Fundação Educacional do Município de Assis
Instituto Municipal de Ensino Superior de Assis
Campus "José Santilli Sobrinho"

JÚLIA DA SILVA BASTOS

DADOS PESSOAIS COMO UM PRODUTO NO MERCADO DIGITAL: OBSERVAÇÕES JURÍDICAS

Assis/SP
2021

Fundação Educacional do Município de Assis
Instituto Municipal de Ensino Superior de Assis
Campus "José Santilli Sobrinho"

JÚLIA DA SILVA BASTOS

DADOS PESSOAIS COMO UM PRODUTO NO MERCADO DIGITAL: OBSERVAÇÕES JURÍDICAS

Projeto de pesquisa apresentado ao curso de direito do Instituto Municipal de Ensino Superior de Assis – IMESA e a Fundação Educacional do Município de Assis – FEMA, como requisito parcial à obtenção do Certificado de Conclusão.

Orientando(a): Júlia da Silva Bastos
Orientador(a): Leonardo de Gênova

Assis/SP

2021

FICHA CATALOGRÁFICA

B327d BASTOS, Júlia da Silva
Dados pessoais no mercado digital: observações jurídicas /
Júlia da Silva Bastos.. – Assis, 2021.

59p.

Trabalho de conclusão do curso (Direito). – Fundação Educacional do Município de Assis-FEMA

Orientador: Ms. Leonardo de Gênova

1.Privacidade 2.Segurança de dados 3.Dados pessoais

CDD 005.8

DADOS PESSOAIS COMO UM PRODUTO NO MERCADO DIGITAL: OBSERVAÇÕES JURÍDICAS

JÚLIA DA SILVA BASTOS

Trabalho de Conclusão de Curso apresentado ao Instituto Municipal de Ensino Superior de Assis, como requisito do Curso de Graduação, avaliado pela seguinte comissão examinadora:

Orientador: _____
Leonardo de Gênova

Examinador: _____
Fernando Antônio Soares de Sá Junior

Assis/SP
2021

AGRADECIMENTOS

Agradeço, primeiramente, aos meus pais, Adriana e Fábio, por serem meus maiores exemplos, por me incentivarem a atingir meus sonhos e por terem sempre se esforçado ao máximo para que eu conseguisse o melhor estudo e educação, por isso, serei sempre grata.

Às minhas irmãs, por serem minhas grandes amigas e estarem sempre ao meu lado.

Ao Vitor, pelo carinho, amor e parceria.

À minha avó Sônia e avô Nelson (*in memoriam)* que com certeza estariam muito felizes com o encerramento desta fase tão importante da minha vida.

Agradeço ainda, aos familiares e amigos, pelo apoio e compreensão da minha ausência, e a todos que de alguma forma contribuíram para que eu pudesse me dedicar para realização dessa pesquisa, em especial à minha avó Maria de Fátima.

Por fim, agradeço ao meu orientador, Professor Leonardo de Gênova, não apenas pela orientação neste trabalho, mas, principalmente, pelos inúmeros ensinamentos ao longo da minha trajetória acadêmica.

Se continuarmos desenvolvendo nossa tecnologia sem sabedoria ou prudência, nosso servo pode acabar se tornando nosso carrasco.

Omar Bradley
(1893-1981)

RESUMO

O objetivo do presente trabalho é apresentar uma análise acerca da utilização de dados pessoais como um produto no mercado digital, à luz da recente temática da proteção de dados pessoais e das consequências jurídicas e sociais deste novo tipo de economia informacional. Para empreender tal discussão, por meio de um estudo bibliográfico, discorremos acerca da implementação da internet (no âmbito da guerra fria); da disputa pelo desenvolvimento da tecnologia; do acesso à informação e esclarecemos o significado de dados. Explanamos, também, sobre o que a legislação atual, a Lei Geral de Proteção de Dados (LGPD), dispõe sobre o tema. Finalmente, baseado em estudos sobre a questão da utilização de dados pessoais, da LGPD e da Constituição Federal de 1988, tecemos uma discussão acerca da proteção de dados pessoais na era da informação, quando a internet medeia relações de acesso a produtos e serviços. Concluímos que, em virtude da recente vigência da LGPD, os desafios de se legislar no mundo digital, espaço movido a dados, é criar barreias legais e efetivas onde a privacidade não seja invadida mesmo que as empresas tenham o efetivo consentimento do titular.

Palavras-chave: Privacidade, Segurança de Dados, Dados pessoais.

ABSTRACT

The objective of this work is to analyse the usage of personal data as a market product, having the recent thematic of personal data protection and the legal and social consequences of this new type of market. To continue this discussion, we developed a study based on written articles with these subjects: the implementation of internet during the Cold War; the dispute for technology development; the information access so, at the end, we could clarify the meaning of data. We also explain the content of the current General Protection of Data Law (LGPD in portuguese). Finally, based in studies about the usage of personal data, the LGPD and the Constitution of Brazil, we had a discussion about the protection of personal data in this technology era, when internet is the key to access almos all products and services. We also concluded that due to the recent LGPD, the big challenge of creating laws is to create legal and effective barriers where our privacy is not invaded, even if the companies who want to collect data have the agreement from the person who is using their services.

Keywords: Privacy, Data Security, Personal Data.

LISTA DE ABREVIATURAS E SIGLAS

ADIs	Ação Direta de Inconstitucionalidade
ANPD	Autoridade Nacional de Proteção de Dados
ARPANET	Advanced Research Projects Agency Network
CA	Cambrigde Analytica
CERN	Conselho Europeu de Pesquisas Nucleares
CC	Código Civil
CDC	Código de Proteção do Consumidor
CF/88	Constituição Federal de 1988
CPF	Cadastro de Pessoas Físicas
DARPA	Defense Advanced Research Project Agency
EUA	Estados Unidos da América
GDPR	General Data Protection Regulation
HTML	Hyper Text Markup Language
HTTP	Hyper Text Transfer Protocol
IBGE	Instituto Brasileiro de Geografia e Estatística
IDC	Internacional Data Corporation
IMPS	Interface de Processamento de Mensagens
INT	Infra News Telecom
IP	Internet Protocol
LGPD	Lei Geral de Proteção de Dados
MIT	Instituto de Tecnologia de Massachestts
MP	Medida Provisória
MILNET	Military Network
NCP	Network Control Protocol
OAB	Ordem dos Advogados do Brasil
ONU	Organização das Nações Unidas
OSI	Open System Interconnection
PEC	Proposta de Emenda à Constituição
RG	Registo Geral
SERPRO	Serviço Federal do Processamento de Dados
SMP	Serviço Móvel Pessoal
STF	Supremo Tribunal Federal

STFC	Sistema de Telefonia Fixa Comutada
TCP/IP	Transmission Control Protocol/ Internet Protocol
UCLA	Universidade da California - Los Angeles
URL	Uniform Resource Locator
WWW	Word Wide Web

SUMÁRIO

INTRODUÇÃO

Na atual sociedade da informação, o mundo tornou-se cada vez mais digital, fazendo com que ocorra a produção exponencial do novo ativo comercial: os dados pessoais. Por conta disso, o mundo jurídico se deparou com situações antes inimagináveis no que se refere ao uso de dados pessoais fazendo-se necessário adequar-se às novas técnicas de análise de dados para que os direitos humanos e fundamentais não sejam ainda mais afetados pelas novas tecnologias.

Em resumida comparação, a proteção de dados pessoais é, em suma, a proteção da pessoa humana, uma vez que seus dados são uma extensão de sua personalidade. Por conta disso, o direito de autodeterminação informativa é cada vez mais defendido e estimulado nas legislações, pois é através desse instituto que o titular dos dados pessoais decide por quem, onde, porque e até quando seus dados serão remetidos a algum tipo de análise.

A Lei Geral de Proteção de Dados (LGPD) é a regulamentação brasileira sobre, como o nome diz, proteção de dados, todavia, ela não é a única que traz reflexões e regulamentações sobre o tema e pode-se encontrar referências do assunto em leis esparsas como Código de Defesa do Consumidor (CDC), no Marco Civil da Internet, na Lei de Acesso à Informação, no Código Civil, entre muitas outras. Devido a tantas matérias regularem apenas um, ou outro aspecto da proteção de dados é que se fez necessário fazer uma lei referência e prioritária no assunto, a supracitada LGPD.

Tendo em vista essa problemática, desenvolvemos o presente trabalho, cujo objetivo é analisar como pode ser prejudicial ou benéfico o armazenamento de dados pessoais em banco de dados, que são em sua enorme maioria contidos em meio digital. Como forma de organização, o dividimos em três partes, na primeira procedemos a uma contextualização histórica e conceitual de termos utilizados ao longo da pesquisa, pelo surgimento da internet e como se configuram os dados. Na segunda, tratamos de atributos relevantes da LGPD e, por fim, na terceira, apresentamos duas questões pertinentes à proteção de dados gerados através da comparação de direitos já positivados na Constituição Federal de 1988, bem como analisamos alguns

acontecimentos contemporâneos nos quais a utilização de dados pessoais, passaram pelo crivo do Superior Tribunal Federal.

Pautamo-nos na certeza de que o mundo do direito digital é multidisciplinar e assim, abrange áreas tecnológicas como programação, *data science*, internet das coisas e que não cabe aprofundamento na proposta jurídica atual. Sendo assim, ressaltamos que a discussão sobre o tema “utilização de dados pessoais na era da informação,” na presente monografia, tem aspecto introdutório de subtemas selecionados, mas não por isso menos relevantes.

1 HISTÓRIA DOS DADOS

1.1 ORIGEM DA INTERNET

Tendo em vista a importância dos dados na atualidade e a relevância da internet nos processos de divulgação e armazenamento de informações pessoais contidas em banco de dados privados e públicos, faz-se necessário compreender mais profundamente o acontecimento histórico da internet como propulsor e revolucionário nos processos da comunicação. O nascimento da Rede Mundial de Computadores, popularmente conhecido como “Internet” deu-se em um momento de conflito mundial, mais especificamente durante a Guerra Fria (1947-1991).

De acordo com Descomplica (2018), com o fim da Segunda Guerra Mundial, em 1945, os aliados, Estados Unidos (EUA) e União Soviética (URSS), saíram fortalecidos da batalha passando a disputar o título de “potência mundial”. Diante desse quadro, cada um pregava incansavelmente suas ideologias econômicas: Capitalismo x Socialismo. A partir disso, criou-se uma duplicidade ideológica no mundo, já que para conseguir aliados e serem protegidos, os demais países que antes eram apenas espectadores desse possível conflito, se veem obrigados a escolher um dos polos, dando início então, ao que se denominou Guerra Fria, em 1947.

Diferentemente das outras guerras, a Guerra Fria não foi marcada por batalhas sangrentas, mas por uma corrida intelectual, tecnológica, espacial, bélica e, sobretudo, ideológica.

Antes disso, o primeiro acontecimento que desencadearia futuramente, a criação da Internet ocorreu ainda durante a Segunda Guerra Mundial quando, em 1945, os EUA lançaram duas bombas nucleares em Hiroshima e Nagasaki no Japão. Esses lançamentos durante o fim da guerra serviram para demonstrar o poderio bélico que os EUA haviam ‘dominado’ uma vez que a guerra já estava praticamente ganha e não havia a necessidade de tal ação. Então, com a Guerra Fria já instaurada, a URSS começou a também dominar as pesquisas de tecnologias nucleares e em 1949 iniciou a produção de suas próprias bombas nucleares.

Segundo Wikipédia (2021), após anos de pesquisas e de uma enorme corrida armamentista, havia também um impasse quanto a quais das potências dominaria o

Espaço Sideral primeiro, a tão famosa Corrida Espacial; quem deu o primeiro passo nesse quesito foi a URSS com o projeto Sputnik I, em 04 de outubro de 1957, com o lançamento do primeiro satélite artificial ao espaço, o qual permaneceu em órbita durante todo o tempo programado. Graças ao sucesso do primeiro projeto, foi lançado em 03 de novembro, do mesmo ano, o Foguete Sputnik II, este bastante conhecido por carregar o primeiro ser vivo para o espaço, a cadela Laika, que não sobreviveu à viagem. Ainda, em 12 de abril de 1961, foi lançado a primeira espaçonave tripulada por um ser humano. O piloto da Força Aérea Soviética, Yuri Gagarin, foi o primeiro ser humano a estar no espaço e completar uma volta ao redor do planeta Terra. Os anos seguintes foram marcados por idas e vindas do espaço, demonstrando como a URSS estava à frente dessa corrida. Após essas diversas investidas da URSS, os EUA se apressaram para também demonstrar seus avanços tecnológicos espaciais e após várias tentativas de superar a URSS em inovação, criaram o projeto Apollo 11 que foi responsável por realizar o primeiro pouso na Lua em 20 de julho de 1969, foi o ápice da corrida espacial (WIKIPÉDIA, 2021).

