UNIVERSIDADE FEDERAL DE SÃO CARLOS
CENTRO DE EDUCAÇÃO E CIÊNCIAS HUMANAS
PROGRAMA DE PÓS-GRADUAÇÃO EM CIÊNCIA, TECNOLOGIA E SOCIEDADE

Ana Cristina Oliveira Mahle

A AUTODETERMINAÇÃO INFORMATIVA COMO FUNDAMENTO DA LEI GERAL DE PROTEÇÃO DE DADOS BRASILEIRA: UMA ANÁLISE A PARTIR DA LGPD

SÃO CARLOS – SP

2021

ANA CRISTINA OLIVEIRA MAHLE

A AUTODETERMINAÇÃO INFORMATIVA COMO FUNDAMENTO DA LEI GERAL DE PROTEÇÃO DE DADOS BRASILEIRA: UMA ANÁLISE A PARTIR DA LGPD

Exame de Qualificação apresentado ao Programa de Pós-Graduação em Ciência, Tecnologia e Sociedade, do Centro de Educação e Ciências Humanas, da Universidade Federal de São Carlos, como parte dos requisitos para a obtenção do título de Mestre em Ciência, Tecnologia e Sociedade.

Linha de pesquisa: Gestão Tecnológica e Sociedade Sustentável

Orientador: Prof. Dr. Vinicio Carrilho Martinez

SÃO CARLOS – SP

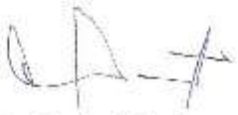
2021

UNIVERSIDADE FEDERAL DE SÃO CARLOS

Centro de Educação e Ciências Humanas
Programa de Pós-Graduação em Ciência, Tecnologia e Sociedade

Folha de Aprovação

Defesa de Dissertação de Mestrado da candidata Ana Cristina Oliveira Mahle, realizada em 01/09/2021.



Comissão Julgadora:

Prof. Dr. Vinício Carrilho Martinez (UNESP)

Prof. Dr. Leandro Innocentini Lopes de Faria (UFSCar)

Profa. Dra. Maria Victoria de Mesquita Benevides Soares (USP)

O presente trabalho foi realizado com apoio da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - Brasil (CAPES) - Código de Financiamento 001.

O Relatório de Defesa assinado pelos membros da Comissão Julgadora encontra-se arquivado junto ao Programa de

São Carlos – SP

2021

Dedico esse trabalho à toda sucessão de sincronicidades felizes e 'in'felizes, que me colocaram novamente na rota acadêmica e que me deram um fôlego novo e ter vontade de querer sempre mais.
Aos meus amados filhos Júlia e Pedro, que dão sentido nessa busca incessante

AGRADECIMENTOS

Agradeço ao professor Dr. Vinício Carrilho Martinez, pela orientação, paciência e apoio.

Agradeço ao meu marido Nelson, por todo incentivo e compreensão das minhas ausências.

Aos meus filhos Júlia e Pedro por servirem de inspiração e por me fazerem voltar a sonhar que o mundo pode ser um lugar melhor.

Aos meus pais por todo amor e dedicação, que me fizeram acreditar que é possível evoluir sempre.

À Marcela Schiavi, pela amizade, pela troca de ideias que foi essencial para a realização desse trabalho, muito obrigada.

A todas as pessoas que passaram na minha vida durante essa jornada que de alguma maneira me estimularam nesse processo, meus sinceros agradecimentos.

Demore o tempo que for para decidir o que você quer da vida, e depois que decidir não recue ante nenhum pretexto, porque o mundo tentará te dissuadir. (Friedrich Nietzsche)

RESUMO

"Seus dados são você", essa é uma frase da campanha de Coalizão dos Direitos na Rede (COALIZÃO…, 2019) que ratifica que a emissão da certidão de nascimento do indivíduo e as informações pessoais sobre os cidadãos brasileiros passariam a ser coletadas e armazenadas, seja na interação nas redes sociais, usando algum serviço público ou mesmo fazendo uma compra na farmácia. Estes exemplos são apenas uma parte de um universo infinito, pois cada clique que o indivíduo dá na internet produz novos dados, que serão coletados, armazenados e utilizados para alguma finalidade. *Mas como fica a gestão desses dados que estão sendo coletados, armazenados e comercializados como uma avalanche desordenada? Qual a proteção legal que as pessoas têm mediante esse tratamento indiscriminado dos seus dados?* No Brasil, existe uma lei que define os direitos e deveres para o uso dos dados pessoais: a Lei Geral de Proteção de Dados veio para definir as regras desse tratamento de dados e trouxe o cidadão como elemento central dessa regulação, trazendo a autodeterminação informativa como pilar fundamental na gestão desse universo digital. O objetivo deste estudo visa trazer à luz a necessidade de transparência e acesso à informação e à educação para que as pessoas possam colocar em prática esse direito, ou seja, a liberdade e controle do indivíduo sobre o fluxo das suas informações. Trata-se de trabalho de método indutivo, uma vez que procura demonstrar como os conhecimentos científico e tecnológico produzem mudanças na sociedade e também resultados, evidenciando que o avanço da tecnologia acarreta um maior volume de informações a cada dia. Nesse sentido, buscou-se reforçar e argumentar que a sociedade atual está alicerçada sobre o compartilhamento de dados pessoais, como o ativo econômico e a Lei Geral de Proteção Dos Dados (LGPD), o que se mostra muito importante nesse contexto, sobretudo por causa dos princípios contidos nessa legislação, entre eles a boa-fé e a transparência. Essa lei entrou em vigor em setembro de 2020, com exceção dos artigos contidos entre o 52 e o 54, que tratam das sanções administrativas e entrarão em vigor em agosto de 2021. A referida legislação estabelece parâmetros sobre o excessivo compartilhamento de dados, assim como estabelece diretrizes de governança e fiscalização sobre o atual 'trânsito" de dados pessoais, matéria-prima dessa sociedade em 'nuvem'. Além disso, a Lei reforça dois direitos fundamentais que se mostram cada vez mais importantes para a gestão desse novo universo regido por dados: a autodeterminação informativa e o direito à proteção de dados, que irão ser analisados no decorrer desse trabalho.

Palavras-chave: Lei Geral de Proteção de Dados. Privacidade. Constituição Federal. Autodeterminação Informativa.

ABSTRACT

“Your data are you”, this is a phrase from the Coalizão dos Direitos na Rede campaign (COALIZÃO..., 2019), where it says that the issuance of an individual's birth certificate, personal information about Brazilian citizens becomes collected and stored. Whether interacting on social networks, using a public service, or even making a purchase at the pharmacy, this is part of an infinite universe, as each click that the individual makes on the internet produces new data to be collected, stored and used for some purpose. *But what about the management of the data that is being collected, stored and traded as a disordered avalanche? What legal protection do people have through this indiscriminate processing of their data?* In Brazil, there is a law that defines the rights and duties for the use of personal data. The General Data Protection Law is a law that came to define the rules for this data processing and brought the citizen as a central element of this regulation when it brings informational self-determination as a fundamental pillar in the management of this digital universe. Therefore, the aim of this study is to bring to light the need for transparency and access to information and education so that people can put this right into practice, that is, the individual's freedom and control over the flow of their information. It is an inductive method work because it demonstrates how scientific and technological knowledge produces changes in society and, even as to the results, it was evident that the advancement of technology entails a greater volume of information every day. Therefore, it sought to reinforce and demonstrate that the current society is founded on the sharing of personal data as an economic asset and the General Data Protection Law (LGPD) which is very important in this context, especially because of the principles contained in this legislation, among them, good faith and transparency. This law came into effect in September 2020, with the exception of Articles 52 to 54, which deal with administrative sanctions, which will come into force in August 2021. This legislation sets parameters on this excessive data sharing, as well as establishing guidelines for governance and inspection of this current 'transit' of personal data, which is the raw material of this 'cloud' society. Furthermore, this law reinforces two fundamental rights that are increasingly important for the management of this new universe governed by data, and mainly informational self-determination and the right to data protection, which will be analyzed in the course of this work.

Keywords: General Data Protection Law. Privacy. Network Society. Federal Constitution. Informative self-determination.

LISTA DE ILUSTRAÇÕES

LISTA DE SIGLAS

ADI	Ação Direta de Inconstitucionalidade
ANPD	Autoridade Nacional de Proteção de Dados
ARPANET	*Advanced Research Projects Agency Network*
CDC	Código de Defesa do Consumidor
CEO	*Chief Executive Officer*
CF	Constituição Federal do Brasil
CLT	Consolidação das Leis do Trabalho
CNET	Consejo Nacional Empresarial Turístico
CNPD	Comissão Nacional de Proteção de Dados
COPPA	*Children On-Line Privacy Protection Act*
COVID-19	Coronavírus
CPF	Cadastro de Pessoas Físicas
DPO	Data Protection Officer
EUA	Estados Unidos da América
GDPR	*General Data Protection Regulation*
IBGE	Instituto Brasileiro de Geografia e Estatística
ICMS	Imposto sobre Operações relativas à Circulação de Mercadorias e sobre Prestações de Serviços de Transporte Interestadual e Intermunicipal e de Comunicação
IDC	*International Data Corporation*
IP	Internet Protocol
LAI	Lei de Acesso à Informação
LC	Lei do Cadastro Positivo
LGPD	Lei Geral de Proteção de Dados
MCI	Marco Civil da Internet
MP	Medida Provisória
MPDFT	Ministério Público do Distrito Federal e Territórios
MPF/DF	Ministério Público do Distrito Federal
OAB	Ordem dos Advogados do Brasil
OCDE	Organização para a Cooperação e Desenvolvimento Econômico
ONU	Organização das Nações Unidas
PEC	Proposta de Emenda Constitucional

PL	Projeto de Lei
PLC	Projeto Lei da Câmara
PNAD	Pesquisa de Amostra por Domicílio
RG	Registro Geral
Senacon	Secretaria Nacional do Consumidor
SERPRO	Serviço Federal de Processamento de Dados
SMP	Serviço Móvel Pessoal
STF	Supremo Tribunal Federal
STFC	Serviço Telefônico Fixo Comutado
TSE	Tribunal Superior Eleitoral
UE	União Europeia

SUMÁRIO

1 INTRODUÇÃO

No mundo atual, a tecnologia é um dos meios mais utilizados e com maior proporção de dados disponibilizados no mundo todo. Ela surge com a necessidade de adequação do direito, já que novas regras têm que ser criadas, portanto podemos dizer que a tecnologia altera o direito. As mudanças tecnológicas surgem na sociedade, o impacto da inovação tem que ser sentido para que depois se adapte o direito, para que este, por sua vez, regule e dite as regras de um mundo cada vez mais conectado. Essa hiperconectividade, de acordo com Schwab (2018), é o que se denomina de Quarta Revolução Industrial, que causará (e já está causando) inúmeras mudanças na sociedade.

Nessa seara, Doneda (2019, p. 53) afirma que "o desenvolvimento da tecnologia cria relações a serem reguladas pelo direito" e que o direito absorve a tecnologia. Seguindo esse pensamento, Bernard Edelman analisa:

> Se por um lado o direito não julga a ciência, por outro ele não tem dúvidas de que ela existe e de que produz efeitos na ordem jurídica. A biologia revolucionou a visão jurídica do homem e da natureza, a informática, aquela dos direitos de autor e dos direitos de personalidade, a pesquisa nuclear renovou a ideia de soberania e de responsabilidade ... Dito de outra forma, a evolução das ciências e das técnicas não é diferente do direito (DONEDA, 2019, p. 53).

Com isso, conclui-se que o direito evolui juntamente com a ciência e a tecnologia, sendo impulsionado por estas e surgindo como uma estrutura responsável por disciplinar a realização das escolhas da técnica (DONEDA, 2019, p. 64). Nesse sentido, pode-se afirmar:

> A tecnologia, potente e onipresente, propõe questões e exige respostas do jurista. Os reflexos dessa dinâmica são imediatos para o direito, pois esse deve se mostrar apto a responder à novidade proposta pela tecnologia com a reafirmação de seu valor fundamental – a pessoa humana – ao mesmo tempo que fornece a segurança necessária para que haja a previsibilidade e segurança devidas para a viabilidade das estruturas econômicas dentro da tábua axiológica constitucional. O verdadeiro problema não é saber o que o direito deve atuar, mas sim de como interpretar a tecnologia e suas possibilidades em relação a valores presentes no ordenamento jurídico (DONEDA, 2019, p. 64).

A Lei Geral de Proteção de Dados nasceu da própria tecnologia, da necessidade de adequação de novas regras para a atual sociedade da informação. Dessa forma, a LGPD surgiu

da datificação[1] da sociedade. De acordo com Van Dijck (2017), nesse contexto, os dados são "apresentados como matéria-prima que pode ser analisada e processada em algoritmos preditivos sobre o comportamento humano futuro", transformando-se em matéria-prima muito valiosa, graças à hiperconectividade alcançada pelo avanço da tecnologia:

> […] a tecnologia é um dos mais fortes agentes de transformação do mundo moderno. Ela viabiliza novas formas de pensar, de se relacionar, de fazer negócios, de trabalhar, de gerenciar, de comprar, de vender. Essas formas rapidamente se constituem em novos paradigmas, em alguns casos tão superiores aos anteriores que, para as organizações, não resta outra opção a não ser adotá-las (HEHN, 1999, p. 15).

Segundo Silva (2021, p. 72), o estudo dos temas proteção de dados e privacidade é interdisciplinar, e o viés jurídico deve ser olhado através da lente da tecnologia, porque exige do operador do direito conhecimento das mais variadas áreas e reforça a ideia que, além de conscientização, é necessária uma união de esforços multidisciplinares para que seja feita uma aplicação correta da LGPD. Para Augusto Marcacini (2017), a máxima dos estudantes de direito de que estão nessa área para fugir dos estudos matemáticos não pode mais prosperar.

Direito e Tecnologia, à primeira vista, poderiam ser comparados a duas substâncias que jamais se misturam, como água e óleo. O Direito é uma ciência humana, e seus estudiosos, salvo poucas exceções, não costumam – ou ao menos não costumavam – despertar muito interesse pelas ciências exatas. Há até uma velha anedota, costumeiramente contada nas Faculdades de Direito, segundo a qual ao se perguntar ao aluno primeiranista o motivo de ele escolhee o curso, tem-se como resposta: "Porque eu não gosto de matemática".

Na verdade, não há ramo do conhecimento que não possa ser relacionado ao Direito, visto que ele regula a vida em sociedade. Isso significa dizer que cada aspecto do universo humano – a família, a vizinhança, o trabalho, os bens, o comércio e os negócios, a política, a ciência, o avanço tecnológico etc. – merece a sua atenção. Portanto, a Lei Geral de Proteção de Dados (LGPD) não abarca somente as ciências humanas, é uma lei tecnológica que conecta os mais diversos setores e fomenta o desenvolvimento tecnológico e econômico e a inovação.

Contudo, como veremos a seguir, a sociedade atual está estruturada em uma nuvem de dados, e o grande desafio é adequá-la às diversas mudanças tecnológicas simultâneas. É justamente nesse contexto que surge a Lei Geral de Proteção de Dados, aprovada pelo

---

1 A datificação, para Mayer-Schoenberger e Cukier (2013), é a transformação da ação social em dados on-line quantificados, permitindo assim monitoramento em tempo real e análise preditiva.

Congresso Nacional no ano de 2018. Dessa forma, a Lei nº 13.709 visa regular as relações entre direitos humanos e a proteção de dados diante do avanço tecnológico em que vivemos.

A aprovação dessa lei aconteceu após diversos escândalos mundialmente conhecidos acerca de incidentes quanto à segurança da circulação de dados pessoais, tais como: os vazamentos das informações feitos pelo WikiLeaks[2], as revelações de Edward Snowden, as interferências (feitas pela empresa Cambridge Analytica) nas eleições presidenciais estadunidenses de 2016, dentre outros inúmeros episódios de vazamentos de dados e manipulação de comportamento humano que acabaram despertando a sociedade para o fato de que a falta de proteção dos dados pessoais pode assolar a própria democracia.

No Brasil, fatos recentes – após a aprovação da LGPD – ratificam a célere necessidade de que essa legislação seja eficaz. Com ela em vigor, espera-se que fatos como os descritos abaixo deixem de acontecer, ou ao menos aconteçam com menor frequência:

1. A campanha presidencial de 2018 no Brasil, que, supostamente, por meio da coleta do número de telefone de usuários feita pelo WhatsApp, deu margem ao "[…] envio massivo de mensagens, com sistemas automatizados contratados por empresas" para fins de campanhas eleitorais";
2. A campanha antivacina[3] em 2020, que gerou muita desinformação;
3. O megavazamento[4] de dados pessoais noticiado em janeiro de 2021 – já com a Lei vigorando (DIÁRIO, 2021; CARDOSO, 2021; FGV, 2021).

Ao longo dessa pesquisa, analisamos a origem do tema privacidade no direito, uma vez que a sua etimologia é muito antiga, datando de quando o ser humano tomou consciência da sua própria individualidade e da consequente necessidade de ficar só, de ser destacado dos demais indivíduos. Diante disso, a contribuição de nosso trabalho à pesquisa científica deu-se através de um breve levantamento histórico, em que verificamos quando a privacidade aparece pela primeira vez como direito e a partir de quando esse conceito se bifurca, dando origem a outro conceito: proteção de dados pessoais.

---

2 WikiLeaks é uma organização que divulga na internet documentos confidenciais obtidos de empresas e agências governamentais do mundo todo. Segundo a organização, os processos aos quais ela responde têm a ver, principalmente, com o seu papel na divulgação de arquivos secretos de países e corporações.

3 Antivacina: campanha que usa as redes sociais para dar eco a conteúdos falsos e gerar desconfianças sobre as campanhas de vacinação.

4 Megavazamento: dados de mais de 223 milhões de brasileiros foram vazados, contento vários tipos de informações (CPF, benefícios do INSS, endereços, fotos de rosto, escolaridade, entre outros).

A privacidade é entendida como um direito humano universal desde 1948, tendo-se atualmente uma Proposta de Emenda Constitucional (PEC) – nº 17, de 2019 (BRASIL, 2019ª) – tramitando no Congresso Nacional, com o objetivo de declarar a proteção de dados um direito fundamental e alterar o artigo 5º da Constituição da República Federativa do Brasil (1988).

Como já mencionado, o conceito de privacidade difere-se do de dado pessoal, tendo esse último uma interpretação muito mais ampla, não restrita à vida privada: os dados têm que circular, porque cada vez mais são usados como matéria-prima e para moverem a economia de uma maneira ordenada e ética. Diante disso, é necessário que haja o fluxo adequado desses dados, e é justamente isso que a LGPD propõe trazer para o ordenamento jurídico: adequar e ordenar essa enxurrada de dados (FUNDO…, 2020).

Porquanto, o objeto de pesquisa é a autodeterminação informativa, que a LGPD traz como um dos seus fundamentos, que nada mais é que o 'empoderamento' do cidadão frente a esse fluxo desordenado de dados. Essa nova legislação traz regras claras e específicas quanto ao nível de transparência que esses dados deverão ser tratados. Os titulares de dados no caso, a pessoa natural, poderá auto gerir seus dados, essa autogestão aparece como uma extensão a um direito de personalidade, onde o indivíduo passa a ter o controle sobre o fluxo de suas informações.

A *modernidade líquida* (BAUMAN, 2001) traz a autodeterminação informativa quando a atividade incessante de individualização torna-se indissociável nesse contexto:

> A modernidade substitui a determinação heterônoma da posição social pela autodeterminação compulsiva e obrigatória. Isso vale para a 'individualização' por toda a era moderna – para todos os períodos e todos os setores da sociedade (BAUMAN, 2001, p. 41).

O autor afirma que o homem tornou-se um ser emancipado, capaz, a princípio, de gerir sua própria autonomia perante a sociedade – fato este que destaca a pessoa do contexto social e faz com que o processo de individualização seja uma constante, dizendo que a sociedade sempre manteve uma relação ambígua com a autonomia individual:

> 'Sociedade' sempre manteve uma relação ambígua com a autonomia individual: era simultaneamente sua inimiga e condição *sine qua non*. Mas as proporções de ameaças e oportunidades no que forçosamente continuará sendo uma relação ambivalente mudaram radicalmente no curso da história moderna. Embora as razões para examiná-la de perto possam não ter desaparecido, a sociedade é hoje antes de tudo a condição de que os indivíduos precisam muito, e que lhes faz falta - em sua luta vã e frustrante

> para transformar seu status de jure em genuína autonomia e capacidade de autoafirmação (BAUMAN, 2001, p. 37-38).

Segundo Bauman (2001), o velho objetivo da teoria crítica é a emancipação humana, enquanto o atual objetivo é unir a realidade do indivíduo com suas próprias expectativas, o que abre espaço ao debate e à negociação da pessoa que reclama o papel de cidadão em busca da sua autonomia. Diante disso, pode-se constatar que a modernidade, ao exigir das pessoas esse processo constante de individualização, interfere também nas relações interpessoais.

A partir desse debate, o presente texto está organizado da seguinte forma:

O segundo capítulo discute a busca histórica, os ativos econômicos principais em cada época, até chegarmos ao dado pessoal como principal capital ativo na atualidade e como ele está sendo monetizado.

No terceiro capítulo, analisou-se o primeiro aparecimento da privacidade como um direito e como a proteção de dados foi se destacando desse conceito no decorrer do tempo e dos avanços tecnológicos.

No quarto capítulo, por sua vez, abordou-se a Lei 13.709/2018 de maneira geral, os caminhos percorridos até a redação final dessa legislação e como a *General Data Protection Regulation* (GDPR), lei de proteção de dados europeia, serviu de inspiração para a brasileira.

Já o quinto capítulo teve como foco a autodeterminação informativa, conceito que surgiu na Alemanha e se mostra cada vez mais necessário, principalmente pelo fato de o avanço tecnológico estar sempre à frente da atualização normativa, isto é, a tecnologia apresenta demandas sociais que trazem consigo a necessidade de instrumentos regulatórios aptos a lidar com essas novas situações. Isso implica diretamente na gestão de empresas e órgãos públicos, que têm que ser cada vez mais transparentes e acessíveis à sociedade. Portanto, demonstraremos que a LGPD é uma lei principiológica e traz, entre seus fundamentos, a autodeterminação informativa, conceito que apesar de não estar expresso na Constituição Federal, pode ser extraído dela, conforme será defendido.

Por fim, no sexto capítulo, faz-se uma análise da aplicação prática da LGPD e da autodeterminação informativa; além da subsequente conclusão desse trabalho.

1.1 PROBLEMA DE PESQUISA

O problema analisado por nossa pesquisa dá-se através da ascensão tecnológica, que está muito além da atualização normativa. Por este motivo, nosso foco será nos principais fundamentos e princípios da Lei Geral de Proteção de Dados Pessoais, aqueles considerados a 'alma' dessa legislação, pois uma sociedade em 'ebulição' precisa ser edificada sobre princípios sólidos, norteadores dessa evolução vertiginosa causada pela tecnologia. Em outras palavras, seria um esforço inútil construir uma legislação para cada avanço tecnológico atingido, porque se isso ocorrer, será humanamente impossível acompanhar tantas legislações, possivelmente até conflitantes entre si – e aí sim teríamos que nos render ao avanço tecnológico e entregar toda a regulamentação normativa nas mãos da Inteligência Artificial, com algoritmos nos dizendo como agir.

Servimos aqui do exemplo dado por ZUBOFF (2019, p. 270-271): em julho de 2017, o aspirador de pó autônomo da iRobot, o Roomba, ganhou notoriedade não por causa da sua eficiência, mas por causa de sua estratégia de negócios, baseada em dados, a partir da qual supostamente ele estaria negociando a venda de plantas baixas das residências dos seus usuários (mapeamento do local feito pelo próprio aparelho, equipado com um GPS) e mais algumas funcionalidades 'extras' para a sua entrada na concorrência da vigilância, como câmera e novos sensores. Essa negociação fez as ações das empresas dispararem de 35 dólares para 102 dólares por ação. Em resposta às críticas, os proprietários da empresa disseram que os clientes poderiam fazer a opção para que o Roomba não fizesse o mapeamento do local, mas não comunicaram que caso não houvesse a concordância, o robô perderia a maior parte das suas funcionalidades, inclusive sua capacidade de acionar ou pausar a limpeza a distância.

Tal exemplo traz à tona nossa problemática, que se aplica aos seguintes questionamentos:

- *Como fica a gestão dos dados que estão sendo coletados, armazenados e comercializados como uma avalanche desordenada?*
- *Qual a proteção legal que as pessoas têm mediante esse tratamento indiscriminado de seus dados?*
- *O cidadão vai ser capaz de autogerir os seus dados? Quais os mecanismos que a LGPD traz para isso?*

Por isso, a necessidade de regras claras, boa-fé, transparência, respeito aos direitos humanos e principalmente autodeterminação informativa, que capacitará os cidadãos a

exercerem os seus direitos, através dos princípios presentes na Lei 13.709/2018, além dos direitos humanos destacados na CF, como a dignidade da pessoa humana.

1.2 OBJETIVOS

O objeto de nossa pesquisa é a autodeterminação informativa como fundamento da LGPD, em que são investigados quais os níveis de transparência e acesso à educação que os cidadãos terão que possuir para colocar em prática os seus direitos. Nesse caso, para regular o fluxo dos seus próprios dados, a autogestão de dados aparece como extensão da liberdade do indivíduo para ter o controle sobre o fluxo de suas informações.

Acredita-se que os dados pessoais são a força motriz do sistema capitalista atualmente. Isso posto, esta pesquisa analisa a LGPD (Lei 13.709/2018), fundamentando-se na evolução histórica que consagrou a construção dessa cultura até o surgimento das primeiras legislações que apareceram em escala mundial e observando os impactos trazidos por essa lei, assim como demais repercussões dentro e fora do território brasileiro.

Foi investigado que o avanço tecnológico está muito além da atualização normativa, as implicações que essa problemática traz para a sociedade e quais as soluções para se evitar uma enxurrada de novas legislações, posto que a gestão de dados pessoais se torna cada vez mais importante para empresas, órgãos públicos e também para os cidadãos, que deverão ter acesso à informação de maneira clara e acessível, para que possam exercer a sua autodeterminação informativa.

1.2.1 Objetivos específicos

Os objetivos específicos desta pesquisa são:

- Realizar levantamento bibliográfico adequando as temáticas conforme as necessidades da pesquisa;
- Investigar a importância dos direitos de privacidade e da proteção de dados para o desenvolvimento da personalidade humana;
- Apresentar contexto histórico para melhor elucidação da pesquisa;

- Analisar de maneira exploratória a autodeterminação informativa inserida na LGPD.

No decorrer da pesquisa, serão expostas outras análises que consideramos relevantes para complementar nosso estudo.

1.3 METODOLOGIA

Do ponto de vista metodológico, a presente investigação visa fazer um trabalho de método indutivo, pois demonstra como a repetição de certos acontecimentos ao longo da história convergem em uma mesma ideia. Lamy (2011, 164) pontua que o método indutivo está conceituado em "[...] sintetizar uma ideia a partir de uma repetição de situações". A autodeterminação informativa, objeto deste estudo, consolida o seu conceito a partir das situações reiteradas através de sua história, portanto é um tema que ganhou força em decorrência dos anos e com o avanço tecnológico. A escolha da abordagem qualitativa se dá pelo desenvolvimento de procedimentos específicos para a elaboração e análise documental com base em materiais da LGPD (vídeos, leis, reportagens) e de artigos científicos. Como o tema está em construção, o desenvolvimento da pesquisa é feito de uma forma dinâmica, com estudos de caso, já que ainda não se encontra com doutrina formada, jurisprudência e documentos científicos mais amplos.

Isso coaduna com um estudo de natureza exploratória, pois é através da coleta de informação que pode ser feita, de maneira única ou conjunta, a análise dos dados informacionais, permitindo-nos verificar conceitos e/ou variáveis das propriedades e características mais importantes de um tema (SAMPIERI; COLLADO; LUCIO, 2003).

O método indutivo, como já mencionado, foi utilizado na presente pesquisa por ser uma temática que já vem sido discutida no decorrer dos anos, porém no Brasil é um tema relativamente novo, visto que a maior parte da construção deste conhecimento foi realizada durante a situação extraordinária da pandemia do Coronavírus. Portanto, a pesquisa foi feita através de exames de sites e notícias recentes, decisões judiciais proferidas durante a pandemia, verificação de legislação, assim como a análise de artigos científicos, que permitiram as conclusões do presente trabalho.

1.3.1 Procedimentos de coleta: levantamento documental (LGPD)

Para embasamento teórico e complementar, realizamos buscas e coletas de informações sobre a LGPD. Por ser um tema atual, pode-se dizer que a coleta de dados foi contínua, pois decorreu de eventos presenciados durante o estudo, sendo registrados em função dos seus acontecimentos.

Para isso, buscou-se por vídeos de autores renomados que estão atualmente abordando a lei e trazendo debates ao vivo em salas de reuniões através de várias plataformas disponibilizadas na rede (Youtube, Zoom, Meet, ClubHouse, entre outras), instrumentos que foram fundamentais para que a pesquisa fosse viabilizada, tendo em vista que a maior parte dela foi realizada no atual contexto pandêmico.

A coleta de artigos científicos foi realizada por diversas bases de dados, como Google School, Scielo, Scientific Direct etc. Também buscou-se por informações atuais expostas em jornais on-line, como o JusBrasil e ConJur – plataformas da área de direito que expõem diariamente notícias sobre a atualidade, configurando-se como fundamentais para quem é desta área.

Sobretudo, nossa pesquisa fundamentou-se na LGPD (objeto de uma leitura exaustiva), a fim de esclarecer e detalhar como o legislador trouxe o fundamento da autodeterminação informativa como um pilar fundamental para que as pessoas (titulares de dados) possam exercer o controle sobre o fluxo de seus dados e assim resguardar seus direitos fundamentais, como a dignidade da pessoa humana e o desenvolvimento da personalidade. Ademais, baseamo-nos também em leituras de livros que abordam esse tema.

2 BUSCA HISTÓRICA DA PRIVACIDADE À PROTEÇÃO DE DADOS

Diante da rápida maneira com que as relações se transformam atualmente, pode-se dizer que a sociedade está estruturada sobre uma 'nuvem' de dados e que as relações humanas, modeladas pela tecnologia, tornaram-se tão fluídas que esse novo modelo de sociedade marcado pelo rápido avanço tecnológico foi definido pelo autor Zygmunt Bauman como *modernidade líquida*:

> […] a passagem da fase 'sólida' para a 'líquida' – ou seja, para uma condição em que as organizações sociais (estruturas que limitam as escolhas individuais, instituições que asseguram a repetição de rotinas, padrões de comportamento aceitável) não podem mais manter sua forma por muito tempo (nem se espera que o façam), pois se decompõem e se dissolvem mais rápido que o tempo leva para moldá-las e, uma vez reorganizadas, para que se estabeleçam. É pouco provável que essas formas, quer já presentes ou apenas vislumbradas, tenham tempo suficiente para se estabelecer, e elas não podem servir de arcabouços de referência para as ações humanas, assim como para as estratégias existenciais a longo prazo, em razão de sua expectativa de vida curta: com efeito, um expectativa mais curta que o tempo que leva para desenvolver uma estratégia coesa e consistente, e ainda mais curta que o necessário para a realização de um 'projeto de vida' individual (BAUMAN, 2007, p. 07).

O ritmo frenético das mudanças da sociedade atual faz com que as pessoas deixem de acompanhar essas transformações em tempo real. Com isso, se a percepção humana está aquém do avanço tecnológico, a atualização normativa fica prejudicada. Nesse sentido, o maior desafio da atualidade é lidar com tantas mudanças tecnológicas simultâneas e ainda assim manter o ordenamento jurídico atualizado. O ideal é ter uma lei principiológica forte e tecnologicamente neutra, isto é, que não traga conceitos de software, tipo de plataformas, pois a tendência é que fique ultrapassada muito rapidamente.

A história sempre foi uma excelente fonte de dados para se prever o comportamento da humanidade, o que é analisado por Harari (2018):

> Antigamente a terra era o ativo mais importante no mundo, a política era o esforço para controlar a terra, e se muitas terras acabassem se concentrando em poucas mãos – a sociedade se dividia em aristocratas e pessoas comuns.
> Na era moderna, máquinas e fábricas tornaram-se mais importantes que a terra, e os esforços políticos focam-se no controle desses meios de produção. Se um número excessivo de fábricas se concentrasse em poucas mãos – a sociedade se dividiria entre capitalistas e proletários. Contudo, no século XXI, os dados vão suplantar tanto a terra quanto a maquinaria como ativo mais importante, e a política será o esforço para controlar o fluxo de dados. Se os dados se concentrarem em muitas poucas mãos – o gênero humano se dividirá em espécies diferentes (Harari, 2018, p. 107).

Nessa mesma perspectiva, o filósofo Pierre Levy diz que a sociedade passou por três grandes ondas de evolução, sendo a primeira quando o homem aprendeu a plantar (revolução agrícola); já a segunda se deu com a criação da máquina a vapor, que foi a responsável pela transição do modelo feudal para o capitalismo; e a terceira onda, por sua vez, é quando a tecnologia passou a fazer parte da vida das pessoas (MACEDO, 1998).

Bioni (2019) observa que a evolução da sociedade foi marcada por períodos de tempo, com isso a 'moeda de troca' foi se transformando, até se chegar aos dados pessoais como *commodity*. A partir dessa perspectiva, o autor afirma que, durante a sociedade agrícola, a matéria-prima era oriunda da terra e os produtos extraídos dela eram utilizados através do escambo. Após esse período, deu-se a sociedade industrial, em meio à qual produção passou a ser em grande escala e as pessoas que estavam concentradas nas áreas agrícolas começaram a migrar para as cidades, atrás de oportunidades de trabalho nas fábricas. Posteriormente, surgiu a sociedade pós-industrial em que o foco eram os serviços:

> Em um terceiro momento, após a Segunda Guerra Mundial, os serviços angariaram papel de destaque no arranjo socioeconômico. A sociedade - dita sociedade pós-industrial - não se caracterizava mais pelo que se poderia produzir, mas pelo que os serviços poderiam ofertar. A prestação de serviços passava a ser a mola propulsora da economia […] (BIONI, 2019, p. 3).

A economia mundial é cada vez mais movida por dados que circulam nas redes, formando o que o Castells (2013) denominou *sociedade em rede*, que transformou trabalhos e empregos, globalizou o processo de produção de bens e serviços e acabou reorgarnizando essas estruturas em forma de rede, com milhares de nós interconectados e com capacidade de se expandir infinitamente.

Nessa esteira, Harari (2018) diz que se os humanos querem evitar que a concentração de toda riqueza e todo poder fiquem restritos a uma pequena elite, postulando que a solução para esse problema seria a regulamentação da proteção de dados e afirmando que os seres humanos tiveram milhares de anos de experiência de regulação de propriedade de terra, isto é, construir uma cerca em torno de um campo, colocar um portão com cadeado na frente da sua casa. Nos dois séculos passados, defende o autor que as pessoas se tornaram especializadas na regulamentação de propriedade industrial, dando como exemplo que uma pessoa pode comprar ações e ser dono somente de um pedaço de uma grande fábrica, mas questionando como será feita a regulamentação sobre os dados:

> […] não temos experiência em regular a propriedade de dados, que é inerentemente uma tarefa muito difícil, porque ao contrário da terra e de máquinas, os dados estão em toda parte e em parte alguma ao mesmo tempo, podem se movimentar à velocidade da luz e podem ser indefinidamente copiados (HARARI, 2018, p. 9).

Harari (Ibid.) reafirma a importância da regulamentação dos dados, dizendo que pode se tratar da questão política mais importante da nossa era. Muitos outros autores também abordam a problemática sobre como os dados pessoais estão sendo gerenciados hoje como ativo econômico, tal como segue:

> […] a expressão da sociedade da informação define uma nova forma de organização social, política e econômica que recorre ao intensivo uso da tecnologia da informação para coleta, produção, processamento, transmissão e armazenamento de informações. Ressalta a autora, no que parece concordar com o argumento desse estudo, como segunda mudança na modernidade líquida, que esta sociedade da informação contribui no tocante à dinamização de produção capitalista, uma vez que a própria informação assume maior relevância para a geração de riquezas (SAUAIA, 2018, p. 49).

De acordo com o autor Sauaia:

> A era digital traz lume entre proteção da privacidade e eficiência de Mercado. Como Richard Warner notou, "Em geral, as economias de mercado dependem de um fluxo de informações." Wagner afirma que a tecnologia melhorou imensamente a eficiência, criando possibilidade de propagandas direcionadas, as quais, sua visão, beneficiam ambos negociantes e clientes (SAUAIA, 2018, p. 25).

Como visto, a geração de riqueza atualmente está voltada para a coleta e o fluxo de informações, e tornou-se corriqueiro o fornecimento de dados pessoais para as atividades do dia a dia – informações essas que serão revertidas, como o exemplo dado pelo Sauaia sobre o marketing direcionado.

2.1 DADOS PESSOAIS A NOVA *COMMODITY*

Conforme exposto, houve diferentes períodos da história, mas com algo em comum: um ativo econômico central. No primeiro período, foram os produtos agrícolas que eram usados como moeda de troca pela prática do escambo; no decorrer do tempo, novas práticas foram surgindo, até chegar a um momento em que o principal ativo econômico é a informação, ou melhor, são os dados, como em uma frase bem popular que circula na internet há um tempo: "Os dados são o novo petróleo" (THE ECONOMIST…, 2020).

As políticas públicas, e praticamente todos os modelos de negócio, são orientadas e movidas pelo fluxo adequado e organizado de dados pessoais. Trata-se de um novo formato da economia atual, no qual o lucro é obtido por meio das das informações que as próprias pessoas fornecem quando usam as redes sociais e aplicativos. Esse novo modelo de economia transforma a pessoa em produto, já que seus dados são usados para as operações econômicas.

Zuboff nomeia essa relação como *capitalismo de vigilância*, que traz a experiência do usuário como matéria-prima gratuita:

> A indústria digital prospera graças a um princípio quase infantil: extrair dados pessoais e vender aos anunciantes previsões sobre o comportamento dos usuários. No entanto, para que os lucros cresçam, os prognósticos devem ser cada vez mais certos. Para tanto, não é necessário apenas prever: trata-se de modificar em grande escala os comportamentos humanos (ZUBOFF, 2019, [s.p]).

As redes transformaram a economia, e esse novo modelo de sociedade foi denominado com nomes distintos por alguns autores, seja como *sociedade da informação* (CASTELLS, 2013) ou *capitalismo de vigilância* (ZUBOFF, 2015), que dizem que a fonte de riqueza atual são os dados pessoais. A informação se transformou em uma fonte de lucro incessante, pois a cada interação que uma pessoa produz na internet, são gerados novos dados, e isso leva a um questionamento: *Como são as fronteiras nesse mundo virtual'?*

> No centro desta transformação está a afirmação da informação como principal fonte de riqueza ou recurso estratégico na 'sociedade pós-industrial' ou 'sociedade da informação'. Da necessidade de regular a informação, isto é, definir direitos e deveres sobre esse novo recurso, de delimitar o seu exercício, de clarificar as condições em que os novos instrumentos técnicos devem ser utilizados, de defender a sociedade e o indivíduo contra eventuais maus usos da informação, nasceu um campo novo do direto, o Direto da Informação (MIRANDA, 2018, p. 61).

