela do direito à reserva sobre a intimidade da vida privada no Regulamento n.º 2016/679 da União Europeia**. 2017. 138 f. Dissertação (Mestrado) - Curso de Direito, Universidade de Coimbra, Coimbra, 2017.

SCHAEFER, Fernanda. **Proteção de dados de saúde na sociedade de informação**: a busca pelo equilíbrio ente privacidade e interesse social. Curitiba: Juruá, 2010.

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

SCHWARTZ, Paul M.; SOLOVE, Daniel J. The PII Problem: Privacy and a New Concept of Personally Identifiable Information. **New York University Law Review**, [s. l.], v. 86, n. 6, p. 1814-1894, Dec. 2011. Disponível em: https://www.nyulawreview.org/wp-content/uploads/2018/08/NYULawReview-86-6-Schwartz-Solove.pdf. Acesso em: 14 jul. 2021.

SEMIDÃO, Rafael Aparecido Moron. **Dados, informação e conhecimento enquanto elementos de compreensão do universo conceitual da ciência da informação**:

contribuições teóricas. 198 f. Dissertação (Mestrado) - Ciência da Informação. Universidade Estadual Paulista, Marília/SP, 2014.

SIBILIA, Paula. **O show do eu**. 2. ed. rev. Rio de Janeiro: Contraponto, 2016.

SILVA, Tiago Vinícius Soares. **O tratamento de dados pessoais sensíveis nas empresas do setor de saúde, segunda a Lei Geral de Proteção de Dados (LGPD**). 2020. 128 f. Dissertação (Mestrado) - Programa de Pós-Graduação em Direito, Universidade do Vale do Rio dos Sinos, Porto Alegre, 2020.

SILVEIRA, S. A.; AVELINO, R.; SOUZA, J. A privacidade e o mercado de dados pessoais. **Liinc em Revista**, [s. l.], v. 12, n. 2, 2016. Disponível em: http://revista.ibict.br/liinc/article/view/3719. Acesso em: 13 ago. 2021.

SILVEIRA, Sergio Amadeu da et al. **A privacidade e o mercado de dados pessoais**. 2016. Disponível em: https://www.rodolfoavelino.com.br/wp-content/uploads/2020/03/902-3567-1-PB.pdf. Acesso em: 14 out. 2021.

SILVEIRA, Sergio Amadeu da. **Tudo Sobre Tod@s**: redes digitais, privacidade e venda de dados pessoais [e-book]. São Paulo: Sesc, 2017.

SILVEIRA, Sergio Amadeu da; SOUZA, Joyce Ariane de Souza. Gestão algorítmica e a reprodução do capital no mercado segurador brasileiro. **Contracampo**, Niterói, v. 39, n. 2, p. 15-27, ago./nov. 2020.

SOFTPLAN. **Healthtechs**. Disponível em: https://www.softplan.com.br/healthtechs. Acesso em: 12 jun. 2021.

SOLOVE, Daniel J. "I've Got Nothing to Hide" and Other Misunderstandings of Privacy. **San Diego Law Review**, v. 44, p. 745, 2011. Disponível em: https://ssrn.com/abstract=998565.

SOUSA, Mariana Leite. **OpenEHR como solução para o Regulamento Geral de Proteção de Dados na área da saúde**. 2017. 90 f. Dissertação (Mestrado) - Curso de Ciência da Informação, Universidade do Porto, Porto, 2017.

SOUZA, Carlos Affonso et al. From privacy to data protection: the road ahead for the inter-American system of human rights. **The International Journal of Human Rights**, [s. l.], v. 25, n. 1, p. 147-177, July 13 2020. Disponível em: http://dx.doi.org/10.1080/13642987.2020.1789108.

SPOHR, Dominic. Fake news and ideological polarization. **Business Information Review**, [s. l.], v. 34, n. 3, p. 150-160, Aug. 23 2017. Disponível em: http://dx.doi.org/10.1177/0266382117722446.

TEPEDINO, Gustavo. **A tutela da personalidade no ordenamento civil constitucional brasileiro**. Disponível em: https://www.academia.edu/31740015/A_tutela_da_personalidade_no_ordenamento_civil_constitucional_brasileiro. Acesso em: 05 jun. 2021.

THIBES, Mariana Zanata. **A vida privada na mira do sistema**: a internet e a obsolescência da privacidade no capitalismo conexionista. 2014. 209 f. Tese (Doutorado) - Curso de Sociologia, Departamento de Sociologia, Universidade de São Paulo, São Paulo, 2014.

TSCHIDER, Charlotte A. The Consent Myth: Improving Choice for Patients of the Future. **Wash. U. L. Rev**, n. 1505, 2019). Disponível em: https://openscholarship.wustl.edu/law_lawreview/vol96/iss6/12.

TSCHIDER, Charlotte. The Healthcare Privacy-Artificial Intelligence Impasse. **Santa Clara High Tech. L. J.**, n. 439, 2020. Disponível em: https://digitalcommons.law.scu.edu/chtlj/vol36/iss4/2.

VALASCO, Irene Hernández. **Falta de privacidade mata mais que terrorismo': o surpreendente alerta de professora de Oxford**. 2020. Disponível em: https://www.bbc.com/portuguese/geral-54558878. Acesso em: 09 out. 2021.

VASCONSELOS, Pedro de Pais. **Direito de personalidade**. Coimbra: Almedina, 2014.

VIERA, Tatiana Malta. **O direito à privacidade na sociedade da informação**: efetividade desse direito fundamental diante dos avanços da tecnologia da informação. 2007, 297 p. Dissertação (Mestrado) – Universidade de Brasília, Faculdade de Direito, Programa de Pós-Graduação em Direito, Estado e Sociedade, 2007.

VIOLA, Mario; TEFFÉ, Chiara Spadaccini de. Tratamento de dados pessoais na LGPD: estudo sobre as bases legais dos artigos 7º e 11. In: MENDES, Laura Schertel et al. **Tratado de proteção de dados pessoais**. Rio de Janeiro: Forense, 2021. p. 118-148.

WARREN, Samuel D.; BRANDEIS, Louis D. The Right to Privacy. **Harvard Law Review**, v. 4, Dec. 1890. Disponível em: http://groups.csail.mit.edu/mac/classes/6.805/articles.

ZANATTA, Rafael A. F.; ABRAMOVAY, Ricardo. Dados, vícios e concorrência: repensando o jogo das economias digitais. **Estudos Avançados**, [s. l.], v. 33, n. 96, p. 421-446, ago. 2019. Disponível em: http://dx.doi.org/10.1590/s0103-4014.2019.3396.0021.