Com o sucesso da URSS na corrida espacial, o presidente dos EUA, na época Eisenhower, criou, em 1958, a Advanced Research Projects Agency (ARPA). De acordo com Techmundo (2018), essa agência contava com diversos acadêmicos, industriais e cientistas para desenvolverem tecnologias em diversos setores. Em 1962, foi recrutado para compor o setor de informática da ARPA o cientista da computação J.C.R Licklider, após teorizar no mundo acadêmico do Instituto de Tecnologia de Massachusetts (MIT), sobre uma “rede galáctica de comunicação” que pudesse ser acessada de qualquer lugar do planeta. Na mesma época do recrutamento do J.C.R Licklider, estava sendo desenvolvido por Paul Baran um novo sistema de comunicação por “pacotes”, um novo método de troca de informações entre máquinas que era mais eficientes que os métodos da época e, ainda, suportava vários destinos diferentes. Esse sistema de comunicação foi simultaneamente estudado por grandes cientistas da informática como Paul Baran do Rand Institutev; Donald Davies e Roger Scantlebury do National Physical Laboratory e Lawrence Roberts da ARPA. Com o avanço da comunicação por pacotes e não mais por circuitos, foi teorizado e desenvolvido o sistema de “nós”, que são pontos de intersecção das informações entre máquinas que se comunicam entre si. Essa tecnologia permitia que o conteúdo dos pacotes transmitidos através da rede não se perdesse no trajeto. Os nós eram conectados via cabos e os primeiros testes foram realizados em bases militares. O próximo desafio foi desenvolver os IMPs (Interface de Processamento de Mensagens),

que eram as máquinas que funcionavam como os nós intermediários que conectavam os pontos de redes.

Ainda de acordo com Techmundo (2018), esses conhecimentos começaram a ser colocados em prática em 1966, quando foi criado um departamento dentro da ARPA chamado de Advanced Research Projects Agency Network (ARPANET) cujo foco era criar a rede idealizada anteriormente por J.C.R Licklider, uma vez que a Guerra Fria estava no auge e havia o temor constante de uma guerra nuclear, intensificado pelo sucesso do projeto Sputnik. Diante disso, essa rede permitiria um sistema de comunicações que seria interrupto, mesmo com um ataque nuclear localizado em alguma das bases dos EUA, todos os dados, comunicações e informações sigilosas ainda assim, fluiriam pelos locais não afetados.

Em meio a esse desenvolvimento, a primeira conexão de internet ocorreu em 29 de outubro de 1969 entre a Universidade da Califórnia em Los Angeles (UCLA) e o Stanford Reserch Institute. A primeira palavra transmitida foi ‘login’ mas, após a identificação das duas primeiras letras, a conexão foi interrompida. Após esse teste, foi aprimorado o sistema de comunicação por nós e no final do ano de 1969 as conexões já funcionavam de maneira correta, com 04 pontos interligados e em comunicação. Nessa época, foi desenvolvido o NCP (*Network Control Protocol*), uma forma padrão de procedimento para conexões entre dois pontos. A partir disso, era possível que fossem enviados arquivos e mensagens maiores e, então, em 1971 haviam 15 pontos de rede interligados nos EUA e, em 1972 foi criado o e-mail e neste período, já haviam 29 pontos de conexões. Nesse mesmo ano, ocorreu o primeiro link Transatlântico via satélite entre a ARPANET e um sistema norueguês chamado de NORSAR.

A partir desses testes, começou a ser elaborada uma rede de arquitetura aberta, chamada de modelo OSI (Open System Interconnection). Tal rede possibilitava a elaboração de equipamentos de diferentes fabricantes que, apesar disso, utilizavam um mesmo protocolo, permitindo a interligação dos pontos de redes ao redor do mundo. Esse processo de interligar redes/nets é chamado de Internetting. Todavia, nesse estágio, o protocolo NCP (*Network Control Protocol*), não era suficiente para que houvesse a frequente troca aberta de pacotes de informações entre diferentes redes e então, começou o desenvolvimento de um novo sistema substituto, elaborado por Vint Cerf e Robert Kahn. Em paralelo a essa pesquisa, o cientista da computação Bob Metcalfe investia fortemente no desenvolvimento do sistema Ethernet, estudo ambientado no Xerox

PARC, no ano de 1973, que é atualmente, uma das camadas de ligação de dados por cabos e sinais elétricos. (TECHMUNDO, 2018).

Ainda naquela época, no ano de 1975 uma empresa de defesa dos EUA assumiu os projetos da ARPA e ela passou a ser chamada de DARPA (Defense Advanced Research Projects Agency), neste mesmo ano Vint Cerf e Robert Kahn iniciaram os testes do novo sistema de comunicação de aparelhos, chamado de TCP/IP (Transmission Control Protocol / Internet Protocol) que é, ainda hoje, um dos sistemas de comunicações mais usados (SANTOS, 2019). Todavia, essa padronização de protocolo ocorre somente em 1983 e no ano seguinte, ocorreu a separação da rede em duas: a MILNET, parte usada apenas para trocas de informações militares e a ARPANET que a partir de então seria segmentada para a parte civil e cientifica. (TECHMUNDO, 2018).

No fim da década de 80 começou a se consolidar o nome Internet pois a estrutura de nets começou a ganhar forma, saindo da concentração pelas universidades e começando a ser adotada pelo mundo corporativo e somente por último, essa tecnologia foi oportunizada ao público consumidor. Vale ressaltar que, apesar dos EUA ter sido o pioneiro no estudo da Rede Mundial de Computadores, durante todo esse período o resto do mundo também estudava e agregava no estudo das conexões por rede e, nesta época, passaram também a adotar o protocolo TCP/IP. (TECHMUNDO, 2018).

Conforme expressado anteriormente, com a consolidação da estrutura Internet, no fim da década de 80, ela passou a ser liberada para uso comercial no EUA. Esse fato ocasiona o surgimento de vários servidores de rede no setor privado e novos pontos de acessos fora das universidades e bases militares.

Em 1989, o cientista Timothy Berners-Lee, que atuava no Conselho Europeu de Pesquisas Nucleares (CERN), iniciou sua pesquisa para obtenção de informações de todos os equipamentos conectados facilitando a troca de arquivos. A partir disso, ele começou a aprimorar o Hipertexto, que são palavras ou imagens que levam o usuário até outro ponto sempre que solicitado. São criados, então, em 1990, a URLs, que permitia a identificação da fonte das páginas acessadas a parir de um endereço único: o HTTP que é a forma básica de comunicação de texto e o HTML que é a formatação escolhida para agregar todas as informações e conteúdo das redes. Assim, iniciou a Word Wide Web (Rede Mundial de Computadores), ou popularmente conhecida como “www”. Neste mesmo ano, a ARPANET foi oficialmente encerrada. Em 1994 Timothy deixou seu emprego no CERN para se dedicar ao seu novo projeto a “Word Wire Web Foundation”

que ajudou a desenvolver e a espalhar os protocolos da internet aberta para todo o mundo (TECHMUNDO, 2018).

A partir da contribuição de Timothy, a internet se difundiu ainda mais e com conceitos abstratos que perduram até hoje. Entre esses conceitos estão um espaço Descentralização da Rede que elimina a necessidade de permissão para que os usuários a utilizem e troquem informações, bem como a Neutralidade das Redes que permite que os usuários paguem por um determinado serviço sem discriminação de qualidade, ou seja, todas as informações navegam à mesma velocidade, garantindo, assim, o livre acesso. (TECHMUNDO, 2018).

Toda essa recente descoberta do mundo cientifico impacta, ainda nos dias atuais, toda a humanidade e está em constante mudança. Neste contexto, pode-se observar que a intenção sempre foi a troca ilimitada de informações.

1.2 O QUE SÃO DADOS

Uma vez exposta, suscintamente, a história da Internet, pela natureza do objetivo dessa pesquisa que é analisar como pode ser prejudicial ou benéfico o armazenamento de dados pessoais em banco de dados, que são em sua enorme maioria contidos em meio digital, é pertinente explicitar a forma de como é extraído um dado que percorre essa rede. Em resumo, o sistema de “pacotes” de informações criado por Paul Baran é utilizado até hoje, apesar de ter sido modificado para acompanhar a modernidade dos tempos atuais, o princípio é o mesmo: um conjunto de informações viaja de um ponto a outro até chegar ao seu destino final, este conjunto de informações é o que chamamos de pacote, esses, carregam dois tipos de informações: dados de controle e dados de usuários (WIKIPÉDIA, 2021)

Considera-se “dado” como um registro isolado e bruto, logo, uma informação é um conjunto de dados contextualizado. A contextualização é importante pois, apenas com os dados não é possível entender o propósito de sua existência (TERRA, 2019). Exemplificando, apenas as palavras “Índia”, “Estados Unidos”, “Brasil”, “Indonésia” e “México” não remetem a uma informação de fato, mas simplesmente a nomes de países aleatórios. Todavia, se esses cinco países estiverem acompanhados da informação

“Ranking dos países com mais usuários ativos no Facebook em 2019” fica evidente que estes nomes não foram escolhidos de forma aleatória. Ainda, explica Doneda (2020. Livro Kindle). “O dado, assim, estaria associado a uma espécie de “pré-informação”, anterior à interpretação e a um processo de elaboração”.

É desta maneira contextualizada que inúmeras empresas trabalham atualmente com a otimização de dados; esses, por sua vez, são considerados o produto mais importante nos tempos atuais, já que é um produto encontrado em abundância e infinitamente, chegando até ser considerado o “novo petróleo”, de acordo com o matemático especializado em dados, Clive Humby. (LEADDATA, 2020)

Diante disso, passando para o contexto jurídico, pode-se dizer que a contextualização ocorre com o Tratamento de Dados. Esse instrumento é conceituado no art. 5º, inciso X, da Lei Nº 13.709/2018 (Lei Geral de Proteção de Dados ou LGPD):

“X- Tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, receptação, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração”.

Sendo assim, o tratamento de algum dado irá acontecer sempre que, de alguma forma, um usuário disponibilizar para uma empresa qualquer informação. No dia-a-dia isso ocorre inúmeras vezes, por exemplo: ao fazer *login* em alguma plataforma social, ao fazer uma compra em um site ou, ainda, ao realizar um cadastro *on-line* ou *off-line*.

Este tratamento (ou também chamado de processamento) de dados não implica dizer que as empresas poderão fazer o que bem quiserem com os dados de seus clientes, muito pelo contrário, a LGPD traz rígidas formalidades a serem seguidas pelas empresas que realizam, de alguma forma, a coleta e processamento de informações. Entre as regras há a necessidade de expor a finalidade exata para qual o dado será utilizado, o consentimento para o uso, além de limitações para o armazenamento dos mesmos. Desta maneira, o indivíduo possui certo controle das informações coletadas, podendo, até mesmo, solicitar a exclusão de todas elas se assim desejar.

1.3 O QUE SÃO DADOS ANÔNIMOS

De acordo com a Lei Nº 13.709/2018 (Lei Geral de Proteção de Dados), em seu artigo 5º, inciso III, considera-se: “III- Dado anonimizado: dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento”. Desta forma, entende-se como dado anônimo aquele que, quando processado, não traz nenhuma identificação a respeito de quem o forneceu, é o que ocorre com os dados estatísticos, por exemplo, mesmo estudando um grupo de pessoas, não é possível obter a titularidade dos mesmos.

Este tipo de dado não é protegido pela LGPD, uma vez que a Lei visa a máxima proteção e controle das informações do cidadão bem como a sua privacidade, já que esses dados afetam diretamente sua vida em sociedade. Sendo assim, se um dado não traz titularidade alguma, não há objetividade jurídica na sua proteção pela LGPD.