Desse modo, como Miranda (2018, p. 46), já que é notoriamente sabido que os bancos de dados têm fins comerciais, que o desenvolvimento econômico está intimamente ligado ao uso dessas informações. Há, assim, a necessidade de um equilíbrio entre o respeito à privacidade, a autodeterminação informativa e o trânsito adequado dessas informações, ou seja, é necessário que se tenha publicidade e transparência nesse fluxo para que haja segurança jurídica, que exista o tratamento proporcional:

> Porém, apesar de serem benéficos aos indivíduos, os bancos de dados possuem um poder de interferência direta na vida dos cidadãos e com isso detêm uma responsabilidade social maior. Por isso, sua atuação deve-se restringir ao objetivo que

> foi criado, ou seja, que não haja desvio de finalidade da informação que foi coletada e tratada, a qual somente poderá ser transmitida, ainda que de forma onerosa, atendendo os preceitos legais para a qual foi coletada, sendo evidenciado o legítimo interesse. O poder dos dados não se encontra na pura coleta e armazenamento da informação, mas sim em seu tratamento para a geração de novos conhecimentos, ou seja, na análise pormenorizada dos dados coletados que, agregados certos valores e know-how, podem gerar informações que o dado de forma isolada não o faria, conhecido como "dado enriquecido", e assim gerar um perfil cada vez mais preciso da pessoa, de suas opções pessoais e intenções. Se utilizadas de forma devida, essas informações favorecerão as relações jurídicas e a própria pessoa, mas se de forma indevida, poderão resultar em prejuízos (MIRANDA, 2018, p. 47-48).

Esse enriquecimento das informações do qual o autor trata é diretamente ligado à responsabilidade social de quem faz o seu tratamento, para que não haja um desequilíbrio na relação de poder e não ocorra um desvio da finalidade, isto é, o dado deve ser usado somente para atingir o objetivo da sua coleta. Sobre isso, Doneda esclarece:

> O diferencial que a informatização proporcionou ao tratamento de dados pessoais apresenta perfis quantitativo e qualitativo; um baseado na 'força bruta', no poder de processar mais dados em menos tempo, e o outro, na aplicação de técnicas sofisticadas a este processamento de forma a obter resultados mais valiosos. Combinados, representam a base técnica que potencialmente pode ser aplicada a toda coleta de dados pessoais e que deve ser levada em consideração em qualquer enfoque funcional da disciplina de dados pessoais (DONEDA, 2019, p. 151).

Quando tal autor faz referência à mudança qualitativa no tratamento de dados pessoais, refere-se às formas de utilização de novos métodos, algoritmos e técnicas, adicionando ainda, dentro de uma dessas técnicas, a elaboração de perfis de comportamento a partir de informações que as pessoas voluntariamente fornecem ao usar as redes sociais, ou mesmo informações que são coletadas durante o seu uso ou de outros bancos de dados, o conhecido *profiling*.

> [...] os dados pessoais são tratados com o auxílio de métodos estatísticos e de técnicas de inteligência artificial, com o fim de se obter uma "metainformação", que consistiria numa síntese dos hábitos e preferências pessoais e outros registros da vida dessa pessoa. O resultado pode ser utilizado para traçar um quadro das tendências de futuras decisões, comportamentos e destino de uma pessoa ou grupo. A técnica pode ter várias aplicações desde o controle de entrada de pessoas em um determinado país pela alfândega, que selecionaria para um exame acurado as pessoas às quais é atribuída a maior possibilidade de realizar atos contra o interesse nacional, até para finalidades privadas, como o envio de mensagens publicitárias de um produto apenas para os seus potenciais compradores, entre inumeráveis outras" (DONEDA, 2019, p. 151-152).

Isso significa que o avatar de um cidadão pode adquirir mais valor que a sua própria pessoa física. O que a massa de dados indica sobre a personalidade de um determinado cidadão

vai ditar as regras de como ele será tratado, adivinhando qual o seu próximo passo – não se trata de ‘futurologia’, mas sim de cálculos estatísticos feitos por algoritmos.

Pierri Lévy abordou a virtualização da sociedade de uma maneira mais filosófica:

> Um movimento geral de virtualização afeta hoje não apenas a informação e a comunicação, mas também os corpos, o funcionamento econômico, os quadros coletivos da sensibilidade ou o exercício da inteligência. A virtualização atinge mesmo as modalidades do estar junto, a constituição do ‘nós’: comunidades virtuais, empresas virtuais, democracia virtual... Embora a digitalização das mensagens e a extensão do ciberespaço desempenhem um papel capital na mutação em curso, trata-se de uma onda de fundo que ultrapassa amplamente a informatização (LÉVY, 1996, p. 11).

Se a virtualização atinge as modalidades do estar junto, da constituição do ‘nós’, segundo Lévy, como seria compreendida essa grande estratificação dos dados, que ao mesmo tempo consegue transformar em dígitos toda uma comunidade e até mesmo fazer análises preditivas sobre comportamentos futuros dessa massa? *Como fazer o mesmo com um único indivíduo, destacando-o e identificando-o nesse grande volume de dados?*

Hoje, as grandes empresas, como *Facebook*, *Tesla*, *Amazon* e *Google*, extraem essas informações e as alocam no que for mais interessante, através da Inteligência Artificial, refinando-as através da *Machine Learning*, a partir da qual conseguem atingir o resultado desejado. É a partir desses dados recolhidos que os padrões são traçados em conformidade com o tipo de negócio e as decisões serão tomadas para otimização de resultados.

Dessa maneira, é através do *big data* que é possível que as empresas e órgãos públicos coletem os dados em grande quantidade, em diversas fontes e com uma grande rapidez, e, a partir disso, podem identificar os melhores modelos que lhes sejam interessantes para a tomada de decisões de negócios. Nota-se, portanto, que a *performance de big data* é imprescindível para o desenvolvimento da economia de dados.

A partir dessas observações, não restam dúvidas que os dados se tornaram essenciais para o desenvolvimento de políticas públicas e para o progresso da tecnologia, mas, para isso, não basta somente possuir um enorme banco de dados, é necessário extrair desses dados a maior quantidade de informações úteis possíveis.

Esse novo tipo interação serviu de base para a abertura de novos campos em diversas áreas, a sociedade da informação trouxe um novo modelo de negócio: a utilização e a comercialização de dados pessoais.

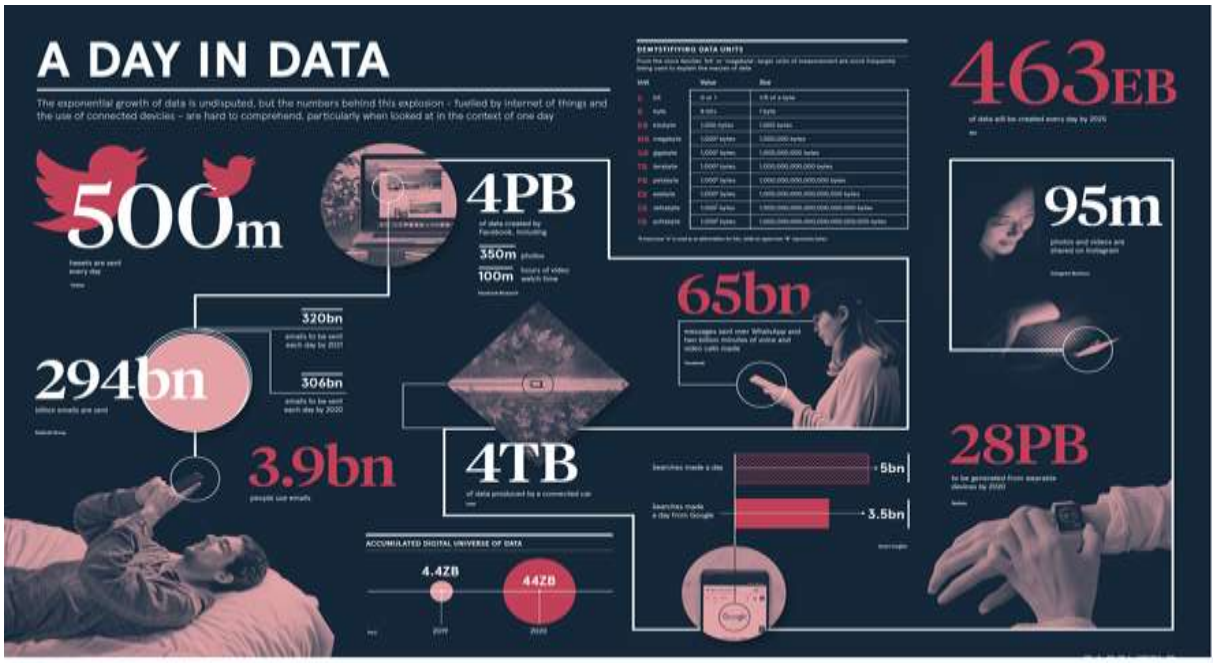
Na edição de 06 de maio de 2017, a revista The Economist trouxe uma matéria intitulada “O recurso mais valioso do mundo não é mais petróleo, mas dados”, dizendo que, há um século, aquele era o principal recurso, mas que atualmente esse objeto mudou, e que grandes empresas, como a *Google*, *Amazon* e o *Facebook*, têm esse tipo de insumo de sobra: os dados, o óleo da era digital (THE ECONOMIST…, 2017).

> Uma NOVA commodity gera uma indústria lucrativa e de rápido crescimento, levando os reguladores antitruste a intervirem para restringir aqueles que controlam seu fluxo. Há um século, o recurso em questão era o petróleo. Agora, preocupações semelhantes estão sendo levantadas pelos gigantes que lidam com dados, o óleo da era digital. Esses titãs - Alphabet (empresa-mãe do Google), Amazon, Apple, Facebook e Microsoft - parecem invencíveis. Eles são as cinco empresas listadas mais valiosas do mundo. Seus lucros estão aumentando: coletivamente, eles acumularam mais de US $ 25 bilhões em lucro líquido no primeiro trimestre de 2017. A Amazon captura metade de todos os dólares gastos online na América. O Google e o Facebook foram responsáveis por quase todo o crescimento da receita em publicidade digital na América no ano passado. Tal domínio fez com que os gigantes da tecnologia fossem desmantelados, como o fez a Standard Oil no início do século XX. Este jornal argumentou contra essa ação drástica no passado. Tamanho por si só não é crime. O sucesso dos gigantes beneficiou os consumidores. Poucos querem viver sem o mecanismo de busca do Google, a entrega de um dia da Amazon ou o feed de notícias do Facebook. Nem essas empresas dão o alarme quando os testes antitruste padrão são aplicados. Longe de enganar os consumidores, muitos de seus serviços são gratuitos (os usuários pagam, na verdade, entregando ainda mais dados) (THE ECONOMIST…, 2017 – Tradução nossa).

O debate sobre proteção de dados engloba principalmente a sua definição, que vai muito além de nome – como Cadastro de Pessoas Físicas (CPF), Registro Geral (RG), endereço e/ou título de eleitor etc. –, porque são todos aqueles dados capazes de levar à identificação de uma pessoa, entre eles os ‘*likes*’ das redes sociais, ‘cookies’, histórico de navegação, enfim, são todos os fragmentos de informação que, quando reunidos, podem tornar uma pessoa identificável; e as pessoas, de uma maneira geral, não fazem ideia de que o conceito de dado pessoal é tão expansivo.

O Fórum Econômico Mundial publicou em seu site um infográfico, produzido pela Raconteur, sobre o volume de dados produzidos em um dia, assim como as perspectivas para o futuro, pois, como visto, se dados produzem poder e riqueza, esse gráfico demonstra a tendência mundial de que todo esse poder e riqueza ficarão concentrados:

Figura 1 - Volumes de dados produzidos em um dia



Abbreviation	Unit	Value	Size (in bytes)
b	bit	0 or 1	1/8 of a byte
B	bytes	8 bits	1 byte
KB	kilobytes	1,000 bytes	1,000 bytes
MB	megabyte	$1{,}000^2$ bytes	1,000,000 bytes
GB	gigabyte	$1{,}000^3$ bytes	1,000,000,000 bytes
TB	terabyte	$1{,}000^4$ bytes	1,000,000,000,000 bytes
PB	petabyte	$1{,}000^5$ bytes	1,000,000,000,000,000 bytes
EB	exabyte	$1{,}000^6$ bytes	1,000,000,000,000,000,000 bytes
ZB	zettabyte	$1{,}000^7$ bytes	1,000,000,000,000,000,000,000 bytes
YB	yottabyte	$1{,}000^8$ bytes	1,000,000,000,000,000,000,000,000 bytes

Fonte: Figura extraída da Raconteur (DESJARDINS, 2019).

O infográfico acima traz unidades de medidas que a maioria dos usuários de internet já ouviram falar, como *kilobytes*, *megabytes*, *gigabytes* e *terabytes*. São medidas correspondentes à quantidade de dados que podem ser enviados ou armazenados em ou através de um dispositivo eletrônico. Acontece que, nos próximos anos, essas unidades de medidas tendem a se multiplicar e, de acordo com o site do Fórum Econômico Mundial (WORLD..., 2021), o universo digital estará cada vez mais presenta na vida da pessoa.

Essas unidades de dados são valores presentes no cotidiano, disponíveis às pessoas comuns. Unidades desse tamanho podem ser grandes o suficiente para quantificar os dados enviados em um anexo de e-mail ou os dados armazenados em um disco rígido, por exemplo. Em 2020, o universo digital bateu a casa dos z*etabytes* – ainda de acordo com o site do Fórum Econômico Mundial –, o que significa que há mais *bytes* existentes do que as estrelas do universo que se pode observar.

Dessa forma, tal cenário aponta para uma questão importante em relação à proteção desses dados: diversas pessoas sequer se dão conta que muitas das informações que o infográfico acima mostra são consideradas dados pessoais – desconhecendo mais ainda o valor econômico que elas possuem.

A *International Data Corporation* – IDC (INTERNATIONAL…, 2020), em maio de 2020, divulgou sua previsão, chamada *Global DataSphere*[5], atualizada, de mais de 59 *zetabytes* de criação e consumo de dados durante o ano e uma taxa de crescimento de dados de 26% até 2024. Essa enorme quantidade – quase o dobro dos dados usados em 2018 – será o suficiente para que os próximos três anos de criação e consumo de dados eclipsem os 30 anos anteriores. Essas projeções estão próximas das estimativas da IDC no final de 2018, que previa 50 zetabytes de uso de dados em 2020 e 175 *zetabytes* de uso de dados até 2025.

> Talvez o mais notável seja o fato de a previsão mostrar um aumento dramático no consumo de dados devido ao boom na atividade de trabalho em casa causado pelo COVID-19. (Este aumento não é compartilhado pela criação de dados, que foi ligeiramente bloqueada pela pandemia.) A IDC espera que a lacuna entre a criação e o consumo de conteúdo aumente nos próximos anos, passando de uma proporção de 1: 9 para uma proporção de 1:10 em 2024. "O crescimento do *Global DataSphere* é impulsionado mais pelos dados que consumimos e analisamos do que pelos que criamos", disse David Reinsel, vice-presidente sênior do programa *Global DataSphere*. Obviamente, os dados devem ser criados antes que possam ser analisados, mas a taxa de recursão dos dados - a taxa em que os mesmos dados são processados novamente - continua a crescer exponencialmente, reduzindo o *DataSphere* 'único' a 10% do *DataSphere* total. A IDC espera que os dados de produtividade se expandam rapidamente, com o uso total de dados corporativos ganhando 4% sobre o uso de dados do consumidor (que fica em torno de 50%). Além disso, o IDC projeta aumentos drásticos nos metadados e nos dados do sensor, ultrapassando potencialmente todos os outros tipos de dados em um futuro próximo. No geral, espera-se que 40% do *DataSphere* seja atribuível aos dados de entretenimento (como o Netflix), com ferramentas de produtividade também impulsionando um aumento no uso de dados de vídeo. Vivemos em um mundo cada vez mais habilitado e assistido por vídeo e consumimos uma quantidade cada vez

5 O Global DataSphere quantifica e analisa os dados criados, capturados e replicados em um determinado ano em todo o mundo. Ele também analisa a quantidade de dados armazenados em várias mídias de armazenamento (HDD, SSD, NVM-NAND, NVM-outro, óptico e fita) no Global StorageSphere. (PECKHAM, 2020).

> maior de vídeos de entretenimento a cada ano - esses são os principais fatores que impulsionam o crescimento da Global DataSphere', disse John Rydning, vice-presidente de pesquisa da *Global DataSphere* programa. 'Ao mesmo tempo, estamos fazendo um uso cada vez mais produtivo dos dados de vídeo que capturamos, o que está contribuindo para o crescimento dos dados de produtividade no DataSphere'(PECKHAM, 2020, [s.p.]).

O infográfico de 2019 aponta números muito altos: 95 milhões de fotos e vídeos são compartilhados por dia no Instagram; 500 milhões de tweets todos os dias; 294 bilhões de e-mails enviados diariamente; 28 *petabytes* são gerados por dia somente com *wearables*, que são as tecnologias que as pessoas literalmente vestem (tecnologias vestíveis[6]), como os *smartwatches*. A tendência é a produção de dados ser cada vez maior, algo que explodiu durante a pandemia do coronavírus e, por causa do avanço da tecnologia e da consequência da facilidade de acesso aos dispositivos eletrônicos, tende a aumentar cada vez mais a inserção de dados pessoais nesse novo modelo de sociedade.

A quantidade de dados com que os próprios titulares dos dados alimentam as plataformas é enorme, e esses mesmos titulares não possuem consciência acerca da importância e do valor disso: quando as pessoas publicam um texto, um vídeo, uma foto ou mesmo interagem nas redes sociais através de *likes*, por exemplo, estão se perpetuando através da rede, porque a internet nunca se esquece: o direito ao esquecimento na rede é precário, pois a natureza desses dados gerados nesse sistema os torna praticamente impossíveis de serem apagados.

As pessoas, de um modo geral, acreditam-se protegidas pelo suposto 'anonimato' que a rede lhes confere e não se atentam ao fato que o anonimato é vedado pela Constituição Federal em seu artigo 5°, inciso IV: "IV – é livre a manifestação do pensamento, sendo vedado o anonimato […]" (BRASIL, 2016, [s. p.]).

Com essa falsa sensação de anonimato ou mesmo de segurança, muitas pessoas, além de espalharem *fake news*, acabam expondo situações pessoais, podendo chegar até a perder o emprego, quando falam mal de seu empregador nas redes sociais, como no artigo trazido a seguir:

> Diante de tal situação surge a indagação; o empregador poderia aplicar a penalidade mais gravosa ao empregado que extrapola os limites em seus comentários em redes sociais, isto é, a demissão por justa causa? A resposta é sim, PODE. A questão aqui é

6 Tecnologias vestíveis são todo e qualquer dispositivo tecnológico que possa ser usado como acessório ou que podemos vestir, é um *wearable* – afinal, essa é a tradução do termo inglês. Dentre eles, os mais populares atualmente são os *smartwatches* e *smartbands*, dispositivos que têm o monitoramento da saúde como seus principais recursos (BOCARD, 2019).

> que o alcance das redes sociais é muito grande e rápido, podendo trazer consequências gravosas para a empresa. O art. 482 da Consolidação das Leis do Trabalho (CLT) traz o rol de hipóteses de dispensa por justa causa: a) ato de improbidade; b) incontinência de conduta ou mau procedimento; c) negociação habitual por conta própria ou alheia sem permissão do empregador, e quando constituir ato de concorrência à empresa para a qual trabalha o empregado, ou for prejudicial ao serviço; d)condenação criminal do empregado, passada em julgado, caso não tenha havido suspensão da execução da pena; e)desídia no desempenho das respectivas funções; f) embriaguez habitual ou em serviço; g) violação de segredo da empresa; h) ato de indisciplina ou de insubordinação; i) abandono de emprego; j) ato lesivo da honra ou da boa fama praticado no serviço contra qualquer pessoa, ou ofensas físicas, nas mesmas condições, salvo em caso de legítima defesa, própria ou de outrem; k) ato lesivo da honra ou da boa fama ou ofensas físicas praticadas contra o empregador e superiores hierárquicos, salvo em caso de legítima defesa, própria ou de outrem; l) prática constante de jogos de azar.
> O que se espera ao contratar um funcionário é que o mesmo siga as normas da empresa, comportando-se de forma ética, seja adepto da moral e dos princípios que a empresa prega (GOES, 2020, [s. p.]).

Esse exemplo é importante porque demonstra claramente a completa falta de informação por parte de uma grande parcela da população, que desconhece até mesmo os seus direitos trabalhistas. *Será que as pessoas estarão aptas para gerir os seus dados pessoais?* Diante desse cenário, a educação digital se mostra cada vez mais importante.

2.2 EDUCAÇÃO DIGITAL E GESTÃO DE BANCO DADOS

Os noticiários trazem sempre uma nova notícia sobre algum vazamento de banco de dados por uma grande empresa. Isso está tão comum que muitas pessoas nem querem saber se existiam dados seus naquela onda de paradeiro incerto. *Mas será que aqueles dados que escoraram não se sabem onde irão se encontrar com mais dados – como os que as pessoas fornecem espontaneamente nas redes sociais ou em suas compras na farmácia –, tornando-se exponencialmente mais valiosos e gerando um tsunami informacional valoroso?*

As leis de proteção de dados são muitos importantes nesse sentido, elas vêm para colocar as rédeas nessa ‘festa dos dados’; é como se fosse uma cartilha de boas maneiras, que deve ser seguida e impõe penalidades se não forem observadas as suas regras. Como exemplo, tem-se o artigo abaixo, que faz um paralelo entre as legislações que abordaremos posteriormente, como a GDPR – que é a legislação de Proteção de Dados da União Europeia (UE) –, e as penalizações que irão ser balanceadas pelas atitudes das empresas. Tal artigo terá um destaque em formato de quadro (*Quadro 1*), pois ressalta-se que, por fazer parte do método

desta pesquisa, a exposição de artigos na íntegra contribui com o desenvolvimento e progresso de nossa investigação:

Quadro 1 - Artigo sobre legislação de Proteção de Dados da União Europeia

Atualmente, notícias sobre vazamento de dados e penalizações às empresas com consequências gravosas têm sido corriqueiras no noticiário e os exemplos abaixo elucidam esta realidade. A empresa Altaba, formada pela venda da Yahoo à Verizon, foi condenada nos Estados Unidos à multa de U$ 35.000.000,00, em razão da Yahoo não ter comunicado o vazamento de dados de ao menos 500 milhões de usuários ainda em 20141, além disso, o referido vazamento gerará indenização estimada em 50 milhões de dólares para cerca de 200 milhões de pessoas, vítimas do vazamento. A comunicação somente ocorreu em 2016. O Banco Inter, réu em Ação Civil Pública proposta pelo Ministério Público do Distrito Federal, por vazar dados pessoais de cerca de 19 mil correntistas, realizou acordo extrajudicial em que arcará com R$ 1.500.000,00 em danos morais destinados a órgãos públicos, que combatem crimes cibernéticos e instituições de caridade. O MPDFT havia entendido que o Banco não teria tomado os cuidados necessários para garantir a segurança dos dados pessoais de seus clientes e não clientes, além disso, inicialmente, o Inter negou o vazamento e se recusou a prestar informações; A UBER, por sua vez, em outubro de 2016 teve dados vazados de 57 milhões de usuários e motoristas em todo o mundo. A empresa demorou um ano para comunicar a respeito do incidente e esta postura já lhe custou um acordo com o governo dos Estados Unidos em U$ 500.000.000,00 e R$ 4,5 milhões a autoridades de proteção de dados da Holanda e Reino Unido3. No Brasil, a UBER é investigada pelo Ministério Público do Distrito Federal e Territórios (MPDFT) a respeito do mesmo vazamento; O Google, recentemente, recebeu multa de 50 milhões de euros por violação a dados pessoais de Autoridade de proteção de dados francesa, com base no GDPR. A Autoridade entendeu que o Google não divulga em seu site com clareza e transparência como as informações dos usuários são utilizadas, por exemplo, informações sobre o processamento de dados não estavam próximas das informações sobre armazenamento de dados pessoais, exigindo que o titular buscasse exaustivamente por tais considerações. Além disso, algumas caixas de texto para coleta de consentimento expresso do usuário já vinham preenchidas, de modo a macular esta base legal para tratamento de dados pessoais; A Senacon (Secretaria Nacional do Consumidor), do Ministério da Justiça e Segurança Pública, instaurou em face do Google Brasil processo administrativo, diante de uma denúncia do Ministério Público Federal do Piauí. O que motivou a instauração do processo foram indícios de análise do conteúdo dos e-mails pessoais, enviados pelo Gmail, sem consentimento expresso do usuário. Todos estes casos poderiam ter tido um desfecho distinto se a postura das empresas tivesse sido outra frente a ocorrência do incidente, conforme podemos averiguar na análise abaixo embasada pela LGPD.

Fonte: Henrique e Andrade (2019)

O quadro acima demonstra que as empresas em maior conformidade com leis de proteção de dados encontram-se em melhores condições para respostas rápidas e eficientes relativas a situações de incidente de segurança de vazamento de dados: as penalidades tendem a diminuir para empresas que têm boas condutas e respostas rápidas mediante este tipo de circunstância. A partir dessa noção, a Tabela 1 apresenta uma análise embasada pela LGPD das empresas que apresentaram violações de dados e suas respectivas conduta.

Tabela 1 - Análise das empresas pela Lei Geral de Proteção de Dados

Empresa	Suposta violação de dados/incidente de segurança	Atuação da autoridade	Conduta esperada/fundamento da LGPD
Altaba	Demora de 2 anos para comunicar vazamento de dados pessoais de 500 milhões de usuários.	Sanção de U$ 35.000.000,00.	A comunicação do incidente à autoridade competente em prazo razoável (art. 48, da LGPD), entendido pelo GDPR como 72 horas (Consideranda 85).
Banco Inter	Vazamento de dados pessoais de 19 mil correntistas. Negativa em prestar informações sobre o ocorrido às autoridades.	Propositura de Ação Civil Pública; e Acordo extrajudicial de R$ 1.500.000,00 a título de danos morais.	Adoção de medidas de segurança adequada para a proteção dos dados pessoais de acessos não autorizados (art. 6º, VII e VIII - princípio da segurança e da prevenção, arts. 46 e ss); e Comunicação da autoridade em prazo razoável (art. 48, da LGPD).
UBER	Demora de um ano para comunicar vazamento de dados pessoais de 57 milhões de usuários.	Autoridade americana: sanção de U$ 500.000.000,00; Autoridades da Holanda e do Reino Unido: sanções somadas em R$ 4,5 milhões; MPDFT: instauração de investigação.	A comunicação do incidente à autoridade competente em prazo razoável (art. 48, da LGPD), entendido pelo GDPR como 72 horas (Consideranda 85).
Google	Não divulgação com clareza e transparência de como os dados dos usuários são utilizados; caixas de texto de consentimento já preenchidas.	50 milhões de Euros.	Atendimento ao princípio da 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 (art. 6º, VI); Coletar consentimento consistente em manifestação livre, informada e inequívoca (art. 5º, XII; art. 7º, I; art. 8º). Caixas de texto preenchidas antecipadamente não revelam consentimento, não revelam manifestação de vontade do titular.
Google Brasil	Acesso não autorizado a conteúdo de e-mail; tratamento de dados sem consentimento expresso (conduta investigada).	Processo administrativo em curso.	Solicitação de consentimento livre, informado, inequívoco e referente à finalidade específica, antes de eventual acesso (art.5º, XII, art.7º, I, art.8º).

Fonte: Tabela extraída do site Migalhas (HENRIQUE; ANDRADE, 2019).

É importante ressaltar que essa preocupação não é nova e as leis protetivas evoluíram bastante no decorrer do tempo, tornando-se cada vez mais cruciais nesse contexto, para impedir ou pelo menos criar obstáculos para evitar que a privacidade do usuário seja usurpada e possa se chegar a um ponto de ferimento a mais um direito fundamental, além da liberdade, da privacidade e do direto ao livre desenvolvimento da personalidade da pessoa natural. As leis de proteção de dados impedem que os dados recolhidos ainda possam ser usados contra o cidadão (por exemplo: um plano de saúde que cruza dados com a farmácia em que seu segurado faz suas compras de medicamentos), assim como cobram responsabilidade das empresas, no sentido de terem um sistema de governança mais transparente e confiável.

Na China, o setor público é extremamente vigilante atualmente, a coleta de dados dos cidadãos é feita de maneira tão intrusiva que pode ser comparada a uma arma de vigilância. O sistema *Quartz* da China é visto por muitos como um sistema de vigilância *orwelliano* (GUIMARÃES, 2019), que identifica e monitora cada indivíduo. A China se caracteriza como o país que mais tem câmeras de vigilância no mundo, fato esse que se agrava, por se tratar de um estado totalitário no qual o governo mantém um dirigismo ideológico sobre a população. Os chineses não têm acesso ao *Facebook* e *Google*, por exemplo; lá só existe uma rede social, com um buscador que é mediado pelo governo, com tem muitos funcionários vigiando todo o tráfego da rede, uma censura para manter a ideologia do governo:

> A China tem sido o usuário de câmeras de vigilância que mais cresce no mundo, uma tendência impulsionada principalmente pelo uso do governo. Na última década, os avanços tecnológicos tornaram essas câmeras instrumentos cada vez mais eficazes para monitorar 1,4 bilhão de pessoas na China. Hoje, o reconhecimento facial e a análise inteligente - tecnologia que sinaliza objetos ou eventos de interesse quando são captados pela câmera - estão se tornando recursos padrão da vigilância por vídeo. O reconhecimento de rostos por câmeras começou a se tornar realidade em 2010, quando pesquisadores fizeram um avanço no algoritmo de aprendizado profundo usado para reconhecimento de voz e imagem. O algoritmo também pode avaliar em tempo real o número e a densidade de pessoas no quadro, o sexo dos indivíduos e as características de roupas e veículos. Comparado a outros países, em que é usado para refinar os sistemas de reconhecimento facial. Além disso, o forte interesse do governo nesta área ajuda a garantir que o setor continue abastecido com amplos recursos para atualização de equipamentos e algoritmos de pesquisa (QIANG, 2019, p. 56 – Tradução da autora).

Ao verificar o exemplo da China, constatamos que a partir do momento que não se tem a liberdade para fazer livres escolhas, o indivíduo está submetido a um estado de vigilância e está ideologicamente submisso. *Mas como está sendo feita a coleta de dados dos cidadãos*

brasileiros? Será a sua realidade muito diferente da China ou de qualquer outro país no mundo?

No início de 2017, a prefeitura de São Paulo anunciou a venda da base de dados dos usuários do sistema público de transporte, conhecido como Bilhete Único (DANTAS, DANTAS, 2017). *Porém, qual a vantagem competitiva que teria uma empresa com posse desses dados?* Através do compartilhamento de dados do Bilhete Único, pode-se averiguar por onde uma grande massa da população passa, qual o seu horário de trabalho e, por conclusão, até o horário que acordam e que vão dormir. A publicidade direcionada a essas pessoas torna-se um negócio muito rentável. De acordo com estudos do site Chupadados, foi constatado o seguinte:

> Dados pessoais: uma viagem com várias paradas e um só destino final. Para fiscalizar o cumprimento dos contratos de concessão, as secretarias de transportes da cidade do Rio (SMTR) e do Estado do Rio de Janeiro (Setrans) recebem relatórios com os dados coletados durante a operação do sistema de bilhetagem. Porém, não há termo legal que deixe claro como os dados do transporte dos cidadãos são utilizados e a quem são transferidos, seja no setor público ou privado (NATUSCH et al., 2020, [s.p.]).

Em 2018, através do Serviço Federal de Processamento de Dados (SERPRO), após três meses de investigação, o Ministério Público do Distrito Federal (MPF/DF) encontrou indícios do uso de base de dados de órgãos públicos pelo site Consulta Pública:

> De acordo com o Ministério Público, o Serviço Federal de Processamento de Dados estaria comercializando a base de dados pessoais dos brasileiros inscritos no Cadastro de Pessoas Físicas (CPF). Por ser uma empresa pública federal, as informações foram encaminhadas na quarta-feira (30/5) ao Ministério Público Federal no DF (MPF/DF) para que seja analisada a legalidade e a moralidade da prática de comercialização dessas informações pela empresa (DELGADO, 2018, [s. p.]).

Ademais, referente ao caso exposto sobre o bilhete único, houve a completa ausência de princípios norteadores que protegessem os direitos dos usuários desse sistema:

> Não há qualquer norma que garanta a segurança e privacidade dos dados pessoais dos passageiros no Rio de Janeiro, diz Flávio Siqueira Junior, advogado especialista em direitos difusos e coletivos. Por ser um serviço público concedido à iniciativa privada, as regras deveriam estar bem claras, para evitar que as empresas tenham uma carta branca para fazer o que quiserem com essas informações (NATUSCH; et. Al., 2020).

Em outro exemplo, Estados se valem de programas para reduzir a sonegação fiscal, como no caso da Nota Fiscal Paulista, um que programa incentiva consumidores a pedirem nota

fiscal em suas compras, informando o seu CPF. Essa foi uma forma muito perspicaz para o governo trazer o cidadão comum como próprio agente fiscalizador. Longe de se despertar na pessoa comum um senso público, o que vem à tona na realidade é a expectativa de, depois de alguns meses, poder resgatar uma pequena parte em dinheiro, referente ao repasse do Imposto sobre Operações relativas à Circulação de Mercadorias e sobre Prestações de Serviços de Transporte Interestadual e Intermunicipal e de Comunicação (ICMS).

Em uma reportagem de 2015, foi abordado o que acontecia na época:

> Dados recolhidos pela Nota Fiscal Paulista podem ser utilizados livremente por empresas varejistas para outros fins que não a apuração dos créditos do programa. Outros órgãos de governo também têm acesso aos dados. A Secretaria da Fazenda do Estado de São Paulo informou a reportagem, via lei de acesso à informação, que não proíbe as empresas de utilizar as informações para outros fins, como compor um histórico de compras, traçar perfis de consumo, ou mesmo revender os dados para terceiros. Estabelecimentos cadastrados no programa não estão submetidos a nenhum tipo de política de privacidade. Quando vamos a uma grande rede varejista, o atendente normalmente faz duas perguntas: se participamos do programa de fidelidade e se queremos a Nota Fiscal Paulista. Se rejeitarmos o programa de fidelidade, mas aceitarmos a Nota Paulista, a rejeição pode não ter efeito prático. Os dados do consumidor podem ainda assim ser recolhidos pela empresa e ele não receberá os benefícios do programa de fidelidade. Isso porque a Secretaria Estadual da Fazenda não tem uma política de privacidade para proteger o consumidor (CARTA..., 2015 [s. p.]).

Em 2013, o Tribunal Superior Eleitoral (TSE) fez um acordo de compartilhamento de dados, mediante a aquisição de certificações digitais:

> Mediante o acordo de cooperação técnica firmado em julho deste ano, o TSE deve fornecer a Serasa dados de cadastro com nomes, datas de nascimento e nome das mães de eleitores em troca do serviço de certificação digital. Ao todo, o acordo prevê o fornecimento das informações de 141 milhões de brasileiros a Serasa, que vende a clientes dados cadastrais e de crédito de consumidores e empresas (BALIARDO, 2013, [s. p.]).

Esses exemplos mostram que no Brasil também acontecem situações que não são em nada diferentes das que acontecem no restante do mundo. O Estado, através dos órgãos públicos, é o maior agente modulador na vida das pessoas comuns. Todas as informações sobre os cidadãos estão contidas nas suas bases de dados, desde o nascimento do indivíduo, suas condições de saúde, suas opções de consumo até a sua certidão de óbito. *O que se pode fazer para cercear o poder desse 'Big Brother' da Sociedade da Informação?*

Sob um ponto de vista mais otimista que o dos exemplos trazidos acima, o Estado também pode atuar melhorando a eficiência das políticas públicas, aproveitando-se da

economia de dados pessoais, para mapear cenários em serviços prestados, como saúde e educação, e, assim, entender como estão sendo desenvolvidas as atividades, a quem está atingindo e onde pode haver uma melhora na prestação do seu serviço.

2.3 PRIVACIDADE E PROTEÇÃO DE DADOS SE TORNAM UM DEBATE GLOBAL

Em 2010, Julian Assange vazou documentos secretos do governo estadunidense e foi categórico ao afirmar que se o Estado tem esse gigantesco tamanho de repositório de dados, ele tem a obrigação de ser transparente sobre a finalidade, o uso e a destinação dessa informação. Ou seja, se o Estado tem um grande poder, ele não poderá pedir por sigilo, porque é o seu dever ser transparente (MÜLLER-MAGUHN et. al., 2013).

As revelações de Assange trouxeram à luz diversos fatos de natureza obscura, como os pedidos da secretária de Estado Hillary Clinton a 33 embaixadas e consulados para que diplomatas espionassem os representantes de muitos países da Organização das Nações Unidas (ONU), documentos que expunham a guerra do Iraque e descreviam até a execução de mulheres e crianças, entre outros vários arquivos escabrosos que fizeram a imprensa e população mundial conhecerem a filosofia de Assange e da comunidade *hacker*: "[…] privacidade para os fracos, transparência para os poderosos […]" e "[…] a informação quer ser livre" (MÜLLER-MAGUHN et. al., 2013, p. 11-12).

Glenn Greenwald, em sua apresentação do TED Talks, "Why Privacy Matters*"*, exibida em 2014, faz uma comparação da privacidade com aqueles vídeos que as pessoas postam aos montes nas suas redes sociais mostrando algum indivíduo que, pensando estar sozinho, começa a agir de forma expressiva, cantando fervorosamente, dançando, rodopiando; e aí essa pessoa descobre que não está sozinha, que há alguém observando escondido e gravando a cena, o que faz com que o indivíduo pare imediatamente de fazer o que estava fazendo, apavorado (GREENWALD, 2014a). A sensação de vergonha e humilhação fica impressa em seu rosto instantaneamente – o que aquela pessoa estava fazendo somente seria feito se ninguém estivesse a observando.

Com essa afirmação, Greenwald levanta a questão: por que a privacidade é tão importante? Essa foi uma questão que surgiu num contexto de debate global (GREENWALD, 2014), em razão das revelações feitas por Edward Snowden de que os Estados Unidos e seus parceiros, sem o conhecimento de todo o restante do mundo, transformaram a internet, antes

conhecida como uma ferramenta ímpar de liberdade e democracia, em uma zona de vigilância em massa indiscriminada sem precedentes.

É importante notar que Greenwald afirma que o sentimento que surge desse debate é o da dualidade, no sentido que faz parecer que o mundo está dividido em apenas dois polos: o bloco das pessoas más e o bloco das pessoa boas. Essa polarização se dá pelo fato de que, aparentemente, quem se preocuparia com a privacidade seriam as pessoas más, partindo-se do princípio que somente as pessoas que tramam ataques terroristas ou premeditam os mais diversos crimes nesse universo online seriam aquelas preocupadas em esconder alguma coisa; enquanto as pessoas 'boas' seriam aquelas que vão para o trabalho, voltam para casa, cuidam dos seus filhos, assistem à TV e não usam a internet para tramar ataques à bomba, mas para ler notícias e planejar as atividades esportivas dos seus filhos, isto é, pessoas que não teriam nenhuma razão para se importar com o monitoramento feito pelo governo. Na realidade, parte-se da premissa que caso se importassem com essa intromissão, estariam tendo um atitude de autodepreciação, mas a realidade é inversa, quando concordam pacificamente com isso é que se desabonam, e, logo, seria como afirmar o seguinte: "Concordei em me tornar uma pessoa tão inofensiva, inocente e sem graça que, na verdade, não tenho medo do que o governo saiba o que eu faço".