1.4 O QUE SÃO DADOS PESSOAIS

Com relação à modalidade Dados Pessoais, especifica a LGPD, em seu art. 5º, inciso I: “Dado pessoal: informação relacionada a pessoa natural identificada ou identificável”. Senso assim, dado pessoal é todo aquele que traz uma identificação a seu titular, seja a identificação de forma direta, por exemplo: nome completo, endereço, endereço eletrônico (*e-mail)*, CPF, RG, número de telefone celular etc.; mas também de forma indireta a partir de informações interligadas como dados de localização e identificadores de rede, como o IP (*Internet Protocol*). (TEPEDINO et al., 2019).

Importante salientar que qualquer informação sobre algum indivíduo é passível de proteção pela LGPD, independe de onde esteja inserido como explica Vitor Paludetto e Henrique Shirassu:

> O conceito de dados pessoais não se limita a informações que possam ser consideradas prejudiciais à vida privada e familiar do indivíduo. Nem o meio em que a informação está contida é relevante: o conceito de dados pessoais inclui informações disponíveis sob qualquer forma; texto, figuras, gráficos, fotográfica, vídeo, áudio ou qualquer outro meio possível. (PALUETTO; BARBIERI, 2019, Livro Kindle)

Regula também a LGPD sobre a sensibilidade dos dados pessoais em seu art. 5º, inciso II:

> 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.

Este tipo de regulamentação, ora emprestada da legislação europeia de 2016 (a General Data Protection Regulation (GDPR)), se atenta às possibilidades do indivíduo, ao ter seus dados processados, poder, de alguma maneira, sofrer discriminações ou ter sua dignidade atingida em razões do conteúdo das informações que muitas vezes são utilizadas em contextos discriminatórios. (TEPEDINO et al., 2019).

Por isso, o legislador dispõe um rol taxativo para as hipóteses em que podem ocorrer o tratamento de tais informações em seu art. 11 da LGPD, são elas:

> Art. 11. 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 terceiros;
> 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.

Importante ressaltar que o legislador ainda garante no §1º do art. 11 da LGPD a dignidade do titular dos dados ao definir que essas mesmas hipóteses são aplicadas quando um dado pessoal, ao ser tratado, se revele como dado pessoal sensível e que possa causar danos ao titular (TEPEDINO et al., 2019), já que nem todo dado pessoal é um dado pessoal sensível.

1.5 DOS CONCEITOS APRESENTADOS NA LEI GERAL DE PROTEÇÃO DE DADOS

Além dos conceitos acima, por se tratar de tema recente e multidisciplinar, o legislador foi didático e trouxe no artigo 5º da lei um rol de conceitos que auxilia no entendimento de termos que mesclam direito e áreas da tecnologia e que ainda serão abordados no decorrer deste trabalho, são eles:

> Art. 5º Para os fins desta Lei, considera-se:
> I - Dado pessoal: informação relacionada a pessoa natural identificada ou identificável;
> 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;
> III - Dado anonimizado: dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento;
> IV - Banco de dados: conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico;
> V - Titular: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento;
> VI - Controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;
> VII - Operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador;
> VIII - Encarregado: pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD);
> IX - Agentes de tratamento: o controlador e o operador;
> X - Tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração;
> 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;
> XII - Consentimento: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada;
> XIII - Bloqueio: suspensão temporária de qualquer operação de tratamento, mediante guarda do dado pessoal ou do banco de dados;
> XIV - Eliminação: exclusão de dado ou de conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado;
> XV - Transferência internacional de dados: transferência de dados pessoais para país estrangeiro ou organismo internacional do qual o país seja membro;
> XVI - Uso compartilhado de dados: comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicos no cumprimento de suas competências legais, ou entre esses e entes privados, reciprocamente, com

autorização específica, para uma ou mais modalidades de tratamento permitidas por esses entes públicos, ou entre entes privados;

XVII - Relatório de impacto à proteção de dados pessoais: documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco;

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

XIX - Autoridade nacional: órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento desta Lei em todo o território nacional.

2 LEI GERAL DE PROTEÇÃO DE DADOS NO BRASIL

Com um olhar minucioso à história dos dados, pode-se perceber como é fácil o tratamento de dados pessoais sensíveis ou não sensíveis, por isso fizeram-se necessários diversos elementos jurídicos para a regulamentação desse tratamento, deixando o procedimento mais formal e distanciando a má-fé de empresas ou entes públicos em questões discriminatórias.

A Lei Geral de Proteção de Dados nasce, em suma, da necessidade de regulamentar a privacidade do cidadão no que tange à distribuição dos seus dados através dos inúmeros bancos de dados no universo digital e também no mundo físico. Essa necessidade já havia sido reparada de forma bem sutil em outras normas legais como por exemplo na Lei de Arquivos Públicos (Lei 8.159/1991); na Lei do *Habeas Data* (Lei 9.507/1997); na Lei de Acesso à Informação (Lei 12.527/2011); no Marco Civil da Internet (Lei 12.965/2014) e, ainda, no Código do Consumidor (Lei 8.078/1990). (TEPEDINO et al., 2019, p. 64-67).

Como observado, são diversos dispositivos e leis esparsas que regulamentam uma ou outra questão relativa ao uso de dados, entretanto, nenhuma delas de fato regulamentou o procedimento para o uso dos dados pessoais em sua totalidade e, por isso, foi fundamental a edição da Lei Geral de Proteção de Dados no ano de 2018 como um norte para orientar entes privados e públicos.

2.1 PRINCÍPIOS REGULADORES DA PROTEÇÃO DE DADOS

Como explica Patrícia Peck Pinheiro (2020), a LGPD é uma legislação principiológica, ou seja, traz um rol de princípios que precisam ser atendidos e, dessa maneira, sempre que ocorre a proteção de dados é, na prática, a efetivação de um princípio e por essa razão eles servem como item de controle de conformidade com a lei, a autora ainda explica que

> Essa metodologia foi uma forma mais objetiva encontrada pelo regulador de se tratar uma regra que, apesar de se referir a direitos fundamentais, como a proteção da privacidade, necessita de uma aplicação procedimental dentro dos modelos de negócios das estruturas empresariais. (PINHEIRO, 2020, p. 41).

Nessa lógica, a LGPD se inspirou em princípios que já estavam consolidados em outras legislações sobre o mesmo tema ao redor do mundo, como por exemplo a Convenção de Estrasburgo (1981) e a já citada legislação europeia, a GDPR (2016), (TEPEDINO et al., 2019, p. 71-72). Portanto, estabeleceu-se no artigo 6º da LGPD onze princípios que, salvo exceções, devem ser observados em todas as situações envolvendo o tratamento de dados:

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

A seguir, será abordado, resumidamente, alguns pontos relativos a cada um dos onze princípios citados acima.

2.1.1 Princípio da Boa-fé

O princípio da Boa-fé, conforme explica Lima (2020), é o princípio norteador da LGPD, uma vez que, inserido no *caput* do artigo 6º, traz, em seguida, os outros princípios em concordância com o mesmo.

Lima (2020) ainda elucida que esse princípio possui duas acepções jurídicas. A primeira, de maneira subjetiva, se contrapõe a má-fé, ou seja, nele se observa a intenção do agente, que desconhece qualquer lesividade sobre o assunto. Outro alcance para esse princípio está no sentido objetivo que compreende a lealdade com que as partes agem uma com a outra (ALMEIDA, 2010).

O referido *caput* deve ser interpretado à luz do caráter objetivo da boa-fé visto que implica em uma regra de conduta para todos os agentes.

2.1.2 Princípio da Finalidade

Exposto no inciso I do art. 6º da LGPD estabelece que “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.”

Percebe-se que existe uma exigência para o tratamento dos dados: o titular deve ser informado do motivo exato pelo qual suas informações estão sendo colhidas. “Desta maneira, esse princípio afasta qualquer pretensão que o controlador faça o tratamento da forma que quiser e o força a respeitar a “correlação entre o tratamento de dados e a finalidade informada.” (TEPEDINO et al., 2019, p. 73).

Sobre esse tema, exemplifica Lima (2020, p.128) “uma startup que solicita o e-mail do cliente para a finalidade específica de login na plataforma. Neste caso, não poderá automaticamente utilizar esse mesmo e-mail para envio de ofertas ou publicidade.” Neste caso hipotético o titular dos dados não foi informado que seu e-mail poderia constar em listas de marketing eletrônico; logo, está afastada essa possibilidade devido ao Princípio da Finalidade.

2.1.3 Princípio da Adequação

O inciso II do artigo 6º da LGPD prevê: “II - adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento”. Neste contexto, o legislador buscou estabelecer uma limitação direta entre o serviço prestado pelo coletor do dado e o motivo da coleta (LIMA, 2020), ainda explica

Lima (2020), “este princípio está intimamente ligado ao princípio da finalidade, mas em um contexto mais objetivo”, o autor por fim exemplifica: “imagine que um aplicativo de transporte queira que os usuários forneçam dados sobre sua saúde. Neste caso, o tratamento se torna inadequado e, portanto, inviável, pois não há uma justificativa plausível para que tal fato ocorra.” (LIMA, 2020, p.130)

Deste modo, o legislador cria um sistema de compatibilidade para o tratamento de dados e sua coleta vedando qualquer tipo de incoerência.

2.1.4 Princípio da Necessidade

O princípio da necessidade encontra-se no artigo 6º, inciso III da LGPD: “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;”.

Entende-se pelo texto legal que este princípio também traz um contexto limitador para o agente coletor, isso ocorre pois somente pode ser coletado o que for imprescindível para o negócio, não devendo ter excessos no tratamento. (LIMA, 2020).

Nessa condição, existe uma oportunidade para grandes empresas reduzirem despesas referentes ao armazenamento e segurança dos mesmos nos bancos de dados uma vez que apenas os dados que tenham real utilidade para o negócio sejam guardados de maneira segura, esclarece Saldanha (2019).

2.1.5 Princípio do Livre Acesso

O princípio do Livre Acesso encontra-se estampado no inciso IV, do artigo 6º da LGPD e estabelece: “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;”.

Além deste inciso, a Lei ainda aprofunda o tema em seu artigo 9º elencando hipóteses em que o titular tem pode solicitar o acesso, são elas:

> 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.

Este princípio estabelece um direito ao titular do dado, uma vez que “quem realiza tratamento de dados pessoais deverá informar, caso o titular requeira, quais são as informações coletadas, o que o provedor faz com estas informações, a forma como é realizado o tratamento, o período entre outras informações.” (LIMA, 2020, p.131).

2.1.6 Princípio da Qualidade dos Dados

Exposto no inciso V do art. 6º da LGPD, o Princícipio da Qualidade dos Dados estabelece que:

> 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;

A qualidade do dado diz respeito a veracidade e atualidade dos dados expostos a tratamento, como explica Lima (2020, p. 131) este princípio “impõe ao controlador um dever de verificação de correção em todos os procedimentos e operações”. A lei ainda resguarda ao titular o direito de ter a correção imediata das suas informações sempre que requerido, conforme explica o artigo 18, §§3º e 4º da LGPD.

2.1.7 Princípio da Transparência

O inciso VI do artigo 6º da LGPD prevê:

> 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;

Como elucida Lima (2020) este princípio veda que as informações do titular sejam compartilhadas, sem o devido consentimento, com terceiros ocultos, ou seja, garante o conhecimento ao titular do fluxo de seus dados.

Ainda neste contexto, é essencial que o titular saiba de tudo o que acontece com suas informações, como por exemplo: quem o controla, quem realiza o tratamento, se há terceiros envolvidos no tratamento, como é finalizado o tratamento etc. Por isso, o legislador foi incisivo em determinar que as informações sejam acessíveis, no sentido de que não tragam uma linguagem extremamente técnica a respeito do tratamento e que seja de fácil entendimento do titular, além de facilitar a fiscalização pelos órgãos de controle. (LIMA, 2020).

2.1.8 Princípio da Segurança

O princípio da segurança está previsto no inciso VII, do artigo 6º, da LGPD que explica: “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;”

Este princípio estabelece, de acordo com Lima (2020), que o tratamento dos dados pessoais deve ser feito de maneira que garanta a segurança e sigilo. Em outras palavras, significa que todos os dados que estiverem no banco de dados do controlador devem ser mantidos em total sigilo, sendo obrigação do mesmo prover um ambiente seguro e criptografado que mesmo em situações de invasão não autorizada, como exemplo, em um ataque de hackers, o titular das informações não sofra nenhum tipo de prejuízo.