Esse comportamento deriva de uma mentalidade que pode ser traduzida através de um comentário de Eric Smith, CEO da Google em 2009 que, questionado sobre as frequentes invasões de privacidade de milhões de usuários através da plataforma Google, disse: "Se estiver fazendo algo que não quer que os outros saibam, talvez nem devesse fazer, em primeiro lugar" (GREENWALD, Ibid.). Greenwald afirma que pessoas com esse tipo de discurso não acreditam nisso e tomam várias precauções para proteger a sua privacidade, como usar senhas nas redes sociais e nos seus e-mails, cercando ainda muito bem a sua propriedade privada para que ninguém invada ou enxergue o seu interior.

Geralmente esse tipo de falácia surge principalmente de pessoas que estão no controle de companhias que impactam seriamente a privacidade de milhões de pessoas ao redor do mundo, o que pode ser notado nas atitudes de Mark Zuckerberg, que, em 2010, anunciou que "privacidade não era mais uma norma social" e, em 2013, ao comprar a sua mansão em Palo Alto, também comprou as casas vizinhas por um total de 30 milhões de dólares para que sua 'zona de privacidade' ficasse garantida (ANDRADE, 2021).

Este último exemplo também se correlaciona à segurança, mas daremos aqui outro exemplo: *quem ao usar um banheiro público, deixa a porta aberta?* As pessoas que negam a importância da privacidade praticam atos no cotidiano que não correspondem com o próprio discurso, demonstrando que necessitam do 'direito de estar só', mesmo que instintivamente.

A privacidade é um direito fundamental, que se relaciona diretamente com a garantia do livre desenvolvimento da personalidade; os humanos são seres sociais, portanto o mundo exterior reflete no seu mundo interno, e é certo que, nesse cenário, em um contexto de mundo conectado e de redes sociais, a personalidade do indivíduo sofre mutações constantes.

Ademais, por serem seres sociais, as pessoas têm a necessidade de compartilhar suas aflições e vitórias, fato que, segundo Glennwald, é o que motiva tantas publicações voluntárias de informações pessoais nas redes sociais. A exposição extrema pode ser entendida como uma abdicação da própria privacidade, já que atualmente o modelo de sucesso pessoal é ter vários 'seguidores' nas redes sociais. Sobre isso, Bauman afirma:

> Numa surpreendente inversão dos hábitos dos nossos ancestrais perdemos de certa forma boa parte da coragem, energia e vontade para persistir na defesa da "esfera do privado". Nos nossos dias, não é tanto a possibilidade de traição ou violação da privacidade que nos assusta, mas seu oposto: fechar todas as saídas do mundo privado, fazer dele uma prisão, uma cela solitária ou uma masmorra do tipo em que antigamente desapareciam as pessoas que perdiam as boas graças do soberano, abandonadas no vácuo da despreocupação e do esquecimento públicos – o dono desse "espaço privado" é condenado a sofrer para sempre as consequências de suas ações (BAUMAN, 2010, p. 27).

Segundo Bauman (2010), essa 'condenação' gera grande sofrimento às pessoas que anseiam por alguém que esteja disposto a "arrancar à força" os seus segredos, afirmando que o maior pesadelo para as pessoas na atualidade é cair no esquecimento, o que significa não ter visibilidade nas redes sociais:

> A falta de ouvintes ansiosos para arrancar à força nossos segredos – ou rasgá-los e surrupiá-los de dentro das muralhas da privacidade, para exibi-los publicamente como propriedade de todos, e incentivar as pessoas a desejar compartilhá-los – talvez seja o maior pesadelo para nossos contemporâneos. "Ser uma celebridade" (quer dizer, estar constantemente exposto aos olhos do público, sem ter necessidade nem direito ao sigilo privado) é hoje o modelo de sucesso mais difundido e mais popular (BAUMAN, 2010, p. 27).

O modelo de sucesso descrito por Bauman não é novo, pode ser encontrado bem antes do surgimento das redes sociais. Segundo Costa Júnior, o fato de as pessoas se sentirem espionadas faz surgir nelas um sentimento de que são importantes de alguma forma:

> É que a civilização da técnica, identificando o homem com a sua função social, transformando-o em insignificante peça da complexa engrenagem industrial, nêle inculca sentimentos de desvalorização. Êle se sente esmagado pelo anonimato, pela diluição de sua individualidade nas grandes concentrações urbanas da era industrial tecnológica, de sorte que a exposição de sua vida à curiosidade e contrôle alheios resulta, paradoxalmente, na superação de sua mediocridade: ser espionado é, de algum modo, ser importante. Êste sentimento a tal ponto foi difundido e prestigiado pela filosofia tecnológica que, nos tempos vertentes, a vida privada, a solidão, é interpretada como um prazer vicioso, índice de excentricidade, sintoma de marginalização e mediocridade (COSTA JÚNIOR, 1970, p. 16).

Além disso, o autor ainda afirma:

> De acordo com esse contexto, as redes sociais significam a liberdade de expressão e a manifestação do pensamento, mas podem também servir de instrumento para a abdicação da privacidade, que pode prejudicar outros direitos fundamentais, como o da dignidade humana e o desenvolvimento da pessoa humana (COSTA JÚNIOR, 1970, p. 16).

Para Glennwald, todas as pessoas têm algo a esconder, seja em maior ou menor grau – pode se tratar de planos de um terrorista ou de um diário de uma adolescente. Assim, o modelo de extrema exposição é um fato que fere diretamente a privacidade e o desenvolvimento da pessoa, sendo essencial que o indivíduo tenha um lugar para ir, onde possa estar livre dos olhares de julgamento dos outros, consiga se destacar da massa crítica, compreenda a si mesmo e, diante dessa percepção, execute os seus direitos de liberdade.

A todo momento, as pessoas ponderam sua fala e seus atos, razão pela qual a privacidade é tão desejada universalmente. Segundo Greenwald, não se trata apenas de uma necessidade básica, pois atualmente existem situações nas quais as pessoas podem ser monitoradas e observadas; e quando elas têm a consciência desse fato, o seu comportamento muda radicalmente. Nesse sentido, temos:

> A proteção **à privacidade** está **relacionada diretamente** ao **livre desenvolvimento da personalidade** humana, na medida em que é necessário garantir ao indivíduo que ele não seja submetido a qualquer forma de controle social que tenderia a anular a sua individualidade e cercear a sua autonomia privada (MAURMO, 2012 – grifo nosso).

Há dezenas de estudos de psicologia que provam que quando uma pessoa sabe da possibilidade de estar sendo observada, demonstra um comportamento muito mais conformista e submisso. A vergonha humana é um fator motivador muito poderoso, bem como o desejo de evitá-la. É por isso que as pessoas, quando estão sendo observadas, tomam decisões que não são produtos de sua própria vontade, mas que têm a ver com que os outros esperam delas, ou com aquilo que a tradição social determina.

Essa percepção foi usada mais poderosamente, com fins pragmáticos, por Jeremy Bentham, filósofo do século 18 que buscou resolver um problema importante trazido pela era industrial. Pela primeira vez, as instituições haviam se tornado tão grandes e centralizadas, que não conseguiam mais monitorar e, consequentemente, controlar cada um dos seus membros individualmente. A solução que criada por ele foi um design estrutural, originalmente gerado para ser usado em prisões, ao que ele chamou de *panóptico*. Sua principal característica era uma enorme torre, construída no centro da instituição, de onde quem a controlasse pudesse observar qualquer interno, a qualquer momento, embora não pudesse observar todos o tempo todo.

A essência desse design estava no fato de que os internos não podiam ver o interior do panóptico, o interior da torre. Assim, eles nunca sabiam se estavam sendo observados, nem quando. O que deixou Bentham tão empolgado com essa descoberta é que ela significava que os prisioneiros teriam de presumir que estavam sendo observados a todo instante, o que seria a tentativa máxima de impor obediência e submissão.

Michel Foucault, filósofo do século XX, percebeu que o modelo poderia ser usado não somente em prisões, mas em qualquer instituição que quisesse controlar o comportamento humano: escolas, hospitais, fábricas, ambientes de trabalho etc. Para ele que a estrutura/mentalidade gerada por Bentham era o principal meio de controle social das sociedades modernas ocidentais, que não precisam mais das armas ostensivas da tirania, punições, prisões ou morte de dissidentes ou forçar legalmente a lealdade de um determinado grupo, porque a vigilância em massa cria uma prisão mental, que é uma forma muito mais sutil, porém muito mais eficaz, de promover submissão a normas sociais ou à tradição social, muito mais eficiente do que a força bruta.

Dentro desse contexto, o romance “1984”, de George Orwell, também traz esse debate sobre privacidade vs. vigilância, com uma advertência principal: não é necessário monitorar as pessoas o tempo todo, só o fato de conhecerem a possibilidade do monitoramento já surtia o efeito desejado.

> Não havia, é claro, uma forma de saber se alguém estava sendo assistido em qualquer dado momento. Com que frequência a Polícia do Pensar sintonizava em qualquer rede individual era apenas especulação. Era até mesmo concebível que assistissem todo mundo o tempo inteiro. Mas, de qualquer forma, eles poderiam sintonizar na sua rede quando quiser. A pessoa tinha que viver – de fato vivia, um hábito que se tornava instinto- com o pressuposto de que todos os sons que fazia eram entreouvidos (ORWELL, 2021, p. 8).

Esse tipo de "observador" também se faz presente nas religiões abraâmicas, que postulam a existência de uma autoridade invisível, que é onisciente e, justamente por isso, sempre observa tudo o que as pessoas fazem, o que significa que elas nunca têm um momento de privacidade – a tentativa máxima de imposição à obediência a suas ordens. O que todas essas obras aparentemente diferentes reconhecem, a conclusão a que todas chegam, é a de que uma sociedade em que as pessoas podem ser monitoradas o tempo todo é uma sociedade que alimenta a passividade, a obediência e a submissão – razão pela qual todo tirano, do mais declarado ao mais sutil, deseja esse sistema (GRENNWALD, 2014).

Com isso, é possível concluir que em uma sociedade na qual as pessoas estão sujeitas a um monitoramento constante, a essência da liberdade é prejudicada – a criatividade, por exemplo, depende da existência da divergência de opiniões e principalmente da liberdade de expressão. Gera-se ainda a ideia de que somente pessoas incorretas teriam algo a esconder, de que a privacidade seria importante somente para ocultar algo ilícito – fato este que transformaria as pessoas que aceitam essa realidade em seres totalmente inofensivos e desprovidos de poder político, pois o sistema de vigilância não teria interesse em 'vigiar' pessoas que se encaixam nessa categoria; assim, somente os dissidentes, aqueles que desafiam o poder, teriam que se preocupar. O de sistema de vigilância em massa inibe, dessa forma, o próprio desenvolvimento da pessoa, visto que ele pode tornar diversos tipos de comportamento "proibidos" sem a pessoa perceber que isso aconteceu.

Rosa Luxemburg, renomada ativista social, disse uma vez: 'Quem não se move não se dá conta que tem correntes' (GREENWALD, 2014, [s.p.]). As correntes da vigilância em massa são invisíveis ou indetectáveis, mas as restrições que ela nos impõe não deixam de ser poderosas , afetando diretamente a proteção à privacidade e aos dados pessoais, assim como a dignidade da pessoa humana, prejudicando o seu livre desenvolvimento.

O mundo está cada vez mais conectado, e a pandemia do coronavírus causou um grande impacto nesse ambiente virtual. As pessoas deixaram seus escritórios e passaram a

trabalhar remotamente, as aulas presenciais passaram a ser virtuais, a transformação digital que estava em curso transformou-se em realidade de uma hora para a outra. A necessidade de adaptação acelerou o processo e fez as pessoas passarem a maior parte dos seus dias no ambiente virtual. Desse modo, fazem-se indispensáveis a transparência e o acesso à educação para que as pessoas tenham conhecimento e exerçam a sua autodeterminação informativa. Assim, a LGPD seria aplicável na prática, e elas mesmas seriam os próprios agentes fiscalizadores, impedindo os fatos de vigilância como os expostos nas revelações de Edward Snowden.

> Sobretudo para as gerações mais jovens, a grande rede não é um universo isolado, separado, no qual são realizadas algumas das funções da vida. A internet não é apenas nosso correio e nosso telefone. Ela é totalidade do nosso mundo, o lugar onde quase tudo acontece. É lá que se faz amigos, se escolhe livros e filmes, se organiza o ativismo político, e é lá que são criados e armazenados os dados mais particulares de cada um. É na internet que desenvolvemos e expressamos nossa personalidade e individualidade (GREENWALD, 2014, [s.p.]).

Como visto, as pessoas estão cada vez mais conectadas, e a preocupação com a vigilância extrema que esse ambiente proporciona é real e fonte de muitas inquietações, posto que grandes corporações são detentoras de muitos dados e concentram um alto poder de vigilância sobre os indivíduos, usando disso para moldar e produzir comportamentos individuais, como ocorreu nas eleições estadunidenses de 2016, com o escândalo do Cambridge Analytica[7]:

> Explora então a proposta de que o *big data* é, acima de tudo, o componente fundamental de uma nova lógica de acumulação, profundamente intencional e com importantes consequências, que chamo de capitalismo de vigilância. Essa nova forma de capitalismo de informação procura prever e modificar o comportamento humano como meio de produzir receitas e controle de mercado. O capitalismo de vigilância se formou gradualmente durante a última década, incorporando novas políticas e relações sociais que ainda não haviam sido bem delineadas ou teorizadas. Mesmo que o *big data* possa ser configurado para outros usos, estes não apagam suas origens em um projeto de extração fundado na indiferença formal em relação às populações que

---

7 Escândalo do Cambridge Analytica: tal empresa, através da coleta de dados individuais do Facebook, "transformou cliques em votos" (LAPOWSKY, 2018). Assim, algumas questões foram levantadas após o advento da associação do Facebook e da Cambridge Analytica, questionamentos esses direcionados principalmente a legalidade das ações de ambas as corporações. Durante muitos anos, o acesso de dados dos amigos de um usuário era permitido pelos termos de uso do Facebook. Esta foi uma brecha explorada pela Cambridge Analytica no contexto do Brexit, por exemplo. Nesse aspecto, para Debord (1968), o indivíduo moderno é um espectador e um consumista dos produtos e notícias, vivendo em uma submissão alienante ao império da mídia (ANASTASIA; LARA, 2019).

> conformam tanto sua fonte de dados quanto seus alvos finais (BRUNO et. al., 2018, p. 18).

Aqui, torna-se relevante a análise de Zuboff (2015), que reforça o modelo da evolução histórica do modelo de capitalismo:

> Cada época da história do capitalismo rumou em direção a uma lógica de acumulação dominante - o capitalismo corporativo baseado na produção em massa do século XX se transformou em capitalismo financeiro no fim do século, uma forma que persiste até hoje. Isso nos ajuda a compreender por que há tão pouca diferenciação competitiva real entre as indústrias. Companhias aéreas, por exemplo, possuem imensos fluxos de informação que são interpretados em linhas mais ou menos similares, com objetivos e métricas semelhantes, já que as companhias são todas avaliadas de acordo com os termos de uma lógica compartilhada de acumulação. O mesmo poderia ser dito em relação a bancos, hospitais, empresas de telecomunicações e muitas outras.
> O sucesso do capitalismo ao longo do tempo dependeu da emergência de novas formas de mercado que expressassem novas lógicas de acumulação mais bem-sucedidas na tarefa de satisfazer as necessidades sempre em evolução das populações e sua expressão na natureza cambiante da demanda (ZUBOFF, 2015, p. 22).

Nessa nova dinâmica da sociedade, a LGPD é de extrema importância e, conforme o professor Bruno Bioni em suas aulas, tem que ser vista como um novo contrato social, porque quem não controla os seus dados pessoais nesse atual contexto não tem controle sobre si mesmo, uma vez que as pessoas são julgadas de acordo com o que os seus dados dizem sobre elas: decisões estão sendo tomadas sobre esses indivíduos, e o principal elemento para a tomada dessa decisão é o que os dados dizem sobre eles. Quando uma pessoa for pedir um crédito no banco, não é o gerente que vai decidir se vai liberar o valor solicitado ou não, a decisão partirá do que um conjunto de dados. A participação social dos sujeitos está cada vez mais subordinada aos relatórios pessoais produzidos pelos algoritmos.

> Essa nova forma de organização social foi sedimentada em razão da evolução tecnológica recente, que criou mecanismos capazes de processar e transmitir informações em uma quantidade e velocidade jamais imaginável. Os relacionamentos sociais foram energizados por um fluxo informacional que não encontra mais obstáculos físicos distanciais. Há uma nova compreensão (mais abreviada) da relação entre tempo-espaço, o que outrora acarretava maior cadência às interações sociais […] Por isso, a informação avoca um papel central e adjetivante da sociedade: sociedade da informação. A informação é o (novo) elemento estruturante que (re)organiza a sociedade, tal como fizeram a terra, as máquinas à vapor e a eletricidade, bem como os serviços, respectivamente, nas sociedades agrícola, industrial e pós-industrial (BIONI, 2019, p. 4-6).

Atualmente, quando uma pessoa se utiliza de um serviço de busca gratuitamente na internet, os seus dados estão pagando por aquele serviço, já que empresas compram o espaço

para oferecer produtos que se encaixem no perfil das pessoas de acordo com o que os dados dizem a seu respeito.

Por ser um tema ‘relativamente’ novo, há muitas discussões; e ainda não foi atingido um nível elevado de maturidade, posto que esses grandes volumes de dados são a engrenagem que move muitas grandes empresas. Com a Lei Geral de Proteção de Dados em vigor no Brasil, essas empresas terão que rever essa dinâmica, visto que a finalidade do tratamento tem que ser específica, as empresas não podem mais sair por aí vendendo bancos de dados indiscriminadamente.

Nesse contexto, diante da amplitude desse fluxo de dados, a fiscalização se torna precarizada: *como as empresas estão monetizando esses dados? Como os órgãos públicos estão lidando com tantas informações cruzadas?*

Uma forma atual de monetização do que os dados afirmam em relação às pessoas é o *Real Time Bidding* (MARSHALL, 2014), ou, em português, “lance em tempo real”. Quando um anúncio (aquele que a pessoa recebe no canto da página) é carregado no navegador da web de um usuário – por exemplo, no Brasil, o navegador mais usado é o Google Chrome –, para aparecer ali, para aquela pessoa específica, houve um processo de filtragem, praticamente uma licitação; e o anunciante que pagou o preço mais alto teve a oportunidade de oferecer o seu produto ao indivíduo do outro lado da tela. O tempo dessa operação é praticamente instantânea, levando alguns milissegundos. Determinadas lojas de *e-commerce* podem identificar quanto tempo o usuário passou olhando uma camiseta, por exemplo, e isso, quando analisado através de estatísticas, pode identificar um usuário mais propenso a adquirir este produto, o que possibilita à empresa que oferece a camiseta dar um lance maior para que o item apareça como propaganda na janela do navegador daquele usuário, já que há indicação que essa pessoa tem maior probabilidade de comprá-lo – e isso tudo acontece em tempo real.

Trata-se de um modelo de negócio eficiente para os anunciantes, tendo em vista que é feita uma ponte direta entre a empresa e o consumidor. Antes, se uma empresa quisesse anunciar os seus produtos para pessoas que gostam de corrida, ela teria que comprar espaços em algum site relacionado a esse tipo de esporte. Com esse novo modelo de marketing, as empresas anunciantes não precisam mais dessa “velha” prática, já que podem usar a tecnologia para acessar um vasto número de banco de dados e escolher com muita precisão uma determinada pessoa, o que reduz o tempo e minimiza a oferta de produtos para pessoas não interessadas em adquiri-los.

Atualmente, o ciclo menstrual de uma mulher pode render mais que ouro. Existem inúmeros aplicativos que são muito práticos e de grande utilidade para as mulheres, mas o que faz esses aplicativos valerem tanto é exatamente a coleta de informações que as mulheres depositam nesses aplicativos. Felizi e Varon (2020) afirmam que esses são um dos aplicativos mais populares na categoria 'aplicativos de saúde' e que não só são um instrumento de autoconhecimento para as mulheres, mas também um negócio muito rentável e promissor para as empresas que usam essa técnica, pois elas recolhem informações íntimas e podem compartilhá-las de acordo com os seus interesses.

A primeira observação feita pelas pesquisadoras foi que esses aplicativos se sustentam na produção e análise de dados para viabilizar anúncios publicitários direcionados a compartilhar tais informações com outras empresas e institutos de pesquisa, ou mesmo vender produtos que se encaixariam no perfil dessas mulheres, como absorventes, termômetros para indicar fertilidade, entre outros. Contudo, ao analisarem a política de privacidade de alguns dos aplicativos, as referidas autoras perceberam que, apesar de as empresas afirmarem que os dados compartilhados seriam anonimizados, também seria possível que as corporações, que compraram informações dos seus bancos de dados pudessem fazer o marketing direcionado, como no caso do *Real Time Bidding*.

Exemplos como esse levantam questões: se as empresas que fazem a coleta de tantos dados teriam legitimidade para estar realizando essa coleta, ou mesmo se há transparência e segurança para garantir que a finalidade dessa captura não seja desviada.

Além do marketing direcionado, tem-se as *câmaras de eco*, termo cunhado pelo pesquisador da *Harvard Law School* Cass R. Sunstein, que diz que a configuração algorítmica das redes sociais faz com que as pessoas não vejam opiniões diferentes. Os algoritmos das redes sociais são projetados para que as pessoas passem mais tempo possível conectadas a ela; e para que a sua navegação seja agradável, é necessário que se tenha acesso apenas a um conteúdo satisfatório e a publicidade seja direcionada somente a produtos aos quais se tenha interesse. Isso faz com que as pessoas, ao invés de encontrarem uma grande diversidade de expressões de pensamento, ouçam só a reverberação da sua própria voz. Essa aglutinação de opiniões similares faz com que os acontecimentos tomem uma proporção maior do que na realidade, "viralizando" os conteúdos na rede (QUATTROCIOCCHI et. al., 2020).

Todas as grandes plataformas têm informações sobre os seus usuários, conseguindo produzir essas segmentações de maneira muito direcionada, pois o intuito é deixar o usuário

mais tempo ‘preso’ à rede. Grande parte do investimento das campanhas de mídia na internet está vinculada a esse aspecto: para alcançar o seu público-alvo, utilizam-se do método *analytics*, isto é, são análises de dados da web que informam o fluxo e determinado padrão de usuários, em outras palavras, são observados o que qualifica essa audiência e quais os grupos de pessoas que consomem, assistem e interagem em determinados conteúdos. Tal serviço é vendido, como visto no caso do *Real Time Bidding*; e seu valor é agregado de acordo com o seu poder de alcance – algo que a mídia não conseguia fazer antes dessa tecnologia.

A partir da vigência da LGPD, essas mesmas plataformas que monetizam indiscriminadamente os dados de seus usuários (fazendo grandes fortunas) terão que alterar sua política. Isso porque o tratamento de dados posterior à finalidade primeira para a qual eles foram coletados não poderá ser realizado para modalidades diversas, como a venda para publicidade direcionada, salvo algumas ressalvas previstas pela própria lei, entre elas: o *legítimo interesse*, que será analisado no terceiro capítulo.

As relações entre essas plataformas e os usuários terão de ser mais transparentes e imbuídas de boa-fé. As empresas e órgãos públicos que lidam com dados estão tendo que reinventar e colocar limites no uso dos seus bancos de dados.

Por isso, ressalta-se, mais uma vez, a importância desse sistema regulatório, que vai nortear essas relações jurídicas de uma sociedade que tem a informação como mola propulsora da economia.

3 EVOLUÇÃO HISTÓRICA DA PRIVACIDADE A PROTEÇÃO DE DADOS

O avanço tecnológico trouxe a possibilidade de fatos e pessoas estarem espalhadas pela mídia, seja em folhetins ou em redes sociais. Com isso, o direito à privacidade foi se incorporando à nossa cultura.

A primeira vez que o tema 'privacidade' aparece como um direito foi justamente por causa de um dispositivo mecânico, a câmera fotográfica Kodak nº 1 (KLEINA, 2017), que facilitou muito a realização fotos, pois era portátil e leve, ao contrário das existentes na época, muito mais pesadas e,por isso, difícil de serem transportadas de um local para o outro. Com a facilidade para se tirar fotos, a partir de um instrumento leve e de fácil manuseio, surgiram os *paparazzis*. A partir daí, as pessoas que eram visadas por esses profissionais perderam o direito ao esquecimento[8], passando a ter os seus atos capturados para a posteridade.

> Invenções recentes e métodos de negócios chamam a atenção para o próximo passo que deve ser dado para a proteção da pessoa […] e numerosos dispositivos mecânicos ameaçam fazer boas previsões de que o que é sussurrando no armário deve ser proclamado dos telhados das casas (WARREN; BRANDEIS, 2007).

A frase acima é de um trecho do documento *The Right to Privacy* (O Direito à Privacidade), de 1890, de autoria de dois juristas norte-americanos Warren e Brandeis, no qual a privacidade aparece pela primeira vez como um direito – por causa da divulgação de fotos não autorizadas – para tutelar o direito à privacidade devido ao avanço da tecnologia. No caso, o surgimento da câmera fotográfica portátil trouxe a privacidade como o '*the right to be alone*', que significa 'o direito de ser deixado só', em que o indivíduo tem direito a ser destacado da sociedade, a ter a sua própria individualidade.

Doneda (2019, p. 102) postula que o vocábulo 'privacidade' deriva do verbo *privare*, de raiz latina, tendo como sua forma adjetiva a palavra '*privatus*'. Hoje, é amplamente utilizado na língua inglesa o termo *privacy*, que não teve paralelo como o idioma latino, mesmo porque no século XVI a língua já utilizava amplamente esse termo, sendo utilizada mais de uma vez pelo próprio Shakespeare.

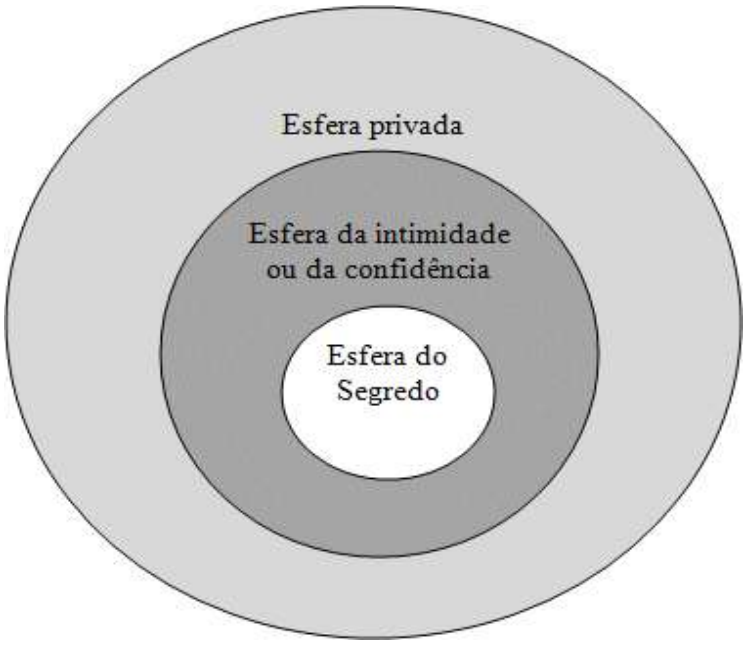
---

8 Direito ao esquecimento: trata-se do direito que as pessoas físicas têm de fazer com que as informações sobre elas sejam apagadas depois de um período de tempo determinado. Tal dispositivo tem por objetivo evitar a disseminação de informação pessoal passada que, deixando de cumprir sua finalidade, provoque um dano à pessoa (CABRERA, 2016).

Nos períodos da Segunda Guerra Mundial e do pós-guerra, principalmente entre 1939 e 1945, ocorreram várias interceptações telefônicas e de correspondências, de forma que o conceito de privacidade se voltou mais para a noção de privacidade em face das intromissões estatais. Foi nesse contexto que começou a se formar um questionamento sobre a privacidade, com mais força do que aconteceu com o Warren e Brandeis. As pessoas começaram a se questionar até onde ia o poder do governo, questionavam a existência de uma esfera íntima que poderia ser preservada.

Por causa desse movimento, em 1950, surgiu a *teoria dos círculos concêntricos*, cunhada pelos juristas Heinrick Hubmann e Heinrick Henkel: a existência de três círculos abstratos – conforme vemos na figura abaixo –, em que o círculo que está do lado externo representa a vida privada, ou seja, a privacidade, relacionada aos costumes e hábitos; a esfera intermediária representa a intimidade, ligada à família, aos amigos e às informações sobre o trabalho da pessoa; já a esfera no núcleo representa o segredo, como a sexualidade da pessoa ou a religião, mais vinculada ao âmbito do sigilo (BIONI, 2019).

Figura 2 – Teoria dos círculos concêntricos da vida privada



Fonte: SOUZA et. al (2019).

De acordo com o Di Fiore (2012), podemos citar como exemplo das esferas:

> 1 - a esfera da vida privada em sentido estrito (*Privatsphäre*), em que repousam as relações interpessoais mais rasas […] É neste círculo que repousa, por exemplo, o sigilo de dados telefônicos (acesso à relação de ligações efetuadas e recebidas), que pode ser quebrado pelo Poder Judiciário ou por CPI. Nesta esfera também se encontram os episódios de natureza pública que envolvam o indivíduo, extensíveis a um círculo indeterminado de pessoas e por isso não protegidos contra a divulgação.
> 2 - A intimidade é o círculo intermediário (*Vertrauensphäre*) […] É neste círculo que se encontram protegidos o sigilo domiciliar, profissional e das comunicações telefônicas, que sofrem restrições mais agudas para sua abertura, a exemplo da última cuja quebra só pode ser decretada por decisão judicial fundamentada.
> 3 - O segredo (*Geheimsphäre*) é o círculo mais oculto das esferas da privacidade *lato sensu*, no qual são guardadas as informações mais íntimas do Eu, que muitas vezes não são compartilhadas com outros indivíduos e sobre as quais o interesse público não poderá se imiscuir, a exemplo da opção sexual, filosófica e religiosa (DI FIORE, 2012, p. 2).

Foi nessa época e com essa percepção que surgiu a Carta de Direitos Fundamentais em 1948, na qual a Organização das Nações Unidas (ONU) reconheceu o direito à privacidade como um direito humano universal. É certo que a guerra foi um elemento decisivo para isso, acelerando as tendências que já estavam em curso, como ressalta Doneda (2019, p. 71), e desenvolvendo a ideia de *estado social*, em que através de uma hierarquia de valores, privilegia-se a pessoa humana, fazendo evoluir o direito à personalidade.

> A proteção da personalidade em seu âmbito próprio […] foi em geral avaliada como insuficiente após a Segunda Guerra Mundial. Após a experiência da Ditadura, havia surgido uma sensibilidade diante de toda forma de menosprezo da dignidade humana e da personalidade; ao mesmo tempo se percebeu que as possibilidades de realizar atos que representem um tal menosprezo, não somente por parte do Estado, mas também por outras associações ou por pessoas privadas tinham se multiplicado devido ao desenvolvimento da tecnologia (por exemplo, fitas magnéticas, aparelhos de escuta, microcâmaras) (LARENZ, 1980 apud DONEDA, 2019, p. 76).

Segundo Maldonado (2020), no pós-guerra, foi como se o conceito de privacidade se materializasse, com um movimento que se espalhou em diversas cartas. Em 28/01/1981, houve a Convenção 108, o primeiro instrumento internacional que apareceu para regular a proteção de dados. Isso significa que, a partir daquele momento, as pessoas dos países europeus regulados por esse documento passaram a ter direito não só à proteção dos dados, mas também à privacidade, tanto que o dia em que foi instituída essa convenção foi a data escolhida para se comemorar o Dia Internacional da Proteção de Dados (RANGEL, 2020).

3.1 SURGIMENTO DO DIREITO À PRIVACIDADE NO BRASIL

No Brasil, o direito à privacidade aparece na Constituição Federal de 1988, que, em seu artigo 5º, inciso X, diz o seguinte: "[…] são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito à indenização pelo dano material ou moral decorrente de sua violação" (BRASIL, 2016, [s. p.]). Nesse sentido, Miranda (2018) faz uma analogia sobre a dignidade da pessoa humana estar intrinsecamente conectada à proteção da privacidade:

> A Constituição Brasileira, ao reconhecer e inserir de forma veemente a proteção à dignidade da pessoa humana, na qual se encontra abarcada a proteção da privacidade, harmonizou-se com os tratados internacionais de Direitos Humanos ratificados pelo Brasil, impondo à sociedade brasileira a mesma consciência mundial acerca da tutela da proteção dos direitos fundamentais do homem (MIRANDA, 2018, p. 75).

Doneda (2019, p. 103) afirma que a CF incluiu no inciso X do seu artigo 5º a proteção da 'intimidade' e da 'vida privada' para trazer à luz que a proteção da pessoa humana abrange esses aspectos.

No mesmo sentido, Sauaia (2018) faz um paralelo entre a Declaração de Universais do Homem (1948), a Convenção Americana sobre Direitos Humanos no Pacto de São José da Costa Rica (1969) e a Constituição Federal Brasileira (1988), que, em seu inciso X do artigo 5º – intitulado "Dos Direitos e Deveres Individuais e Coletivos" –, assegura o direito fundamental à privacidade (sendo esta inviolável), além de, em outros incisos do mesmo artigo, afirmar diretos ligados à proteção da privacidade, podendo-se entender que abordam também a questão da proteção de dados:

> Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:
> XI - a casa é asilo inviolável do indivíduo, ninguém nela podendo penetrar sem consentimento do morador, salvo em caso de flagrante delito ou desastre, ou para prestar socorro, ou, durante o dia, por determinação judicial;
> XII - é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal; (Vide Lei nº 9.296, de 1996)
> 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 (BRASIL, 2016, Art. 5).

Dentre os incisos expostos acima, o de número XI afirma o domicílio do indivíduo como inviolável, sendo sua invasão por terceira vista como a quebra de um princípio constitucional; o inciso XII, por sua vez, dispõe sobre a proibição de interceptações telefônicas, telegráficas e de dados; já no inciso LXII, o titular dos dados pode impetrar o *habeas data* para ter conhecimento de informações a seu respeito advindas de registros e bancos de dados públicos, assim como pedir a sua retificação se for necessário.

Sauaia (2018) salienta que o favorecimento da interpretação dos incisos X e XII se dá pelo movimento atual de ressaltar a importância da proteção de dados:

> No estado atual da consolidação da proteção de dados pessoais no ordenamento e na própria cultura jurídica brasileira, o esforço a ser empreendido pela doutrina seria primeiramente o favorecimento de uma interpretação mais fiel ao nosso tempo para os incisos X e XII do Art. 5º, isto é, reconhecendo a íntima ligação que passam a ostentar os direitos relacionados à privacidade e à proteção de dados, aliás, como única forma de garantir o pleno desenvolvimento da personalidade e ao próprio princípio da dignidade humana. Infelizmente os problemas e os riscos relacionados à informação pessoal são demasiadamente complexos para poderem serem submetidos às referidas rotulações binárias com as quais tão frequentemente demandas pontuais são resolvidas sem que a grande questão de fundo seja tocada – qual a real expectativa de privacidade que o cidadão brasileiro pode ostentar em relação aos seus dados pessoais (SAUAIA, 2018, p. 154).

No Brasil, as pessoas ainda confundem os termos “privacidade” e “proteção de dados”, mas na Europa esses dois termos já estão separados desde 1981 (com a referida Convenção). Cada um tem a sua estrutura distinta, o direito à proteção de dados começou a ser inserido na Constituição Brasileira através de uma PEC, de número 17, em 2019, que, se aprovada, vai modificar o artigo 5º da CF e incluir o *Direito à Proteção de Dados* como um direito fundamental no ordenamento jurídico nacional.

Tal dispositivo legal, embora derivado do *Direito à Privacidade*, é diferente, encontrando-se relacionado à circulação adequada dos dados, com fluxo de acordo com regras, como na Lei Geral de Proteção de Dados.

O *Direito à Privacidade* está mais relacionado ao segredo, ao direito de ficar só, por exemplo o smartphone de uma adolescente (protegido por senha para ninguém acessar a sua vida íntima), a privacidade se vincula ao direito de permanecer em segredo em maior ou menor grau, ao sigilo. Já o *Direito à Proteção de Dados* se refere ao nível de controle que o indivíduo pode ter sobre as operações realizadas com os seus dados, sua transparência, sua finalidade e ao nível de segurança com que seus dados estão sendo tratados, princípios trazidos no rol do

artigo 6° da LGPD e que fazem parte da autodeterminação informativa do cidadão – abordada adiante. Os dados pessoais, como já visto, precisam circular para alimentar a sociedade da informação, já que são fontes de riqueza. Já a privacidade encontra o seu conceito no direito que o indivíduo tem de possuir os seus próprios segredos.

3.2 O INÍCIO DA INTERNET E A PROTEÇÃO DE DADOS PESSOAIS ATÉ OS DIAS ATUAIS

O *Direito à Proteção Dados Pessoais* se formou principalmente por causa do advento da internet, surgida na década de 60, nos EUA, inicialmente com o objetivo de promover a troca de comunicação e de informações científicas entre as instituições de ensino; posteriormente, com o início da Guerra Fria, essa tecnologia foi voltada para o uso militar. Os americanos perceberam que a rede proporcionada pela internet era uma melhor forma de comunicação que as redes de telefone e de telégrafos. Era um cenário de muita preocupação, já que havia o risco de ataque nuclear, assim, para proteger a rede americana de computadores de um eventual ataque, foi criada a *Advanced Research Projects Agency Network* (ARPANET)[9] em 1968, que é a semente da internet, pois ela criou pacotes de dados que passaram a ser transportados e transmitidos por redes (INTERNET…, 2020).

A partir de 1987, houve a liberação pela primeira vez ao uso comercial da internet nos Estados Unidos; já no Brasil a internet chegou por volta do ano de 1995 (GRECCO, 2018).

> Conforme nos esclarece Juan José López Ortega, ‘em seus primeiros anos de existência, a internet parecia pressagiar um novo paradigma da liberdade. Um espaço isento de intervenções públicas, no qual os internautas desfrutavam de um poder de ação ilimitado. A liberdade para se comunicar e se expressar se estendia sem possibilidade de censura a todos os cantos do planeta. A propriedade intelectual, necessariamente, devia ser compartilhada e a intimidade se encontrava assegurada preservando o anonimato da comunicação e pelas dificuldades técnicas de rastrear as fontes e identificar os conteúdos.
> As novas tecnologias de recolhimento dos dados, associadas à economia do comércio eletrônico, transformaram a liberdade e a privacidade na internet, e isso em consequência direta de sua comercialização. A necessidade de assegurar e identificar a comunicação para ganhar dinheiro por meio da rede, junto com a necessidade de proteger direitos os direitos de novas arquiteturas de software, que possibilitam o controle da comunicação. Tecnologias de identificação (senhas, marcadores, digitais,

9 A ARPANET foi criada pela ARPA (Advanced Research Projects Agency), agência de pesquisas do Departamento de Defesa do Governo dos EUA – atualmente chamada DARPA. Ao contrário do que muita gente pensa, a rede não foi criada com o propósito de controlar sistemas nucleares de defesa (RIGUES, 2019).