2.1.9 Princípio da prevenção

Previsto no inciso VIII do artigo 6º, da LGPD, o princípio da prevenção estabelece: “VIII – prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;”

Neste inciso, o legislador se atentou em garantir o ambiente seguro tratado no tópico acima utilizando a prática da prevenção, isto significa que “as empresas devem atuar antes de eventuais danos, e não somente após a ocorrência destes”, explica Lima (2020, p.135).

Ainda nessa perspectiva, é obrigação de quem realiza o tratamento de dados a capacitação dos seus colaboradores, a conscientização de que eventuais vazamentos ou acessos não permitidos aos dados podem trazer prejuízos ao seu titular e, também, a logística de procedimentos que impeçam a violação das informações.

2.1.10 Princípio da Não Discriminação

Exposto no artigo 6º, inciso IX, da LGPD, este princípio determina: “IX – Não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;”.

Como já citado anteriormente, os dados pessoais sensíveis, de acordo com o Serviço Federal de Processamento de Dados (SERPRO), “são os que revelam origem racial ou étnica, convicções religiosas ou filosóficas, opiniões políticas, filiação sindical, questões genéticas, biométricas e sobre a saúde ou a vida sexual de uma pessoa.” (SERPRO, 2020). Por conta disso, a lei decreta que é inadmissível, o tratamento de dados de modo que cause qualquer tipo de dano contra a dignidade da pessoa humana, liberdade e igualdade material, como exemplifica Lima (2020, p.136):

> Outro exemplo plausível de violação ao princípio da não discriminação é o de um determinado usuário que utiliza um aplicativo para controlar suas performances em exercícios físicos. Este aplicativo pode armazenar dados como batimentos cardíacos, doenças vasculares, se o indivíduo possui um hábito sedentário etc. Não será possível que este aplicativo forneça tais dados para empresas de seguros informando o hábito e questões pessoais do usuário para que elas calculem os riscos e aumentem, por exemplo, o valor do seguro de vida desta pessoa, pois estaria violando o princípio da não discriminação do usuário.
> (LIMA, 2020, p.136)

2.1.11 Princípio da Responsabilização e Prestação de Contas

Este princípio está consagrado no artigo 6º, inciso X da LGPD, e prevê:

> 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.

Uma vez que o inciso impõe um dever ao controlador, este princípio está diretamente relacionado com o artigo 37 e 38 da mesma lei que estabelece que o controlador deve manter registro das operações de tratamentos de dados pessoais e, ainda, que a autoridade nacional competente poderá determinar que o controlador elabore relatórios referentes a esses tratamentos.

> O relatório deverá conter, no mínimo, a descrição dos tipos de dados coletados, a metodologia utilizada para a coleta e para a garantia da segurança das informações e a análise do controlador com relação a medidas, salvaguardas e mecanismos de mitigação de risco adotados.

Desta forma, os relatórios são meio de comprovação de que o controlador possui boa-fé na adoção de medidas eficazes para o tratamento seguro de dados pessoais “sob pena de responsabilização caso haja algum dano decorrente da sua atuação”, explica Lima (2020, p.138).

2.2 ASPECTOS GERAIS DA LEI GERAL DE PROTEÇÃO DE DADOS

Seguindo a tendência mundial dos últimos anos o Brasil tratou de regular o tratamento de dados pessoais promulgando a Lei nº 13.709/18 em 14 de agosto de 2018 que teve vigência ampla em 1º de agosto de 2021.

Estabeleceu o legislador no capítulo 1º, *caput* da LGPD, que o objetivo da lei é proteger os direitos fundamentais de liberdade e de privacidade, além do livre desenvolvimento da personalidade da pessoa natural.

Como já citado anteriormente, os dados são hoje o produto mais importante no mercado. Isso ocorre pois eles são uma fonte infinita de mercadoria, a todo momento os usuários estão disponibilizando informações com sites e aplicativos para terem o direito a permanecer conectados a uma determinada rede.

Por conta disso a regulamentação do tratamento de dados é de extrema importância uma vez que:

> Além da privacidade, há outros desdobramentos da personalidade que são colocados em risco pela economia movida a dados, como a própria individualidade e autonomia. Mais do que isso, não é exagero afirmar que a própria democracia também passa a estar sob ameaça. (FRAZÃO, 2019, p. 100)

Ainda para Ana Frazão (2019, p. 100), o objetivo central da LGPD é "resgatar a dignidade dos titulares de dados e seus direitos básicos relacionados à autodeterminação informativa"[1].

2.2.1 Da Abrangência

Conforme explica o site LGPD Brasil (2021) a lei se aplica a "qualquer atividade que envolva utilização de dados pessoais, inclusive nos meios digitais, por pessoa natural ou jurídica, no território nacional ou em países onde estejam localizados os dados".

Como já explicado acima, no contexto da proteção de dados, considera-se "atividade que envolve utilização de dados pessoais" como "tratamento", desta forma, regula o art. 5º, inciso X da LGPD que

> X - Tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração;

[1] "O direito à autodeterminação informativa se constitui na faculdade que toda pessoa tem de exercer, de algum modo, controle sobre seus dados pessoais, garantindo-lhe, em determinadas circunstâncias, decidir se a informação pode ser objeto de tratamento por terceiros, bem como acessar bancos de dados para exigir correção ou cancelamento de informações".

Neste sentido, a lei abrange “não apenas aos brasileiros, mas toda e qualquer pessoa que esteja no Brasil, quando qualquer operação de tratamento de dados pessoais tenha sido realizada” (LIMA, et al., 2020, p. 84). Sendo assim, a LGPD estabelece no artigo 3º a sua competência territorial:

> Art. 3º Esta Lei aplica-se a qualquer operação de tratamento realizada por pessoa natural ou por pessoa jurídica de direito público ou privado, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados, desde que:
> I - A operação de tratamento seja realizada no território nacional;
> II - A atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional; ou
> III - os dados pessoais objeto do tratamento tenha sido coletados no território nacional.
> § 1º Consideram-se coletados no território nacional os dados pessoais cujo titular nele se encontre no momento da coleta.
> § 2º Excetua-se do disposto no inciso I deste artigo o tratamento de dados previsto no inciso IV do caput do art. 4º desta Lei.

Ainda neste contexto, explica Leonardi (2019) que o legislador se atentou em regular as transferências internacionais de dados podendo a LGPD se aplicar também aos serviços prestados no exterior desde que a informação tenta sido coletada no Brasil ou passado por uma das fases do processo de tratamento de dados em território brasileiro.

2.2.2 Das situações Legais Para o Tratamento de Dados Pessoais

A LGPD traz em seu artigo 7º um rol taxativo das situações autorizantes do tratamento de dados pessoais, são elas

> Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:
> I - Mediante o fornecimento de consentimento pelo titular;
> II - Para o cumprimento de obrigação legal ou regulatória pelo controlador;
> III - Pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei;
> IV - Para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;

> V - Quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados;
> VI - Para o exercício regular de direitos em processo judicial, administrativo ou arbitral, esse último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem);
> VII - Para a proteção da vida ou da incolumidade física do titular ou de terceiros;
> VIII - Para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária;
> IX - Quando 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; ou
> X - Para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente.

Uma das questões mais enfatizadas na proteção de dados é a questão do consentimento do titular, por conta disso, ele vem elencado no inciso I do artigo 7º. A LGPD tem como um dos objetivos principais a proteção da privacidade e o livre desenvolvimento da personalidade da pessoa natural (Art. 1º, *caput,* da LGPD). Dessa maneira, uma via de manutenção da privacidade é o direito adquirido pelo cidadão de manter o controle de suas próprias informações, para isso nasce o conceito da 'autodeterminação informativa', que "representa a faculdade de o particular controlar a obtenção, a titularidade, o tratamento e a transmissão de dados relativos a ele". (TEPEDINO et al., 2019, p. 291).

Tepedino et al., (2019), ainda explica que esse conceito nasce do auxílio do Direito com o mais vulnerável que, neste caso, é o titular da informação. Esse auxílio, conforme já expusemos, se dá nas imposições da lei de que as empresas públicas e privadas ofereçam ao cidadão, da maneira mais transparente possível, todas as informações do procedimento do tratamento com linguagem acessível para que assim o titular dos dados entenda por onde seus dados passarão e após isso aceite ou não com o uso dos mesmos.

2.2.3 Dos Agentes de Tratamento de Dados

Ao longo da leitura da LGPD encontra-se diversas vezes a palavra "controlador" no sentido de ser a pessoa que realiza o tratamento de dados pessoais; porém, a lei traz três diferentes figuras que de fato realizam o tratamento, são elas: o controlador, o operador e, ainda, o encarregado.

O artigo 5º da lei, responsável por apresentar os conceitos das figuras, indica em seus incisos VI, VII e VIII o papel que cada um desempenha no procedimento do tratamento:

> VI - Controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;
> VII - Operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador;
> VIII - Encarregado: pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD);

As seções I, II e III da LGPD trazem diversas informações acerca das funções exercidas pelos diversos agentes envolvidos, a começar pelo de que o encarregado, responsável por explicar a lei, é uma pessoa indicada pelo controlador e operador que procede à intermediação da comunicação entre empresa, Poder Público e os titulares dos dados. Explica o site LGPD Brasil (2020) que o Encarregado também precisa dominar todas as etapas do ciclo dos dados. Conforme estabelece a LGPD, é ele que garante a conformidade com a lei durante os procedimentos. Pode “ser um funcionário do próprio controlador ou este pode contratar uma empresa (pessoa jurídica) especializada em proteção de dados pessoais”, (LIMA, et al., 2020, p. 292-293).

O artigo 41, §2º da LGPD, explica as atividades que serão exercidas pelo encarregado, são elas:

> § 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.

Já no artigo 42, da LGPD, o legislador explica que a responsabilidade pelos danos causados a outrem cabe apenas ao controlador e operador, ficando excluído o encarregado. Para Lima (2020) este funcionário responde de maneira subjetiva nos moldes das regras da responsabilidade contratual, uma vez que se aplicam às leis trabalhistas.

No topo da hierarquia das figuras do tratamento de dados, existe o controlador, esse pode ser “pessoa natural ou jurídica, de direito público ou privado, a quem

competem as decisões sobre o tratamento dos dados pessoais" (art. 5º, inciso VI da LGPD). As principais obrigações do controlador são:

> a) elaborar relatório de impacto de proteção de dados pessoais quando determinado pela ANPD (art. 38 LGPD);
> b) manter registro das operações de tratamento de dados (art. 37 LGPD);
> c) dever de notificação sobre qualquer ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares dos dados pessoais (art. 48 LGPD);
> d) adotar medidas de segurança, técnicas e administrativas para a proteção de dados pessoais (art. 46 LGPD);
> e) formular regras de boas práticas e de governança (art. 50 LGPD);
> f) dever de informar (transparência) e de respeitar os demais direitos dos titulares estabelecidos no art. 17 e seguintes da LGPD; e
> g) dever de sigilo. (LIMA, et al., 2020, p. 290).

Lima (2020, p. 290) ainda explica que "a caracterização do controlador é de suma importância, pois determina o responsável pelos danos que causar a outrem em decorrência do tratamento de dados pessoais." Esclarece o legislador no artigo 42, da LGPD, que se o controlador e operador durante o exercício de suas atividades causarem danos a terceiros serão obrigados a repará-lo. Se for o caso de ter mais de um controlador, todos responderão de forma solidaria (art. 42, §3º, LGPD).

Por último, existe a figura do operador, este pode ser "pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador" (art. 5º, inciso VII da LGPD). O operador é quem "deverá realizar o tratamento segundo as informações fornecidas pelo controlador, que verificará a observância das próprias instruções e das normas sobre a matéria." (art. 39, da LGPD)

Observa-se que o legislador salienta que o operador deverá estar sempre em conformidade com a LGPD. Lima (2020, p.291), explica que isso ocorre pois "caso as instruções dadas pelo controlador sejam ilícitas, o operador não pode observá-las, sob pena de ser equiparado ao controlador para fins de responsabilidade civil decorrente do tratamento ilícito dos dados pessoais", conforme o artigo 42, §1º, inciso I, da LGPD.

2.2.4 Dos Direitos e Obrigações do Titular dos Dados Pessoais

Uma vez estabelecidas as obrigações de quem de fato realiza os procedimentos do tratamento de dados pessoais (controlador, operador e encarregado), o legislador discorre ainda sobre os direitos e obrigações dos titulares das informações que passam por este procedimento.

É possível encontrar os direitos do titular ao longo do texto da lei, na sua maioria, eles estão elencados do artigo 17 ao artigo 22 da LGPD. Esclarece Lima (2020), que os direitos elencados nesta lei são de caráter fundamental, ou seja, não podem ser alterados ou excluídos por leis infraconstitucionais. De acordo com o autor, estes direitos derivam do conceito já citado, da Autodeterminação Informacional (art. 2º, inc. II), fundamento este que consagra o direito do titular de controlar as informações a seu respeito.

O artigo 17 da lei, estabelece que “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.”. O artigo 18 por sua vez, traz um rol de situações em que o titular pode exigir do controlador, mediante requisição, informações sobre seus dados, sendo elas:

> 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.

Conforme explica Lima (2020), o inciso I, do artigo 18, trata-se de direito subjetivo do titular, uma vez que é através da confirmação da existência de tratamento que o titular pode exercer seus direitos de acordo com a LGPD. Por padrão, os sites dos agentes de tratamento devem conter um formulário de requisição, que necessita ser respondido no prazo de 15 dias ou em prazo diferente quando estabelecido pela ANPD (Autoridade Nacional de Proteção de Dados).

O inciso II, por sua vez, permite que o titular consiga uma cópia dos dados pessoais contidos na empresa de tratamento. Um direito importante, que garante a aplicação do princípio da Qualidade dos Dados no âmbito do tratamento de dados, é a possibilidade de o titular solicitar uma correção de dados pessoais quando estes forem incompletos, inexatos ou desatualizados, conforme explica o inciso III.

O conceito de ‘anonimização’, contido no inciso IV, permite que o titular tenha seus dados protegidos, solicitando aos agentes de tratamento que tornem seus dados anônimos, isto é, o dado passa por um processo que o torna impossível de ser vinculado a um indivíduo, explica o site Get Privacy (2020).

Ainda de acordo com o referido site, o inciso V permite que o titular tenha o direito de requisitar a portabilidade dos dados a outro fornecedor de serviço/produto. Para que isso ocorra, a solicitação deve seguir um procedimento especifico junto a ANPD. Todavia, não pode o titular fazer esta solicitação quando os dados estiverem anonimizados, pois estes não são objeto de proteção pela LGPD.

Quanto aos dados já consentidos para o tratamento, o legislador oferece ao titular o direito de solicitar a exclusão dos mesmos desde que estes dados não estejam enquadrados no artigo 16 da lei, que são situações onde é autorizada a sua conservação para fins de cumprimento da obrigação legal ou regulatória pelo controlador, os fins de pesquisa (quando possível de forma anonimizada) e para uso exclusivo do controlador, desde que anonimizados.

Em seguida, o inciso VII trata da possibilidade de o titular solicitar informações sobre o compartilhamento de seus dados pessoais com terceiros pelo controlador; como explica Lima (2020, p.272), o legislador optou por regular o compartilhamento de dados, por isso, “titular dos dados pessoais tem o direito de ser informado sobre o uso compartilhado de suas informações pessoais para que possa consentir ou não com tal prática pelo controlador do tratamento de dados pessoais.” Em complemento, o site Get Privacy (2020) expõe que “é direito do titular saber exatamente com quem o controlador está compartilhando seus dados. Isso inclui entidades públicas e privadas, que devem ser expressamente nomeadas, e não mencionadas apenas de forma genérica”.

O inciso VIII do mesmo artigo, remete ao Princípio da Transparência ao garantir ao titular as informações sobre o que acontece nos casos de não consentimento, explica o site INT (*Infra News Telecom):*

> Para que o consentimento seja considerado realmente livre, é necessário que a empresa dê a informação sobre a possibilidade de não fornecer consentimento. Junto a essa informação, devem ser apresentadas as consequências de não fornecer o consentimento, como possíveis prejuízos na experiência do usuário, menor customização, limitação de acesso a determinadas “áreas logadas” que necessitem desse consentimento, dentre outras.

Por fim, o inciso IX reforça um direito inicialmente exposto no artigo 8º, §5º:

> “consentimento pode ser revogado a qualquer momento mediante manifestação expressa do titular, por procedimento gratuito e facilitado, ratificados os tratamentos realizados sob amparo do consentimento anteriormente manifestado enquanto não houver requerimento de eliminação, nos termos do inciso VI do caput do art. 18 desta Lei.”

O site INT (*Infra News Telecom*), explica que a revogação deve ser feita de maneira expressa do titular e ressalta que “os tratamentos realizados anteriormente sob amparo desse consentimento retirado continuam válidos, até que haja expressa manifestação do titular pela eliminação de tais dados”.

2.2.5 Dos Incidentes de Segurança

2.2.5.1 Grandes Casos de Incidentes de Segurança

Apesar da temática dos dados e de sua proteção estarem ganhando cada vez mais espaço no cenário brasileiro e mundial, as leis ainda não conseguem garantir a efetivação no âmbito prático. O site Techtudo (2020) lista que apenas no ano de 2020, quando a LGPD já estava vigente, houve diversos vazamentos de dados dos usuários de empresas enormes como por exemplo, a Nintendo (160 mil contas), Zoom (500mil contas), Uber (57 milhões de contas), Netshoes (2 milhões de contas), Microsoft (250 milhões de contas) e a empresa Facebook, que frequentemente é alvo de processos envolvendo uso indevido dos dados dos usuários, já foram mais de 530 milhões de dados vazados, explica o site G1 (2021).

Com foco no Documentário Privacidade Hackeada, de 2019, produzido pela Netflix, relata como o Facebook permitiu que a Cambridge Analytica (CA), uma empresa de mineração, outra de análise de dados e uma de análise comportamental tivessem acesso a mais de 87 milhões de dados sensíveis dos usuários da plataforma, através de uma

falha de segurança que o Facebook, por mais de 03 anos, sabia da existência e não agiu para impedir.

O documentário causou grande revolta, pois foi exposto como foi fácil trapacear atos democráticos quando se tem poderio informacional e financeiro. De início é apresentado que a Cambidge Analytica realizou a campanha eleitoral do senador estadunidense Ted Cruz, que durou cerca de 14 meses, a empresa realizou diversas pesquisas de personalidades dentro do Facebook e todos aqueles que respondiam aos questionários permitiam que a empresa coletasse todos os seus dados e, ainda, os dados de familiares e amigos sem o devido consentimento. Após a vitória surpreendente do senador, a empresa virou o centro das atenções dos partidos políticos, ganhando, em seguida, clientes como Donald Trump para as eleições presidências dos EUA de 2016 e partidos que apoiam o Brexit[2], também em 2016, ambos vitoriosos.

Basicamente, o tratamento de dados na CA ocorria da seguinte forma: a empresa abusava da falha de segurança do Facebook através de testes que os usuários respondiam e conseguiam milhões de dados por dia sem consentimento dos titulares; em seguida a empresa criava um perfil psicométrico[3] e, a partir disso, criavam conteúdo personalizado para cada tipo de perfil. Esses conteúdos eram entregues novamente através do feed, em posts patrocinados, ao titular dos dados (conteúdo que na maioria das vezes eram classificados como *fake news sendo* benéficos para quem contratava a empresa para fazer a sua campanha eleitoral). A CA chegou a gastar 1 milhão de dólares por dia em anúncios no Facebook. A empresa ainda relatou, durante as audiências judiciais, que possuíam de 4.000 a 5.000 pontos de medição de comportamento e personalidade de cada adulto dos EUA.

O documentário ainda nos apresenta o consultor de dados da CA, Christopher Wylie, exposto com o escândalo. De acordo com ele, se não fosse a manipulação da empresa, o Brexit nunca teria ocorrido; após o escândalo, a diretora de desenvolvimento de negócios da CA, Britany Kaiser, afirmou que as campanhas eleitorais em que a empresa trabalhou foram conduzidas ilegalmente e com manipulação do público de quem eles tinham acesso aos dados.

---

[2] Abreviação de “British exit” ou saída britânica em tradução literal para o português, é o nome dado para o evento de decisão do Reino Unido deixar o acordo da União Europeia.

[3] Sua definição consiste no conjunto de técnicas utilizadas para mensurar, de forma adequada e comprovada experimentalmente, um conjunto ou uma gama de comportamentos que não podem ser observados diretamente, com o intuito de obter informações sobre o funcionamento de um determinado sujeito. Exemplos desses construtos seriam inteligência, personalidade, atenção, satisfação com o trabalho, medos etc.

Foi desta maneira que a empresa conseguiu fraudar dois dos maiores eventos políticos mundiais, além de eventos menores como a eleição do senador Ted Cruz, sem que a população soubesse. A empresa reconheceu que manipulou os eleitores americanos e europeus e se declarou culpada perante a corte Britânica.

Tendo como parâmetro os casos expostos, justifica-se o fato de que leis como a LGPD e a GDPR são essências para manter a democracia e liberdade de escolha na sociedade, além de manter o titular dos dados seguro de golpes, uma vez que as informações vazadas são usadas para diversos ilícitos. A LGPD regula casos onde há incidentes de segurança e, ainda, orienta o que fazer nestes casos.

2.2.5.2 Como Atuar em Casos de Incidentes de Segurança

O site LGPD Brasil (2021) conceitua que “Incidente com Dados Pessoais é um evento que leva à destruição, perda, alteração, divulgação ou acesso não autorizados, de forma acidental ou ilícita, a dados pessoais transmitidos, armazenados ou processados pela empresa”.

Embora qualquer pessoa física possa reportar violação à LGPD, outros órgãos públicos e entes privados podem apresentar denúncia à ANPD, especialmente quando afetar interesses coletivos, como, por exemplo, de consumidores e empregados, explica Almeida (2021).

A LGPD traz no capítulo VII, intitulado como “Da segurança e boas práticas”, ações baseadas nos princípios da segurança e da prevenção para o tratamento de dados pessoais.

> Art. 46. Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.
> § 1º A autoridade nacional poderá dispor sobre padrões técnicos mínimos para tornar aplicável o disposto no caput deste artigo, considerados a natureza das informações tratadas, as características específicas do tratamento e o estado atual da tecnologia, especialmente no caso de dados pessoais sensíveis, assim como os princípios previstos no caput do art. 6º desta Lei.
> § 2º As medidas de que trata o caput deste artigo deverão ser observadas desde a fase de concepção do produto ou do serviço até a sua execução.

Neste sentido, o legislador reforça a ideia de os ambientes corporativos efetivarem as medidas protetivas durante e após o tratamento de dados. Elucida, Bioni:

> A segurança que se espera não é aplicada exatamente aos dados em si, mas sim aos sistemas que os mantêm (medidas técnicas) e ao ambiente geral da instituição (medidas organizativas). Isso significa que não bastam as medidas técnicas, como o uso de *firewalls*, métodos criptográficos e controles de conteúdo, se elas não vierem acompanhadas de outras medidas, como treinamentos de segurança, criação de políticas de segurança da informação, inventários de ativos etc. (BIONI, 2020, p. 357)

Se por acaso, mesmo com as medidas de segurança em dia a empresa venha a sofrer algum tipo de ataque ou incidente, o artigo 48, da LGPD traz um rol de ações a serem seguidas nestes casos, são elas:

> Art. 48. O controlador deverá comunicar à autoridade nacional e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares.
> § 1º A comunicação será feita em prazo razoável, conforme definido pela autoridade nacional, e deverá mencionar, no mínimo:
> I - A descrição da natureza dos dados pessoais afetados;
> II - As informações sobre os titulares envolvidos;
> III - A indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados, observados os segredos comercial e industrial;
> IV - Os riscos relacionados ao incidente;
> V - Os motivos da demora, no caso de a comunicação não ter sido imediata; e
> VI - As medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo.
> § 2º A autoridade nacional verificará a gravidade do incidente e poderá, caso necessário para a salvaguarda dos direitos dos titulares, determinar ao controlador a adoção de providências, tais como:
> I - Ampla divulgação do fato em meios de comunicação; e
> II - Medidas para reverter ou mitigar os efeitos do incidente.
> § 3º No juízo de gravidade do incidente, será avaliada eventual comprovação de que foram adotadas medidas técnicas adequadas que tornem os dados pessoais afetados ininteligíveis, no âmbito e nos limites técnicos de seus serviços, para terceiros não autorizados a acessá-los.