> processos de identificação), colocadas nas mãos das empresas e dos governos, deram passo ao desenvolvimento de tecnologia de vigilância que permitem rastrear os fluxos de informação. Através destas técnicas, qualquer informação transmitida eletronicamente pode ser recolhida, armazenada, processada e analisada. Para muitos isso supôs o fim da privacidade e, se não é assim, ao menos obriga a redefinir o âmbito privado na internet, um espaço no qual por sua dimensão global já não basta garantir o controle dos dados pessoais. Noções até agora válidas, como 'fichário' ou 'base de dados', deixam de ter significado. A nova fronteira não é o computador pessoal ou a internet, senão a rede a global, e isso tem consequências ao delimitar o conteúdo do direito à intimidade, que no espaço digital se transmuda no direito ao anonimato (GRECCO, 2018, p. 540).

Vê-se, assim, que a partir do surgimento da internet, diversas mudanças ocorreram na sociedade. Ao analisarmos o contexto atual, de pandemia do coronavírus, houve a aceleração do processo de virtualização, trazendo mudanças profundas a todos os setores da economia: as pessoas foram obrigadas a migrar para o modelo *home office*, as escolas e universidades foram fechadas e as casas passaram a ser ambiente de trabalho e de estudo. Ademais, as políticas públicas adotadas pelo Estado tiveram que se readaptar, como no caso do censo.

No ano de 2020, estava previsto o Censo Brasileiro, com cerca de 180 mil recenseadores, que visitariam cerca de 71 milhões de domicílios em todo território nacional para a coleta de dados dos cidadãos. No entanto, com a justificativa de que não seria possível a visita presencial em decorrência da pandemia, foi editada em 17 de abril de 2020 a medida Provisória 954/2020, que tratava do compartilhamento de dados pelas empresas de telecomunicação, prestadoras de Serviço Telefônico Fixo Comutado (STFC) e de Serviço Móvel Pessoal (SMP) com o Instituto Brasileiro de Geografia e Estatística (IBGE), tendo como finalidade dar suporte à produção de estatísticas oficiais durante a situação de emergência de importância internacional decorrente do COVID-19 (ALMEIDA, 2020).

As empresas de telefonia teriam que entregar todos os dados cadastrais (nome, endereço, telefone etc.) de todos os seus assinantes para o IBGE, a partir do argumento de que o mesmo teria que fazer a Pesquisa de Amostra por Domicílio (PNAD) e que usaria esses dados para a produção de estatística oficial enquanto durasse a situação da atua pandemia. Dessa forma, a MP 954/2020 ordenou às operadoras de telefonia fixa e celular que repassassem o cadastro de seus clientes para IBGE, que utilizaria os dados "exclusivamente" para realizar pesquisas domiciliares por telefone (CÂMARA…, 2020).

Diante disso, a Ordem dos Advogados do Brasil (OAB) entrou com uma Ação Direta de Inconstitucionalidade (ADI), alegando que a referida medida provisória feria diversos preceitos constitucionais que tutelam o direito à personalidade. A principal preocupação foi que

esses dados poderiam ser reutilizados para fins que não fossem restritos aos mencionados, utilizando-se deles, por exemplo, para um eventual disparo de mensagens em massa ou falsas (as conhecidas *fake news)* ou outras táticas de modulação de comportamento de pessoas.

Em sua decisão, a juíza Rosa Weber analisou que a MP 954/2020 em nenhum momento explicitou a finalidade do uso da pesquisa estatística, além de não ter demonstrado que os dados estavam sendo coletados apenas para finalidade específica daquela pesquisa, nem informado qual a necessidade da coleta de todos os dados mencionados no documento ou tampouco delimitado o campo de proteção na operação de processamento dos dados – isto é, não comprovou a eficácia das medidas adotadas (SUPREMO…, 2020).

Como foi muito bem colocado pela juíza no julgamento, não existe mais o mundo de listas telefônicas; hoje, os dados cadastrais estão em um outro patamar. Antes, por mais que estivessem públicos em uma lista de endereços, os dados não chegavam nem perto da capacidade de estruturação deles que se tem hoje, com a velocidade de processamento de informações, a partir do que pode haver interferência em muitos outros resultados pela quantidade e qualidade dos dados solicitados pela MP 954/2020 (SUPREMO..., 2020).

Bioni (2019) afirmou em sua uma sustentação oral como Amicus Curiae[10] (caso excepcional que acontece em determinadas situações que se tenha interesse jurídico relevante – como o caso da MP 954/2020) que milhões de brasileiros teriam seus dados cadastrais das empresas de telefonia repassados ao IBGE sem que a Lei Geral de Proteção de Dados no Brasil estivesse já em vigor para auxiliar os Ministros a se posicionarem a respeito da matéria. Para o pesquisador, é muito importante ressaltar o paralelo entre esse episódio e uma outra decisão muito importante no campo da proteção de dados pessoais: a decisão da Corte Suprema da Alemanha, que, em 1983, reconheceu a inconstitucionalidade de uma lei do Censo, justamente porque ela não vinha acompanhada de salvaguardas necessárias para que os riscos daquelas atividades fossem mitigados. Com uma grande semelhança ao caso brasileiro, a Lei do Censo Alemã permitia que houvesse um compartilhamento dos dados recolhidos para planejamento urbano com vários outros órgãos dentro da administração pública, usando-se dos mesmos dados coletados para outros fins.

10 Amicus curiae: amigo da corte, ou também amigo do tribunal (amici curiae, no plural), é uma expressão em latim utilizada para designar uma instituição que tem por finalidade fornecer subsídios às decisões dos tribunais, oferecendo-lhes melhor base para questões relevantes e de grande impacto (NOVO, 2018).

Esse é um marco inicial na proteção de dados pessoais, visto que o Poder Judiciário traz explicitamente que o *Direito à Proteção de Dados Pessoais* é um direito destacado do *Direito à Privacidade*.

Bioni (2019) disse na sua sustentação que a MP 954/2020 não atendia às medidas de segurança, uma vez que, como a pesquisa do IBGE é amostral, não haveria a necessidade do repasse da totalidade do banco de dados das empresas de telefonia, apenas uma parcela deles já seria o suficiente. Ademais, o autor corroborou a perspectiva de que não havia um conjunto de salvaguardas necessárias para que o uso de dados pessoais não fossem desviados de sua finalidade. De acordo com ele:

> No desenrolar da 2ª Guerra Mundial, por que foi tão mais fácil para os nazistas perseguirem os judeus em Amsterdã? Como relata o diário de Anne Frank e os livros de História? Porque lá o planejamento urbano municipal se valeu do uso de dados pessoais, sem as devidas precauções, coletou-se dados desnecessários que possibilitaria inferir até a crença religiosa das pessoas, mesmo que isso não estivesse anotado nos bancos de dados (DATA…, 2020).

O autor ainda menciona um segundo caso, mais recente: a situação referente à empresa *Cambridge Analytica*, na qual, ao que tudo indica, pleitos eleitorais foram manipulados, não apenas porque se soube através de um *quizz* de uma determinada rede social qual era a personalidade de centenas de pessoas, mas sobretudo porque houve a possibilidade de saber o nome de milhares de pessoas que eram amigas dos respondentes desse *quizz.* Nesse episódio, os dados coletados deveriam ter sido utilizados apenas para essa finalidade específica, mas na verdade acabaram sendo usados para finalidades muito diferentes. Há uma estimativa que dados de mais de 50 milhões de pessoas tenham sido coletados e utilizados indevidamente, para fins de envio de publicidade direcionada – o que ficou conhecido como *MicroTargeting* (publicidade direcionada) –, além da suspeita de que esse escândalo tenha influenciado a votação da saída do Reino Unido do bloco da União Europeia. Nos Estados Unidas da América (EUA), por sua vez, o uso dos dados pessoais para finalidades políticas com direcionamento de publicidades teria ajudado a eleger o ex-presidente Donald Trump.

A decisão do STF foi referente ao um julgamento de cinco Ações Direitas de Inconstitucionalidade (ADI), apresentadas pela Ordem dos Advogados do Brasil (OAB) e também pelos partidos PSDB, PCdoB, PSOL e PSB, que são bem diferentes entre si. Sobre uma dessas ações, afirma Doneda de acordo com o Data Privacy Brasil (2020):

> No caso da proposta da ADI na qual eu trabalhei, pelo Partido Socialista Brasileiro, foi justamente para proteger a atividade estatística, evitando que a atividade do IBGE fosse eventualmente prejudicada por ser politizada, por ser corrompida, contaminada por um potencial interesse de natureza política. (DATA..., 2020)

No que se refere à decisão do STF, Laura Mendes (DATA..., 2020) afirmou: nessa decisão histórica o STF superou um paradigma de que apenas as informações privadas devem ser protegidas, de que proteção deveria versar apenas sobre o que é considerado íntimo, para a visão de que dado neutro não existe mais, isto é, que a partir desse momento o STF proporcionou uma ampliação de um direito constitucional, pois já que não existem mais dados insignificantes, restou reconhecido o direito à proteção de dados como um direito fundamental e que mesmo com a aprovação da PEC 17/2019, que irá assegurar a Proteção de Dados como um direito constitucional, já foi anteriormente reconhecido como tal, através da decisão do caso IBGE.

Foi uma votação de um placar expressivo: 10 votos a favor da suspensão do compartilhamento de dados contra 1 que autorizava o compartilhamento. Alguns votos, como da Ministra Relatora Rosa Weber, ressaltam que a partir do momento que se faz tratamento de dados pessoais, isso precisa vir acompanhado das medidas de proteção cabíveis para tal modalidade.

4 LEI GERAL DE PROTEÇÃO DE DADOS BRASILEIRA (LGPD)

Nos capítulos anteriores, foi analisada a evolução histórica do conceito privacidade e proteção de dados. Ao se voltar para o Brasil e analisar quais os motivos que levaram o país a finalmente promulgar uma Lei Geral de Proteção de Dados, o Marco Civil da Internet (MCI) mostra-se uma mola propulsora. A sociedade ainda não possui, de maneira geral, um discernimento correto de como as plataformas digitais tratam os seus dados, e é um grande desafio trazer esse entendimento para as pessoas. *Será que os cidadãos realmente se preocupam com o que é feito das suas informações pessoais? Quais os riscos que eles correm, quando fornecem seus dados indiscriminadamente?*

A educação digital aliada à legislação vai ser fundamental nesse cenário, para que as pessoas tenham mais autonomia e possam exercer seus direitos, como a autodeterminação informativa. Nesse capítulo, a lei 13.709/2018 foi tratada de uma maneira geral, destacando-se alguns apontamentos de maior relevância para nossa pesquisa.

A LGPD é um marco regulatório que tem um grande impacto no ordenamento jurídico brasileiro, tendo sido foi promulgada pelo então presidente Michel Temer no dia 14/08/2018 e origem no Projeto Lei da Câmara (PLC) n. 53/2018. Inicialmente, a lei entraria em vigor após 18 (dezoito) meses da sua publicação, depois houve uma prorrogação para 24 (vinte e quatro) meses, isto é, para agosto de 2020; posteriormente, o presidente Jair Bolsonaro pediu mais uma prorrogação, através da MP 959/2020, que adiava a vigência da lei para maio/2021. Entretanto, o artigo da referida medida provisória foi julgado prejudicado pelo Senado Federal, que alegou que essa matéria já havia sido objeto de votação, portanto a MP 959/2020 foi convertida na Lei 14.058/2020, que entrou em vigor sem o artigo que adiava a LGPD para 2021. Desse modo, a vigência da lei ocorreu no dia 18 de setembro de 2020.

Essa legislação traz algumas terminologias que serão citadas nesse capítulo. O conhecimento delas é importante para que se tenha um melhor entendimento da LGPD:

- **Titular**: Pessoa a quem se referem os dados pessoais que são objeto de algum tratamento.
- **Tratamento de Dados**: Toda operação realizada com algum tipo de manuseio de dados pessoais – coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento,

armazenamento, edição, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

- **Dados Pessoais**: Toda informação relacionada a uma pessoa identificada ou identificável, não se limitando, portanto, a nome, sobrenome, apelido, idade, endereço residencial ou eletrônico, podendo incluir dados de localização, placas de automóvel, perfis de compras, número do Internet Protocol (IP), dados acadêmicos, histórico de compras, entre outros. Sempre relacionados à pessoa natural viva.
- **Dados Pessoais Sensíveis**: São dados relacionados a características da personalidade do indivíduo e suas escolhas pessoais, tais como: origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou à 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.
- **Dados Anonimizados**: São os dados relativos a um titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião do seu tratamento.
- **Consentimento**: Manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada. Não é o único motivo que autoriza o tratamento de dados pessoais, mas apenas uma das hipóteses.
- **Agentes de tratamento**: O controlador que recepciona os dados pessoais dos titulares de dados por meio do consentimento ou por hipóteses de exceção, e o operador que realiza algum tratamento de dados pessoais motivado por contrato ou obrigação legal.
- **Encarregado**: Pessoa indicada pelo controlador e operador que atua como canal de comunicação entre controlador e titulares de dados e a Autoridade Nacional de Proteção de Dados (ANPD).
- **Transferência Internacional de Dados**: Transferência de dados pessoais para país estrangeiro ou organização internacional da qual o país seja membro (PINHEIRO, 2018, p. 25-27).

O MCI é uma lei de 2014 que regulamenta o uso da internet no Brasil, e o contexto histórico que trouxe a necessidade dessa legislação para o Brasil foi um acontecimento impactante, referente às informações trazidas por Edward Snowden, que divulgou que o governo norte-americano tinha acesso às empresas de telefonia e tecnologia sem ordens judiciais, com o objetivo de espionagem estratégica, deixando de lado o motivo alegado de segurança nacional. Snowden revelou que os e-mails da ex-presidente do Brasil Dilma Rousseff estavam nessa lista de espionagem, assim como os da chanceler alemã Angela Merkel. Por causa dessas denúncias, gerou-se uma discussão sobre quais tipos de acesso poderiam ser feitos. *Qual a possibilidade de um governo poder usar esse tipo de informação de forma estratégica?*

Depois desse incidente, o Brasil passou a ter uma lei específica acerca da internet. Em 2014, é promulgado o Marco Civil da Internet (Lei 12.965/2014), cujos pilares estruturados são: 1) Privacidade on-line; 2) Neutralidade da rede, isonomia do tratamento dos pacotes de dados, ausência de limite nos conteúdos; 3) Responsabilidade dos Provedores de Serviço da Internet. Outro ponto muito importante que o MCI traz é a educação digital. Embora esse assunto também apareça na LGPD, o "Marco" foi o precursor nessa discussão ao trazer necessidade da educação para o uso adequado da tecnologia.

O MCI cria regras específicas e foi uma reação do governo brasileiro aos fatos trazidos pelo Snowden, levando o Brasil, à época, a ser um dos poucos a terem uma legislação específica para tratar sobre o uso da internet no Brasil.

Antes do MCI, há a Lei de Acesso à Informação (LAI) – Lei 12.527/11 (BRASIL, [2011], [s. p.]), que já traz uma definição acerca de dado pessoal: "Art. 4º Para os efeitos desta Lei, considera-se: IV - informação pessoal: aquela relacionada à pessoa natural identificada ou identificável" (BRASIL, [2018], Art. 4).

O MCI, através do Decreto n.º 8.771/2016, trouxe a definição de *dado pessoal*:

> Para os fins do disposto neste Decreto, considera-se:
> I - dado pessoal - dado relacionado à pessoa natural identificada ou identificável, inclusive números identificativos, dados locacionais ou identificadores eletrônicos, quando estes estiverem relacionados a uma pessoa (BRASIL, [2016a], Art. 14).

Já o artigo 5º da LGPD traz uma definição mais abrangente de *dado pessoal* e, como já visto, se ramifica em uma outra categoria denominada *dado sensível*. A LGPD foi aprovada em agosto de 2018, mas vem sendo discutida desde de 2010, quando aconteceu a primeira consulta pública, num anteprojeto de lei que era muito diferente da versão que foi aprovada.

Entre 2010 e 2014, não ocorreram muitas discussões acerca dessa lei, mas, em julho de 2013, houve os escândalos de espionagem revelados pelo Edward Snowden. Com isso, a partir de outubro de 2013 até abril de 2014, houve a aceleração da discussão do Projeto de Lei (PL) do MCI, que culminou justamente com a sua aprovação em abril de 2014, criando um microssistema de proteção de dados pessoais, no âmbito online.

A Lei nº 12.965/2014 não é uma lei exaustiva – justamente para não ficar obsoleta, devido às constantes atualizações da tecnologia e do mundo online –, mas é uma legislação norteadora para o ambiente virtual. A internet é uma forma atual de manifestação da democracia, com o exemplo das eleições: até pouco tempo as campanhas eleitorais ocorriam pelas emissoras de televisão, hoje elas acontecem principalmente pelas redes sociais.

Quando o Marco Civil foi promulgado, já veio expresso no seu artigo 3º, inciso III, que haveria a necessidade de uma legislação de proteção de dados pessoais: "[...] A disciplina do uso da internet no Brasil tem os seguintes princípios: III - proteção dos dados pessoais, na forma da lei" (BRASIL, 2018, [s. p.]). Já em seu artigo 8º, o documento traz um conceito que reforça a democratização do espaço virtual: "[...] A garantia do direito à privacidade e à liberdade de expressão nas comunicações é condição para o pleno exercício do direito de acesso à internet". (Ibid.). Todavia, o tratamento de dados pessoais não se dá só na internet, assim, de 2014 até 2015, ocorreu um reinício das discussões da LGPD.

Em 2015, houve a segunda consulta pública do anteprojeto. Naquele momento, houve mais de 2500 contribuições de atores nacionais e internacionais de governos e entidades privadas, gerando a aglutinação das melhores sugestões. Dessa forma, em outubro de 2015 surgiu uma nova versão do anteprojeto da Lei Geral de Proteção de Dados Pessoais. Esse anteprojeto, então no começo de 2016, foi enviado para a Câmara dos Deputados (na verdade um dos últimos atos da então presidente Dilma Rousseff); ao chegar na Câmara, ele foi juntado a outros projetos de lei que discorriam sobre essa matéria, tal como o PL 4060/2012, que tramitava em paralelo com o PLS 330/2013 (que corria no Senado Federal).

Entre 2016 e 2018, portanto, ocorreu uma série de discussões, com várias audiências públicas (mais de treze), audiências temáticas e eventos específicos para ajudar na discussão dos principais temas da construção da Lei Geral de Proteção de Dados Pessoais. Todavia, em 2018 aconteceu uma determinada conjuntura política que culminou com a aprovação da LGPD, em que se destaca quatro situações:

1) Entrada em vigor, em 25 de maio de 2018, da Regulamentação Europeia de Proteção de Dados Pessoais (GDPR), que, apesar de ser europeia, tem aplicação extraterritorial, o que levou muitas empresas brasileiras, mesmo sem presença física na UE, a se adequarem a esta legislação por causa de elementos de conexão, como a oferta de serviços para o velho continente;
2) Escândalo da Empresa *Cambridge Anaylitca*: como já mencionado neste trabalho houve um desvio grosseiro de finalidade de dados coletados, onde o teste de personalidade feito em determinada rede social dava ensejo a publicidade eleitoral direcionada (*microtargeting*);
3) Tentativa, ainda existente, de o Brasil entrar para um grupo econômico, a Organização para a Cooperação e Desenvolvimento Econômico (OCDE), um grupo dos países ricos. A OCDE, desde 1980, tem diretrizes para a transferência de tratamento de dados pessoais e para o uso adequado desses dados. Para que os países possam entrar nesse grupo, eles têm que se adequar, prometer que vão seguir essas orientações. O fato de o Brasil, à época, não ter uma Lei Geral de Proteção de Dados significava que não tinha um nível adequado de proteção de dados pessoais, e isso dificultava muito o seu ingresso na OCDE;
4) As tentativas de alteração da Lei do Cadastro Positivo (LC 166/2019) (DONEDA, 2019).

A Lei do Cadastro Positivo, aprovada em 2011, determinava que era necessário ter o consentimento expresso do titular dos dados para que seus dados de adimplência, ou seja, seus dados de históricos de pagamento e de crédito, pudessem ser alocados em uma base de dados. Muitas empresas, conhecidas como gestoras, teriam muito interesse nessas informações. Só que a adesão do Cadastro Positivo por meio do consentimento sempre foi muito baixa, ou pelo menos era inferior ao que as instituições financeiras e outros gestores de dados pretendiam, então houve um debate para que não fosse mais necessário ter esse consentimento prévio, para que houvesse uma adesão automática ao cadastro positivo, com um direito de oposição, mas isso significaria praticamente a entrada automática de informações de mais de 100 milhões de brasileiros economicamente ativos nas bases de dados.

Numa discussão de fundo na Câmara dos Deputados, por vários agentes representantes da sociedade civil organizada, chegou-se à seguinte conclusão: antes de colocar os dados de mais de 100 milhões de pessoas automaticamente na sua base de dados, com seu histórico de

crédito e de pagamento, o que poderia revelar muito sobre suas vidas, havia a necessidade de se discutir regras e direitos adequados para os titulares no âmbito da LGPD. Foi justamente isso que aconteceu, a Câmara e o Senado apoiaram a aprovação da LGPD, para que fossem feitas as alterações da LCP, culminando na aprovação da Lei Complementar 166, de 2019. Os 4 elementos dessa conjuntura política foram fundamentais para a aprovação da lei 13.709/2018, em 14 de agosto de 2018.

É importante ressaltar que, fora todos esses anos de discussão, houve uma coalizão multissetorial de entidades de todas as áreas, que se juntaram em uma manifestação pública, redigindo e enviando uma carta para a Câmara dos Deputados e para o Senado, motivando e apoiando a aprovação e explicando porque isso era necessário colocar o Brasil dentro do mapa econômico de países que já tinham leis de proteção de dados, com um nível adequado de proteção de dados pessoais.

Figura 3 - Linha do tempo da Lei Geral de Proteção dos Dados 2010-2020

Fonte: Bioni (2019).

Na Figura 3, por exemplo, pode-se mencionar que a discussão da LGPD teve início no ano de 2010, quando ocorreu a primeira consulta pública, e em 2013 houve uma aceleração dessa discussão em decorrência das revelações feitas por Edward Snowden. Após isso, foram inúmeras discussões e debates diante da possibilidade de adesão da lei, que culminou na sua aprovação em 2018 e a sua entrada em vigor aconteceu em 18 de setembro 2020.

Figura 4 - Linha do Tempo LGPD - 2018-2019

Fonte: Bioni (2019).

A Figura 4 demonstra os principais acontecimentos históricos que levaram à aprovação da Lei Geral de Proteção de Dados: a entrada em vigor da GDPR; o escândalo de Cambridge; a PEC 17/2019.

Figura 5 - Linha do Tempo LGPD - Primeira Consulta Pública

Fonte: Bioni (2019).

Já a Figura 5 apresenta, com maior detalhamento, o que ocorreu no decorrer dos anos em relação à LGPD: em 2010, ocorreu a primeira consulta pública; após o Marco Civil da Internet, houve um amadurecimento do tema para que o conceito ‘Proteção de Dados’ englobasse não só o ambiente digital, mas também o físico.

Figura 6 - Linha do Tempo - Caso IBGE

Fonte: Bioni (2019).

A Figura 6 mostra as discussões acerca da entrada em vigor da LGPD: a medida provisória 14.010/20 prorrogava a entrada em vigor da LGPD para maio de 2021, só que, em votação no Senado, a parte que adiava a vigência da Lei foi retirada da MP, fato este que ocasionou a entrada em vigor imediatamente da LGPD em 18 de setembro de 2020, restando somente prorrogadas as sanções da LGPD para 1 de agosto de 2021.

Entre os anos de 2010 a 2018, o Brasil vivia um período de transição para um entendimento maior desse contexto de privacidade e proteção de dados. Essa demora de oito

anos da primeira consulta pública até a aprovação da LGPD ratifica a morosidade do legislativo em se adequar às novas tecnologias, mesmo sendo pressionado por uma discussão constante no resto do mundo e já existindo o Marco Civil da Internet.

A Lei 13.709/2018 se aproxima mais das pessoas do que o Marco Civil da Internet, pois, de certa forma, quando a LGPD fala da autodeterminação informativa, traz o empoderamento do usuário. Dado que este passa a ter o poder de decidir se quer ou não compartilhar os seus dados, a pessoa precisa ter conhecimento sobre o fluxo dos seus dados, ou seja, o caminho que aquela informação vai percorrer, além de ter o direito de fazer a portabilidade ou pedir a exclusão do mesmo de determinada plataforma. A perspectiva trazida pela LGPD faz com que as empresas tenham mais responsabilidade quanto ao tratamento de dados dos usuários, fator que tende a mudar gradativamente a dinâmica dessa relação.

Nenhuma mudança de comportamento da sociedade ocorre de uma hora para outra, mas aos poucos essa mudança comportamental das pessoas irá acontecer, até porque os crimes virtuais aumentaram muito, principalmente durante o período da pandemia. Nesse âmbito, a LGPD traz dois assuntos intrinsecamente ligados: *segurança da informação* e *proteção de dados*, que são duas áreas de atuação distintas, mas que, no cenário atual, ficarão cada vez mais interligadas, e a tendência é que essa nova concepção irá se moldar aos poucos à cultura social, trazendo como consequência pessoas mais conectadas e conscientes quanto aos seus direitos e deveres.

Como exemplo, pode-se citar o uso de cinto de segurança, negligenciado até a legislação que obrigou o seu uso. Anteriormente à lei, era comum ver pessoas viajando sem ele, hoje é culturalmente inviável pegar estrada sem esse equipamento de segurança, e isso equipara-se à cultura que está sendo construída em relação à proteção de dados pessoais, diante da qual, em um futuro próximo, será inviável as pessoas aderirem a um termo de política de privacidade sem ter o conhecimento de seu conteúdo.

A LGPD vai exigir das empresas e órgãos públicos transparências quanto ao tratamento dos dados e que estes estejam de acordo com as bases legais prevista na lei elaborada especialmente para o tratamento de dados pela gestão pública.

A transparência quanto ao tratamento dos dados gera confiança dos usuários, e isso agrega valor a uma empresa, mesmo porque se as pessoas não confiarem no aplicativo ou na plataforma que utilizam, deixarão de alimentá-las com os seus dados. Essa é uma mudança que

está ocorrendo, tendo a LGPD como agente principal, e a transparência, a confiança e o respeito selam essa relação.

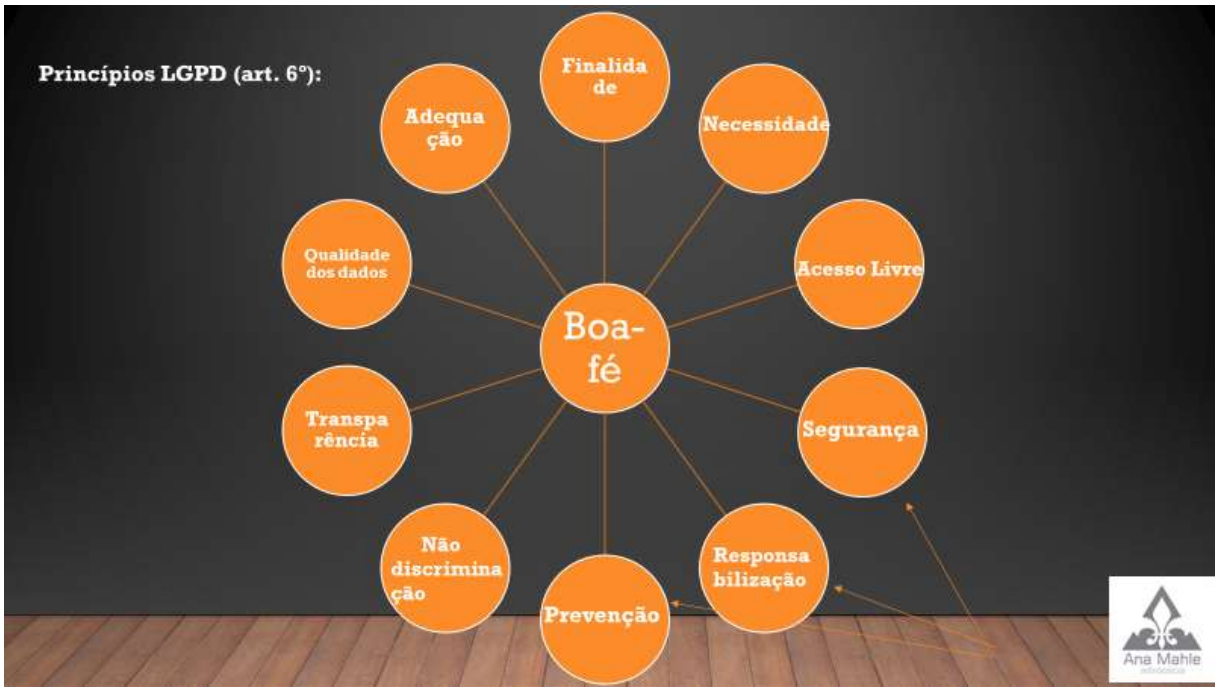
4.1 DOS PRINCÍPIOS E DIREITOS DOS TITULARES DA LGPD

Até esse momento analisou-se o processo de construção da Lei Geral de Dados Pessoais, deste tópico em diante trata-se da análise de artigos contidos na LGPD que permitem entender os princípios que a norteiam, o alicerce dessa legislação. O disposto no Art. 6º diz o seguinte:

> 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 (BRASIL, 2019, [s. p.]).

No artigo 6° da lei LGPD, há a definição das regras que conduzem a legislação, são os princípios que estão dispostos neste artigo, no qual além da boa-fé, disposta no seu caput, há outros 10 princípios. No Direito é ordinariamente entendido que boa-fé é o grau de confiança que se estabelece entre as partes, é a crença de que as partes estão sendo leais, partindo do pressuposto de que não haverá nenhum comportamento abusivo ou lesivo.

Figura 7 – Princípios da LGPD norteados pela Boa-Fé



Fonte: Elaborado pela autora.

Abaixo, tem-se os demais princípios dispostos nos incisos do art. 6º da LGPD:

1) **Princípio da Finalidade:** quando se coleta um dado, é necessária uma finalidade específica, pois não se pode sair coletando dados sem saber o que vai fazer com eles, há que saber exatamente qual a necessidade da coleta daquele dado. Assim, depois da entrada, com a LGPD em vigor, há a impossibilidade de tratamento de dados com finalidades genéricas ou indeterminadas;
2) **Adequação:** as finalidades do tratamento têm que ser compatíveis com as que foram informadas ao titular, elas têm que ser adequadas ao motivo que originou sua coleta. Por exemplo, a Lei do Cadastro Positivo dispõe do armazenamento dos dados por um período de 5 anos, passado esse prazo, se os dados continuarem armazenados, há um desvio de finalidade logo o seu tratamento se torna inadequado, portanto, os dados devem ser descartados;
3) **Princípio da Necessidade:** também conhecido como o princípio da minimização, em que o tratamento dos dados deve ser feito sempre com o mínimo necessário para atingir a finalidade. Por exemplo, se não há necessidade da coleta do CPF de uma pessoa para realizar o tratamento, esta não será feita. Outro exemplo que se tem é ao realizar um cadastro em site de *e-commerce* de produtos eletrônicos ser

obrigatório a inserção de dados relacionados à saúde daquele cliente, pois isso fere o princípio da necessidade. Quanto maior a quantidade de dados de uma empresa, maior será a responsabilidade dela, já que há mais suscetibilidade a vazamentos;

4) **Livre Acesso:** os titulares têm garantia de consulta facilitada e gratuita a todos os dados que as empresas tenham deles: se a pessoa solicitou os seus dados, as empresas têm que observar até qual o formato do arquivo que vão entregar para o usuário, posto que ele tem que ser de fácil acesso para as pessoas comuns;
5) **Qualidade dos Dados:** os dados coletados têm que estar sempre atualizados, sem erros. Com a virtualização, o avatar eletrônico goza de um maior valor do que a pessoa física; se informações nesse avatar estiverem erradas, decisões sobre esse indivíduo serão tomadas erroneamente. Para as empresas, também é muito importante que os dados estejam corretos, pois além de isso diminuir a vulnerabilidade de seus negócios, garante que as informações sejam sempre positivas e relevantes para sua área de atuação no mercado;
6) **Princípio da transparência:** as informações têm que ser claras e acessíveis, salvos os segredos comerciais e industriais;
7) **Segurança:** mecanismos para coibir situações de acidentes ou criminosas, como invasão ou perda dos dados;
8) **Prevenção:** quais as medidas adotadas pela empresa para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais, ou seja, as empresas devem agir antes dos problemas;
9) **Não discriminação:** o tratamento não pode ser realizado para fins discriminatórios ou abusivos;
10) **Responsabilização e prestação de contas:** o agente que trata os dados tem que mostrar que está tomando as medidas necessárias para o cumprimento das normas (MALDONADO; BLUM, 2019).

Como visto, A LGPD traz, no seu artigo 6º, seus princípios, e são eles que vão dar o norte, que mostrarão a ideia central da Lei e demonstrarão o motivo real da sua existência. Com o entendimento dos princípios, consegue-se visualizar a lei como um todo, sendo assim possível interpretar a lei de forma correta.

O princípio de acordo com o ordenamento jurídico se configura como a norma que determina a promoção de um estado ideal das coisas. Desse modo, as decisões devem ser

tomadas em conformidade com os princípios da lei, para que o sistema seja coeso. Segundo a definição de Humberto Ávila (2012, [s.p.]), o princípio "é a norma que determina a promoção de um estado ideal das coisas".

Como exposto, a LGPD é regida por 11 princípios, sendo a boa-fé o primeiro deles. Além do mais, há três princípios que, se destacados do art. 6º, transferem para o particular a responsabilidade de gerenciamento, que são: os princípios da *segurança*, da *prevenção* e da *responsabilização e prestação de contas*, que têm a função de evitar incidentes, garantindo assim os direitos dos titulares de dados. Esses três princípios reunidos reforçam a ideia de que o agente que trata dados pessoais tem de comprovar que está adotando medidas eficazes para o cumprimento da norma, caso contrário ele poderá ser responsabilizado. Tais princípios estão diretamente ligados à noção de *compliance,* que significa estar em conformidade com as regras, o que nada mais é do que a adequação da empresa/particular ou órgão público às normas existentes, no caso à LGPD.

Afora os três princípios mencionados acima, há um outro princípio que é fundamental para que o titular dos dados exerça a autodeterminação informativa (o objeto dessa pesquisa): o *princípio do livre acesso*, que garante que os titulares tenham garantia de consulta facilitada e gratuita à forma e à duração do tratamento, bem como à integralidade de seus dados pessoais – o que reforça a ideia da autodeterminação informativa, fundamento da LGPD que prega que o titular dos dados tem que ter autonomia sobre o fluxo dos seus dados, conceito extensivamente abordado em nossa investigação.

Se nossa pesquisa tivesse que se resumir em uma só pergunta, seria: *Como o titular dos dados vai ter autonomia sobre o fluxo dos seus dados?* A resposta para essa questão é a seguinte: isso se dá através dos direitos dos titulares que estão dispostos na LGPD nos artigos de 17 a 22, que se conectam com os princípios e se concretizam através do livre acesso.

O primeiro artigo, na parte que a LGPD trata dos direitos dos titulares (art. 17), dispõe o seguinte: "Toda pessoa natural tem assegurada a titularidade de seus dados pessoais e garantidos os direitos fundamentais de liberdade, de intimidade e de privacidade, nos termos desta Lei" (BRASIL, 2019, [s. p.]).

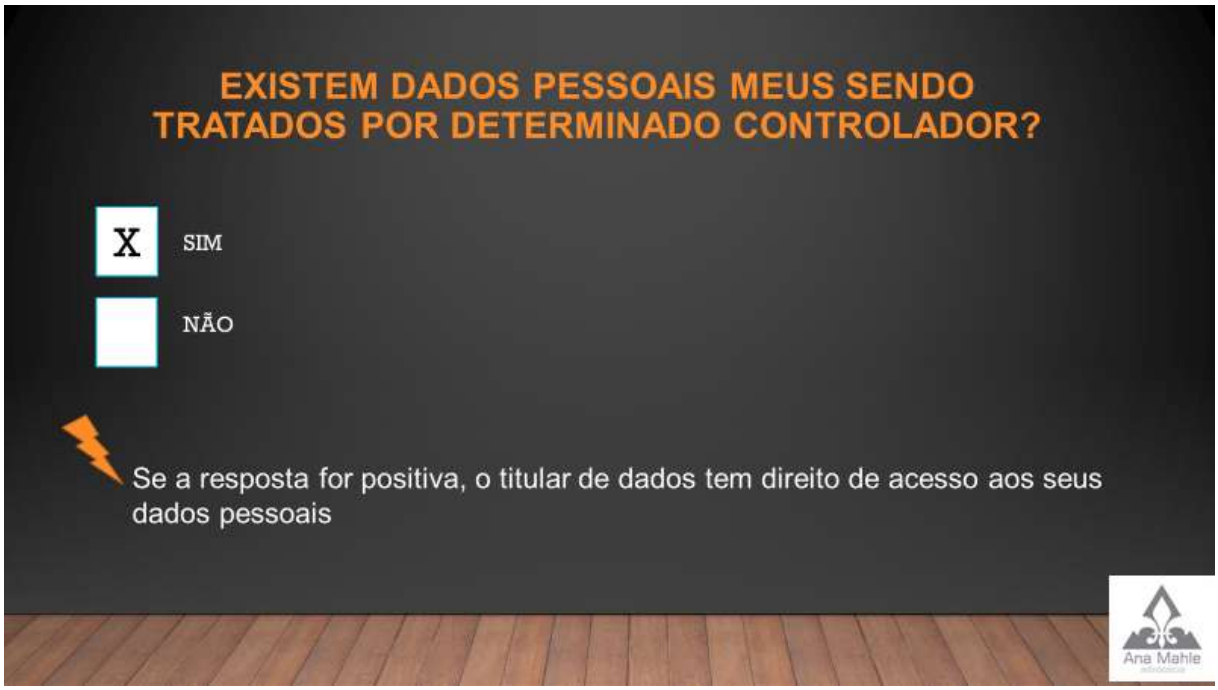
Tal artigo é mais genérico, assegurando a toda pessoa natural (o titular de dados) os seus direitos fundamentais garantidos (dispostos no art. 2º da LGPD – abordado posteriormente) e reforçando a ideia de que o titular é quem tem o domínio dos dados. Já no art. 18, existem direitos muito relevantes que elencam essa relação:

> 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:
> I - Confirmação da existência de tratamento;
> II - Acesso aos dados;
> III - Correção de dados incompletos, inexatos ou desatualizados;
> IV - Anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto nesta Lei;
> V - Portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial;
> VI - Eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no art. 16 desta Lei;
> VII - Informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados;
> VIII - Informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa;
> IX - Revogação do consentimento, nos termos do § 5º do art. 8º desta Lei.
> § 1º O titular dos dados pessoais tem o direito de peticionar em relação aos seus dados contra o controlador perante a autoridade nacional.
> § 2º O titular pode opor-se a tratamento realizado com fundamento em uma das hipóteses de dispensa de consentimento, em caso de descumprimento ao disposto nesta Lei.
> § 3º Os direitos previstos neste artigo serão exercidos mediante requerimento expresso do titular ou de representante legalmente constituído, a agente de tratamento.
> § 4º Em caso de impossibilidade de adoção imediata da providência de que trata o § 3º deste artigo, o controlador enviará ao titular resposta em que poderá:
> I - Comunicar que não é agente de tratamento dos dados e indicar, sempre que possível, o agente; ou
> II - Indicar as razões de fato ou de direito que impedem a adoção imediata da providência.
> § 5º O requerimento referido no § 3º deste artigo será atendido sem custos para o titular, nos prazos e nos termos previstos em regulamento.
> § 6º O responsável deverá informar, de maneira imediata, aos agentes de tratamento com os quais tenha realizado uso compartilhado de dados a correção, a eliminação, a anonimização ou o bloqueio dos dados, para que repitam idêntico procedimento, exceto nos casos em que esta comunicação seja comprovadamente impossível ou implique esforço desproporcional. (Redação dada pela Lei nº 13.853, de 2019) Vigência.
> § 7º A portabilidade dos dados pessoais a que se refere o inciso V do caput deste artigo não inclui dados que já tenham sido anonimizados pelo controlador.
> § 8º O direito a que se refere o § 1º deste artigo também poderá ser exercido perante os organismos de defesa do consumidor (BRASIL, 2019, [s. p.]).