Importante destacar que a lei especifica no *caput* do artigo 48 que “a comunicação deve ser realizada em situações em que o incidente ‘possa acarretar risco ou dano relevante aos titulares’, o que significa que não é todo incidente de segurança que deve ser comunicado”, explica Bioni (2020, p. 361). O autor ainda ressalta a importância da criptografia na segurança de dados uma vez que no §3º, do mesmo artigo, classifica dados criptografados vazados como um incidente de menor gravidade, mas ressalta que depende do caso concreto e de análise da autoridade nacional.

2.2.6 Das Penalidades

As sanções administrativas são reguladas no capítulo VIII da Lei Geral de Proteção de Dados, a partir do artigo 52, são elas

> Art. 52. 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:
> 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;
> 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;
> XII - Proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados.

O §1º do mesmo artigo trata de atender ao princípio da ampla defesa e considera como parâmetros para a aplicação de penalidades os seguintes critérios:

> § 1º As sanções serão aplicadas após procedimento administrativo que possibilite a oportunidade da ampla defesa, de forma gradativa, isolada ou cumulativa, de acordo com as peculiaridades do caso concreto e considerados os seguintes parâmetros e critérios:
> I - A gravidade e a natureza das infrações e dos direitos pessoais afetados;
> II - A boa-fé do infrator;
> III - A vantagem auferida ou pretendida pelo infrator;
> IV - A condição econômica do infrator;
> V - A reincidência;
> VI - O grau do dano;
> VII - A cooperação do infrator;
> VIII - A adoção reiterada e demonstrada de mecanismos e procedimentos internos capazes de minimizar o dano, voltados ao tratamento seguro e adequado de dados, em consonância com o disposto no inciso II do § 2º do art. 48 desta Lei;
> IX - A adoção de política de boas práticas e governança;
> X - A pronta adoção de medidas corretivas; e
> XI - A proporcionalidade entre a gravidade da falta e a intensidade da sanção.

Explica o §6º do artigo 52 da LGPD que as sanções previstas nos incisos X, XI e XII do *caput* apenas serão aplicadas após já ter sido imposta ao menos 01 das sanções dos incisos II, III, IV e VI do *caput* do artigo para o mesmo caso concreto.

Importante ressaltar que a própria LGPD reconhece que não é a única a aplicar sanções para os incidentes com dados pessoais, a proteção de dados pessoais também está presente no Código Civil (Lei nº 10.406/02), no Código de Defesa do Consumidor (Lei nº 8.078/90) e, ainda, no Marco Civil da Internet (Lei nº 12.965/14). Logo, o §2º do artigo 52, da LGPD estabelece que "O disposto neste artigo não substitui a aplicação de sanções administrativas, civis ou penais definidas na Lei nº 8.078, de 11 de setembro de 1990, e em legislação específica." Em vista disso, permite-se a cumulação de penalidades quando a infração envolver mais de uma norma reguladora.

Neste sentido, Bioni (2020) faz uma observação pontual em seu livro "Tratado de Dados Pessoais". O autor explica que como existem diversas normas que visam a proteção de dados pessoais, é possível que exista um conflito de decisões dos órgãos reguladores caso não esteja bem estabelecido a definição da atuação que cada órgão deve desempenhar perante a fiscalização de dados, ele exemplifica com a seguinte situação

> "A utilização indevida de dados de cobrança de clientes de uma prestadora de serviços de telecomunicações, por exemplo, poderia ser considerada problemática simultaneamente à luz da Lei Geral de Proteção de Dados, da Lei Geral de Telecomunicações e do Código de Defesa do Consumidor, atraindo as competências da ANPD, da Anatel e de Procons." (BIONI, 2020, p.392)

Por enquanto, o artigo 55-K da LGPD estabelece que compete exclusivamente à ANPD a aplicação das sanções previstas na lei e que suas competências prevalecerão, no que se refere à proteção de dados pessoais, sobre as competências correlatas de outras entidades ou órgãos da administração pública.

O legislador definiu a vigência dos artigos penalizadores – artigos 52, 53 e 54 - a partir de 1º de agosto de 2021, a demora na aplicação da fiscalização se deu por conta da pandemia do COVID-19.

3 PROTEÇÃO DE DADOS E O DIREITO A PRIVACIDADE

No livro “Comentários à Lei Geral de Proteção de dados”, Cíntia Lima (2020), apresenta o conceito de “dadosfera” criado pelo jurista francês Jean-Sylvestre Bergé. De acordo com o jurista, atualmente há dois mundos, o mundo físico, já conhecido e um outro mundo que a cada dia se expande e se desenvolve na sociedade informacional e em reflexo ao mundo físico que “se mantém por infraestruturas físicas, de armazenamento e comunicação, localizadas ao redor do planeta, que interage com a sociedade no espaço digital por diferentes maneiras, face às suas diferentes camadas”. (LIMA, 2020, p.69).

Ainda de acordo com o jurista, a dadosfera, como o nome já diz, é recheada de dados pessoais e dados pessoais sensíveis que vagam pelo meio digital de jurisdição e por isso

> A proteção aos dados pessoais deve, assim, ser analisada de forma a delimitar o âmbito de aplicação dos instrumentos protetivos e a limitação dos ciclos de tratamento, que devem se ater à utilidade dos dados, às finalidades consentidas pelos titulares dos dados ou necessárias para a consecução dos deverem impostos pelas leis aos agentes de tratamento e ao Estado. (LIMA, 2020, p.69-70).

É neste contexto que as legislações reguladoras, como a LGPD, foram formuladas, para criar barreiras quanto ao uso de dados pessoais de maneira que a sociedade possa manter direitos estabelecidos pela Constituição Federal de 1988 (CF/88), como a liberdade e a democracia. Como visto acima, com respeito ao escândalo da Cambridge Analytica, o uso irrestrito de dados por uma empresa com capital suficiente, pode fazer estragos enormes, não apenas a indivíduos, mas a populações inteiras.

Assim, este último capítulo visa uma análise de como a proteção dos dados garante também, direitos fundamentais assim como os dados se tornaram um produto com o passar dos anos e quais perigos esse novo mercado pode trazer para o futuro.

3.1 O DIREITO A PRIVACIDADE E O NOVO ATIVO COMERCIAL

As legislações mundiais posteriores a 2º Guerra Mundial foram marcadas por regularem, em grande escala, os direitos humanos. Além disso destaca-se a criação da Organização das Nações Unidas (ONU), em 1945, imediatamente após a derrota nazista. A concepção de tal organização teve como finalidade manter mundialmente a paz, a união e, ainda, as condições mínimas para preservar a dignidade da pessoa humana inserida na sociedade, na forma de acordos, declarações ou tratados. Atualmente é composta por 193 Estados-membros, sendo o Brasil um dos membros fundadores da organização.

No Brasil, apesar de ser membro da ONU que preza pelos fatores que levam a manutenção da dignidade humana, como o direito à liberdade, igualdade e fraternidade, ocorreu em 1964, a ditadura militar que persistiu até o ano de 1985. A ditatura militar foi marcada por inúmeros casos de tortura, violência sexual, desaparecimentos e assassinatos de inimigos do regime, motivo pelo qual após a retomada da democracia no país foi promulgada a Constituição Federal, em 1988.

A Constituição de 1988, consagra em seu artigo 5º, com 78 incisos, os direitos e garantias fundamentais. Esses direitos são garantidos a todos os seres humanos, enquanto indivíduos de direito, já os adquirindo no momento em que nascem. O *caput* do artigo 5º estabelece que “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”.

O inciso X do mesmo artigo impõe que “são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação;”. Explica, Gabriel Oliveira (2020 apud SILVA, 2017, p.208-211), em seu artigo que

> o conceito de intimidade é geralmente empregado para designar a esfera secreta da vida do indivíduo, que busca evitar o conhecimento dos demais, como, por exemplo, suas relações sexuais. Já o conceito de privacidade engloba informações restritas da vida do indivíduo, como sua relação com familiares e amigos, o que o renomado autor chama de vida interior, que envolve atividades que geralmente não são tornadas públicas, não devendo ser objeto de divulgações por terceiros.

Ainda, estabelece a CF/88 no inciso XII que

> 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.

Porém, a própria questão temporal impede que, em 1988, a Constituição Federal pudesse prever e regular previamente as situações envolvendo o uso exorbitante da internet e o uso indiscriminado de dados pessoais uma vez que a internet era na época, de uso corporativo e acadêmico. Desta maneira, faz-se necessário as normas e decisões jurídicas acompanharem a evolução da humanidade e as tecnologias, afim de manter os direitos e garantias fundamentais.

Neste sentido, Patrícia Peck Pinheiro elucida que

> O Direito Digital tem o desafio de equilibrar a difícil relação existente entre interesse comercial, privacidade, responsabilidade e anonimato, gerada pelos novos veículos de comunicação. Esta equação só pode ser equilibrada se socialmente aceita e cobrada mediante procedimento de vigilância e punibilidade que devem ser determinadas pelo próprio Direito Digital. (PINHEIRO, 2016, p. 94)

O uso comercial de dados pessoais cresce diariamente e não é para menos, o documentário citado anteriormente, Privacidade Hackeada (2019), explica que é um comércio que fatura trilhões por ano e grande parte do sucesso dessa comercialização é porque os próprios usuários das plataformas inseridas na internet pagam o preço para estarem inseridos no mundo digital, disponibilizando seus dados pessoais para os enormes bancos de dados dessas plataformas, sem nem ao menos lerem os termos de uso ou política de privacidade. Como diz pontualmente David Caroll, ainda no documentário, “estávamos tão apaixonados com este presente de livre conectividade que ninguém se incomodou em ler os termos e condições”.

É deste modo que, de acordo com sociólogo Manuel Castells, estamos vivendo uma nova forma de economia, sucessora ao industrialismo, chamado de informacionalismo (ou economia da informação), ele explica que

> No informacionalismo, as tecnologias assumem um papel de destaque em todos os segmentos sociais, permitindo o entendimento da nova estrutura social – sociedade em rede – e consequentemente, de uma nova economia, na qual a tecnologia da informação é considerada uma ferramenta indispensável na manipulação da informação e construção do conhecimento pelos indivíduos”, pois “a geração, processamento e transmissão de informação torna-se a principal fonte

> de produtividade e poder". De sorte que a informação passou a ser a matéria prima mais valiosa. (BIONI et al., 2020, p.211, apud CASTELLS, 1999, p.21)

Conforme as tecnologias foram avançando e novas plataformas sociais e comerciais foram aumentando a partir do advento da internet, a sociedade mundial passou então a criar, de maneira exponencial e irreflexiva, rastros digitais, tornando cada vez mais frágil a ideia de privacidade neste ambiente. (BIONI, 2020).

É ainda nesse ambiente, que se concretiza o *Big Data*, nome dado para as técnicas capazes de extrair informações das enormes quantidades de dados para gerar análises e resultados significativos e, em seguida, armazená-los, explica o site Cetax (2020). De acordo com o site Digital House (2021), a previsão da International Data Corporation (IDC) é de que serão criados mais de 103 zettabytes (ZB)[4] de novos dados até o ano de 2023.

Por conta dessa extravagante quantidade, o mercado começou a buscar por formas de utilizar esses dados para gerar resultados nos mais diversos negócios. Essa ação, de início, não era regulada e nem se imaginava que tomariam as proporções atuais, como ser considerado o "novo petróleo*"*. A essa relação de consumo vem atrelada a promessa de proporcionar aos consumidores benefícios e otimização dos serviços e produtos, quando se concede um dado pessoal (TEPEDINO et al., 2019).

É neste contexto que "os dados pessoais passam a ser considerados um ativo dentro dessa nova estrutura econômica" (LACE, 2005, 1, apud BIONI, 2018, 22-23), uma vez que

> A economia da informação baseia-se, dessa maneira, na possibilidade de precificar os dados coletados e tratados, isto é, na capacidade de conceder aos dados valor monetário a ser explorado pelos atores que se valem desse insumo em seus modelos de negócio.
> (TEPEDINO et al., 2019, p. 616).