Esses direitos que o titular pode requerer do controlador serão discutidos a seguir:

> I - confirmação da existência de tratamento; (ou seja, o titular de dados pessoais, poderá ir a qualquer controlador de dados – lembrando que controlador é quem determina o tratamento dos dados pessoais, é quem vai dar as ordens sobre o tratamento de dados pessoais), o titular dos dados poderá exigir do controlador para que este confirme se trata dados pessoais dele ou não.
> Esses controladores (pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais) têm que estar preparados para responder a essa pergunta: ou que sim ou que não, confirmando ou não a existência desse tratamento (BRASIL, 2019, [s. p.]).

Figura 8 – Confirmação de tratamento de dados pessoais



Fonte: Elaborado pela autora.

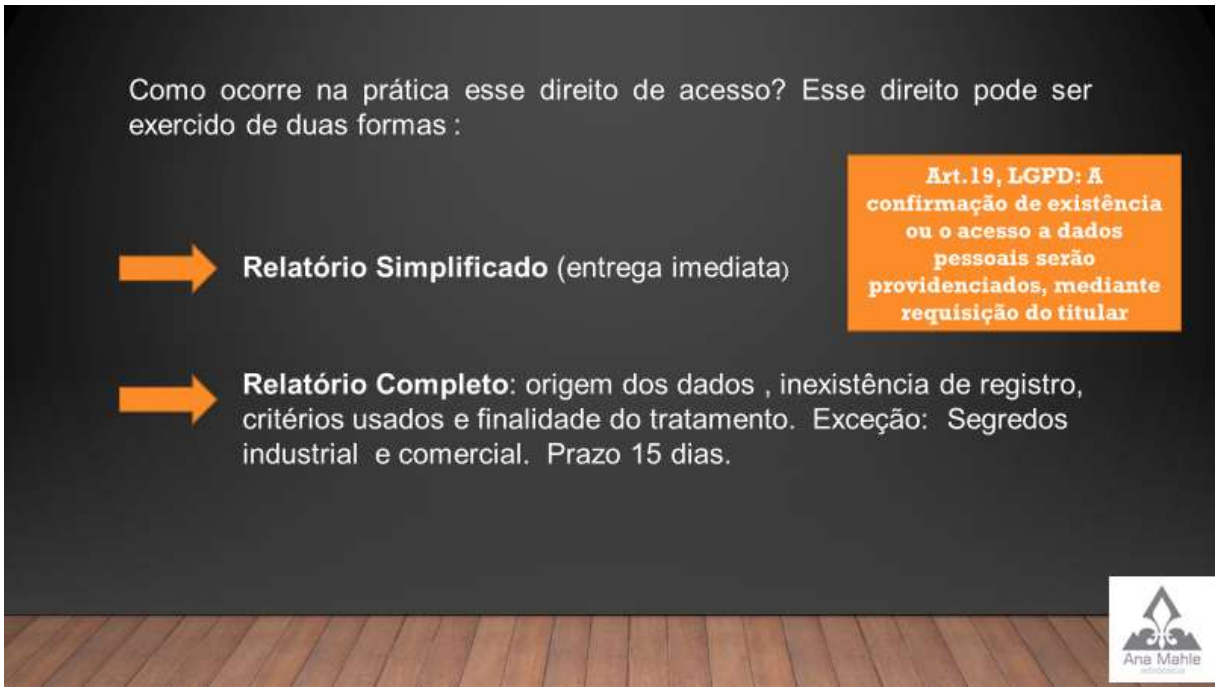
Como demonstrado na figura acima, se o controlador confirmar que há o tratamento de dados pessoais, o seu titular poderá exercer o direito disposto no inciso II do art. 18 ("II - acesso aos dados") (BRASIL, 2019, [s. p.]). Esse direito de acesso se desdobrará em muitos pontos importantes, mas dele também surge uma dúvida: *Como é que o titular dessas informações poderá acessar os dados seus que estão armazenados por um controlador?*

Este é um ponto crucial, porque além do exercício da autodeterminação informativa, as organizações (controladores de dados em geral) devem estar estruturadas para responder as questões levantadas pelos titulares de dados. O controlador terá que saber responder de forma eficaz ou que sim ou que não; e uma vez que se confirme que há a existência de tratamento, as organizações[11], deve estar apto a informar as especificidades das informações armazenadas nos bancos de dados.

Antes de voltar aos incisos restantes do artigo 18, será feita uma conexão com o art. 19 da LGPD, que foca especificamente no direito de acesso.

11 "Organização" está sendo tratada aqui de maneira genérica, porque conforme já exposto, os controladores podem ser pessoas jurídicas públicas ou privadas ou mesmo um particular.

Figura 9 – Formas de relatório sobre requisição de titulares de dados



Fonte: Elaborado pela autora.

O direito de acesso versa o quê? É o direito que o titular tem de acessar e se informar sobre quais de seus dados estão nas mãos dos controladores, e esse direito se divide em dois. O controlador tem que ter a capacidade de entregar ao titular dois relatórios diferentes:

1) O primeiro relatório, em formato simplificado (apenas com os dados pessoais que constam no banco de dados), tem que ser entregue de imediato;

2) O outro tipo de relatório é o relatório completo, previsto no artigo 19 inciso II, que diz que o titular tem direito a acessar os seus dados pessoais por meio de declaração clara e completa que indique além dos dados pessoais, tendo que se entregar: a origem dos dados, a confirmação sobre a inexistência de registro, os critérios utilizados e a finalidade do tratamento, observados os segredos comercial e industrial, que não precisarão ser entregues. Tal relatório deverá ser fornecido no prazo de até 15 (quinze).

Quanto à forma de entrega desses relatórios, ela pode ser feita tanto de forma eletrônica quanto impressa, gratuitamente, havendo a possibilidade de exceções – há casos de cobrança na Europa (Regulamento Geral de Proteção de Dados) em situações excepcionais, a partir do abuso de direito pelo titular – com pedidos excessivos, solicitando vários relatórios em um curto período de tempo, mas isso ainda deverá ser regulado pela ANPD.

Para a elaboração do relatório completo, é interessante analisar o art. 9º da LGPD, que traz o direito de acesso do titular dos dados. É como se esse artigo trouxesse uma recomendação para fazer constar nesse relatório:

> Art. 9º O titular tem direito ao acesso facilitado às informações sobre o tratamento de seus dados, que deverão ser disponibilizadas de forma clara, adequada e ostensiva acerca de, entre outras características previstas em regulamentação para o atendimento do princípio do livre acesso:
> I - finalidade específica do tratamento;
> II - forma e duração do tratamento, observados os segredos comercial e industrial;
> III - identificação do controlador;
> IV - informações de contato do controlador;
> V - informações acerca do uso compartilhado de dados pelo controlador e a finalidade;
> VI - responsabilidades dos agentes que realizarão o tratamento; e
> VII - direitos do titular, com menção explícita aos direitos contidos no art. 18 desta Lei (BRASIL, 2018, [s. p.]).

Esse artigo traz o princípio da finalidade, isto é, será necessário informar um motivo, uma justificativa para cada atividade. Outro ponto muito importante que ele traz é quanto à forma e duração do tratamento: *Como o tratamento vai acontecer? É um tratamento automatizado (feito por inteligência artificial) ou é feito por pessoas? Há previsão para a exclusão desse dado?*

Nesse artigo, diz-se ainda que há a necessidade de informar o titular de dados quanto à identificação do controlador; isso é muito importante para que o titular saiba quem é o controlador e também tenha acesso às suas informações de contato (se for em ambiente virtual, qual a página, e-mail de contato do responsável pelo tratamento; se for em ambiente físico, será preciso fornecer endereço, o telefone).

Por seu turno, o artigo 9º traz os seguintes pontos sobre o direito de acesso: s*erá que houve um uso compartilhado dos dados pessoais? Se houve o compartilhamento, quais as empresas/organizações que acessaram esses dados?*

Logo, as organizações precisam ter o mapeamento dos seus dados em dia. A boa gestão de dados é extremamente importante, porque elas têm que conseguir dizer se compartilharam dados e com quem compartilharam, assim como entender todo o ciclo de vida dos dados pessoais que elas tratam, visto que se o titular vier bater à sua porta e questioná-las, essas companhias vão ter que informá-lo. Resumindo, os controladores terão que identificar todas as atividades da organização: quais os dados coletados, qual o uso (finalidade), com quem compartilham, como armazenam e em quanto tempo irão apagá-los. Isso vale para todo tipo de

atividade, em ambiente físico ou digital, relações empregatícias, com consultores, fornecedores ou prestadores de serviços – trata-se de um leque bem extenso de atividades.

Além disso, o art. 9 traz as responsabilidades dos agentes que realizarão o tratamento; há a necessidade de declarar quais são as responsabilidades dos agentes que vão lidar com o trânsito dos dados; se tiver mais de um agente, mais de um controlador ou operador, há a necessidade de especificar qual o limite da responsabilidade de cada um, ou seja, quem armazena e enriquece os dados e a sua base, quem faz estudos sobre aqueles dados ou inferências neles, sempre limitando as questões de segredo comercial e industrial – que serão entregues somente mediante auditoria da ANPD, se houver necessidade.

Por fim, o artigo também faz menção explícita aos direitos dos titulares contidos no art. 18 da LGPD. Por consequência, ele poderá funcionar como um manual de boas práticas na elaboração de um relatório completo de acordo com artigo 19 da LGPD, que demonstrará a boa-fé dos agentes de tratamento de dados, assim como facilitará aos titulares o exercício dos seus direitos, dentre eles a autodeterminação informativa.

Voltando para o art. 18 (dos direitos dos titulares), foi abordado até o momento os dois primeiros incisos, que falam sobre a confirmação da existência do tratamento, a partir do qual o titular poderá ter acesso aos seus dados, direito contido nos artigos 9 e 19 da LGPD. Em adição a esses direitos, o titular tem mais sete, dispostos no art. 18.

Um diz respeito à correção de dados incompletos, inexatos ou desatualizados – também conhecido como o *direito de retificação*, que é o direito de se corrigir os dados que estejam gravados de forma errada. Como titular, uma determinada pessoa pode solicitar que suas informações sejam corrigidas ou atualizados mediante requisição (remete-se ao princípio da qualidade dos dados, que diz que os dados pessoais têm sempre que estar corretos e atualizados, o que se faz muito importante, posto que muitas vezes perfis errados, ou um conjunto de dados equivocados, podem levar a decisões erradas acerca da pessoa).

Outro direito do art. 18 é: "IV - anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto nesta Lei" (BRASIL, 2018, [s. p.]). *Mas no que consiste essa anonimização?*

O conceito de anonimização está disposto no art. 5º, inciso XI, da LGPD: "XI - anonimização: 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" (BRASIL, 2018, [s. p.]).

De acordo com esse inciso, o titular pedir a retirada de dados que possibilitem a sua identificação; os dados vão continuar armazenados, mas não vai mais ser possível identificar a quem aqueles dados correspondem. Para que essa técnica seja eficiente, ela tem que tornar 'impossível' a identificação do titular daqueles dados. Com o avanço da tecnologia, fica cada vez mais possível a reversão dessa técnica, mas a própria lei diz que o mecanismo que for usado no momento dessa anonimização tem que ser considerado razoável e disponível, logo dependente de interpretação.

Mas por que a anonimização é tão importante? Porque dados anonimizados não são considerados dados pessoais, logo a LGPD não se aplica a eles, como disposto em seu art. 12:

> Art. 12. Os dados anonimizados não serão considerados dados pessoais para os fins desta Lei, salvo quando o processo de anonimização ao qual foram submetidos for revertido, utilizando exclusivamente meios próprios, ou quando, com esforços razoáveis, puder ser revertido (BRASIL, 2018).

Os 'esforços razoáveis e meios próprios' contidos nesse artigo também são dignos de interpretação, por exemplo: se o titular pede para determinada empresa anonimizar os seus dados pessoais, ela terá que garantir, de alguma certa forma, que isso não será reversível, pois se a empresa/organização retirar algumas letras do nome do titular e ainda continuar fácil a sua identificação (a partir da junção com outros dados), ou seja, a entidade não dispôs das suas melhores técnicas para retirar o fator de identificação do dado pessoal. Com a anonimização uma vez revertida, torna-se novamente um dado pessoal identificável, desrespeitando o direito ora citado. Assim, mostra-se crucial a eficiência desse processo.

Maldonado e Blum (2019) dizem que os meios de reversão de dados anonimizados para dados que identifiquem uma pessoa, para não serem regidos pela LGPD, deverão demandar um esforço relevante e complexo, a ponto de se tornar impossível o seu atingimento, do contrário tais dados não deverão ser considerados anonimizados.

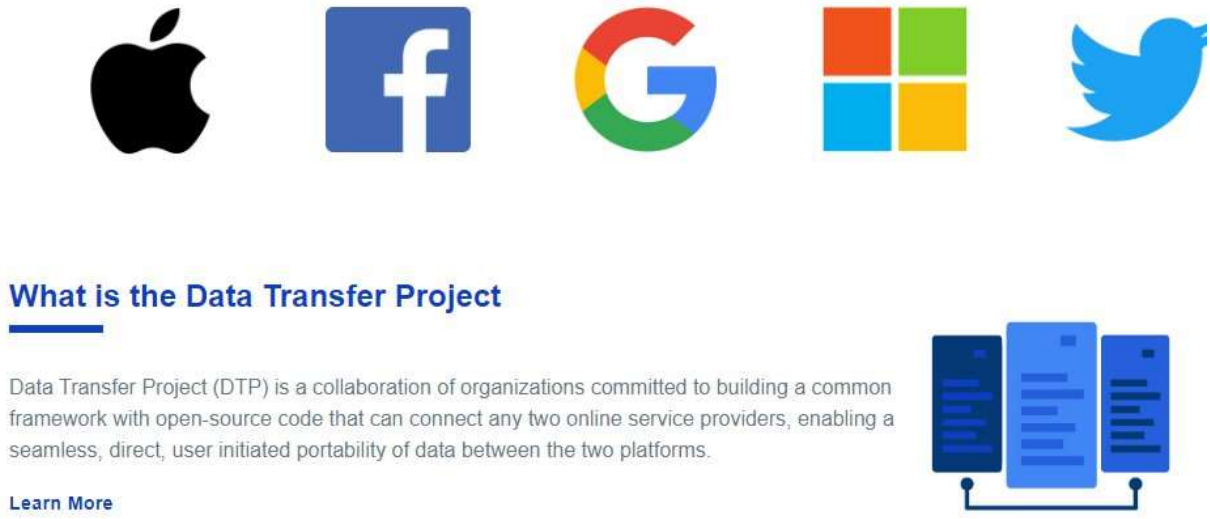
Um direito um tanto mais complexo é o que fala da portabilidade dos dados do titular mediante requisição expressa, conforme regulamentação da ANPD. Como exemplo, temos: imagine um motorista de aplicativo, com um bom histórico de corridas, bem pontuado, mas que resolveu mudar de plataforma, da empresa X para a Y. Será que ele vai ter que começar todo o seu histórico do zero? Quando alguém for pedir uma corrida com ele, verá que ele não possui histórico de viagens? Isso dificultaria o seu trabalho. Dessa maneira, pensando que na outra empresa ele tinha um histórico muito bom, *será que ele pode portar esses dados para a outra*

plataforma? Se houver o entendimento de que isso é um dado pessoal, ele vai, sim, conseguir a portabilidade.

Contudo, isso vai exigir diversos investimentos, por exemplo: que as empresas fiquem atentas a como essa questão vai acontecer na prática; os sistemas das empresas vão ter que conversar, para que se consiga fazer a portabilidade de um conjunto de dados para outro banco de dados, para que ocorra essa transferência dentro de determinados padrões de segurança, porque se os sistemas forem incompatíveis, caberá à ANPD estabelecer padrões de interoperabilidade (para essa conversa entre os sistemas das empresas acontecer e ocorrer a portabilidade), e nisso a ANPD ainda terá muito trabalho.

Trata-se de um direito que pode ser considerado como um diferencial competitivo, posto que se os usuários puderem fazer a migração de uma plataforma para outra sem perder seus benefícios, as empresas terão um incentivo extra para melhorar a oferta dos seus serviços. Por isso que essas gigantes da tecnologia (figura) estão trabalhando em conjunto:

Figura 10 – *Data Transfer project*



Fonte: Imagens extraídas da plataforma Google imagens.

Essa cooperação visa permitir uma portabilidade direta, que poderá ser feita pelo próprio usuário de dados entre as duas plataformas, permitindo a conversa entre diferentes sistemas operacionais, essa operação específica é denominada de *Data Transfer Project*[12].

Com vistas à conformidade às leis de proteção de dados, o WhatsApp está prestes a mudar suas configurações. O *WABetaInfo* está desenvolvendo uma função que vai permitir a migração do histórico de chats para outro sistema operacional: se a pessoa usa um dispositivo iOS vai poder fazer a portabilidade para um Android, e vice-versa. Resumindo, poderá ser feita a portabilidade de informações de uma plataforma para outra; a pessoa que mudar de sistema operacional não vai mais perder todo o seu histórico de conversa (ANDRION, 2021).

Outro direito trazido no art. 18 é o que se refere à eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no art. 16 desta Lei. De acordo com esse direito, os titulares podem solicitar a exclusão dos seus dados pessoais, exceto nas hipóteses previstas no artigo 16, que são situações em que o término do tratamento não vai acontecer, como exemplo do cumprimento de obrigação legal. Essa eliminação é um direito que o titular possui, tendo como base legal o consentimento. É um direito mais simples, mais direto, mais objetivo, não tem muita discussão relacionada a esse direito, também conhecido como *direito ao cancelamento de dados pessoais*.

Há ainda o direito expresso no art. 18, em que o titular pode solicitar informação das entidades públicas e privadas com as quais o controlador compartilhou os dados. Essa é uma informação que todos os controladores de dados têm que ter desde da aprovação da Lei. Atualmente os titulares de dados já podem questionar as companhias acerca disso: "*Empresa, você tem dados pessoais meus aí na sua base de dados? Com quem você os compartilhou*?" As organizações deverão estar aptas a responder esses possíveis questionamentos.

Mais um direito elencado no art. 18 é que o titular tem direito à informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa. *Quantas vezes as pessoas são praticamente forçadas dar o consentimento a um aplicativo, a um serviço?* Esse direito diz que os titulares devem receber a informação sobre os riscos de não fornecer o

12 O projeto de *Data Transfer* foi lançado em 2018 para criar uma plataforma de portabilidade de dados de serviço de código aberto para que todos os indivíduos na *web* pudessem facilmente mover seus dados entre provedores *online* sempre que quisessem. Os contribuintes do Projeto de *Data Transf* acreditam que a portabilidade e a interoperabilidade são fundamentais para a inovação. Tornar mais fácil para os indivíduos escolher entre os serviços facilita a competição, capacita os indivíduos a experimentarem novos serviços e permite que eles escolham a oferta que melhor se adapta às suas necessidades (DATA..., 2021).

seu consentimento, exemplificando: se a pessoa não quiser dar o seu consentimento, ela vai ser comunicada sobre as limitações de navegação em um site ou de acesso a determinado produto. É direito do titular ser informado das consequências sobre a negativa do seu consentimento.

Por fim, o último direito do art. 18 é a revogação do consentimento previsto no §5º do art. 8. O titular deve saber que tem direito de revogar seu consentimento, além de saber das consequências disso, porque, em alguns casos, quando se revoga o consentimento, não é mais possível usufruir do produto ou serviço – como visto no parágrafo anterior.

Com todo o exposto, contemplou-se os nove incisos do art. 18 da LGPD, que são direitos relevantíssimos para os titulares dos dados, principalmente para que possam exercer sua autodeterminação informativa. Explicou-se ainda como os arts. 9 e 19 orientam a realização do acesso aos dados pessoais. A partir daqui serão brevemente analisados os arts. 20, 21 e 22, que constam no Capítulo III da LGPD, dos direitos dos titulares.

O art. 20 diz que o titular terá direito de solicitar revisão de decisões automatizadas:

> O titular dos dados tem direito a solicitar a revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, incluídas as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade (BRASIL, 2018).

Nesse artigo, pode-se destacar cinco grandes aspectos (pessoal, profissional, consumo, crédito e personalidade). Se houver decisões automatizadas (decisões tomadas automaticamente por inteligência artificial, por robôs) baseadas em uma dessas características, o titular dos dados pode solicitar a revisão dessas decisões.

Tal tema teve e tem bastante discussão na legislação, mesmo porque os seres humanos estão cada vez mais sujeitos a decisões automatizadas, desde um crédito solicitado no banco até a solicitação de exclusão de um número de telefone. *Por que se debate até onde seria interessante tantos questionamentos? Até que ponto isso seria permitido?*

Quando se olha para os dois parágrafos do artigo 20, consegue-se extrair que não é necessário haver uma pessoa na revisão das decisões automatizadas, podendo ser um robô revendo decisões tomadas por outro robô. Isso ainda está no devir do tempo e deverá se tornar mais compreensível através de decisões judiciais e regulamentações a serem elaboradas.

> § 1º O controlador deverá fornecer, sempre que solicitadas, informações claras e adequadas a respeito dos critérios e dos procedimentos utilizados para a decisão automatizada, observados os segredos comercial e industrial.

> § 2º Em caso de não oferecimento de informações de que trata o § 1º deste artigo baseado na observância de segredo comercial e industrial, a autoridade nacional poderá realizar auditoria para verificação de aspectos discriminatórios em tratamento automatizado de dados pessoais. (BRASIL, 2018)

Para encerrar o tópico dos direitos dos titulares na LGPD, temos os artigos 21 e 22:

> Art. 21. Os dados pessoais referentes ao exercício regular de direitos pelo titular não podem ser utilizados em seu prejuízo.
> Art. 22. A defesa dos interesses e dos direitos dos titulares de dados poderá ser exercida em juízo, individual ou coletivamente, na forma do disposto na legislação pertinente, acerca dos instrumentos de tutela individual e coletiva. (BRASIL, 2018)

Em resumo, tais artigos dizem o seguinte: os dados pessoais referentes ao exercício regular de direitos pelo titular não poderão ser usados em seu prejuízo, e a defesa dos interesses do titulares de dados poderá ser exercida tanto de forma individual quanto coletiva.

De acordo com Maldonado e Blum (2019, p. 236), a lista trazida na seção de Direitos dos Titulares da LGPD é restrita aos titulares de dados, uma vez que terceiras pessoas não possuem autorização para demandar em nome alheio. Assim, é o próprio titular quem formula o requerimento expresso – ou através do seu representante legal constituído para essa finalidade específica.

Salienta-se que a maioria dos direitos exemplificados no rol do art. 18 da LGPD não é novidade no ordenamento jurídico brasileiro. Por mais inovadora que essa Lei seja, ela traz muitos direitos existentes no Brasil já há muito tempo – os direitos dos titulares de dados não tiveram início nessa lei, fato que será melhor abordado na seção 4.2.

Mediante todos os direitos dos titulares que a Lei trouxe, criou-se, como mencionado anteriormente, um canal de acesso rápido e direto que as companhias terão que ter para o recebimento de requisições dos titulares, conforme disposto no artigo 41 da LGPD, Seção II, chamada “Do Encarregado pelo Tratamento de Dados Pessoais”:

> O controlador deverá indicar encarregado pelo tratamento de dados pessoais.
> § 1º A identidade e as informações de contato do encarregado deverão ser divulgadas publicamente, de forma clara e objetiva, preferencialmente no sítio eletrônico do controlador.
> § 2º As atividades do encarregado consistem em:
> I - aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências;
> II - receber comunicações da autoridade nacional e adotar providências;
> III - orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais; e

> IV - executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares.
> § 3º A autoridade nacional poderá estabelecer normas complementares sobre a definição e as atribuições do encarregado, inclusive hipóteses de dispensa da necessidade de sua indicação, conforme a natureza e o porte da entidade ou o volume de operações de tratamento de dados (BRASIL, 2018, [s. p.]).

Além das duas figuras que tratam dados (controlador e operador), a Lei concebe uma outra, denominada de 'encarregado' (*Data Protection Officer* – DPO), que não é considerado agente de tratamento (como os já mencionados), mas é uma nova profissão. O encarregado é o responsável por verificar se os dados que estão dentro da empresa estão em acordo com a norma; essa pessoa deverá ter conhecimentos técnicos e jurídicos e saber onde os dados foram coletados (origem), para o que a empresa os quer (finalidade) e qual é sua sensibilidade (BIONI, 2019). Logo, é um instrumento a mais para auxiliar os titulares a exercerem os seus direitos e, portanto, a autodeterminação informativa.

A Lei ainda traz 10 bases legais para que os dados pessoais sejam tratados, ou seja, o consentimento não é a única forma para que ocorra essa ação. O tratamento de dados pessoais tem que obedecer às regras previstas na LGPD. Além dos princípios, essa legislação traz hipóteses legais, que vão muito além do consentimento, sendo ele apenas uma dessas 10 bases desse "cardápio". Bioni (2019) faz o apontamento dessas bases:

1) **Consentimento**: autorização do titular dos dados;
2) **Base legal**: cumprimento de obrigação legal regulatória – por exemplo: o Banco Central (órgão regulador) exige que os bancos deem informações sobre cheques sem fundo; essas informações identificam uma pessoa, mas são permitidas de acordo com essa base legal.
3) **Execução de políticas públicas**: execução de uma política que é de interesse da sociedade, como exemplo tem-se a vacinação, que é de interesse dos órgãos públicos e da sociedade, consequentemente não é necessária a autorização pessoal para tratar os dados para esse tipo de situação;
4) **Execução de um contrato**: *como executar um contrato se não souber quem é a outra parte? Como se faz a cobrança?*. É necessário ter acesso ao endereço da pessoa devedora ou o CPF, que são considerados dados pessoais;

5) **Exercício regular de direitos**: pode-se deixar um dado armazenado em base de dados pelo tempo da prescrição, mesmo que já tenha terminado a obrigação para poder exercer um direito se eventualmente ocorrer um processo;
6) **Proteção da vida**: em caso de acidente, por exemplo, uma pessoa com ferimentos graves dá entrada em um hospital em que ela nunca esteve, que fica autorizado a trocar dados com outro hospital a fim de descobrir o histórico do paciente, por exemplo se ele é alérgico a algum tipo de medicamento;
7) **Realização de estudos por órgão de pesquisa**: Fica autorizada a coleta de dados para atividade acadêmica e de pesquisa, mas sempre que possível deverá ser feita a anonimização desses dados;
8) **Tutela da Saúde**: exclusivamente realizado por profissionais da saúde, serviços de saúde ou autoridade sanitária – assim sendo as atividades que estão sendo feitas pelas autoridades sanitárias para a contenção da pandemia do coronavírus ficam respaldadas por essa base legal, salvo exceções;
9) **Proteção de Crédito**: o banco tem que ter condições de verificar se determinada pessoa tem capacidade para adimplir uma dívida. A Lei do Cadastro Positivo é uma legislação que vigora paralelamente à LGPD. Um exemplo de Proteção de Crédito seria um titular dos dados requerer a exclusão dos seus dados nos cadastros do SPC e Serasa, sob a alegação que não autorizou o referido tratamento ou que isso violaria a sua privacidade, porém ele não pode usar dessa alegação para fugir da cobrança dessa dívida;
10) **Legítimo Interesse**: necessário para atender aos interesses legítimos do controlador ou de terceiros, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais. *Quando atende aos interesses legítimos do controlador?* O legítimo interesse é uma base legal muito ampla e tem um conceito jurídico indeterminado. O que é legítimo interesse para uma pessoa pode ser diferente para outra pessoa, é subjetivo (BIONI, 2019).

Para essa base legal não se tornar um cheque em branco, Bioni (2019) criou diretrizes para a interpretação e fiscalização dessa base, um teste de 4 fases (*Teste de Legítimo Interesse*) – descritas abaixo – para definir se há legítimo interesse ou não:

1) **Avaliação de legitimidade:** a finalidade só será analisada sob o plano de interesse comercial ou público de quem está processando esses dados – *Existe uma finalidade legítima de quem está processando aqueles dados?*
2) **Teste de Necessidade:** é o princípio da minimização dos dados – *É possível atingir essa mesma finalidade coletando a menor quantidade possível de dados?*
3) **Regra de Balanceamento:** tem que existir um equilíbrio no legítimo interesse de quem está processando, tratando esses dados com os direitos do titular – *Como isso vai impactar na liberdade e garantir direitos fundamentais do sujeito? Se houver algum impacto, será muito intrusivo ou não?*
4) **Mitigação de riscos:** adoção de ações que reduzam riscos, por exemplo anonimizar os dados ou ser mais transparente quanto à coleta (BIONI, 2019).

É possível colocar opções fáceis de *opt in*[13] ou *opt out*[14] (isto é, a autodeterminação informativa: a pessoa tem que ter autonomia sobre as decisões tomadas com base nos seus dados, assim como a coleta dos dados deve estar dentro da "legítima expectativa da pessoa"), por exemplo: quando se baixa um aplicativo de corrida, com a finalidade de medir a distância do trajeto, pode estar dentro da legítima expectativa de quem realizou o download oferecer para ele anúncios de suplementos alimentares ou de acessórios para esse tipo de esporte. *Mas será que há legítima expectativa no fato de haver o cruzamento dos dados do usuário do app com o convênio de saúde para dizer se a pessoa é sedentária ou não?*

Outro exemplo: talvez o banco não precise do consentimento para ver qual é o padrão de consumo de alguém, porque com base nesse padrão de consumo, o banco pode identificar operações financeiras que serão de possíveis fraudadores. O banco, quando coleta o dado, traça um perfil, mas ele tem um legítimo interesse que vai de encontro com a proteção dos direitos de seus clientes.

A ideia que o legítimo interesse traz é a ideia de boa-fé, e a GDPR traz o conceito de *lealdade* para expressar o significado de legítimo interesse. A LGPD não traz a palavra lealdade expressa na sua legislação, mas no dicionário brasileiro esse termo é conceituado como: o "[...]

13 *Opt In*: é a maneira mais comum de uma pessoa entrar na lista de contato do negócio, pois oferecerá seus dados com o objetivo de estar por dentro do que ocorre naquela organização. Sendo assim, a pessoa que não concordar em fazer o opt in não estará apta para acessar a seus conteúdos de SMS (TWW..., 2019).
14 *Opt Out*: a possibilidade de você se descadastrar daquela lista que já não mais fornece conteúdos relevantes. No campo de vista empresarial, não faz sentido você continuar enviando mensagens para aquela pessoa que já foi interessada pelos seus assuntos (TWW..., 2019).

respeito aos princípios e regras que norteiam a honra e a probidade. Fidelidade aos compromissos assumidos" (OXFORD…, 2021, [s. p.]). Por isso, espera-se que o legítimo interesse seja feito dentro dos termos estipulado por Bioni (2019) e que o termo lealdade trazido pela GDPR acabe se tornando o resumo dessa base legal que é o legítimo interesse.

Como visto neste capítulo, o direito à proteção de dados já existia de modo disperso na legislação brasileira, como no caso do Marco Civil da Internet; mas antes de estar disposto nessa legislação, já podia ser extraído do Código de Defesa do Consumidor, como será descrito no tópico abaixo, principalmente no tocante aos direitos dos titulares.

4.2 CDC e LGPD E CASOS ESPECIAIS DE TRATAMENTO DE DADOS

Já existia uma correlação na legislação brasileira com os direitos que são manifestados pela LGPD desde 1990: o Código de Defesa do Consumidor (CDC), que é uma legislação consolidada com mais de 30 anos e já trazia diversos desses direitos. No entanto, a proteção à privacidade do CDC é voltada para proteção do consumidor e restrito a ele, enquanto a LGPD protege todas as pessoas naturais, estando elas em uma relação de consumo ou não, em ambiente virtual ou físico. No que diz respeito ao CDC, pode-se encontrar direitos de titulares de dados (consumidores) no artigo 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.
> § 1° Os cadastros e dados de consumidores devem ser objetivos, claros, verdadeiros e em linguagem de fácil compreensão, não podendo conter informações negativas referentes a período superior a cinco anos.
> § 2° A abertura de cadastro, ficha, registro e dados pessoais e de consumo deverá ser comunicada por escrito ao consumidor, quando não solicitada por ele.
> § 3° 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.
> § 4° Os bancos de dados e cadastros relativos a consumidores, os serviços de proteção ao crédito e congêneres são considerados entidades de caráter público.
> § 5° 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 (BRASIL, 1990, [s. p.]).

Esse artigo traz o direito do consumidor de ter acesso às suas informações (o *direito de acesso*, previsto no artigo 18, inciso II, da LGPD). Além disso, o consumidor tem direito de conhecer as respectivas fontes (caput, artigo 43 – CDC), o que significa que o consumidor tem direito de saber da origem daqueles dados. Assim, o consumidor, a priori, tem o direito de pedir um relatório que lhe informe sobre esses dados; mas como o Brasil ainda está construindo a cultura de proteção de dados, essa é uma prática que ainda não é usual e deve se tornar recorrente conforme a sociedade for aderindo a essa nova cultura. Também, como visto, já havia a obrigação de os fornecedores informarem a origem e o conteúdo dos dados.

No parágrafo 4° do artigo 43, nota-se que qualquer banco de dados de consumo ficará sujeito ao *habeas data*, pois lá diz expressamente que os bancos de dados e os cadastros de consumidores são considerados entidades de caráter público, portanto se encaixam na descrição legal do artigo 5º, inciso LXXII da Constituição Brasileira:

> Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:
> 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 (BRASIL, 2016, [s. p.]).

Nesse artigo, no parágrafo 1º, encontram-se diversos direitos dos titulares (consumidores, para o CDC), segundo os quais os cadastros devem ser objetivos, claros, verdadeiros e compreensíveis. Já no parágrafo 2º, há o direito à comunicação: o consumidor terá que ser comunicado da abertura de um cadastro que não tenha sido solicitado. Visto que o CDC é uma legislação com mais de 30 anos, o armazenamento de dados do consumidor era permitido sem o consentimento do titular, mas era necessária a sua comunicação. Porém, com o advento da LGPD, essa prática não será mais possível, porque para se tratar dados pessoais, essa ação tem que encontrar respaldo legal no artigo 7º da LGPD, em que estão previstas as bases legais que autorizam o tratamento desses dados.

Já no parágrafo 3°, há o direito de retificação: o consumidor, se encontrar algum erro em seus dados, poderá exigir a retificação dos mesmos. No parágrafo 6º, por sua parte, há o direito à inclusão de pessoas com deficiência – incluído em 2015, pela lei nº 13.146/15 (Estatuto da Pessoa com Deficiência).

Conforme demonstrado, a LGPD trouxe vários direitos que já existiam há bastante tempo no ordenamento jurídico brasileiro, assim como também trouxe muita coisa da GDPR, que é a lei de proteção de dados europeia.

4.3 CASOS ESPECIAIS DE TRATAMENTOS DE DADOS

A LGPD, como já mencionado, traz uma diferenciação referente ao tratamento de dados pessoais nos casos, o que será discutido nas subseções 4.3.1 e 4.3.2.

4.3.1 Tratamento de Dados Pessoais Sensíveis

Dados pessoais sensíveis são informações que receberam um tratamento diferenciado. Na Europa são conhecidos como *dados de categoria especial*; no Brasil, foram denominados *dados sensíveis*, considerados como informações com um maior potencial lesivo ao titular, por terem características que podem ferir a esfera da privacidade do indivíduo com maior severidade, isto é, podem levar à maior chance de discriminação da pessoa, como definido no artigo 5º, inciso II, da LGPD. Para os fins desta Lei, considera-se:

> (...) II - dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural […] (BRASIL, 2018, [s. p.]).

É preciso observar que alguns dados são originalmente não sensíveis, podendo se tornar como exemplo o dado de geolocalização: quando uma pessoa frequenta determinada igreja, por exemplo, mostrando uma frequência de hábito. A biometria também é considerada dado sensível, por ser um dado imutável: se a pessoa perde o seu cartão de crédito, é só cancelar e será feito um cartão novo, com um novo número; mas os dados biométricos não podem ser modificados. As bases legais que a LGPD traz para o tratamento de dados – que são dez hipóteses legais (como já analisado) – não poderão ser utilizadas em sua totalidade, ficando restrita a oito fundamentos legais, passíveis de serem usados quando se tratar de dado pessoal sensível, conforme disposto no artigo 11º da LGPD:

> O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses:
> I - quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas;
> II - sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para:
> a) cumprimento de obrigação legal ou regulatória pelo controlador;
> b) tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos;
> c) realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis;
> d) exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral, este último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem);
> e) proteção da vida ou da incolumidade física do titular ou de terceiro;
> f) tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; ou
> g) garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no art. 9º desta Lei e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais.
> § 1º Aplica-se o disposto neste artigo a qualquer tratamento de dados pessoais que revele dados pessoais sensíveis e que possa causar dano ao titular, ressalvado o disposto em legislação específica.
> § 2º Nos casos de aplicação do disposto nas alíneas ‘a’ e ‘b’ do inciso II do caput deste artigo pelos órgãos e pelas entidades públicas, será dada publicidade à referida dispensa de consentimento, nos termos do inciso I do caput do art. 23 desta Lei.
> § 3º A comunicação ou o uso compartilhado de dados pessoais sensíveis entre controladores com objetivo de obter vantagem econômica poderá ser objeto de vedação ou de regulamentação por parte da autoridade nacional, ouvidos os órgãos setoriais do Poder Público, no âmbito de suas competências.
> § 4º É vedada a comunicação ou o uso compartilhado entre controladores de dados pessoais sensíveis referentes à saúde com objetivo de obter vantagem econômica, exceto nas hipóteses relativas a prestação de serviços de saúde, de assistência farmacêutica e de assistência à saúde, desde que observado o § 5º deste artigo, incluídos os serviços auxiliares de diagnose e terapia, em benefício dos interesses dos titulares de dados, e para permitir:
> I - a portabilidade de dados quando solicitada pelo titular; ou
> II - as transações financeiras e administrativas resultantes do uso e da prestação dos serviços de que trata este parágrafo.
> § 5º É vedado às operadoras de planos privados de assistência à saúde o tratamento de dados de saúde para a prática de seleção de riscos na contratação de qualquer modalidade, assim como na contratação e exclusão de beneficiários (BRASIL, 2018, [s. p.]).

Diante desse dispostivo legal, nota-se que o legislador deixou de fora o tratamento de dados sensíveis nas hipóteses de legítimo interesse e proteção de crédito (Art. 7º, IX e X). O consentimento em relação ao tratamento de dados sensíveis ganhou uma definição extra do disposto no artigo 5º, XII, da LGPD, no qual se diz que o consentimento é uma manifestação livre, informada e inequívoca em que o titular dessas informações tem que concordar com o seu tratamento. De acordo com Teffé e Viola (2020), será um desafio compreender o que o

legislador quis englobar quando acrescentou ao consentimento as palavras ‘destacado’ e ‘específico’ no que diz respeito aos dados sensíveis:

> Um dos desafios será compreender a dimensão e o real significado do consentimento caracterizado como específico e destacado. Segundo doutrina, deve-se “enxergá-lo como um vetor para que haja mais assertividade do titular com relação a esses movimentos ‘específicos’ dos seus dados.” A noção, no caso, aproxima-se da ideia de consentimento expresso, por exigir maior atuação do titular dos dados, além de cuidado mais elevado com o tratamento da informação pelo agente.
> *Específico* deve ser compreendido como um consentimento manifestado em relação a propósitos concretos e claramente determinados pelo controlador e antes do tratamento dos dados, havendo também aqui, e com mais ênfase, as obrigações da granularidade.
> *Destacado* pode ser interpretado no sentido de que é importante que o titular tenha pleno acesso ao documento que informará todos os fatos relevantes sobre o tratamento, devendo tais disposições vir destacadas para que a expressão do consentimento também o seja. Além de se referir a dados determinados e haver declaração de vontade que esteja ligada a objetivo específico, a manifestação de vontade deverá vir em destaque no instrumento de declaração que autoriza o tratamento (TEFFÉ; VIOLA, 2020, p. 142).

Vê-se, assim, a diferença entre os adjetivos trazidos pelo legislador no elemento volitivo sobre dados pessoais gerais e dados pessoais sensíveis. Há que se ter um maior cuidado quando o consentimento for tomado quanto aos dados sensíveis, posto que são dados que podem levar à discriminação de uma pessoa. Para demonstrar essa diferenciação, buscamos exemplos acontecidos na Europa referente ao vazamento de dados sensíveis, já que o assunto é relativamente novo no Brasil e, consequentemente, com poucos exemplos.

A primeira multa depois que a GDPR entrou em vigor em Portugal foi o caso do Centro Hospitalar Barreiro Montijo. Nesse caso, não houve efetivamente o vazamento de dados para fora do hospital, a violação se deu pela ausência de uma gestão de acesso aos prontuários médicos, pois todos os profissionais do local tinham acesso a ele. Nesse exemplo, a Autoridade de Proteção de Dados de Portugal constatou que houve três violações à GDPR:

> Centro Hospitalar Barreiro Montijo foi multado em 400.000 euros por violar o Regulamento Geral de Proteção de Dados. A autoridade de supervisão do país, a Comissão Nacional de Proteção de Dados, constatou que houve três violações do GDPR. Primeiro, foi uma violação do Artigo 5 (1) (c), um princípio de minimização, ao permitir acesso indiscriminado a um número excessivo de usuários, e uma violação do Artigo 83 (5) (a) uma violação dos princípios básicos de processamento. Para esses, a multa foi de 150.000 euros. A segunda, violação da integridade e da confidencialidade em resultado da não aplicação de medidas técnicas e organizacionais para impedir o acesso ilícito a dados pessoais ao abrigo do artigo 5.º, n.º 1, alínea f), e também do artigo 83.º, n.º 5, alínea a); uma violação dos princípios básicos de processamento. Lá, a multa foi de 150.000 euros. Ambos os itens acima foram puníveis com uma multa de até 20 milhões de euros ou 4 por cento do volume de negócios total anual. Finalmente, a Comissão Nacional de Proteção de Dados

> (CNPD) foi multada com base no artigo 32 (1) (b), a incapacidade do réu para garantir a continuação da confidencialidade, integridade, disponibilidade e resiliência dos sistemas e serviços de tratamento, bem como a não implementação das medidas técnicas e organizacionais para garantir um nível de segurança adequado ao risco, incluindo um processo para testar, avaliar e avaliar regularmente as medidas técnicas e organizacionais para garantir a segurança do processamento. Lá a multa foi de 100.000 euros, embora a multa máxima fosse de 10 milhões de euros para 2% do total do faturamento anual (JOSEPH, 2019, [s. p.]).

Outro exemplo foi o caso do Hospital de Haga, que também foi multado pela falta de gerenciamento no acesso a prontuários médicos. A diferença em relação ao exemplo anterior é que uma celebridade deu entrada no local com uma tentativa de suicídio e, logo nos primeiros minutos, ocorreram diversos acessos ao seu prontuário, muito mais do que os profissionais que estavam cuidando desse caso. Não houve uma restrição de acesso aos seus dados por parte do hospital, por mais que essa informação pudesse ficar interna, para que não fosse exposta na mídia. Pelo simples fato de os funcionários terem acesso a dados que não condizem com o trabalho daqueles profissionais, os princípios de *adequação*, *necessidade* e *prevenção* da LGPD (BRASIL, 2018, [s.p.]) já deixaram de ser atendidos, isso já configura uma violação à privacidade dessa celebridade – por isso a Autoridade Holandesa multou o hospital no valor de 460 mil euros (KAC; LÓPEZ, 2020).

Com isso, vemos que a Lei Geral de Proteção de Dados teve como objetivo, ao trazer o rol de dados sensíveis, proteger os dados mais valiosos à própria personalidade humana. Na GDPR, além de se especificar os dados acerca da vida sexual, também se fala da orientação sexual, algo que a legislação brasileira não trouxe expressamente. Contudo, embora ausente do corpo da lei, o STF tem uma opinião protetiva quanto aos direitos das uniões homoafetivas[15], como efeito a orientação sexual deverá ser consolidada como dado sensível.

4.3.2 Tratamento de Dados Pessoais de Crianças e Adolescentes

O tratamento de dados pessoais de crianças e adolescentes está regulado no artigo 14º da LGPD, que visa defender os direitos desses sujeitos:

---

15 Uniões Homoafetivas: por unanimidade, o Plenário do Supremo Tribunal Federal (STF) decidiu que, para fins de aplicação de políticas públicas no Distrito Federal, o reconhecimento de união estável entre pessoas do mesmo sexo não pode ser excluído do conceito de entidade familiar. A decisão foi tomada no julgamento em sessão virtual da Ação Direta de Inconstitucionalidade (ADI) 5971 (SUPREMO, 2021a).

> O tratamento de dados pessoais de crianças e de adolescentes deverá ser realizado em seu melhor interesse, nos termos deste artigo e da legislação pertinente.
> § 1º O tratamento de dados pessoais de crianças deverá ser realizado com o consentimento específico e em destaque dado por pelo menos um dos pais ou pelo responsável legal.
> § 2º No tratamento de dados de que trata o § 1º deste artigo, os controladores deverão manter pública a informação sobre os tipos de dados coletados, a forma de sua utilização e os procedimentos para o exercício dos direitos a que se refere o art. 18 desta Lei.
> § 3º Poderão ser coletados dados pessoais de crianças sem o consentimento a que se refere o § 1º deste artigo quando a coleta for necessária para contatar os pais ou o responsável legal, utilizados uma única vez e sem armazenamento, ou para sua proteção, e em nenhum caso poderão ser repassados a terceiro sem o consentimento de que trata o § 1º deste artigo.
> § 4º Os controladores não deverão condicionar a participação dos titulares de que trata o § 1º deste artigo em jogos, aplicações de internet ou outras atividades ao fornecimento de informações pessoais além das estritamente necessárias à atividade.
> § 5º O controlador deve realizar todos os esforços razoáveis para verificar que o consentimento a que se refere o § 1º deste artigo foi dado pelo responsável pela criança, consideradas as tecnologias disponíveis.
> § 6º As informações sobre o tratamento de dados referidas neste artigo deverão ser fornecidas de maneira simples, clara e acessível, consideradas as características físico-motoras, perceptivas, sensoriais, intelectuais e mentais do usuário, com uso de recursos audiovisuais quando adequado, de forma a proporcionar a informação necessária aos pais ou ao responsável legal e adequada ao entendimento da criança (BRASIL, [2018], [s. l.], Art. 14).

Como já observamos, atualmente tudo gira em torno do mundo virtual, e as crianças e adolescentes estão cada vez mais conectadas, ainda mais com a pandemia do coronavírus, que acelerou ainda mais esse processo. As redes sociais estão no centro da atenção desse público, crianças e adolescentes têm acesso cada vez mais cedo às conexões de rede.

Nesse cenário, é importante relembrar que a LGPD não se aplica somente ao universo digital, tendo seu alcance também no mundo físico, como os dados coletados por escolas, clubes, empresas etc. Sendo assim, todas as entidades que tratam de dados de crianças e adolescentes, mesmo que seja somente em cadastros físicos, estão sujeitas à Lei.

A coleta de dados de crianças e adolescentes também pode ser feita através de jogos online, aplicativos e até brinquedos aparentemente inofensivos, como o caso da boneca Cayla, que foi banida da Alemanha por “espionar” o que as crianças diziam, através de suas câmeras e microfones com conexão à internet – o que permitiu que hackers conversassem com os infantes através da boneca (REDE GLOBO, 2017).

Esse é um problema real, do qual a LGPD visa proteger-nos. Há uma opacidade na coleta de dados de menores, a mudança cultural que surge com essa legislação apresenta a necessidade de maior transparência, pois não se trata apenas de uma questão ética, mas sim de uma obrigação legal. O princípio do melhor interesse do menor está previsto na Declaração

Universal dos Direitos da Criança e do Adolescente e também contemplado no Estatuto da Criança e do Adolescente brasileiro, além de estar disposto no caput do artigo 14 da LGPD, o qual também trouxe a proteção desses direitos.

Nos Estados Unidos, há uma legislação existente desde 1998, a *Children On-Line Privacy Protection Act* (COPPA) – aplicada para crianças menores de 13 anos –, que coloca os pais no controle das informações coletadas de seus filhos no ambiente digital e traz várias diretrizes para a coleta, os prazos, o acesso a informações pessoais deles e garantias de confidencialidade e segurança (REINALDO FILHO, 2013).

Já o regulamento europeu (GPDR) diz que as crianças merecem proteção especial quanto aos seus dados pessoais pelo motivo de estarem menos cientes dos riscos, consequências e garantias em relação aos seus direitos relacionados ao tratamento dos seus dados. Dessa forma, as empresas devem envidar esforços razoáveis, levando em consideração a tecnologia disponível, para verificar se o consentimento dado está realmente em conformidade com a lei. Isso pode envolver a implementação de medidas de verificação de idade, como fazer uma pergunta que uma criança comum não seria capaz de responder ou solicitar que o menor forneça o e-mail de seus pais para permitir o consentimento por escrito (EUROPEAN…, 2021).

Portanto, como os menores não possuem um discernimento eficaz e completo, os dados pessoais de crianças e adolescentes têm que ter um tratamento diferenciado, e isso é feito através da obtenção do consentimento dos pais.

4.4 PODER PÚBLICO E PRINCÍPIOS PARA O TRATAMENTO DE DADOS PESSOAIS

Conforme vimos nos capítulos anteriores, vários eventos políticos e sociais aconteceram nas últimas décadas, moldando o Estado e as pessoas através do tempo. Como o Estado é composto de pessoas, resume-se que o seu alicerce está estruturado sobre um amontoado de dados pessoais. A coleta de dados pessoais do cidadão é feita desde o seu nascimento até a sua morte, por conseguinte o Estado é um dos principais atores quando se fala em Proteção de Dados, visto que as primeiras leis de proteção de dados surgiram em decorrência das limitações impostas ao seu poder.

Wimmer (2020) afirma que o tratamento de dados pessoais é condição indispensável para as atividades do Poder Público:

> A Lei Geral de Proteção de Dados Pessoais brasileira – LGPD, fortemente inspirada na tradição europeia, se propõe a proteger dados pessoais tanto no que se refere ao seu uso em ambientes de mercado como também no contexto de seu uso pelo próprio Estado. Tal amplitude de escopo reflete a constatação de que a crescente digitalização da sociedade e da economia vem acompanhada da transformação digital do próprio Estado, que com cada vez mais intensidade, tem adotado tecnologias digitais para prestar serviços e para formular, monitorar e implementar políticas públicas nas mais diversas searas. O tratamento de dados pessoais pelo Estado não é novidade; seria possível mesmo afirmar que tal atividade está na essência das atividades do Poder Público e constitui condição indispensável para o cumprimento de suas missões. O ingrediente novo na discussão, entretanto, relaciona-se às mudanças quantitativas e qualitativas no tratamento de dados propiciadas pelos novos métodos, algoritmos e tecnologias. As possibilidades cada vez mais sofisticadas de coleta e cruzamento de dados, associadas à natural assimetria entre cidadãos e Poder Público, têm tornado mais relevante e urgente o debate acerca das condições de contorno para o uso e tratamento de dados de cidadãos pelo Estado (WIMMER, 2020, p. 271).

A definição de Poder Público vem elencada no artigo 23, 'caput' da LGPD, que faz remissão ao artigo 1º, Parágrafo Único da Lei de Acesso à Informação (LAI) (Lei 12.527/11):

> Parágrafo único. Subordinam-se ao regime desta Lei:
> I - os órgãos públicos integrantes da administração direta dos Poderes Executivo, Legislativo, incluindo as Cortes de Contas, e Judiciário e do Ministério Público;
> II - as autarquias, as fundações públicas, as empresas públicas, as sociedades de economia mista e demais entidades controladas direta ou indiretamente pela União, Estados, Distrito Federal e Municípios (BRASIL, 2011, [s. l.]).

É importante destacar que, desde a Emenda Constitucional 80 de 2014, a Defensoria Pública está no mesmo nível do Ministério Público; mas como a LAI é de 2011, a Defensoria ainda não estava prevista como uma entidade específica. Assim sendo, quem faz parte do Poder Público é a **Administração Direta** (Executivo, Legislativo, Judiciário; Tribunais de Contas; Ministério Público e Defensoria Pública) e a **Administração Indireta** (Autarquias, Fundações Públicas, Empresas Públicas, Sociedade de Economia Mista em Regime de Monopólio e Consórcios Públicos e os Serviços Extrajudiciais). Quanto a isso, a LGPD traz em seu artigo 23, parágrafos 4º e 5º:

> § 4º Os serviços notariais e de registro exercidos em caráter privado, por delegação do Poder Público, terão o mesmo tratamento dispensado às pessoas jurídicas referidas no caput deste artigo, nos termos desta Lei.
> § 5º Os órgãos notariais e de registro devem fornecer acesso aos dados por meio eletrônico para a administração pública, tendo em vista as finalidades de que trata o caput deste artigo (BRASIL, 2018, [s. l.]).

A Sociedade de Economia Mista, para ser vista como Estado, tem que atuar em regime de monopólio, já que se for concorrencial, ela deixa de ser vista com esse caráter, visto que

concorre com outras empresas. Desse modo, as entidades que se encaixam na descrição de Poder Público devem se submeter ao regime estipulado pela LGPD.

4.4.1 Dicotomia do Tratamento de Dados pelo Poder Público

A coleta de dados feita pelo Poder Público é justificada principalmente pelo interesse social, para que ele preste um serviço à sociedade, elabore políticas públicas, tenha eficiência, suprima fraudes e traga inovação e excelência. Entretanto, em contrapartida, há a necessidade de se apresentar segurança ao cidadão, como salvaguardas necessárias para prevenir o vazamento de dados e o respeito à finalidade da coleta, a fim de evitar perfilamento ou até mesmo controle social, como já abordado.

A grande concentração de dados pessoais nas mãos do Estado é benéfica para a elaboração de políticas públicas, *mas qual é a barreira para que não seja feito um uso indiscriminado dessa grande massa de dados?*

As primeiras leis de proteção de dados, conforme trazido, consistiam em uma liberdade negativa, coibindo o abuso de controle por parte do Estado dos dados das pessoas. Porém, com o advento da tecnologia, houve a evolução da *liberdade negativa* para a *liberdade positiva*, posto que a concentração de informação já não está mais apenas nas mãos do Estado (*Big Brohter*), mas em várias plataformas (*Little Brothers*) que estão espalhadas pela rede, como o Facebook, Google, Amazon, entre outras, ocorrendo o tratamento descentralizado dos dados, com cada uma dessas plataformas tendo a sua própria base de dados e trocando informações entre si.

A distinção entre liberdade positiva e negativa segundo a "Enciclopédia de filosofia de Stanford" é a seguinte:

> A liberdade negativa é a ausência de obstáculos, barreiras ou restrições. A pessoa tem liberdade negativa na medida em que as ações estão disponíveis para ela neste sentido negativo. A liberdade positiva é a possibilidade de agir - ou o fato de agir - de forma a assumir o controle de sua vida e realizar seus propósitos fundamentais. Enquanto a liberdade negativa é geralmente atribuída a agentes individuais, a liberdade positiva é algumas vezes atribuída a coletividades ou a indivíduos considerados principalmente como membros de determinadas coletividades (STANFORD…, 2016).

Explorando o que foi exposto, a Lei Geral de Proteção de Dados não aparece no ordenamento jurídico brasileiro para dizer ao Estado o que não se deve fazer para proteger os

dados dos cidadãos, e sim para orientar a todos em relação ao que têm que fazer, que é o próprio fundamento da LGPD, ou seja, a própria autodeterminação informativa, que é vista como uma liberdade positiva (TASSO, 2020).

Nesse sentido, se as leis de proteção de dados surgiram para evitar que o controle do Estado sobre os cidadãos seja abusivo, o argumento é rebatido em parte pela necessidade de que o Estado tem que ter uma grande quantidade de dados de qualidade – em outras palavras, dados verdadeiros – para traçar políticas públicas que beneficiem a sociedade como um todo.

A autodeterminação informacional tem o seu limite, pois não é possível que, por exemplo, um cidadão deixe de disponibilizar os seus dados em um censo, pois é através desta informação que políticas públicas de qualidade serão elaboradas. Todavia, há que se observar essa linha tênue, como no caso da China, onde os dados são utilizados para o ranqueamento das pessoas: se determinado cidadão pode ter acesso a determinado crédito ou não, se pode frequentar determinado lugar ou não. Esses dados acabam sendo utilizados como insumo, e quanto menos alinhado o cidadão estiver às políticas de governo de seu país, menos "regalias" ele terá. Assim, não pode haver uso discriminatório dos dados fornecidos.

A partir disso, chegou-se a um grande avanço nas Leis de Proteção de Dados, a *autodeterminação informativa*, que envolve o cidadão no processo de tratamento dos seus dados, um dos fundamentos da LGPD. No entanto, o alto custo da defesa individual pode gerar privação de acesso a bens e benefícios, por isso a última geração de leis de proteção de dados são gerais, para que haja um padrão coletivo, determinando que tanto o Estado quanto outras entidades que tratem dados pessoais ajam de acordo com a legislação.

Maldonado e Blum (2019) afirmam que há 4 gerações de leis de proteção de dados:

> A primeira das quatro gerações de leis, que vai até aproximadamente 1977, com a *Budesdatenschutzgesetz* (Lei Federal da República Federativa da Alemanha sobre proteção de dados pessoais), girava em torno da concessão de autorizações para a criação de bancos de dados pessoais e do seu controle a posteriori por órgãos públicos. Os princípios nela existentes eram focados na atividade de processamento de dados, em razão da "ameaça" representada pela tecnologia e, especificamente, pelos computadores. Não demoraram muito a se tornarem ultrapassadas em razão do enorme aumento dos centros de processamento de dados, que inviabilizou o controle baseado em um regime de autorizações, rígido e detalhado. A segunda geração surgiu no final da década de 1970, justamente em razão da "diáspora" dos bancos de dados informatizados, contando como grande exemplo a Loi Informatique et Libertées, de 1978, na França. A modificação central passou a ser uma liberdade negativa, a ser exercida pelo próprio cidadão, e não mais em torno do fenômeno computacional em si. Foi elaborado um sistema que fornecia instrumentos para o cidadão identificar o uso indevido de suas informações e propor a sua tutela (MALDONADO; BLUM, 2019, p. 135).

Na segunda geração, houve uma mudança de padrão, e a coleta de dados se tornou indispensável para que o indivíduo participasse ativamente da sociedade:

> Foi, então, que surgiu uma terceira geração de leis, na década de 1980, aprimorando a tutela de dados pessoais, ainda centrada no indivíduo, porém abrangendo mais do que a liberdade de fornecer ou não os próprios dados pessoais, de forma a também garantir a efetiva manutenção dessa liberdade. Nesse momento, é entendida a complexidade do tema proteção de dados pessoais, que envolve a própria participação do indivíduo na sociedade e leva em consideração o contexto no qual lhe é solicitada a revelação dos seus dados, estabelecendo meios de proteção para as ocasiões em que sua liberdade de decidir livremente é cerceada por eventuais condicionantes. Buscava-se incluir o titular de dados em todas as fases do processo de tratamento e na utilização de suas informações por terceiros (autodeterminação informativa).
> Porém a autodeterminação informativa, que inclusive é fundamento da LGPD, ainda era privilégio de uma minoria que tinha condição econômica e social para exercer esse direito. Assim, uma quarta geração de leis, como as que existem hoje em diversos países, focaram no problema integral da informação, com instrumentos elevando o padrão coletivo, fortalecendo a posição da pessoa em relação às entidades que coletam e processam seus dados e estabelecendo autoridades independentes para fiscalização, como a Diretiva da UE 95/46. É possível enxergar alguns princípios comuns, presentes em diversos ordenamentos, como tendência de consolidação da vinculação mais estreita com a proteção da pessoa e direitos fundamentais. (MALDONADO; BLUM, 2019, p. 136-137).

Conforme visto, a legislação que iniciou esse movimento foi a Diretiva 95/46/CE do Parlamento Europeu, que afirma que hoje a sociedade está constituída pelo tratamento de dados e que as atividades econômicas são impulsionadas por essa atividade, então regras são necessárias para balancear essa relação. Essa diretiva traz diversas considerações regulatórias das atividades de tratamento de dados, embasando a GDPR, fonte de inspiração da LGPD.

Sobre isso, Nissenbaum (2011) postula o seguinte:

> A elevação do direito à proteção de dados ao patamar constitucional será um avanço ao afirmar que não se trata de direito ao sigilo ou ao controle, mas sim de um fluxo apropriado de informações pessoais, conforme normas informacionais orientadas pelos contextos sociais (NISSENBAUM, 2011, p. 448 – Tradução da autora).

Diante da perspectiva da autora, a questão sobre proteção de dados não é dizer para o Estado ou para outras entidades que tratem dados o que eles não têm que fazer (liberdade negativa), não se restringe a não circulação dos dados, visto que a atual sociedade precisa desse fluxo. O que precisa ser ajustado é o fluxo desses dados, esse acervo tem que fluir adequadamente, dentro de regras previamente previstas nas Leis Gerais de Proteção de Dados.

De acordo com a LGPD, o adequado fluxo informacional é baseado em premissas que são os princípios previstos, já mencionados anteriormente: finalidade, adequação, necessidade, livre acesso, transparência, qualidade dos dados, segurança, prevenção, não discriminação e responsabilização.

Em síntese, o poder do Estado é assimétrico em relação ao do cidadão[16], e antes de os princípios de proteção de dados serem elencados no art. 6º da LGPD, os princípios administrativos já existiam na CF, de modo que será feito um paralelo entre eles, demonstrando que por mais que as normas protetivas aos cidadão sofram uma evolução constante, as normas constitucionais sempre estarão presentes.

Os princípios administrativos estão dispostos no artigo 37 da CF: "[...] A administração pública direta e indireta de qualquer dos Poderes da União, dos Estados, do Distrito Federal e dos Municípios obedecerá aos princípios de legalidade, impessoalidade, moralidade, publicidade e eficiência" (BRASIL, 2016, [s. p.]).

O princípio da legalidade diz que o Estado só pode fazer algo que a lei permita, diferindo-se do conceito de legalidade do direito privado, segundo o qual o cidadão pode fazer tudo que a lei não vede. Já o princípio da impessoalidade diz que o Poder Público deve atuar sempre de forma imparcial e neutra, atendendo ao interesse da coletividade, sem ocorrer o favorecimento pessoal. O princípio da moralidade é a observância dos preceitos éticos em todos os atos administrativos. Por sua vez, o princípio da publicidade permite o controle externo da administração pública, é a divulgação de tudo que diz respeito à Administração Pública. Por fim, o princípio da eficiência é aquele que impõe ao Poder Público a melhor utilização possível dos seus recursos, isto é, a persecução do bem comum.

Um princípio de proteção de dados sempre estará ligado a um princípio administrativo. Com isso, temos onze princípios de proteção de dados, sendo dez deles listados nos incisos do art. 6º da LGPD e o *princípio da boa-fé*, disposto no caput do artigo e não menos importante que os demais. Em relação a isso, Maldonado e Blum afirmam:

> Newton de Lucca (2015, p. 39), comentando sobre o grande autor Ronald Dworkin, esclareceu que há distinção entre princípios, regras e políticas. Dos princípios em sentido estrito, emanam orientações gerais, decorrentes das exigências de equidade, de justiça ou de moralidade. Das regras, decorrem consequências jurídicas que se deduzem automaticamente das condições previstas na hipótese. As políticas

16 Entende-se que assimetria constitucional é ter uma certa flexibilidade diante da rigidez das normas constitucionais.

> (princípios em sentido lato) são padrões a serem observados como exigência econômica, política ou social desejável. Ao comentar o ensinamento de Norberto Bobbio e Vezzio Crisafulli, de Lucca adere irrestritamente à tese de que os princípios gerais são normas fundamentais ou generalíssimas do sistema, as normas mais gerais. Prossegue entendendo que não há dúvida de que princípios gerais são normas como todas as demais. Os princípios gerais estão para as normas particulares como o mais está para o menos, como o que é anterior e antecedente está para o posterior e consequente. Princípio, assim, é toda norma jurídica considerada determinante de outra ou outras que lhe são subordinadas, que a pressupõem, desenvolvendo e especificando ulteriormente o preceito em direções mais particulares (MALDONADO; BLUM, 2019, p. 135-136).

Os princípios administrativos, por exemplo, da legalidade, moralidade e impessoalidade estão intimamente ligados aos princípios da finalidade e da adequação da LGPD. O artigo 7º da LGPD, em seu inciso III, traz as bases legais que permitem o tratamento de dados:

> O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses: 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 (BRASIL, 2018, [s. p.]).

Todo princípio traz um padrão para uma norma, que se fundamenta na preservação de um direito, e os princípios da finalidade e da adequação são atendidos dentro desses três princípios administrativos (legalidade, moralidade e impessoalidade) quando estão previstos em regulamentos, como a base legal da LGPD (art. 7º, III), ou quando é praticado no exercício de competências ou em prol do interesse público, conforme o artigo 23 da LGPD:

> O tratamento de dados pessoais pelas pessoas jurídicas de direito público referidas no parágrafo único do art. 1º da Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação), deverá ser realizado para o atendimento de sua finalidade pública, na persecução do interesse público, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público (BRASIL, 2018, [s. p.]).

O tratamento de dados pessoais pelas pessoas jurídicas de direito público referidas no parágrafo único do art. 1º da Lei n.º 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação), deverá ser realizado para o atendimento de sua finalidade pública, na persecução do interesse público, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público:

> 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 (BRASIL, 2018, [s. p.]).

É dever das entidades e dos órgãos públicos promover, independentemente de requerimentos, a divulgação em local de fácil acesso, no âmbito de suas competências, de informações de interesse coletivo ou geral por eles produzidas ou custodiadas.

> § 1º Na divulgação das informações a que se refere o caput, deverão constar, no mínimo:
> I - registro das competências e estrutura organizacional, endereços e telefones das respectivas unidades e horários de atendimento ao público;
> II - registros de quaisquer repasses ou transferências de recursos financeiros;
> III - registros das despesas;
> IV - informações concernentes a procedimentos licitatórios, inclusive os respectivos editais e resultados, bem como a todos os contratos celebrados;
> V - dados gerais para o acompanhamento de programas, ações, projetos e obras de órgãos e entidades; e
> VI - respostas a perguntas mais frequentes da sociedade. (BRASIL, 2011, [s. p.]).

Ou, ainda, quando se implementa outras formas de publicidade alvitradas pela Autoridade Nacional de Proteção de Dados (ANPD), conforme disposto no artigo 23, parágrafo 1º da LGPD:

> § 1º A autoridade nacional poderá dispor sobre as formas de publicidade das operações de tratamento. (BRASIL, 2018, [s. p.]).

E também quando há a expedição de informes e comunicados, conforme elencado nos artigos 26, parágrafo 2º, e artigo 27, inciso II, da LGPD:

> O uso compartilhado de dados pessoais pelo Poder Público deve atender a finalidades específicas de execução de políticas públicas e atribuição legal pelos órgãos e pelas entidades públicas, respeitados os princípios de proteção de dados pessoais elencados no art. 6º desta Lei.
> § 2º Os contratos e convênios de que trata o § 1º deste artigo deverão ser comunicados à autoridade nacional. (BRASIL, 2018, [s. p.])

> A comunicação ou o uso compartilhado de dados pessoais de pessoa jurídica de direito público a pessoa de direito privado será informado à autoridade nacional e dependerá de consentimento do titular, exceto:
> II - nos casos de uso compartilhado de dados, em que será dada publicidade nos termos do inciso I do caput do art. 23 desta Lei (BRASIL, 2018, [s. p.]).

Como visto, a transparência quanto ao tratamento de dados está prevista para as entidades e os órgãos públicos, o que vai ao encontro do artigo 9 da LGPD, que promove o acesso facilitado a essas informações e, por conseguinte, atende a princípios administrativos como da *publicidade* e *eficiência*, que estão previstos na Constituição Federal do Brasil.

Diante do exposto, ficou evidenciado que os princípios previstos na LGPD estão intimamente ligados aos princípios administrativos e incidem simultaneamente em toda operação de tratamento de dados. Quando há a violação dos princípios previstos da LGPD, as consequências ou as sanções estão previstas no artigo 52 da LGPD:

> Os agentes de tratamento de dados, em razão das infrações cometidas às normas previstas nesta Lei, ficam sujeitos às seguintes sanções administrativas aplicáveis pela autoridade nacional: (Vigência).
> I - advertência, com indicação de prazo para adoção de medidas corretivas;
> II - multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R$ 50.000.000,00 (cinquenta milhões de reais) por infração;
> III - multa diária, observado o limite total a que se refere o inciso II;
> IV - publicização da infração após devidamente apurada e confirmada a sua ocorrência;
> V - bloqueio dos dados pessoais a que se refere a infração até a sua regularização;
> VI - eliminação dos dados pessoais a que se refere a infração;
> VII - (VETADO);
> VIII - (VETADO);
> IX - (VETADO);
> X - suspensão parcial do funcionamento do banco de dados a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período, até a regularização da atividade de tratamento pelo controlador; (Incluído pela Lei nº 13.853, de 2019);
> XI - suspensão do exercício da atividade de tratamento dos dados pessoais a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período; (Incluído pela Lei nº 13.853, de 2019);
> XII - proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados (Incluído pela Lei nº 13.853, de 2019) (BRASIL, 2018, [s. p.]).

Portanto, como analisado no artigo 52, compete exclusivamente à ANPD a aplicação de sanções administrativas, e é importante ressaltar que o disposto no inciso II do artigo 52 não é aplicável à administração pública, isto é, ela não vai poder ser multada pelo mau uso de dados pessoais. Porém, ao se analisar o parágrafo 3º desse artigo, temos:

> § 3º O disposto nos incisos I, IV, V, VI, X, XI e XII do caput deste artigo poderá ser aplicado às entidades e aos órgãos públicos, **sem prejuízo do disposto** na Lei nº 8.112, de 11 de dezembro de 1990 (Estatuto do Servidor Público Federal), na Lei nº 8.429, de 2 de junho de 1992 (Lei de Improbidade Administrativa), e na Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à informação) (BRASIL, 2018, [s. p.]).

Logo, o disposto nos incisos I, IV, V, X, XI E XII do *caput* do artigo 52 da LGPD será aplicado às entidades e aos órgãos públicos sem prejuízo do que é trazido na Lei do Estatuto do Servidor Público Federal, na Lei de Improbidade Administrativa e na Lei de Acesso à Informação, que poderão ser aplicadas cumulativamente com as sanções previstas nessas legislações. Se cada princípio de proteção de dados está atrelado a um princípio administrativo no âmbito de tratamento de dados pessoais pelo Poder Público, quando este deixa de cumprir um princípio de proteção de dados, ele automaticamente viola um princípio administrativo, com isso o gestor público incorre em ato de improbidade administrativa.

Segundo Tasso, (2019) temos as seguintes conclusões:

> 1) A operação de tratamento de dados pessoais pelo Poder Público é ato administrativo;
> 2) A violação do princípio de proteção de dados pelo administrador público resulta em violação a princípio Constitucional da administração pública;
> 3) A consequência do desatendimento a princípio de proteção de dados repercute:
> a) No ato administrativo – há a invalidade da operação de tratamento;
> b) No patrimônio do administrador (controlador) – as consequências pessoais da Lei de Improbidade Administrativa (artigo 12) e do Estatuto do Servidor Público Federal, isto é, o patrimônio pessoal do gestor público responde pelo ato administrativo que violou um princípio administrativo decorrente da violação de um princípio da proteção de dados;
> c) Consequências para o ente ou órgão público (artigo 52 da LGPD) (TASSO, 2019, [s. p.]).

No que concerne ao tratamento de dados pessoais pela Administração Pública, as penalidades são piores do que na esfera privada, pois no primeiro caso há a incidência da lei de improbidade administrativa. Wimmer (2020) ratifica essa maior responsabilidade do Estado frente setor privado da seguinte forma:

> O desafio de interpretação e aplicação da legislação de proteção de dados pessoais ao setor público é significativo, e deve partir do reconhecimento das tensões e dualidades anteriormente exploradas. Se a motivação e a legitimidade do governo ao tratar dados pessoais devem necessariamente ser compreendidas como distintas daquela dos agentes privados, sua responsabilidade é, também, maior, dado que eventual mau uso de dados pelo Estado produz impactos abrangentes não apenas sobre a esfera de direitos individuais, mas sobre a sociedade como um todo. É por essa razão que os mais importantes instrumentos internacionais de proteção de dados indicam que os princípios e regras referentes à proteção de dados pessoais se aplicam tanto ao setor público como ao setor privado. Convém, assim que antes de destrinchar as regras concretas previstas na LGPD para o tratamento de dados pessoais pelo Poder Público, se examine o conjunto de princípios que devem orientar essa atividade – tanto aqueles oriundos da LGPD, como também os que decorrem do arcabouço legal e constitucional mais amplo que orienta o Poder Público em todas as suas formas de expressão (WIMMER, 2020, p. 274-275).

Ainda de acordo com Wimmer (2020, pp. 274-275), princípios constitucionais como o da eficiência e o da supremacia do interesse público "frequentemente são postos em tensão com princípios de proteção de dados, como os da finalidade, da necessidade e da adequação". Assim sendo, é fundamental que haja uma mudança de cultura e de medidas administrativas para que a relação entre cidadão e Poder Público se dê dentro das normas constitucionais e da proteção de dados, diante do que é uma obrigação do Poder Público a observância tanto de princípios constitucionais quanto os princípios previstos na LGPD. A construção da relação entre cidadão e governo deve ser baseada na transparência, na confiança, na prestação de contas e no livre acesso, para que as pessoas possam ter autonomia sobre o fluxo de seus dados (autodeterminação informacional).

5 AUTODETERMINAÇÃO INFORMATIVA NA LGPD

Como argumentado antes, a circulação dos dados possui um papel fundamental na inserção do indivíduo na sociedade e, consequentemente, no desenvolvimento da sua própria personalidade. Este capítulo é dedicado a demonstrar como a autodeterminação informativa se relaciona com direitos fundamentais, como o livre desenvolvimento da personalidade e da dignidade humana, podendo ser entendido como um novo direito de personalidade.

Conforme exposto em nosso texto, após a Segunda Guerra Mundial houve uma proliferação do princípio da dignidade humana no mundo todo, com isso ocorreu uma *despatrimonialização* do direito à personalidade, pois antes esse direito havia uma excessiva carga patrimonialista, que era apoiada nos conceitos de *declaração de vontade*, r*elação* e *negócio jurídico*. Posteriormente, começou-se a tutelar o direito à proteção de dados, que surge do que se pode chamar de um novo direito da personalidade:

> Os direitos da personalidade são uma noção inacabada que deve ser cultivada, especialmente frente ao abordado manancial de dados produzidos pelas pessoas na sociedade da informação. Por meio dessa premissa, será possível identificar uma nova variante dessa categoria jurídica para nela enquadrar a proteção dos dados pessoais.
> Nesse sentido, os direitos da personalidade não se limitam àquelas situações previstas no Código Civil (CC), sendo seu rol *numerus apertus* (rol aberto). Eles não se exaurem naquelas espécies enumeradas nos arts. 11 a 21 do CC, o que abre caminho para o reconhecimento da proteção de dados pessoais como *um novo direito da personalidade* (BIONI, 2019, pp. 59-60).

O autor, ao dizer que o rol de direitos à personalidade é *numerus apertus,* fez uma clara referência à sua elasticidade, a partir do que se faz importante uma perspectiva mais ampla, que não se trata da aptidão de um sujeito ser titular de direitos e deveres, mas da proteção jurídica canalizada para o desenvolvimento da pessoa humana. A respeito disso, Marighetto (2019) afirma:

> Os direitos da personalidade são direitos inerentes e inseparáveis do próprio conceito de personalidade humana, independentemente de qualquer "reconhecimento" ou "sistematização" pela ordem ou sistema jurídico. A personalidade, todavia — uma vez reconhecida pelo ordenamento jurídico — torna-se "personalidade jurídica". Em outras palavras, o ordenamento jurídico contribui para preservar e tutelar o valor, a autonomia e o fim individual do ser humano, não unicamente de forma geral e abstrata, mas também no respeito à ordem atual e jurisdicional do direito positivo.
> O ser humano é o sujeito principal e destinatário de todas as relações jurídicas [enquanto sujeito em si dessas relações]. Por essa razão, o ser humano é sempre titular da capacidade jurídica [art. 1° do Código Civil], que é a qualificação virtual e potencial do agir juridicamente. A personalidade jurídica é — em outras palavras — a veste formal da substância humana.

> A personalidade jurídica — por ser intrínseca e comum a todos os seres humanos – torna-se também pressuposto jurídico formal e substancial da igualdade jurídica, que se concretiza no pressuposto segundo o qual cada ser humano necessariamente há de respeitar a personalidade jurídica dos outros, enquanto "reflexo" da sua própria (MARIGHETTO, 2019, [s. p.]).