Complementa Danilo Doneda que

> A chamada monetização dos dados justificaria o reconhecimento da qualidade de bem jurídico à informação, sendo possível se utilizar, dentro da sistemática do direito privado, das normas protetivas do direito de propriedade para a sistematização de sua tutela. (DONEDA, 2006, p.164)

[4] Zettabite é uma unidade de memória, corresponde a 1.000.000.000.000.000.000.000 (10^{21}) bytes.

Em última análise, Doneda (2012), explica, ainda, que o maior desafio é a conciliação do mercado que utiliza os ativos (dados) com as novas regulamentações existentes.

Ao examinar a questão da privacidade dentro dessa nova economia, pode-se observar um paradoxo: se nos termos de condições e uso o usuário encontra todas as informações sobre os mais diversos usos que seus dados terão na empresa (inclusive compartilhamento dos mesmos com outras empresas) e, ainda assim, consente com o tratamento, não existe lesão a direito. (PINHEIRO, 2016).

A advogada Patrícia Peck Pinheiro, ainda, faz uma observação pontual a respeito do direito à propriedade das informações e explica que

> Todo indivíduo deve ter direito a proteção de suas propriedades e de sua privacidade. Isso é indiscutível. No tocante à propriedade, há tanto bens tangíveis como bens intangíveis. Nesse sentido, suas informações, em última análise, são um ativo de sua propriedade e, portanto, merecem proteção.
> (PINHEIRO, 2016, p. 95)

Nestas circunstâncias que a as recentes leis como a GRDP e a LGPD foram criadas, a nova lei brasileira exige que se cumpra o princípio da Transparência, de modo que o usuário esteja ciente de todas as etapas do tratamento. Da mesma forma, deve ter acesso à política de privacidade previamente a coleta de dados. Desta forma, o usuário pode escolher entre compartilhar ou não seus dados, colocando em prática a sua autodeterminação informativa, assim como a empresa pode escolher não ter esse indivíduo como seu cliente quando não ocorrer a disponibilização dos dados para o devido tratamento. (PINHEIRO, 2016).

3.2 A PROTEÇÃO DE DADOS PESSOAIS COMO DIREITO FUNDAMENTAL NO ÂMBITO PRÁTICO-JURÍDICO

Como exposto ao longo deste trabalho monográfico, o titular dos dados pessoais está sempre em posição de inferioridade, por isso tamanha insistência na proteção de seus dados pessoais, sejam eles sensíveis ou não. No ambiente capitalista onde, como já visto, empresas como a Cambrigde Analytica podem gastar até 1 milhão de dólares por dia em propagandas direcionadas em plataformas digitais a partir da mineração e do *data*

profilling[5] disponíveis no *Big Data* faz-se prevalecer a urgência de um ordenamento jurídico protetivo, “para equilibrar a relação entre os mais fracos e os mais fortes. Senão, voltaríamos ao estado de natureza e abandonaríamos tudo que foi construído de civilidade” (PINHEIRO, 2016, p. 101). Atualmente, o uso de dados pessoais ocorre mesmo para procedimentos onde anteriormente era necessário a presença física do titular, por isso, entende-se que os dados pessoais são “projeções da personalidade humana”. (TEPEDINO et al, 2019, p.162)

Danilo Doneda (2020), parte da ideia que proteção de dados pessoais é uma subespécie direta da privacidade, desta maneira simplista, pode-se considerar a tutela a privacidade, extensiva à proteção de dados.

Como já visto, a Constituição Federal de 1988, regulou no rol dos direitos e garantias fundamentais, mais especificamente no artigo 5º, inciso X, as questões relativas à intimidade e privacidade das pessoas e em seguida, no inciso XII estabelece que

> 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;

Desta maneira, criou-se especulações doutrinárias no sentido de que “a privacidade é encarada como um direito fundamental, as informações pessoais em si parecem, ser protegidas somente em relação à sua “comunicação”, conforme art. 5, XII, que trata da inviolabilidade da comunicação de dados.” (DONEDA, 2020, Livro Kindle)

A partir dessa interpretação, o jurista e professor Tércio Sampaio Ferraz Junior, publicou, já em 1993, o artigo “Sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do Estado” onde traz a tese de que o ordenamento constitucional não tutela os dados em si, mas apenas a comunicação (fluxo) dos mesmos. (QUEIROZ; PONCE, 2020). Baseado nesta tese que o Ministro do STF, Sepúlveda Pertence, decidiu expressamente em 2006, como relator no julgamento do Recurso Ordinário 418.416-8 - SANTA CATARINA que

> Os dados armazenados na memória do computador não têm direito ao sigilo que a Constituição reserva à correspondência. O ministro relator sustentou que a Constituição protege a troca de dados, e não os dados em si. A inviolabilidade alcança a interferência de um terceiro na troca de informações. (CONJUR, 2006)

[5] De Danilo Doneda “consiste na elaboração de perfis de comportamento de uma pessoa (ou de um grupo de pessoas) a partir de suas informações pessoais, que podem ser disponibilizadas por ela mesma ou que são colhidas.” (DONEDA, 2006, p.173 apud LIMA, 2019, 34).

Esta decisão criou um precedente para outros casos envolvendo a proteção de dados pessoais, que fez com que a decisão do Ministro relator ficasse atrasada em face do avanço tecnológico e do aumento do uso de dados pessoais nas ações comerciais e de segurança. Em vista disso, em março de 2019, foi proposta a Emenda Constitucional nº 17 (PEC 17/2019), com objetivo de alterar os artigos 5º, XII, e 22, XXX, da CF/88 para formalizar à proteção de dados pessoais um direito fundamental e, ainda, atribuir a competência da legislação sobre o tema, privativa da União. A PEC 17/2019 visa alterar os respectivos incisos para:

> Art. 5° (…) 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, bem como é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais;
>
> Art. 22. Compete privativamente à União legislar sobre: (…)
> XXX – proteção e tratamento de dados pessoais.

Atualmente a PEC 17/2019 foi aprovada no Senado Federal e remetida à Câmara dos Deputados onde aguarda apreciação. Se aprovada, a emenda constitucional pode tornar mais harmônica as discussões sobre o tema, já que poderia uniformizar futuros entendimentos estaduais nas mais diversas esferas jurídicas, além de modernizar os direitos e garantias fundamentais para os tempos e situações atuais como já fizeram outros países.

Apesar da demora na apreciação da PEC 17/2019, por conta da pandemia do COVID-19, já é de entendimento do Supremo Tribunal Federal (STF) que a proteção de dados é, sim, um direito fundamental. A decisão histórica ocorreu nos dias 06 e 07 de maio de 2020, tal decisão derivou do caso no qual, devido à pandemia, o Governo Federal editou a Medida Provisória 954 (MP 954) em 17 de abril de 2020, a qual assinalava em seu artigo 2º que

> As empresas de telecomunicação prestadoras do STFC e do SMP deverão disponibilizar à Fundação IBGE, em meio eletrônico, a relação dos nomes, dos números de telefone e dos endereços de seus consumidores, pessoas físicas ou jurídicas.

De acordo com Mendes e Fonseca (2020), o Governo pareceu ignorar a magnitude da já então conhecida, Lei Geral de Proteção de Dados (2018) e todos os debates envolvendo o compartilhamento de dados. Por conta disso, diversos partidos políticos e o Conselho Federal da OAB, ajuizaram no STF, cinco Ações Diretas de Inconstitucionalidade (ADIs) (nº 6.387, 6.388, 6.389, 6.390 e 6.393).

Em votação no plenário da Suprema Corte, a Medida Cautelar, que foi concedida pela relatoria Ministra Rosa Weber, suspendeu a eficácia da Medida Provisória 954/2020, com a maioria de dez votos favoráveis, com argumento de que a MP 954 não atendeu aos requisitos de relevância e urgência necessários para edição de Medida Provisória, nos termos do art. 62 da CF/88. (OLIVEIRA; MELO, 2021)

No seu voto, a Ministra Cármen Lúcia pontuou que

> Foi-se o tempo das antigas listas telefônicas de papel" de modo que, no atual contexto de desenvolvimento tecnológico, "não existem dados insignificantes" ou neutros. Dessa maneira, o Tribunal ultrapassou o discurso de que não haveria problema no compartilhamento de dados como nome, endereço e número de telefone, uma vez que esses teriam "caráter público".
> (MENDES; FONSECA, 2020, p.02)

Já a ministra Rosa Weber apontou que apesar de os dados compartilhados com a permissão da Medida Provisória serem de caráter público, quando cruzados com outras informações poderiam ganhar novos valores permitindo a identificação do seu titular ou até mesmo permitiria o *profilling* dos mesmos. Neste mesmo sentido, acenou o Ministro Luiz Fux, que relembrou o caso envolvendo o Facebook e a Cambrigde Analytica. (MENDES; FONSECA, 2020).

A relatora ainda sustentou que a MP 954 "se mostrava insuficiente na proteção dos dados pessoais, uma vez que não contemplava nenhuma previsão de auditoria externa e tampouco de responsabilização por eventual acesso indevido ou mau uso dos dados coletados." (OLIVEIRA; MELO, 2021).

O acórdão integral foi publicado em 12 de novembro de 2020 e acabou por reconhecer a proteção de dados e a autodeterminação informativa como direitos fundamentais e autônomos, ou seja, a decisão confere uma dimensão subjetiva em que o indivíduo deve ser protegido contra intervenções indevidas do Estado e de empresas privadas. Confere, também, uma dimensão objetiva no sentido de o Estado realizar esforços para a garantia de tais direitos nas relações públicas e privadas. (FERREIRA, 2020).

Como consequência da referida decisão, ocorreu, ainda, o “reconhecimento do *habeas data* enquanto instrumento de tutela material do direito à autodeterminação informativa.” (FERREIRA, 2020). O *habeas data* é regulado pela lei nº 9.507/97, além de ser um dos remédios constitucionais que existe para “proporcionar ao cidadão um instrumento para conhecer diretamente e, se necessário, retificar as informações sobre sua própria pessoa armazenadas em bancos de dados”. (DONEDA, 2020).

CONCLUSÃO

Com a presente monografia, objetivou-se analisar, de maneira introdutória, aspectos selecionados e pertinentes envolvendo a utilização de dados pessoais à luz da recente normativa Lei Geral de Proteção de Dados. Através do estudo doutrinário de autores relevantes deste tema, como Patrícia Peck Pinheiro, Bruno Bioni, Danilo Doneda, Cíntia Lima entre outros, pôde-se observar que esta temática ainda está nos estágios iniciais de entendimento pela população que, no geral, não entende o papel de inferioridade que se encontra. Ademais disso, observou-se a complexidade envolvendo o tratamento de dados na atualidade, motivo pelo qual não se dá a devida atenção aos termos de uso e privacidade das inúmeras plataformas existentes.

Neste estudo, observou-se que o desenvolvimento da sociedade e suas tecnologias não cessam, tornando-se necessário ao mundo jurídico acompanhar tais mudanças, para que nenhum direito fundamental ou humano seja afetado. Se tratando do informacionalismo, ou economia da informação, torna-se necessário e urgente regulamentações como a LGPD e GDRP, uma vez que tal economia está inserida no sistema capitalista.

Nesse modelo econômico, as grandes corporações como Google ou Grupo Facebook possuem excessivo capital financeiro e detém, ainda, as plataformas necessárias e mais frequentadas (por exemplo: Instagram e Facebook), onde o uso indisciplinado das informações pessoais, combinadas com a análise em massa de dados e técnicas como profilling podem não apenas colocar o livre arbítrio dos usuários em risco, sem que os mesmos saibam, como também interferir de forma direta na democracia.

Agregado a isso, o titular dos dados pode ter sua vida, dignidade e direitos básicos, totalmente afetados quando não observados os princípios e limitações trazidas pela LGPD. Um exemplo fictício que demonstra tal problemática pode ser representado pela seguinte situação: imaginemos que um aplicativo de medição diária de dados referentes à saúde (números de passos dados durante os dias, tipo de alimentação seguida, remédios de rotina, batimentos cardíacos, qualidade de sono etc.) disponibilizasse, de maneira indevida, essas informações para empresas que vendem planos de saúde que por sua vez, através da análise da performance diária do titular dos dados, prejudicasse, de maneira abusiva, seus serviços para a pessoa que viesse a solicitar seus serviços.