A personalidade jurídica é a possibilidade de o indivíduo se relacionar com as demais pessoas, sempre respeitando o espaço alheio, podendo 'adquirir direitos e contrair obrigações' (CC, art. 1º), sendo a capacidade jurídica o limite dessas ações:

> A capacidade jurídica distingue-se da capacidade de agir, que consiste na aptidão do indivíduo para manifestar vontades aptas a modificar a própria situação jurídica (ou seja, é a capacidade de exercer concretamente a capacidade geral de ser titular de direitos e deveres). Capacidade jurídica e capacidade de agir permitem ao indivíduo criar, modificar e extinguir todas as posições jurídicas subjetivas, que podemos distinguir [sumariamente] em direitos, interesses legítimos, poderes, obrigações, deveres e ônus. O art. 1o da Declaração Universal dos Direitos do Homem estabelece que "todos os seres humanos nascem livres e iguais em dignidade e direitos. Dotados de razão e de consciência, devem agir uns para com os outros em espírito de fraternidade". A Carta Constitucional de 1988 do Brasil consagra a dignidade da pessoa humana como princípio fundamental do Estado Democrático de Direito (art. 1o, III), e positiva expressamente o reconhecimento dos direitos e garantias fundamentais (incluindo os direitos da personalidade) no art. 5o, *caput*, V, X e XXXVI, em particular no que concerne ao direito à vida, à intimidade, à vida privada, à imagem, à honra, entre outros (MARIGHETTO, 2019, [s. p.]).

O direito à personalidade humana é passível de uma ampla interpretação, e esse direito quando conectado à autodeterminação informativa busca tutelar o próprio desenvolvimento do indivíduo. Os direitos à personalidade não estão fixados a um rol taxativo, trata-se de um rol aberto, estando suscetível a mudanças de acordo com a evolução da sociedade. Em relação a isso, Marighetto (2019) complementa:

> Os direitos da personalidade são regulamentados nacional e internacionalmente pelos arts. 11 a 21 do Código Civil (aspectos privatísticos), pela própria Carta Constitucional como direitos e garantias fundamentais (veja-se supra) e por várias Convenções Internacionais, como a Declaração Universal dos Direitos do Homem da ONU de 1948; a Declaração do Conselho da Europa para a salvaguarda dos Direitos do Homem e das Liberdades Fundamentais de 1950; o Pacto internacional sobre os Direitos Civis e Políticos de 1966; o Tratado da União Europeia de 1992, e modificado em 2007; a Carta dos Direitos Fundamentais de 2000; e a Convenção sobre Direitos Humanos e a Biomedicina de 1997.
> Pelo ordenamento jurídico, são direitos da personalidade: o direito à dignidade; o direito à liberdade (e o direito à livre iniciativa na forma e nos limites estabelecidos pela Lei); o direito à igualdade; o direito à segurança; o direito à cidadania; o direito à vida, o direito à integridade física e psíquica, o direito ao nome; o direito à imagem; o direito à inviolabilidade da vida privada; o direito à liberdade de pensamento e de expressão; o direito à propriedade; o direito a ser submetido ao justo processo; e o direito ao meio ambiente ecologicamente equilibrado (direito novo, difuso e de

> exclusiva natureza pública). Trata-se de elenco "aberto" e não necessariamente taxativo, mas que muda e evolui conforme o "nível de civilização" da sociedade, ou seja, que depende das conquistas da sensibilização e do progresso das ciências naturais e humanas (MARIGHETTO, 2019, [s. p.]).

Desta forma, a autodeterminação informativa se relaciona com o princípio da dignidade de duas formas: com o desenvolvimento da personalidade e o nível de autonomia do indivíduo. Sarlet (apud MARIGHETTO, 2019, [s. p.]) postula que os direitos da personalidade e os direitos humanos estão intrinsecamente vinculados, guiando tanto o direito público quanto o direito privado a um só objetivo: o respeito à dignidade da pessoa humana, valor universal que rege todo o ordenamento jurídico. Desse modo, visto que os direitos da personalidade são direitos subjetivos, que individuam as características e os atributos próprios da personalidade humana e que refletem a tutela de interesses públicos, o ordenamento jurídico não traz um rol de direitos específicos, mas o direito à reparação do dano moral:

> Observa-se que o ordenamento não atribui ao seu titular um poder de disposição em relação a tais direitos, mas se limita a reconhecer o direito à cessação de um fato lesivo e o eventual ressarcimento do dano. Assim, consequentemente, os direitos humanos representam o pressuposto essencial e funcional que permite a qualquer indivíduo viver dignamente enquanto pessoa. Unicamente através do respeito destes direitos será possível obter a tutela da liberdade, da justiça e da paz para o indivíduo e toda a coletividade (MARIGHETTO, 2019, [s. p.]).

Portanto, verifica-se que os direitos humanos estão intrinsecamente conectados à condição humana. Assim, o direito fundamental da dignidade se entrelaça com o da autodeterminação informativa, principalmente na ocasião (vista anteriormente) em que a Corte Constitucional Alemã, em 1983, decidiu, em julgamento sobre a Lei do Censo Alemã, que o direito à autodeterminação informativa possuía natureza material, sendo derivado dos princípios do livre desenvolvimento da pessoa natural e da dignidade da pessoa humana. Além disso, trata-se de um instrumento através do qual os cidadãos podem proteger os seus dados pessoais. Nessa mesma seara, o referido autor analisa:

> É principalmente a Kant que se deve a base das modernas teorias do fundamento do reconhecimento universal dos direitos humanos, que coincidem com a tutela da dignidade humana. A dignidade do ser humano se concretiza em um valor intrínseco absoluto, que impõe a todos os outros seres humanos o recíproco respeito [veja-se supra]. Não por acaso, segundo Kant, a falta de respeito à dignidade em relação aos outros concretiza a falta de respeito para o próprio gênero humano!
> Para Kant, a dignidade é qualidade inerente aos seres humanos enquanto seres dotados de moral. O exercício da razão prática através da moral concretiza a dignidade do ser humano. Na medida em que os seres humanos exercem, de forma autônoma, a própria

> razão prática, constroem diferentes personalidades humanas, cada uma delas independente e insubstituível. Isso faz com que a dignidade seja inseparável da autonomia (e abstrata) no exercício da razão prática.
> A liberdade e a autonomia em exercer a razão prática é ínsita ao ser humano. Sartre ensina que a liberdade não é uma qualidade ou característica a mais no homem, mas o homem é livre em si, sendo que homem e liberdade são a mesma coisa: o agir, ou melhor, o escolher é expressão pura da natureza humana que é livre, livre até de não agir, ou fracassar, ou seguir o seu próprio caminho. A liberdade é uma aspiração natural da humanidade.
> O respeito da dignidade humana, portanto, significa essencialmente autodeterminação e liberdade de decisão em relação a finalidades, desejos e necessidades! (MARIGHETTO, 2019, [s. p.]).

Para Bioni (2021, p. 99), é imperioso que o indivíduo tenha capacidade para gerir os seus dados pessoais, para poder desenvolver livremente a sua identidade através da autodeterminação informativa. Isto posto, a convergência dos direitos de personalidade com gestão dos próprios interesses do cidadão configura a autodeterminação informativa, que é um pressuposto para a existência da dignidade da própria pessoa, quer dizer, a liberdade de gerenciar os seus direitos e valores, o que faz parte do Estado Democrático.

> Essa concepção da dignidade humana, como autodeterminação dos próprios interesses – seja isso em uma ótica moral ou jurídica – se encontra também como fundamento das Cartas Constitucionais Ocidentais e da Declaração Universal dos Direitos dos Homens, que tutelam interesses importantes dos indivíduos como a vida, a integridade física, a liberdade e a propriedade.
> Consequentemente, considerando que o pressuposto para a existência da dignidade é a liberdade no exercício da razão prática, e que todos os homens são dotados dessa liberdade (ou melhor, dessa autonomia), deve-se considerar que a dignidade pertence necessariamente ao ser humano, independentemente de qualquer tipo de reconhecimento social ou jurídico, a ponto de a jurisprudência comparativa contemporânea, partindo da própria Declaração Universal dos Direitos do Homem, confirmar que ninguém pode renunciar à própria dignidade!
> A dignidade é, pois, bem indisponível e – de acordo com quanto supra – concretiza o princípio fundamental do Estado Democrático de Direito do Brasil. A sua finalidade resume-se a assegurar à pessoa os principais direitos que devem ser respeitados pela sociedade e pelo próprio poder público, de forma a preservar a valorização do ser humano.
> Sendo o direito à dignidade um fundamento da República, não há como ser "negociada", sob pena de gerar a instabilidade não unicamente em relação aos princípios gerais do Direito mas do próprio regime democrático! (MARIGHETTO, 2019, [s. p.]).

MARIGHETTO (2019) observa que, pelo fato de esses direitos de personalidade serem patrimoniais (direitos que não podem ser convertidos em dinheiro), absolutos (são direitos rígidos, que não possuem exceções à regra), irrenunciáveis (não estão sujeitos à negociação com terceiros), intransmissíveis (não podem ser transferidos para outrem) e imprescritíveis (a perda do direito de punir do Estado em decorrência da sua inércia), nem as

pessoas nem as instituições públicas e privadas deveriam dispor deles de maneira que desrespeitasse a condição humana do indivíduo a ponto de reduzir a pessoa a uma condição de bem ou coisa. Como já visto em nossa investigação, a mineração de dados pessoais transforma o indivíduo em insumo.

Com a cultura do compartilhamento excessivo de dados e o aumento do volume da produção de dados, a autodeterminação informativa aparece na LGPD para tutelar o direito de personalidade referente à gestão dos dados pessoais, o que será discutido a seguir.

5.1 AUTODETERMINAÇÃO INFORMATIVA E O DIREITO À PROTEÇÃO DE DADOS

Como visto, o Art. 18 da LGPD traz uma relação de direitos para os cidadãos. Através das regras contidas nele, visa-se regular a aplicação da autodeterminação informativa, que dá ao titular dos dados pessoais o protagonismo das matérias relacionadas ao tratamento de seus dados. Diante do que é trazido por esse artigo, o titular pode: opor-se a operações de tratamento de seus dados pessoais realizadas sem o consentimento; pedir a correção se seus dados estiverem incompletos, inexatos ou desatualizados; pedir a eliminação de dados pessoais que foram tratados pela base legal do consentimento, ressalvando-se algumas exceções; enfim, todas as hipóteses legais elencadas no art. 18 da LGPD.

Assim, temos que o princípio da autodeterminação informativa confere ao titular, via de regra, a palavra final no que diz respeito às operações de tratamento dos seus dados; e mesmo quando não puder opor-se ao tratamento, nos casos em que este se der com base em outros interesses, tal princípio confere ao menos o direito à informação sobre a limitação de finalidade desses dados e quanto à segurança conferida a eles.

Outrossim, o art. 18 confere ao titular autonomia sobre o tratamento dos seus dados, porém é nítido que não se trata de um direito absoluto, pois mesmo sendo a autodeterminação informativa considerada como um direito fundamental, há que ser feito um balanceamento com outros direitos fundamentais e as próprias regras contidas na legislação. No tocante a isso, Maldonado (2020) observa:

> E, para buscar dar efetividade ao fundamento da autodeterminação informativa, a LGPD, em seu Capítulo III, dispõe sobre os direitos dos titulares, entre eles: de obter do controlador a confirmação da existência de tratamento; de ter acesso aos seus dados; da correção de dados incompletos, inexatos ou desatualizados; da anonimização, bloqueio ou eliminação dos dados desnecessários, excessivos ou

> tratados em desconformidade com a Lei; da portabilidade dos dados a outro fornecedor de serviço ou de produto; da revogação do consentimento do titular; da informação das entidades públicas e privadas com as quais o controlador realizou o uso compartilhado de dados; da informação sobre a possibilidade de não fornecer consentimento e sobre as consequências dessa negativa, entre outros.
> O distanciamento do controle e da autoridade sobre os seus próprios dados, a partir do momento em que o indivíduo não consegue mais identificar quais informações suas são utilizadas, para quais propósitos, e como isso interfere e influencia em sua vida, é um sinal preocupante de tolhimento da autodeterminação informativa, que muitas vezes ocorrerá de forma imperceptível ao titular. Daí o motivo pelo qual referido conceito também se apresenta de forma certeira, como fundamento, da LGPD (MALDONADO, 2020, p. 28)

A autodeterminação informativa só poderá ser exercida se o titular souber o que de fato será feito com seus dados. Ela traz o poder, a autonomia do indivíduo – no caso das crianças e adolescentes, são os responsáveis legais que as representam, pois os direitos das crianças são deveres dos adultos, justamente em razão da sua falta de discernimento, maturidade; são direitos que precisam ser exercidos e não devem ser garantidos apenas pelos responsáveis legais, trata-se de um dever de todos, principalmente daqueles que querem oferecer um produto ou um serviço a uma criança. Com isso, constata-se que os objetivos da Lei Geral de Proteção de Dados são os seguintes: a) Garantia do direito à privacidade; b) Garantia da autodeterminação informativa; c) Garantia dos direitos humanos, livre desenvolvimento da personalidade, dignidade e exercício da cidadania; d) Fomentar a inovação e o desenvolvimento econômico e tecnológico. Esses objetivos podem ser observados de uma maneira mais ampla no artigo 2° da LGPD:

> 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 (BRASIL, 2018, [s. p.]).

São esses fundamentos que dão validade à legislação; e entre eles a autodeterminação informativa é o único que não se encontra expresso na Constituição Federal, embora já reconhecido pelo STF na decisão que suspendeu a MP 954/20 (Caso IBGE). Esse fundamento ganha força porque o Brasil ainda não tem uma cultura de proteção de dados, ganhando muita visibilidade com o advento da Lei – mesmo sendo um conceito reconhecido pela Corte Alemã desde 1983.

O fundamento desse conceito deriva da autodeterminação da pessoa, da autodeterminação dela enquanto cidadão, é de caráter republicano, democrático, tem um aspecto individual forte, necessário ao desenvolvimento da personalidade, mas também tem um aspecto coletivo isolado: não é um direito absoluto da sociedade, sobre mitigações no direito do coletivo, tanto que a Corte Alemã decidiu que o censo deveria ser feito, porque quando se vive em sociedade, o indivíduo encontrará limites perante o coletivo. Isso tem respaldo legal na nossa Constituição Federal, no tocante ao desenvolvimento da personalidade para o livre desenvolvimento da pessoa natural:

> O significado histórico da decisão do STF pode ser equiparado ao clássico julgamento do Tribunal Constitucional Federal alemão, em 1983, relativamente à Lei do Recenseamento. Ao fazer referência ao julgado, o STF expressamente mencionou o conceito de autodeterminação informativa, já positivado na Lei n. 13.709/2018 (Lei Geral de Proteção de Dados), a fim de ressaltar o necessário protagonismo exercido pelo cidadão no controle do que é feito com seus dados. Assim, pôs-se em destaque a existência de finalidade legítimas para seu processamento, bem como a necessidade de implementação de medidas de segurança para tanto. Segundo o ministro Gilmar Mendes, o conteúdo desse direito fundamental exorbita àquele protegido pelo direito à privacidade, pois não se limita apenas aos dados íntimos ou privados. Ao contrário, refere-se a qualquer dado que identifique ou possa identificar um indivíduo. Esse direito fundamental autônomo e com contornos próprios, seria extraído de uma: 'Compreensão integrada do texto constitucional lastreada (i) no direito fundamental à dignidade da pessoa humana, (ii) na concretização do compromisso permanente de renovação da força normativa da proteção constitucional à intimidade (art. 5°, inciso X, da CF/88) diante do espraiamento de novos riscos derivados do avanço tecnológico e ainda (iii) no conhecimento da centralidade do habeas data enquanto instrumento de tutela material do direito à autodeterminação informativa' (MENDES et. al., 2020, p. 67).

O conceito de autodeterminação informativa, cunhado em 1983 pela corte Alemã, no contexto atual, em que há dados excessivos, torna-se um desafio ao titular dos dados, uma vez que o acesso facilitado às suas informações e a transparência tornam-se cada vez mais imprescindíveis para que se possa exercer esse direito.

Ainda sobre o fundamento desse conceito, Mendonça afirma:

> O núcleo da proteção de dados pessoais, por sua vez, também confere ao consentimento posição de destaque, de modo a ostentar a autodeterminação informativa como um de seus fundamentos. A comunicação eficiente em relação à coleta de dados adquire maior consistência em um cenário no qual o consentimento mostra-se essencial para desencadear o tratamento, enquanto o vício de consentimento trava exatamente a possibilidade de operação de dados pessoais. Garante-se ao titular, por meio da comunicação eficiente, o controle sobre a forma como seus dados serão manuseados, de modo a conferir maior segurança não somente quanto à autorização de uso, como também da medida em que serão utilizados. O consentimento informado, nesse sentido, insere-se no cenário atual como uma relevante ferramenta

> de participação ativa do usuário em todo o processo de conhecimento e posterior anuência de tratamento de dados pessoais (MENDONÇA, 2019, [s.p.]).

Com a base legal do consentimento, Nissenbaum (2010, p. 203) postula que o trânsito das informações tem um "valor social, guiado por considerações políticas e morais". Diante disso, pode se concluir que:

> […] a proteção dos dados pessoais não se baseia única e exclusivamente nos desígnios do próprio titular dos dados pessoais. Pelo contrário, as chamadas normas informacionais impõem restrições ao fluxo informacional que independem do controle (consentimento) exercido pelo indivíduo (Bioni, 2021, p. 205).

É evidente, assim, que apesar do consentimento ter uma posição de destaque, como afirma Mendonça, a autodeterminação informativa não encontra amparo apenas nessa base legal, porque, ainda de acordo com Bioni, criou-se uma nova equação normativa:

> Nessa nova equação normativa, o consentimento não está presente a priori. A sua fórmula é composta da seguinte maneira: contexto + integridade = normas informacionais. É o produto (normas informacionais) dos citados elementos (contexto e integridade) dessa equação que deve governar o trânsito dos dados. Invertendo-se a ordem dos fatores, mas não do seu resultado: as normas informacionais restringem o fluxo dos dados, verificando-se a sua integridade de acordo com o contexto que estão inseridos (BIONI, 2021, p. 204).

Diante disso, extrai-se que a autodeterminação informacional não acontece somente quando a base legal da coleta for o consentimento, sendo imperioso analisar toda a estrutura (desde a coleta ao tráfego/compartilhamento/exclusão de dados pessoais), para que posteriormente se faça o sopesamento sobre a autodeterminação informacional, independentemente do dispositivo legal a partir do qual a coleta foi inicialmente justificada.

5.2 EXCESSO INFORMACIONAL E A GESTÃO DA AUTODETERMINAÇÃO INFORMATIVA

Atualmente há um contexto de desordem informacional. Como demonstrado por nós, na Figura 1, o número de usuários na internet aumenta a cada ano, crescendo exponencialmente o compartilhamento das informações ao passar do tempo, principalmente através de plataformas de redes sociais e aplicativos online. O processo de compartilhamento na internet

se tornou uma constante, a cultura atual é a de compartilhamento automático de dados, sem a devida tomada de consciência do porquê isso está sendo feito.

Qual a transparência da informação? Esse grande volume de dados está sendo tratado com boa-fé e transparência? Os titulares de dados têm acesso facilitado e gratuito aos seus dados? Diante dessa crescente 'desordem informacional', o titular dos dados tem uma compreensão do valor dos seus dados? Ele tem interesse em exercer os seus direitos elencados no art. 18 da LGPD e com isso exercer a sua autodeterminação informativa?

A transparência se torna um fator indissociável, porque o direito que a pessoa tem de decisão sobre as suas informações pessoais tem que ser encarado como ele é: um princípio do direito à personalidade, logo um direito fundamental.

A discussão sobre a autodeterminação da informação ganhou mais visibilidade com o advento da LGPD, mas, como já vimos, é algo que veio sendo discutido desde a década de 1980, como fato social e jurídico. O fato social sempre antecede o processo de judicialização, a discussão da LGPD é pensar na Gestão da Informação antes da judicialização (fato bem delineado no capítulo 4.1) de três princípios dessa lei que trazem a ideia de *compliance*, que são os princípios da prevenção, da segurança e da responsabilização e prestação de contas, com os quais se transfere para o particular a responsabilidade de gerenciamento, com a função de evitar incidentes, garantindo assim os direitos dos titulares de dados. No capítulo ora mencionado, foi destacado que esses três princípios reforçam a ideia de que o agente de tratamento de dados tem a responsabilidade de comprovar que está adotando medidas eficazes para o cumprimento da norma, para que, somados a outro princípio, o do *livre acesso*, confira ao titular o exercício da sua autodeterminação informacional.

É notório que os fatos sociais se renovam ininterruptamente, e o conceito de privacidade foi evoluindo até chegar ao conceito de proteção de dados atual, no contexto da virtualização, dentro das novas tecnologias de informação, nas redes sociais.

Para Souza (2020), quando se discute o processo de produção de conhecimento e de compartilhamento de informações, há um processo constante de comunicação, ao mesmo tempo que separa, aproxima, é inerente, permite a troca de conhecimento mútuo, é a condição humana atual. Trata-se de uma condição de inerência e de separação, muito próxima daquilo que Bauman chama de construções de "novos laços mais frágeis", construídos principalmente em um processo de compartilhamento momentâneo, mas que deixam marcas profundas e difíceis de serem superadas, por fugirem ao escopo da gestão humana.

Nesse sentido, Sibilia (2015, p. 199) afirma que a capacidade de lembrar-se da própria experiência é imprescindível para compor a identidade do indivíduo, mas a partir do momento que outros passam a ter acesso às narrativas dessa memória, ela pode se tornar "editável", como fosse projetada através de um caleidoscópio e se fragmentasse em outros "modos de ser". A editabilidade da memória passou a ser possível, e, com o avanço da tecnologia, as palavras do advogado Miguel Sumer Elias tornaram-se um tema muito debatido hoje: "Você é o que o Google diz que você é". Sobre isso, Sibilia afirma:

> A fonte da verdade a respeito de quem é – e quanto vale – cada sujeito parece ter se deslocado. Esse saber já não brota mais das próprias entranhas, onde se acreditava que ficavam hospedadas as lembranças das vivências, bem como pensamentos, as emoções, os princípios éticos e os sentimentos de cada um, de acordo com a perspectiva moderna de uma interioridade laica assimilável a conceitos como os de psiquismo ou mente (SIBILIA, 2015, p. 200).

Sibilia (Ibid.) ainda reitera que, a partir dessa mudança de ambiente, onde a internet habilita olhares alheios a interferirem na personalidade de outrem, dá-se ao Google a capacidade de atestar quem é cada um, retirando do indivíduo a faculdade de reter a própria memória. A informação passa a ter suas condições redimensionadas a partir desse processo de compartilhamento, e nisso é necessária a observância das ambivalências, das contradições e dos desafios que são constantes. A condição humana é viver determinada situação, produzir uma memória e posteriormente esquecer – justamente em virtude da sua condição humana.

Porém, o esquecimento se torna cada vez mais difícil; em função do processo constante de rememoração, o passado se torna presente, e lembrar e esquecer são atos de poder, atos políticos, e os artefatos tecnológicos ampliam o poder desses atos (SOUZA, 2020).

Se a tônica do século XX foi a luta entre a memória e o esquecimento, o exercício do século XXI parece ser aprender a conciliar da melhor forma possível a memória e o esquecimento, sempre fincado em fundamentos justos e democráticos, quer seja escopo do direito quer seja no da ética, da política, do social, do econômico – sendo o jurídico necessário para o processo da gestão.

Como dito, há um processo crescente de compartilhamento de informações, e a autodeterminação informativa aparece para impor limites a essa desordem informacional que vem junto com o conjunto de proteção desses dados.

5.3 AUTODETERMINAÇÃO INFORMATIVA, O DIREITO AO ESQUECIMENTO E A DESINDEXAÇÃO

Outro elemento muito importante que anda junto ao fundamento da autodeterminação informativa e auxilia muito a entender esses processos gerenciais é o *direito ao esquecimento* – abordado no início de nosso trabalho e também no tópico anterior –, que é o direito de estar só. Como já mencionado em relação ao artigo da *Harvard Review* de 1890, a intenção dos juristas era haver direito à intimidade em fatos passados; nessa época não existiam gigantescos bancos de dados conectados entre si, ao contrário da atualidade, em que fatos pretéritos ficam disponíveis com apenas um clique. *Qual a gestão que o titular dessas informações tem? Como fica a autodeterminação informativa do cidadão, por exemplo, quando uma pessoa voluntariamente compartilha seus dados nas redes sociais para os seus "cinco minutos de fama"? Ao resolver apagá-los, como fica a possível propagação na rede dessas informações? Como saber se determinado conteúdo foi retirado totalmente da rede?*

Caso o sujeito decida apagar os dados que não fazem mais sentido dentro de um novo contexto social, o art. 11º do Código Civil Brasileiro também tutela esse direito: "[…] Com exceção dos casos previstos em lei, os direitos da personalidade são intransmissíveis e irrenunciáveis, não podendo o seu exercício sofrer limitação voluntária" (BRASIL, 2002). Com isso, constata-se que a tutela da dignidade da pessoa humana na sociedade da informação inclui o direito ao esquecimento e que o enunciado 531 do CNJ (MOREIRA, [2021]) já traz essa preocupação desde 2013, como uma ramificação do direito à personalidade e uma sub-ramificação do direito à autodeterminação informativa.

O direito ao esquecimento nos dias atuais, que teve sua origem nos EUA, hoje é voltado ao fato do porquê esses fatos estão sendo lembrados? Esses dados que estão sendo rememorados encontram algum respaldo legal no artigo 7° da LGPD, por exemplo – isto é, eles estão legalmente protegidos por alguma das dez bases legais da LGPD, como por na execução de um contrato?

O *direito ao esquecimento* configura-se como um direito que, assim como a autodeterminação informativa, tem fundamento no *direito à personalidade*, que é um direito de abrangência muito ampla e está consolidado tanto no direito brasileiro como no internacional (por exemplo, na Declaração Universal dos Direitos Humanos). A grande questão é o balanceamento com outros direitos fundamentais; quando houver conflito entre eles, é importante reconhecer que, muitas vezes, como diz o Bauman:

> O imediato e profundo esquecimento de informações defasadas e o rápido envelhecimento de hábitos pode ser mais importante para o próximo sucesso do que a memorização de lances passados e a construção de estratégias sobre um alicerce estabelecido pelo aprendizado prévio (BAUMAN, 2007, p. 9).

O direito ao apagamento de dados pessoais na Europa é expressamente assegurado no art. 17 da GDPR de 2016, mas é um direito anterior a essa legislação, posto que, em um julgado de maio de 2014 do Tribunal de Justiça da União Europeia, o cidadão Mario Costeja González requereu a desindexação do buscador Google de dois editais de leilão para o pagamento de dívida de seguridade social. Sobre esse caso, Cueva (2020) comenta:

> Em resumo, em 2009 Mario Costeja requereu ao jornal que publicara os editais a supressão dessa informação, ao argumento que a dívida já havia sido quitada. Em vista da negativa do periódico, fundada pelo fato de que se tratava de informação oficial, o interessado em 2010, solicitou à subsidiária da Google na Espanha que excluísse tais dados, tendo o requerimento sido encaminhado à matriz norte americana, que não o atendeu. Em seguida a agência espanhola de proteção de dados acolheu o pedido relativamente à Google, embora tenha afastado a responsabilidade do jornal. Em vista de recurso da empresa espanhola e da matriz norte-americana, que sustentaram ser o processamento da informação efetuado fora da União Europeia, a Suprema Corte espanhola remeteu o caso ao Tribunal de Justiça da União Europeia, que reconheceu expressamente o direito ao esquecimento. Com fundamento na Diretiva 95/46/CE, a Corte Europeia asseverou que os provedores de busca na internet praticam atividade que se qualifica como de tratamento de dados e, portanto, são responsáveis por esse tratamento no âmbito de um Estado-Membro, sempre que criem nesse território, uma filial ou sucursal, que promova e venda espaços publicitários, incumbindo-lhes, em consequência, suprimir os links que remetam ao interessado, ainda que que a divulgação da informação, seja em si, lícita. O direito ao apagamento da informação deve prevalecer sobre interesses econômicos do provedor ou do interesse público em ter acesso à informação, salvo em situações especiais, como quando se trate de pessoa pública e o interesse preponderante do público seja o acesso a tal informação.
> Em consequência desse julgamento, a Google imediatamente pôs à disposição dos consumidores da União Europeia uma ferramenta para que formulassem seus pedidos de apagamento ou remoção de dados. Segundo Viviane Maldonado, "quase cinco anos depois, a ferramenta continua sendo disponibilizada pelo Google e as estatísticas demonstram que desde a sua implantação, foram submetidas cerca de três milhões de requisições, havendo significativa parcela delas (44,2% - janeiro/2019) sido atendida (CUEVA, 2020, p. 628).

Vê-se, assim, que o direito ao esquecimento carrega algumas limitações, em especial porque colide com outros direitos que são igualmente fundamentais. Então, essa condição colocada à pessoa da autodeterminação ou ao desejo de compartilhar informações mesmo que pessoais se coloca sempre diante de alguns dilemas, sendo importante que as pessoas tenham uma cultura de proteção de dados e compartilhem apenas os necessários.

No Brasil, não existe nenhuma norma que disponha expressamente o direito ao apagamento de dados pessoais. Pelo contrário, em decisão do STF, na conclusão do julgamento do Recurso Extraordinário 1.010.606/RJ, no dia 11 de fevereiro de 2021, apenas dois dos dez ministros que participaram da votação reconheceram expressamente a existência do direito ao esquecimento no ordenamento jurídico brasileiro.

É preciso ter cuidado ao balancear o acesso à informação com a proteção de dados, como nessa decisão no STF sobre o Direito ao Esquecimento, na qual foi feito um sopesamento desses direitos. A LGPD, em seu artigo 4º, elenca as exceções para o tratamento de dados pessoais – que ficam restritas aos fins exclusivamente jornalísticos e artísticos (BRASIL, 2018).

Ao se analisar esse artigo, parece que LGPD privilegia a liberdade de informação em detrimento da proteção de dados pessoais; enquanto na GDPR isso é um pouco diferente: há uma flexibilidade na legislação para que os países que fazem parte de União Europeia façam o balanceamento entre a liberdade de imprensa e a de expressão, para um ajuste desses direitos.

Bauman (2001), quando faz referência à modernidade líquida, sugere um desbalanceamento entre as relações que acontecem na esfera global e a esfera local:

- **Esfera local**: a autodeterminação informativa, as instituições, normas regulamentadoras e a política estão localizadas em um lugar específico;
- **Esfera global**: as tecnologias digitais e as grandes plataformas que modelam o comportamento da sociedade fluem universalmente.

Com isso, surge uma polarização entre a macro e a microestrutura, entre a liberdade de informar e posteriormente a dificuldade do exercício da autodeterminação informativa, em razão desse descompasso que existe entre o local e o global. *Como exercer o direito ao esquecimento se esse se encontra na esfera global, espalhado pelas plataformas, se a autodeterminação da pessoa está geograficamente limitada?*

Mesmo que surjam mecanismos mais eficazes para o "apagamento", é importante observar que há limites para o direito ao esquecimento, entre os quais: quando o fato for de interesse público e quando ferir outros direitos como o direito à memória e à liberdade de expressão (TRIBUNAL…, 2020). No Estado Democrático de Direito, memória e esquecimento compreendem direitos fundamentais da personalidade, porém não são ilimitados, isolados e absolutos, possuem limitações constitutivas, que requerem ponderação e proporcionalidade:

> O direito ao esquecimento não pode ser entendido como direito absoluto. Algumas das limitações à sua aplicação são o interesse público, o direito e a liberdade de

> informação, discutidos na audiência pública realizada pelo Supremo Tribunal Federal no dia 12.07.2017, que teve por objeto o direito ao esquecimento na esfera civil, tema versado no Recurso Extraordinário n° 1.010/606/RJ, de relatoria do Ministro Dias Tóffoli, com repercussão geral reconhecida, que impugna o acórdão do TJRJ no caso Aída Curi e já foi debatido pelo STJ no REsp n° 1.335.153/RJ. O interesse público deve preponderar sempre que se trate de fato genuinamente histórico, ou seja, que tenha preservado sua atualidade a despeito do decurso do tempo. Como ressaltado no voto condutor do REsp nº 1334.097/RJ, a historicidade deve ser analisada em concreto e o interesse público e social deve ter sobrevivido à passagem do tempo, Em outras palavras, "{...} se não houver atualidade no interesse pela notícia, fato pretérito, o interessado poderá exercer o seu direito ao esquecimento, pleiteando que seja impedida veiculação de notícias sobre aqueles, que deverão ser mantidos no passado e não ser retomados sem uma justificativa plausível. Parte-se da premissa que o decurso do tempo dilui ou pode diluir o interesse público" (MENDES et. al. 2020, p. 638).

Isso demonstra que interesse público não se confunde com fatos que as pessoas consideram interessantes, mas que são irrelevantes em um contexto histórico. Trata-se de um direito de acesso à informação, assegurado na CF (Arts. 5º, IV, IX e XIV, e 220), que tutela direitos públicos como a liberdade de expressão, de pensamento e da informação:

> IV - é livre a manifestação do pensamento, sendo vedado o anonimato;
> IX - é livre a expressão da atividade intelectual, artística, científica e de comunicação, independentemente de censura ou licença;
> XIV - é assegurado a todos o acesso à informação e resguardado o sigilo da fonte, quando necessário ao exercício profissional;
> Art. 220. A manifestação do pensamento, a criação, a expressão e a informação, sob qualquer forma, processo ou veículo não sofrerão qualquer restrição, observado o disposto nesta Constituição (BRASIL, 1988).

Por conseguinte, o direito à memória é um direito do coletivo (difuso), que assegura o direito à preservação da cultura de uma determinada coletividade:

> Vê-se que direito à memória é difuso e envolve a preservação da identidade cultural de um povo, nação ou Estado. Tal identidade é plasmada pela tradição que permite transmissão de um quadro de referências a interligar fatos de que outro modo seriam desconexos e não permitiriam o reconhecimento de traços comuns de união de coletividades expressivas. É preciso muito cuidado ao sopesar o direito à privacidade e o direito à memória, pois nem sempre é fácil, distinguir o essencial do acessório (MENDES et. al. 2020, p. 638).

A Lei Geral de Proteção de Dados não traz o direito ao apagamento de dados pessoais expresso em sua legislação, mesmo com uma forte influência da GDPR, que em seu art. 17 traz previsão expressa a esse direito. No Brasil, houve um julgamento recente, que se refere ao caso da Aída Curi, no qual o STF rejeitou por nove votos a um o direito ao esquecimento no país. A ministra Cármen Lúcia disse o seguinte acerca deste julgamento:

> Em um país de curta memória, discutir e julgar o esquecimento como direito fundamental, nesse sentido aqui adotado, ou seja, de alguém poder impor o silêncio e até o segredo de fato ou ato que poderia ser de interesse público, pareceria, se existisse essa categoria no direito, o que não existe um desaforo jurídico (TEIXEIRA, 2021, [s.p.]).

Assim como a ministra Cármen Lúcia, a maioria dos ministros aprovaram a seguinte tese jurídica:

> É incompatível com a Constituição Federal a ideia de um direito ao esquecimento, assim entendido como o poder de obstar, em razão da passagem do tempo, a divulgação de fatos ou dados verídicos e licitamente obtidos e publicados em meios de comunicação social – analógicos ou digitais. Eventuais excessos ou abusos no exercício da liberdade de expressão e de informação devem ser analisados caso a caso, a partir dos parâmetros constitucionais, especialmente os relativos à proteção da honra, da imagem, da privacidade e da personalidade em geral, e as expressas e específicas previsões legais nos âmbitos penal e cível (SUPREMO…, 2021).

Foi verificado, nesse caso, que por mais que o direito ao esquecimento esteja intrinsecamente ligado ao da personalidade (em que o indivíduo deve permanecer em seu estado de paz de espírito) e ao da autodeterminação informativa do cidadão, ele entra em conflito com o direito à informação e o da liberdade de imprensa. Desse modo, a análise do STF fez um sopesamento entre os direitos fundamentais, buscando um equilíbrio na decisão proferida. Mas quando a ministra Cármen Lúcia aborda o direito ao esquecimento como “um poder de obstar”, não parece que houve o devido cuidado com o sopesamento com direitos tão valiosos ao ordenamento jurídico brasileiro. Em relação a isso, Mansur analisa:

> Ao definir o direito ao esquecimento como o "poder de obstar, em razão da passagem do tempo, a divulgação de fatos ou dados verídicos e licitamente obtidos e publicados em meios de comunicação social analógicos ou digitais", o Supremo parece ter caído na armadilha de tentar compreender um direito (rectius, situação jurídica subjetiva) tipicamente existencial — vale dizer, intrinsecamente associado ao desenvolvimento da personalidade humana — sob as lentes do vetusto direito subjetivo, categoria formulada para a tutela de interesses patrimoniais (MANSUR, 2021, [s.p.]).

O direito à família, julgado no caso acima, poderia ser invocado de outra maneira, sem citar o termo direito ao esquecimento, pois o art. 5º, inciso da X, da CF resguarda o direito à intimidade, assim como o poder de alegar dano para posterior reparação. Logo, o que se extrai do julgamento do STF é que não há a possibilidade de se declarar a completa

inexistência/exclusão de um direito de todo o ordenamento jurídico, já que sempre haverá a possibilidade de reparação de danos por fatos que extrapolam os direitos de personalidade.

5.4 PROTEÇÃO DE DADOS UM DIREITO FUNDAMENTAL

A proteção de dados já é considerada um direito fundamental, porém implícito, já que não está expresso no artigo 5º da CF. Mas antes do caso do IBGE, analisado anteriormente, ela já poderia ser considerada um direito fundamental por causa da abertura de entendimento do parágrafo 2º do referido artigo: "[…] § 2º Os direitos e garantias expressos nesta Constituição não excluem outros decorrentes do regime e dos princípios por ela adotados, ou dos tratados internacionais em que a República Federativa do Brasil seja parte" (BRASIL, 2018, [s. l.]).

Isso também ocorre com o direito à personalidade, também um direito fundamental, que decorre de outro princípio, o da *dignidade da pessoa humana* (que é um dos fundamentos da CF, prevista no artigo 1). Nesse sentido:

> Assim, no caso brasileiro (que, em maior ou menor medida, corresponde a outras experiencias), existem direitos fundamentais sediados em outras partes do texto constitucional (fora do título próprio, ou seja, o catálogo de direitos em sentido estrito), mas também direitos não expressamente positivados, conquanto deduzidos, na condição de direitos implícitos, dos princípios fundamentais ou mesmo de outros direitos, consoante, aliás, demonstra o exemplo do direito à autodeterminação informativa e, mais recentemente ligado ao tema da proteção de dados, o assim chamado o direito ao esquecimento. [...] Com isso, fixados alguns pressupostos, é possível avançar no tocante à qualificação do direito à proteção de dados como direito humano e fundamental (SARLET, 2015, [s. p.]).

Nessa mesma perspectiva, Sarlet observa:

> Assim, uma compreensão/interpretação/aplicação constitucionalmente adequada do direito fundamental à proteção de dados deverá sempre ser pautada por uma perspectiva sistemática, que, a despeito do caráter autônomo (sempre parcial), desse direito, não pode prescindir do diálogo e da interação (por vezes marcada por concorrências, tensões e colisões) com outros princípios e direitos fundamentais, que, dentre outros pontos a considerar, auxiliam a determinar o seu âmbito de proteção, inclusive mediante o estabelecimento de limites diretos e indiretos.
> De particular relevância no caso brasileiro – justamente pela existência, além da nova LGPD e de outras leis que versam sobre o tema, é ter sempre presente que, independentemente de sua inclusão no texto da CF, impõe-se ao Estado, por força de seus deveres de proteção, não apenas zelar pela consistência constitucional do marco normativo infraconstitucional (inclusive da LGPD) no tocante aos diplomas legais isoladamente considerados, mas também de promover sua integração e harmonização produtiva, de modo a superar eventuais contradições e assegurar ao direito

> fundamental à proteção de dados, sua máxima eficácia e efetividade (SARLET, 2020, [s.p.]).

Para o referido autor, o direito à proteção de dados pode ser extraído do texto constitucional desde que ocorra um devido balanceamento com outros direitos fundamentais. Mesmo assim, há uma PEC (17/2019) tramitando no Congresso Nacional que visa trazer uma previsão legal expressa do direto à proteção de dados como um direito fundamental, no rol de direitos no art. 5º da CF. Com essa previsão, torna-se mais fácil o controle de constitucionalidade de outras normas que eventualmente coloquem em vulnerabilidade o titular dos dados, com o intuito de trazer maior proteção legal, já que, como a LGPD é uma lei infraconstitucional, poderá ocorrer a existência de conflitos com outras legislações. Assim, se o direito à proteção de dados estiver expresso na CF, o ônus argumentativo para se sustentar uma eventual inconstitucionalidade é mais facilitado do que para se buscar o entendimento de um direito fundamental implícito. Por consequência, a proteção de dados se torna um direito autônomo se a PEC 17/19 for aprovada.

Essa PEC também traz que as questões referentes à proteção de dados é matéria de competência privativa da União. Isso também é importante porque permite a uniformidade: se cada Estado tivesse normas diferentes sobre essa matéria, se o controlador tivesse que observar todas essas normas, dificultar-se-ia ou até mesmo tornar-se-ia inviável o controle diante do grande fluxo desses dados e de diferentes jurisdições. *Como que seria feito um compliance das 'leis' de proteção de dados no Brasil dentro desse contexto?* Por isso que se diz que a Proteção de Dados deve ser uma matéria de competência privativa da União.

6 ANÁLISE DA APLICAÇÃO PRÁTICA DA LGPD E DA AUTODETERMINAÇÃO INFORMATIVA

A eficácia da LGPD será colocada à prova somente na prática; e, como visto no decorrer desse trabalho, a atualização normativa está muito aquém do avanço da tecnologia. Para que Lei Geral de Proteção de Dados (nosso objeto de análise) tenha validade, é preciso que ela seja cumprida por todos os grupos sociais:

> Norma eficaz é aquela observada e cumprida pelos diversos grupos sociais. Implica o chamado 'hábito geral de obediência' (essa observação deve ser aprofundada, mas no começo, quando se afirma a LGPD), sendo garantia de cumprimento da norma. Assim a pressão social é que daria origem à obrigação vinculada pela norma que preestabeleceria os critérios de conduta a serem seguidos. A adaptação à mudança é uma exigência de sobrevivência da própria norma. Atualmente a problemática está na velocidade que a mudança vem adquirindo e na dificuldade do sistema jurídico em incorporá-la. Um breve exemplo; Lawrence Lessig, um dos maiores especialistas em Direito Digital, afirma que os códigos de software podem ser comparados a leis, ou seja, o código fonte dos softwares, assim como as leis, tem o efeito de controlar o comportamento de maneiras específicas. Por exemplo, você sabe que, quando quer usar os serviços de determinado provedor de acesso, precisa fornecer sua senha. É requisito imposto a você pelo código do Provedor de Acesso. Portanto seria possível escrever uma lei dizendo que você deveria se identificar adequadamente. Mas isso seria menos eficiente. Ambos são estruturas projetadas para controlar o comportamento. São diferentes de uma maneira importante: é mais fácil violar uma lei do que violar um código-fonte. Então certamente seria uma mudança se algumas leis sagradas fossem implementadas com a tecnologia de software (PINHEIRO, 2012, p. 56).

Pinheiro (Ibid.) afirma que esse raciocínio demonstra como o direito pode ser transformado por uma realidade social e que a capacidade de adaptação do Direito irá nortear a estabilidade do ordenamento jurídico. As suas atualizações têm que estar em conformidade com todo o contexto para que o Sistema Jurídico seja capaz de produzir normas válidas e eficazes, garantindo segurança à sociedade. Foi para isso que a LGPD foi criada.

Ainda que exista o processo de educação digital – visto que só a legislação cria limites para o uso dos dados –, trazer punições para o excesso desse uso não é o suficiente. As pessoas têm que entender a importância dos seus dados pessoais, assim como os efeitos colaterais causados pelo excesso de uso da rede, por exemplo: o aumento de ansiedade e da depressão.

Essa tomada de consciência das pessoas está, simultaneamente, expressa e implícita na LGPD, quando esta traz todos os seus princípios voltados para uma boa governança de dados, tanto que o presidente da Autoridade Nacional de Dados, Wlademar Gonçalves Ortunho Junior, disse que o principal foco da atuação do órgão, a princípio, será a educação, e não a

aplicação de multas e sanções – segundo ele “pouco eficientes”. Perspectiva chancelada por Miriam Wimmer, diretora da ANPD, que disse que o chicote não tem a mesma eficácia que o diálogo e que a maioria das multas acabam sendo judicializadas e não pagas.

Com tudo o que foi exposto em nossa pesquisa, chega-se à conclusão que a autodeterminação informativa é o coração da LGPD, sendo ela fundamental para que essa legislação tenha eficácia; assim como também é crucial a boa aplicação do artigo 18 da LGPD, que aborda os direitos dos titulares, e do artigo 6º, que traz os princípios e boas práticas, pilares fundamentais para a autodeterminação informativa.

É gigantesca a quantidade de dados com os quais os próprios titulares alimentam as plataformas, sem terem consciência da importância e do valor dessas informações; sendo a gerência atual desses dados muito precária, visto que esses dados se perpetuam através das redes, o que torna o direito ao esquecimento muito instável. Diante disso, a LGPD aparece como uma legislação de boas práticas, pois quanto mais transparente a empresa for na sua gestão e no gerenciamento do fluxo desses dados, melhor será a “conversa” com o titular, tendo como consequência uma maior autodeterminação informativa.

O gatilho para a grande propagação de leis gerais de proteção de dados ao redor do globo foi o caso Snowden, quando a autodeterminação informativa dos cidadãos não existia e as pessoas não faziam a mínima ideia de como seus dados estavam sendo tratados. Relembrando a fala recorrente do professor Bruno Bioni em suas aulas: “Se você não controla os seus dados pessoais, é a mesma coisa de não ter controle sobre si mesmo”, reforçando ele ainda a ideia de que a LGPD tem que ser vista como um novo contrato social, pois não existem mais dados insignificantes.

Finalmente, como amplamente discutido, a autodeterminação informativa é baseada no fortalecimento da pessoa diante das empresas e dos órgãos públicos que tratam dados. Como consequência disso, houve a necessidade de legislações generalistas (leis gerais de proteção de dados): como a atual sociedade é movida por dados, são necessárias regras para equilibrar essas relações, para que o fluxo de dados esteja de acordo e dentro dos princípios previstos nessas legislações.

7 CONCLUSÃO

Acreditamos que ficou evidenciado que, com o avanço da tecnologia, o volume de dados produzido no ambiente virtual aumenta a cada dia. Esses dados estão cada vez mais estruturados, gerando informação com maior valor agregado, fato esse que transformou a sociedade. A atual *sociedade da informação* é movida por dados, sendo a informação o seu maior ativo econômico. Por tudo isso, a preocupação com o fluxo e a gestão das informações é vital para que ocorra o equilíbrio entre Estado, gigantes da tecnologia e pessoas.

Levando-se em conta o que foi observado, a autodeterminação informativa, fundamento da LGPD, revela-se um instrumento muito eficaz, aparecendo como uma extensão da liberdade do indivíduo ao ter o controle sobre o fluxo das suas informações e incorporando às gigantes de tecnologia, Estados e empresas em geral a responsabilidade de adotarem medidas educacionais e boas práticas para que as pessoas tenham acesso às suas informações de forma clara e transparente e consigam colocar esse direto (da autodeterminação informativa) em prática.

REFERÊNCIAS

ALMEIDA, Ivan. MP 954 e o compartilhamento de dados: entenda a medida. **Politizei**. 2020. Disponível em: https://www.politize.com.br/mp-954-e-o-compartilhamento-de-dados/#:~:text=A%20Medida%20Provis%C3%B3ria%20n%C2%BA.,Geografia%20e%20Estat%C3%ADstica%20(IBGE). Acesso em: 13 ago. 2020.

ANASTASIA, Vittoria Alvares; LARA, Caio Augusto de Souza. O escândalo Cambridge Analytica: a manipulação de dados na era digital. In: Congresso Luso-Brasileiro de Direito Empresarial e Cidadania, 31., 2019, Curitiba. **Anais eletrônicos** [...]. Curitiba: Percurso, 2019. p. 164-167. Disponível em: http://revista.unicuritiba.edu.br/index.php/percurso/article/view/3722/371372086. Acesso em: 09 de ago. 2021.

ANDRADE, Walmar. Por que a privacidade está mais viva do que nunca. Walmar Andrare – Direito Digital. 2021. Disponível em: https://walmarandrade.com.br/privacidade/. Acesso em: 14 fev. 2021.

ANDRION, Roseli. WhatsApp vai permitir migração de backup entre sistemas operacionais. **Tilt Uol**. 2021. Disponível em: https://www.uol.com.br/tilt/noticias/redacao/2021/05/22/whatsapp-vai-permitir-migracao-de-conversas-entre-sistemas-operacionais.htm#:~:text=WhatsApp%20vai%20permitir%20migra%C3%A7%C3%A3o%20de%20backup%20entre%20sistemas%20operacionais&text=Quem%20usa%20o%20WhatsApp%20e,todas%20as%20conversas%20acabam%20perdidas.&text=Quando%20voc%C3%AA%20troca%20de%20aparelho,chat%20deixe%20de%20ser%20recuperada. Acesso em: 23 mai. 2021.

ÁVILA, Humberto. **Teoria dos princípios:** da definição à aplicação dos princípios jurídicos. 13. ed., rev. e ampl. São Paulo: Malheiros, 2012, p. 85-141.

BALIARDO, Rafael. Cármen questiona falta de discussão sobre Serasa. **Consultor Jurídico**. 2013. Acesso em: https://www.conjur.com.br/2013-ago-07/carmen-lucia-estranho-convenio-serasa-nao-ido-plenario. Acesso em: 17 ago. 2020.

BAUMAN, Zygmunt. **44 cartas do mundo líquido moderno**. Rio de Janeiro: Zahar, 2010.

BAUMAN, Zygmunt. **Modernidade Líquida**. Rio de janeiro: Jorge Zahar, 2001.

BAUMAN, Zygmunt. **Tempos líquidos**. Tradução: Carlos Alberto Medeiros. Rio de Janeiro: Jorge Zahar, 2007.

BIONI, Bruno Ricardo. **Proteção de dados pessoais:** a função e os limites de consentimento. 3. ed. Rio de Janeiro: Editora Forense, 2021.

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

BOCARD, Taysa. Wearables: o que são as “tecnologias vestíveis”. **Usemobile**. 2019. Disponível em: https://usemobile.com.br/wearable/. Acesso em: 21 nov. 2020.

BOHRER, Jerusa. O que é o consentimento granular na LGPD? **Immplementando a LGPD.** 2020. Disponível em: https://www.implementandoalgpd.com.br/blog/o-que-e-o-consentimento-granular-na-lgpd/. Acesso em: 07 jan. 2021.

BRASIL. [Constituição (1988)]. **Constituição da República Federativa do Brasil de 1988**. Emendas Constitucionais. Brasília, DF: Presidência da República, 2016. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 06 out. 2020.

BRASIL. **Decreto-lei nº 8.771, de 11 de maio de 2016.** Dispõe sobre das hipóteses admitidas de discriminação de pacotes de dados na internet e de degradação de tráfego indicar procedimentos para guarda e proteção de dados por provedores de conexão e de aplicações, apontar medidas de transparência na requisição de dados cadastrais pela administração pública e estabelecer parâmetros para fiscalização e apuração de infrações. Brasília, DF: Presidência da República, 2016a. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2016/decreto/d8771.htm. Acesso em: 20 set. 2020.

BRASIL. **Lei nº 10.406, de 10 de janeiro de 2002.** Institui o Código Civil. Brasília, DF: Presidência da República, 2002. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/2002/l10406compilada.htm. Acesso em: 18 fev. 2021.

BRASIL. **Lei nº 12.527, de 18 de novembro de 2011.** Dispõe sobre os procedimentos a serem observados pela União, Estados, Distrito Federal e Municípios, com o fim de garantir o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal. Brasília, DF: Presidência da República, 2011. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm. Acesso em: 09 de ago. 2021.

BRASIL. **Lei nº 12.965, de 23 de abril de 2014.** Estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil. Brasília, DF: Presidência da República, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 15 set. 2020.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018.** Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 17 set. 2020.

BRASIL. **Lei nº 8.078, de 11 de setembro de 1990.** Dispõe sobre a proteção do consumidor e dá outras providências. Brasília, DF: Presidência da República, 1990. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm. Acesso em: 19 jan. 2021.

BRASIL. **Proposta de emenda constitucional – PEC 17/2019**. Brasília, DF: Senado Federal, 2019a. Disponível em:

https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2210757. Acesso em: 14 out. 2020.

CABRERA, Pierina Andrea Aimone. Direito ao esquecimento na internet: uma comparação entre as legislações do Brasil e Chile. Fórum de Cortes Supremas do Mercosul [impresso]. 2016.

CANALTECH. Por privacidade Mark Zuckerberg compra casas de vizinhos por US$ 30 milhões. **CanalTech**, 2013. Disponível em: https://canaltech.com.br/mercado/Por-privacidade-Mark-Zuckerberg-compra-casas-de-vizinhos-por-US-30-milhoes. Acesso em: 1 mai. 2021.

CARDOSO, Bruno; BRUNO, Fernanda; MELGAÇO, Lucas; GUILHOM, Luciana; KANASHIRO, Marta. **Tecnopolíticas da vigilância**: perspectivas da margem. São Paulo: Boitempo, 2018. 432 p.

CARDOSO, Thais. Campanha de ursodesinformação da vacina contra covid avança em testes no Brasil. **Faculdade de Medicina de Ribeirão Preto,** Editorial do Jornal, 2020. Disponível em: http://jornal.fmrp.usp.br/campanha-de-desinformacao-sobre-vacina-contra-covid-avanca-com-testes-no-brasil/. Acesso em: 2 mai. 2021.

CARVALHO, Flâmila Machado de. **A tutela jurídica do direito fundamental à privacidade e a necessidade de atuação jurisdicional do estado**: uma análise do conflito entre o público e o privado. 2017. Trabalho de Conclusão de Curso (Bacharelado em Direito). Faculdade de Direito, Universidade Federal do Ceará, Fortaleza, 2017. Disponível em: http://www.repositorio.ufc.br/bitstream/riufc/29406/1/2017_tcc_fmcarvalho.pdf. Acesso em: 17 abr. 2021.

CASTELLS, Manuel. **A sociedade em rede.** Rio de janeiro: Paz & Terra. 2013.

COALIZÃO DIREITOS NA REDE. SEUS dados são você: liberdade, proteção, regulação. **Coalizão Direitos na Rede**, Campanha dados pessoais, 2019. Disponível em: https://direitosnarede.org.br/campanha/seus-dados-sao-voce/. Acesso em:06 out. 2020.

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

CUEVA, Ricardo Villas Bôas. PROTEÇÃO DE DADOS PESSOAIS E DIREITO AO ESQUECIMENTO. *In*: IN: MENDES, Laura Schertel; DONEDA, Danilo; SARLET, Ingo Wolfgang; RODRIGUES JR., Otávio Luiz (coord.). **Tratado de proteção de dados pessoais**. São Paulo: Editora Forense, 2020. p. 627-640.

DANTAS, Thiago; DANTAS, Dimitrius. Dória oferece dados de usuários do bilhete único a iniciativa privada. O Globo – Política. 201. Disponível em: https://oglobo.globo.com/politica/doria-oferece-dados-de-usuarios-do-bilhete-unico-iniciativa-privada-20942133. Acesso em: 14 fev. 2021.

DATA PRIVACY BRASIL. Amicus Curiae – STF – Caso IBGE. [*S. l.*: *s. n.*], 2020. 1 vídeo (11min 46s). Publicado pelo canal Data Privacy Brasil. Disponível em: https://www.youtube.com/watch?v=ExDTifFxpnQ&t=11s. Acesso em: 20 dez. 2020.

DATA TRANSFER PROJECT. About us. Data Transfer Project. 2021. Disponível em: https://datatransferproject.dev/. Acesso em: 21 maio 2021.

DEBORD, Guy. **Sociedade do espetáculo**. Rio de Janeiro: Contraponto, 1968.

DELGADO, Márcia. Serpro é suspeito de vender dados pessoais para administração pública. **Metrópolis**, 2018. Disponível em: https://www.metropoles.com/distrito-federal/serpro-e-suspeito-de-vender-dados-pessoais-para-administracao-publica. Acesso em: 17 ago. 2020.

DESJARDINS, Jeff. How much data is generated each day?. **Word Economic Forum**. 2019. Disponível em: https://www.weforum.org/agenda/2019/04/how-much-data-is-generated-each-day-cf4bddf29f/. Acesso em: 14 set. 2020.

DI FIORE, Bruno Henrique. Teoria dos círculos concêntricos da vida privada e suas repercussões na praxe jurídica. **Portal professor Flavio Tartuce**, 2012. Disponível em: https://scholar.google.com.br/scholar?hl=pt-BR&as_sdt=0%2C5&q=TEORIA+DOS+C%C3%8DRCULOS+CONC%C3%8ANTRICOS+DA+VIDA+PRIVADA+&btnG=. Acesso em: 18 fev. 2021.

DIÁRIO DE NOTÍCIAS. Whatsapp admite envio massivo de mensagens de forma irregular nas eleições ganhas por Bolsonaro. **Diário de Notícias**, 2019. Disponível em: https://www.dn.pt/mundo/whatsapp-admite-envio-massivo-de-mensagens-de-forma-irregular-nas-eleicoes-ganhas-por-bolsonaro-11385334.html. Acesso em: 2 mai. 2021.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. 2. ed. São Paulo: Revista dos tribunais, 2019.

EUROPEAN COMMISSION. Can personal data about children be collected? **Europa – Topic**, 2021. Disponível em: https://ec.europa.eu/info/law/law-topic/data-protection/reform/rights-citizens/how-my-personal-data-protected/can-personal-data-about-children-be-collected_en. Acesso em: 11 jan. 2021.

FELIZI, Natasha; VARON, Joana. Menstruapps: como transformar sua menstruação em dinheiro para os outros. **Chupadados**, 2020. Disponível em: https://chupadados.codingrights.org/menstruapps-como-transformar-sua-menstruacao-em-dinheiro-para-os-outros/. Acesso em: 14 ago. 2020.

FUNDO INTERNACIONAL DE EMERGÊNCIA DAS NAÇÕES UNIDAS PARA A INFÂNCIA – UNICEF. Declaração Universal dos Direitos Humanos: adotada e proclamada pela Assembleia Geral das Nações Unidas (resolução 217 A III) em 10 de dezembro 1948. 2020. Disponível em: https://www.unicef.org/brazil/declaracao-universal-dos-direitos-humanos. Acesso em: 14 out. 2020.

GOES, Evelise. Postagens em redes sociais podem levar à demissão por justa causa? **JusBrasil**. 2020. Disponível em: https://custodiogoes.jusbrasil.com.br/artigos/658384243/postagens-em-redes-sociais-podem-levar-a-demissao-por-justa-causa. Acesso em: 14 set. 2020 .

GRECCO, Rogério. **Código Penal comentado**. 12. ed. Niterói: Editora Impetus, 2018.

GREENWALD, Glenn. **Sem lugar para se esconder**: Edward Snowden, a NSA e a espionagem do governo americano. Rio de Janeiro: Sextante, 2014.

GREENWALD, Glenn. Why privacy Matters. TED Talks. [*S. l.*: *s. n.*], 2014a. 1 vídeo (22 min). Publicado pelo canal TED. Disponível em: https://www.youtube.com/watch?v=pcSlowAhvUk. Acesso em: 17 ago. 2020.

GUIMARÃES, C. Chineses passarão por registro facial para se cadastrar na internet: medida é considerada, por muitos, uma nova forma de censura e controle do governo chinês sobre as atividades online. **Olhar Digital**, 2019. Disponível em: https://olhardigital.com.br/fique_seguro/noticia/chineses-passarao-por-registro-facial-para-se-cadastrar-na-internet/91416. Acesso em: 17 ago. 2020.

HARARI, Yuval Harari. **21 lições para o século 21**. Tradução: Paulo Geiger. São Paulo: Companhia das letras, 2018.

HENRIQUE, Lygia Maria M. Molina; ANDRADE, Vitor Morais de. Vazamento de dados: uma preocupação da Lei Geral de Proteção de Dados. **Migalhas**, 2019. Disponível em: https://www.migalhas.com.br/depeso/298452/vazamento-de-dados-uma-preocupacao-da-lei-geral-de-protecao-de-dados. Acesso em: 15 set. 2020.

INTERNATIONAL DATA CORPORATION. International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications, and consumer technology markets. **Internacional Data Corporation**, 2020. Disponível em: https://www.idc.com/about. Acesso em: 14 set. 2020.

INTERNET. O que é Arpanet. **Sites Record**. 2020. Disponível em: https://sites.google.com/site/sitesrecord/o-que-e-arpanet. Acesso em: 20 dez. 2020.

JOSEPH, Amanda Camolez. Em Portugal, centro hospital é multado em 400 mil euros por violar GDPR. **LGPD Brasil**. 2019. Disponível em: https://www.lgpdbrasil.com.br/em-portugal-centro-hospital-e-multado-em-400-mil-euros-por-violar-gdpr/#:~:text=O%20Centro%20Hospitalar%20Barreiro%20Montijo,houve%20tr%C3%AAs%20viola%C3%A7%C3%B5es%20do%20GDPR.&text=Para%20esses%2C%20a%20multa%20foi%20de%20150.000%20euros. Acesso em: 09 jan. 2020.

KAC, Fernanda; LÓPEZ, Nuria. Proteção de dados na área da saúde: harmonização da LGPD frente as normas setoriais. **Abatista**, 2020. Disponível em: http://abatista.adv.br/artigo/protecao-de-dados-na-area-da-saude-harmonizacao-da-lgpd-frente-as-normas-setoriais. Acesso em 09 jan. 2020.

KLEINA, Nilton. A história da Kodak, a pioneira da fotografia que parou no tempo. **TECMUNDO**, 2017. Disponível em: https://www.tecmundo.com.br/mercado/122279-historia-kodak-pioneira-da-fotografia-nao-evoluiu-video.htm. Acesso em: 15 ago. 2020.

LAMY, Marcelo. **Metodologia de pesquisa jurídica**: técnicas de investigação, argumentação e redação. Imprenta: Rio de Janeiro, Elsevier, 2011.

LAPOWSKY, Issie. How Cambridge Analytica sparked the great privacy awakening. **Wired**, São Francisco, 17 mar 2018. Disponível em: https://www.wired.com/story/cambridge-analytica-facebook-privacy-awakening/. Acesso em: 20 nov. 2020.

LEI do do DF que prevê políticas públicas para famílias deve incluir união homoafetiva, decide STF. **Portal do STF**, 2021a. Disponível em: https://portal.stf.jus.br/noticias/verNoticiaDetalhe.asp?idConteudo=423582. Acesso em: 21 fev. 2021.

LÉVY, Pierre. **O que é Virtual?** São Paulo: Editora 34, 1996.

LEVY, Pierre. O terceiro estágio da humanidade. **Folha UOL**, 1998. Disponível em: https://www1.folha.uol.com.br/fsp/mais/fs180104.htm. Acesso em: 16 out. 2020.

LUCCA, Newton de. Marco civil da internet: uma visão panorâmica dos principais aspectos relativos as suas disposições preliminares. *In*: LUCCA, Newton de.; SIMÃO FILHO, A. LUCCA, Newton de; SIMÃO FILHO, Adalberto; LIMA, Cintia Rosa Pereira de Lima. (coord.). **Direito & Internet III**: marco civil da internet. Quartier Latin, 2015, p. 39.

MALDONADO, Viviane Nóbrega. A Influência Europeia na Proteção de Dados no Brasil. [*S. l.: s. n.*], 2020. 1 vídeo (58 min). Publicado pelo canal Advogado de Startups. Disponível em: https://www.youtube.com/watch?v=ZfCCemXIYfw. Acesso em: 14 jul. 2020.

MALDONADO, Viviane Nóbrega; BLUM, Renato Opice (coord.). **Lei Geral de Proteção de Dados Comentada.** São Paulo: Revista dos Tribunais; Nova Edição. 2019.

MANSUR, Rafael. Decisão do STF não é 'pá de cal' no direito ao esquecimento. **Conjur**, 2021. Disponível em: https://www.conjur.com.br/2021-fev-24/mansur-stf-nao-jogou-pa-cal-direito-esquecimento. Acesso em: 30 mai. 2021.

MARCACINI, A. Aspectos fundamentais do Marco Cívil da internet: lei n. 12.965/2014 [*e-Book*]. Kindle. 2017.

MARIGHETTO, Andrea. A dignidade humana e o limite dos direitos da personalidade. **Conjur**, 2019. Disponível em: https://www.conjur.com.br/2019-ago-21/marighetto-dignidade-humana-limite-direitos-personalidade. Acesso em: 25 jan. 2020.

MARSHALL, Jack. WTF is real-time bidding? **Digiday**, 2014. Disponível em: https://digiday.com/media/what-is-real-time-bidding/. Acesso em: 14 ago. 2020.

MAYER-SCHOENBERGER, Viktor; CUKIER, Kenneth. **Big Data**: a revolution that will transform how we live, work, and think. Londres: John Murray, 2013.

MEDIDA provisória ordena teles a compartilhar dados de clientes com IBGE. **Câmara dos Deputados**, Brasília, 2020. Disponível em: https://www.camara.leg.br/noticias/655297-medida-provisoria-ordena-teles-a-compartilhar-dados-de-clientes-com-ibge/#:~:text=A%20Medida%20Provis%C3%B3ria%20954%2F20,realizar%20pesquisas%20domiciliares%20por%20telefone.&text=A%20norma%20atende%20pedido%20do%20IBGE. Acesso em: 18 fev. 2020.

MEGAVAZAMENTO de dados: o que se sabe e o que falta saber. **FGV – Educação executiva**, 2021. Disponível em: https://www.ibe.edu.br/megavazamento-de-dados-o-que-se-sabe-e-o-que-falta-saber/. Acesso em: 02 mai. 2021.

MENDES, Laura Schertel; DONEDA, Danilo; SARLET, Ingo Wolfgang; RODRIGUES JR., Otávio Luiz (coord.) **Tratado de proteção de dados pessoais**. São Paulo: Forense. 2020. 1516 p.

MENDONÇA, Suzana. A autodeterminação informativa no contexto de proteção de dados pessoais. **Consultor jurírico**, 2019. Disponível em: https://www.conjur.com.br/2019-out-20/suzana-mendonca-autodeterminacao-informativa-protecao-dados. Acesso em: 22 mai. 2021.

MIRANDA, Leandro Alvarenga. **A proteção dos dados pessoais e o paradigma da privacidade**. São Paulo: All Print, 2018.

MOREIRA, Rogério Meneses Fialho (coord.). A tutela da dignidade da pessoa humana na sociedade da informação inclui o direito ao esquecimento. **Conselho da Justiça Federal,** 2021. Disponível em: https://www.cjf.jus.br/enunciados/enunciado/142. Acesso em: 25 jan.2021.

MÜLLER-MAGUHN, Andy; ZIMMERMANN, Jérémie; ASSANGE, Julian; APPELBAUM, Jacob. **Cypherpunks**: liberdade e o futuro da internet. Tradução: Cristina Yamagami. São Paulo: Boitempo, 2013.

NATUSCH, Igor; FELIZI, Natasha; VARON, Joana. Bilhete único: concentração de dados e dinheiro no transporte público do Rio. **Chupadados**, 2020. Disponível em: https://chupadados.codingrights.org/com-o-riocard-seus-dados-passeiam-pelo-rj-e-ninguem-sabe-onde-vao-descer/. Acesso em: 17 ago. 2020.

NISSENBAUM, Helen. **Privacy in context**: technology, policy, and the integrity of social life. Stanford: Stanford University Press, 2010.

NISSENBAUM, Helen. Review: a quest for a theory of privacy: context and control. **American Bar Association**, v. 51, n. 4, 2011, p. 447-479. Disponível em: https://www.jstor.org/stable/41307137?seq=1. Acesso em: 30 dez. 2020.

NOTA fiscal paulista não tem política de privacidade. **Carta Capital**, 2015. Disponível em: https://www.cartacapital.com.br/economia/nota-fiscal-paulista-nao-tem-politica-de-privacidade-4802/. Acesso em: 17 ago. 2020.

NOVO, Benigno Núñez. Amicus Curiae: análise da figura do amicus curiae trazida pelo Código de Processo Civil. A origem, conceito, a natureza jurídica e quais são os limites e os direitos que o abarcam. **Direito Net**, 2018. Disponível em: https://www.direitonet.com.br/artigos/exibir/10419/Amicus-Curiae. Acesso em: 18 jan. 2021.

OPT-IN e Opt-out: tudo que você precisa saber sobre o assunto. **Tww Sinch Company**, 2019. Disponível em: https://blog.tww.com.br/opt-in-e-opt-out/. Acesso em: 19 jan. 2021.

ORWELL, George. **Box**: o horizonte de George Orwell. Tradução de Luísa Geisler. São Paulo: Editora Novo Século, 2021.

OXFORD LANGUAGES AND GOOGLE. LEALDADE. *In*: OXFORD LANGUAGES AND GOOGLE, 2021. Disponível em: https://languages.oup.com/google-dictionary-pt/. Acesso em: 19 jan. 2020.

PECKHAM, Oliver. Global DataSphere to Hit 59 Zettabytes in 2020 Alone, IDC Projects. **Datanami,** 2020. Disponível em: https://www.datanami.com/2020/05/19/global-datasphere-to-hit-59-zettabytes-in-2020-alone-idc-projects/. Acesso em 14 set. 2020.

PINHEIRO, Patricia Peck. **Direito digital**. 6. ed. São Paulo: Saraiva Jur., 2012.

PINHEIRO, Patricia Peck. **Proteção de dados pessoais**: comentários à lei 13.709/2018 – LGPD. 1. ed. São Paulo: Saraiva Jur., 2018.

QIANG, Xiao. The Road to Digital Unfreedom: President Xi's Surveillance State. **Journal of Democracy**, v. 30, n. 1, 2019, p. 53-67. Disponível em: https://muse.jhu.edu/article/713722. Acesso em: 17 ago. 2020.

QUATTROCIOCCHI, Walter; SCALA, Antonio; SUNSTEIN, Cass R. Echo Chambers on Facebook. **SSRN**, 2016. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2795110. Acesso em: 16 set. 2020.

RANGEL, J. M. B. Dia da privacidade de dados: IN estuda proteção de dados pessoais. **Arquivo Nacional: ministério da justiça e segurança pública**, 2020. Disponível em: http://www.arquivonacional.gov.br/br/ultimas-noticias/2039-dia-de-privacidade-de-dados-an-estuda-protecao-de-dados-pessoais. Acesso em: 14 jul. 2020.

REDE GLOBO. Banida da Alemanha, boneca Cayla desaparece das lojas do país. **Jornal Naciona**, 2017. Disponível em: http://g1.globo.com/jornal-nacional/noticia/2017/02/banida-da-alemanha-boneca-cayla-desaparece-das-lojas-do-pais.html. Acesso em: 11 jan. 2021.

REINALDO FILHO, Demócrito. Lei americana protege dados de crianças na internet. **Conjur**, 2013. Disponível em: https://www.conjur.com.br/2013-jan-02/democrito-filho-lei-americana-protege-dados-criancas-internet. Acesso em: 18 jan. 2021.

RIGUES, Rafael. Mãe da internet faz 50 anos: conheça a história da ARPANET. **Olhar Digital.** 2019. Disponível em: https://olhardigital.com.br/2019/10/24/noticias/mae-da-internet-faz-50-anos-conheca-a-historia-da-arpanet/#:~:text=A%20ARPANET%20foi%20criada%20pela,controlar%20sistemas%20nucleares%20de%20defesa. Acesso em: 18 fev. 2021.

SARLET, I. W. Precisamos da previsão de um direito fundamental à proteção de dados no texto da CF? **Consultor Jurídico**. 2020. Disponível em: https://www.conjur.com.br/2020-set-04/direitos-fundamentais-precisamos-previsao-direito-fundamental-protecao-dados-cf. Acesso em: 15 fev. 2020.

SARLET, Ingo Wolfgang. Uma Constituição aberta a outros Direitos Fundamentais? **Consultor Jurídico**, 2015. Disponível em: https://www.conjur.com.br/2015-mar-13/direitos-fundamentais-constituicao-aberta-outros-direitos-fundamentais. Acesso em: 27 jan. 2021.

SAUAIA, Hugo Moreira Lima. **A proteção dos dados pessoais no Brasil**. Lumen Juris: Rio de Janeiro, 2018.

SCHWAB, Klaus. **A quarta revolução industrial**. São Paulo: Edipro. 2018.

SIBILIA, Paula. Você é o que o google diz que você é: a vida editável, entre controle e espetáculo. *In*: CARDOSO, Bruno; BRUNO, Fernanda; MELGAÇO, Lucas; GUILHOM, Luciana; KANASHIRO, Marta. **Tecnopolíticas da vigilância: perspectivas da margem**. São Paulo: Boitempo, 2015, p. 199-216.

SILVA, F. O. B. A LGPD na saúde: desafios na adequação à LGPD em uma clínica multidisciplinar. *In*: LIMA, A. P. M.C.; CRESP, M.; PINHEIRO, P. P. **LGPD aplicada**. São Paulo: Atlas, 2021.

SOUZA, Edivanio Duarte de. A autodeterminação informativa na cultura de compartilhamento. [*S. l.*: *s. n.*], 2020. 1 vídeo (1h 31 min 08s). Publicado pelo canal Programa de Pós-Graduação em Ciência, Tecnologia e Sociedade. Disponível em: https://www.youtube.com/watch?v=ntvJ4H39cds. Acesso em 9 dez. 2020.

SOUZA, Gabriel Vinicius; SANTOS, Marcela de Freitas; TEOTÔNIO, Paulo José Freire. Direito à privacidade em meio à sociedade da informação. **JUS**, 2019. Disponível em: https://jus.com.br/artigos/77595/direito-a-privacidade-em-meio-a-sociedade-da-informacao. Acesso em 4 dez. 2020.

STANFORD ENCYCLOPEDIA OF PHILOSOPHY.Positive and negative liberty. *In:* STANFORD ENCYCLOPEDIA OF PHILOSOPHY, 2016. Disponível em: https://plato.stanford.edu/entries/liberty-positive-negative/. Acesso em: 01 jan. 2021.

STF conclui que direito ao esquecimento é incompatível com a Constituição Federal. **Portal STF**, 2021. Disponível em: https://portal.stf.jus.br/noticias/verNoticiaDetalhe.asp?idConteudo=460414&ori=1. Acesso em: 21 fev. 2021.

SUPREMO começa a julgar compartilhamento de dados de usuários de telefonia com o IBGE. **Portal STF**, 2020. Disponível em: https://portal.stf.jus.br/noticias/verNoticiaDetalhe.asp?idConteudo=442823&ori=1. Acesso em: 14 out. 2020.

TASSO, F. Tratamento de dados pessoais pelo poder público – Tema 4. EBRADI, Módulo: Lei Geral de Proteção de Dados. Pós Graduação em Direito Digital, 2019. [Conteúdo Pago].

TEFFÉ, Chiara Spadaccini de; VIOLA, Mario. Tratamento de dados pessoais na LGPD: estudo sobre as bases legais. **civilistica.com**, v. 9, n. 1, p. 1-38, 9 mai. 2020.

TEIXEIRA, Matheus. Por 9 a 1, Supremo vê risco à liberdade de expressão e barra direito ao esquecimento no Brasil. **Folha de São Paulo**, 2021. Disponível em: https://www1.folha.uol.com.br/poder/2021/02/stf-forma-maioria-para-declarar-que-nao-existe-direito-ao-esquecimento-no-brasil.shtml. Acesso em: 21 fev. 2021.

THE ECONOMIST. The world's most valuable resource is no longer oil, but data. **The Economist**, 2017. Disponível em: https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data. Acesso em: 15 fev. 2021.

THE ECONOMIST. The worlds most valuable resurce is no longer oil but data: the data economy demands a new approach to antitrust rules. **The Economist**, 2020. Disponível em: https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data. Acesso em: 17 ago. 2020.

TRIBUNAL DE JUSTIÇA DO DISTRITO FEDERAL E DOS TERRITÓRIOS. O direito ao esquecimento e o conflito com os direitos a liberdade e informação e de expressão. **Constituição Federal – TJDFT**, 2020. Disponível em: https://www.tjdft.jus.br/consultas/jurisprudencia/jurisprudencia-em-temas/direito-constitucional/o-direito-ao-esquecimento-e-o-conflito-com-os-direitos-a-liberdade-de-informacao-e-de-expressao. Acesso em: 15 fev. 2021.

VAN DIJCK, José. Confiamos nos dados? As implicações da datificação para o monitoramento social. **Revista Matrizes**. v.11, n. 1. São Paulo, 2017. p. 39-59.

WARREN, Samuel Dennis; BRANDEIS, Louis Dembitz. The Right to Privacy. **Harvard Law Review**, v. 4, n. 5, 2007, p. 193-220.

WIMMER, Miriam. O Regime Jurídico do Tratamento de Dados Pessoais pelo Poder Público. IN: **Tratado de Proteção de Dados Pessoais**. MENDES, Laura Schertel; DONEDA, Danilo; SARLET, Ingo Wolfgang; RODRIGUES JR., Otávio Luiz (coord.). São Paulo: Editora Forense, 2020.

WORLD ECONOMIC FORUM. Inforgráficos. 2021. Disponível em: https://www.weforum.org/. Acesso em: 14 fev. 2021.

ZUBOFF, Shoshana. Big other: capitalismo de vigilância e perspectivas para uma civilização de informação. In: BRUNO, F.; CARDOSO, B.; KANASHIRO, M.; GUILHON, L. **Tecnopolíticas da vigilância: perspectivas da margem**. São Paulo: Boitempo. 2015. p. 17-68.

ZUBOFF, Shoshana. Um capitalismo de vigilância. **Le Monde diplomatique Basil,** 2019. Disponível em: https://diplomatique.org.br/um-capitalismo-de-vigilancia/. Acesso em: 15 fev. 2021.