É neste cenário de inferioridade que o titular dos dados pessoais se encontra e a criação de novos dados aumenta vetorialmente. Por isso, tais pessoas (a população em geral) dependem da eficaz regulamentação e fiscalização, passo em que a Lei Geral de Proteção de Dados e figuras jurídicas como o Supremo Tribunal Federal vêm trazendo resultados positivos para a tutela do direito à privacidade e à manutenção do pleno exercício da autodeterminação informativa.

Durante o trabalho pôde-se, também, analisar que a vigência da fiscalização é recente e, por isso, ainda passará por inúmeros desafios para uma consolidação eficaz, uma vez que, mesmo já instaurada a LGPD, ainda ocorrem inúmeros vazamentos de dados pessoais diariamente. Por isso, entendemos que a cultura da prevenção e segurança desejada ao longo da LGPD é de difícil e onerosa implementação, não recebendo, ainda, a devida atenção pelas empresas privadas.

Percebemos, ao longo do estudo, que este tema é de enorme complexidade e atualidade, trazendo o obstáculo de estar relacionado com diversas outras áreas do conhecimento humano: áreas da tecnologia, matemática, sociologia, psicologia e outras questões pertinentes a outros territórios do Direito. Isso posto, explica-se sua amplitude e consequente dificuldade em reunir todas essas perspectivas em um único trabalho, por isso, buscamos construir um panorama que pudesse dar sentido à temática de forma que possamos auxiliar em outros estudos, bem como abrir a possibilidade de aprofundarmos, futuramente, em investigações posteriores.

REFERÊNCIAS

ALMEIDA, J. E. **A Boa-Fé No Direito Obrigacional.** Âmbito Jurídico, 2010. Disponível em: https://ambitojuridico.com.br/cadernos/direito-civil/a-boa-fe-no-direito-obrigacional/. Acesso em: 06 jul, 2021.

ALMEIDA, U. R. **LGPD e contagem regressiva para sanções administrativas:** quando serei fiscalizado?, Conjur, 2021. Disponível em: https://www.conjur.com.br/2021-jun-16/almeida-lgpd-sancoes-administrativas-quando-serei-fiscalizado. Acesso em: 22 jul, 2021.

APOLLO 11. In: Wikipédia: a enciclopédia livre. Disponível em: https://pt.wikipedia.org/wiki/Apollo_11. Acesso em: 30 Mar, 2021.

BARBIERI, H.; PALUDETTO, V.; **Guia Sobre A Nova Lei Geral De Proteção De Dados**. Livro Kindle. 20 páginas

BESSA, L. R. **A Lgpd E O Direito À Autodeterminação Informativa,** Genjurídico, 2020. Disponível em: http://genjuridico.com.br/2020/10/26/lgpd-direito-autodeterminacao-informativa/. Acesso em: 15 jul, 2021.

BIONI, B. R. et al (Coords.). **Tratado De Proteção De Dados Pessoais**. Rio de Janeiro: Grupo GEN, 2020. 9788530992200. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788530992200/. Acesso em: 21 Jun 2021.

BIONI, B. **Compreendendo O Conceito De Anonimização E Dado Anonimizado**. Genjurídico, 2020. Disponível em:

https://genjuridico.jusbrasil.com.br/artigos/889500718/compreendendo-o-conceito-de-anonimizacao-e-dado-anonimizado. Acesso em: 25 Jun, 2021.

BIONI, B. R. (Coord.). **Proteção de Dados Pessoais**: A Função e os Limites do Consentimento. Rio de Janeiro: Grupo GEN, 2021. 9788530994105. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788530994105/. Acesso em: 22 Jun 2021.

BRASIL. **Constituição Da República Federativa Do Brasil De 1988**. Brasil, 05 de outubro de 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/Constituicao/Constituicao.htm. Acesso em: 28 de maio de 2020.

BRASIL. **Lei Geral De Proteção De Dados.** Brasil, 14 de agosto de 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 13 de Mar de 2020.

CETAX. **Diferença entre Data Science, Big Data & Data Analytics,** Cetax, 2020. Disponível em: https://www.cetax.com.br/blog/data-science-vs-big-data-vs-data-analytics/. Acesso em: 29 jul, 2021.

DESCOMPLICA. **Guerra Fria**: o que foi e resumo | História | Quer que desenhe?. Youtube, 14/06/2018. Disponível em: https://www.youtube.com/watch?v=cAwsLaO4HGQ&ab_channel=Descomplica. Acesso em: 30/03/2021.

DONEDA, D. C. M. **DA PRIVACIDADE À PROTEÇÃO DE DADOS PESSOAIS**: Elementos Da Formação Da Lei Geral De Proteção De Dados. 2. ed. São Paulo: Thomson Reuters Brasil, 2020. Livro Kindle

FERREIRA, L. M. T. **A decisão histórica do STF sobre o direito fundamental à proteção de dados pessoais.** Conjur, 2020. Disponível em: https://www.conjur.com.br/2020-nov-25/lucia-ferreira-stf-direito-protecao-dados-pessoais/. Acesso em: 31 jun, 2021.

IURI Gagarin. In: Wikipédia: a enciclopédia livre. Disponível em: https://pt.wikipedia.org/wiki/Iuri_Gagarin#:~:text=Iuri%20Alexeievitch%20Gagarin%20(em%20russo,a%20bordo%20da%20Vostok%201. Acesso em: 30 Mar, 2021.

GARCIA, M. **Data Analytics, Big Data, Data Science.** Cetax, 2020. Disponível em: https://www.cetax.com.br/blog/big-data/. Acesso em: 29 jul, 2021.

GET privacy. **Conheça os direitos dos titulares de dados na LGPD,** Getprivacy, [s.d]. Disponível em: https://getprivacy.com.br/direitos-titulares-de-dados-lgpd/. Acesso em: 21 jul, 2021.

KAUER, G. **LGPD: Quais são os direitos dos titulares?** Infra News Telecom, [s.d]. Disponível em: https://www.infranewstelecom.com.br/lgpd-quais-sao-os-direitos-dos-titulares/. Acesso em: 21 jul, 2021.

LEADDATA. **Os dados são ou não o novo petróleo.** Leddata, 2020. Disponível em: http://leaddata.com.br/blog/index.php/2020/05/25/os-dados-sao-ou-nao-o-novo-petroleo. Acesso em: 20 maio, 2021.

LIMA, C. F. de. **O profiling e a proteção de dados pessoais**. 2019. 80. Trabalho de Conclusão de Curso – Departamento de Direito Privado e Processo Civil – Universidade Federal do Rio Grande do Sul, Rio Grande do Sul, Porto Alegre, 2019.

LIMA, C.R.P. D. (Coord.). **Comentários à lei geral de proteção de dados.** São Paulo: Grupo Almedina, 2020. 9788584935796. Disponível em:

https://integrada.minhabiblioteca.com.br/#/books/9788584935796/. Acesso em: 06 Jul 2021.

LISBOA, R. S. **Boa-fé e confiança na lei geral de proteção de dados brasileira**. Academia, 2019. Disponível em: https://www.academia.edu/42604203/Boa_f%C3%A9_e_confian%C3%A7a_na_LGPD_brasileira. Acesso em: 06 Jul, 2021.

LGPDBRASIL. **O que muda com a nova lei de dados pessoais,** Lgpdbrasil, 2021. Disponível em: https://fernandapossatti21.jusbrasil.com.br/artigos/1151459556/lei-geral-de-protecao-de-dados-pessoais-lgpd-lei-13709-2018. Acesso em: 06 jul, 2021.

NONES, F. **Princípios da lgpd:** importância na adequação de bases legais. Resultados Digitais 2020. Disponível em: https://resultadosdigitais.com.br/blog/principios-da-lgpd/. Acesso em: 06 jul, 2021.

OLIVEIRA, C. G. B; MEIRA, R. **Inteligência artificial e proteção de dados:** Desafios e Debates – Parte 2. IAPD, 2021. Disponível em: https://iapd.org.br/inteligencia-artificial-e-protecao-de-dados-profiling/

OLIVEIRA, A. F.; MELO, G. **Acórdão da adi nº 6387, do supremo tribunal federal, considerou o direito à proteção de dados e à autodeterminação informativa como direitos fundamentais autônomos.** PL&C Advogados [s.d]. Disponível em: http://www.plcadvogados.com.br/artigo/acordao-da-adi-no-6387-do-supremo-tribunal-federal-considerou-o-direito-a-protecao-de-dados-e-a-autodeterminacao-informativa-como-direitos-fundamentais-autonomos/. Acesso em: 31 jul, 2021.

PINHEIRO, P. P. **#direitodigital.** 6. ed. São Paulo: Saraiva, 2016.

PINHEIRO, P. P. **Proteção de dados pessoais**. São Paulo Editora Saraiva, 2020. 9788553613625. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788553613625/. Acesso em: 2021 jul. 31.

POSSATTI, F. **Lei geral de proteção de dados pessoais - LGPD lei 13.709/2018**: O que altera da vida das pessoas. Jusbrasil, 2021. Disponível em: https://fernandapossatti21.jusbrasil.com.br/artigos/1151459556/lei-geral-de-protecao-de-dados-pessoais-lgpd-lei-13709-2018. Acesso em: 06 jul, 2021.

REDE de computadores. In: Wikipédia: a enciclopédia livre. Disponível em: https://pt.wikipedia.org/wiki/Rede_de_computadores. Acesso em: 15 Jun, 2021.

SALDANHA, J. **O princípio da necessidade na LGPD:** A Minimização de Dados como Redutor de Custos. Tripla, 2019. Disponível em: https://triplait.com/o-principio-da-necessidade-na-lgpd/. Acesso em: 06 jul, 2021.

SANTOS, R. **O que é TCP IP?** Aprenda de uma vez por todas como funciona. Blog Hosts, 2019. Disponível em: https://blog.hosts.green/tcp-ip/. Acesso em: 30 mar, 2021.

SPUTINIK. In: Wikipédia: a enciclopédia livre. Disponível em: https://pt.wikipedia.org/wiki/Sputnik. Acesso em: 30 Mar, 2021.

SPUTINIK 2. In: Wikipédia: a enciclopédia livre. Disponível em: https://pt.wikipedia.org/wiki/Sputnik_2. Acesso em: 30 Mar, 2021.

QUEIROZ, R. M. R; PONCE, P. R. **Tércio Sampaio Ferraz Júnior e sigilo de dados**: O Direito À Privacidade E Os Limites À Função Fiscalizadora Do Estado: O Que Permanece E O Que Deve Ser Reconsiderado. Internet & Sociedade 2020. Disponível em: https://revista.internetlab.org.br/tercio-sampaio-ferraz-junior-e-sigilo-de-dados-o-direito-a-

privacidade-e-os-limites-a-funcao-fiscalizadora-do-estado-o-que-permanece-e-o-que-deve-ser-reconsiderado/. Acesso em: 31 jul, 2021.

TCP/IP. In: Wikipédia: a enciclopédia livre. Disponível em: https://pt.wikipedia.org/wiki/TCP/IP. Acesso em: 30 Mar, 2021.

TECHMUNDO. **A HISTÓRIA DA INTERNET** – TecMundo. Youtube, 24 mai, 2018. Disponível em: https://www.youtube.com/watch?v=pKxWPo73pX0&ab_channel=TecMundo. Acesso em: 30 abr, 2021.

TEPEDINO, G.; FRAZÃO, A.; OLIVA, M. **Lei Geral De Proteção De Dados Pessoais E Suas Repercussões No Direito Brasileiro.** 1. ed. São Paulo: Thomson Reuters Brasil, 2019.

TERRA, K. **Você sabe extrair informações de dados?** | Análise de Dados #1. Youtube, 13 jul, 2019. Disponível em: https://www.youtube.com/watch?v=RlGOaSPFtXc&ab_channel=Programa%C3%A7%C3%A3oDin%C3%A2mica. Acesso em: 30 abr, 2021.

VOSTOK 1. In: Wikipédia: a enciclopédia livre. Disponível em: https://pt.wikipedia.org/wiki/Vostok_1. Acesso em: 30 mar, 2021.

Big Data Statistics & Facts- Are You In Control? Waterford Technologies 2021. Disponível em: https://waterfordtechnologies.com/big-data-interesting-facts/. Acesso em: 29 jul, 2021.

ZETTABYTE. In: Wikipédia: a enciclopédia livre. Disponível em: https://pt.wikipedia.org/wiki/Zettabyte. Acesso em: 27 jul, 2021.