UNIVERSIDADE FEDERAL DE OURO PRETO
Departamento de Direito

Bárbara Natália Meynard Godinho

A TRAJETÓRIA DO CONSENTIMENTO COMO ELEMENTO FUNDAMENTAL PARA A AUTODETERMINAÇÃO INFORMATIVA:
um estudo a partir da Lei Geral de Proteção de Dados

Ouro Preto - MG
2023

Bárbara Natália Meynard Godinho

A TRAJETÓRIA DO CONSENTIMENTO COMO ELEMENTO FUNDAMENTAL PARA A AUTODETERMINAÇÃO INFORMATIVA:

um estudo a partir da Lei Geral de Proteção de Dados

Monografia apresentada ao Curso de Direito da Universidade Federal de Ouro Preto – MG como requisito parcial para obtenção do título de Bacharel em Direito.

Orientador (a): Juliana Evangelista de Almeida
Co-orientador(a): Márcio Mello Chaves

Ouro Preto - MG

2023

MINISTÉRIO DA EDUCAÇÃO
UNIVERSIDADE FEDERAL DE OURO PRETO
REITORIA
ESCOLA DE DIREITO, TURISMO E MUSEOLOGIA
DEPARTAMENTO DE DIREITO

FOLHA DE APROVAÇÃO

Bárbara Natália Meynard Godinho

A TRAJETÓRIA DO CONSENTIMENTO COMO ELEMENTO FUNDAMENTAL PARA A AUTODETERMINAÇÃO INFORMATIVA: um estudo a partir da Lei Geral de Proteção de Dados)

Monografia apresentada ao Curso de Direito da Universidade Federal
de Ouro Preto como requisito parcial para obtenção do título de bacharel em Direito

Aprovada em29 de março de X2023

Membros da banca

Doutora- - Orientador(a) Juliana Evangelista de Almeida- UFOP
Doutor - Corientador(a) Márcio Mello Chaves - CEDIN
Doutor - André de Abreu Costa- UFOP
Bacharel - Teresa Viegas Maciel - UFOP

Juliana Evangelista de Almeida, orientadora do trabalho, aprovou a versão final e autorizou seu depósito na Biblioteca Digital de Trabalhos de Conclusão de Curso da UFOP em 29/03/2023

Documento assinado eletronicamente por **Juliana Evangelista de Almeida**, **PROFESSOR DE MAGISTERIO SUPERIOR**, em 03/04/2023, às 11:55, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

A autenticidade deste documento pode ser conferida no site http://sei.ufop.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 , informando o código verificador **0503112** e o código CRC **91AD4D25**.

R. Diogo de Vasconcelos, 122, - Bairro Pilar Ouro Preto/MG, CEP 35402-163
Telefone: (31)3559-1545 - www.ufop.br

AGRADECIMENTOS

Este trabalho não poderia ter sido realizado se eu não tivesse o apoio incomensurável de pessoas importantes na minha vida, como os meus pais Giselle, e Kessel e familiares e amigos. Por essa razão, não olvidarei dos conselhos e palavras de apoio numa das etapas mais desafiadoras da minha vida.

Também gostaria de dedicar meus agradecimentos aos orientadores, pelas críticas construtivas e dicas imprescindíveis para poder elaborar uma pesquisa de qualidade; aos meus colegas da Universidade e a todos que contribuíram, direta e indiretamente, com palavras de apoio e ânimo.

Foram cinco anos muito difíceis, em virtude das adversidades que foram se apresentando na minha vida, sobretudo, por vivenciar em primeira pessoa uma pandemia global que nos obrigou a readaptar as rotinas das nossas vidas, refletir sobre a fragilidade de vida e da importância da solidariedade para o enfrentamento do vírus.

Sinto-me orgulhosa por ter chegado até aqui e realizado o meu sonho de graduar-me em Direito, mas esse sonho não teria sido possível sem a colaboração de todos aqueles que torceram e estiveram comigo nos momentos mais difíceis. Meu muito obrigada a todos!

RESUMO

A presente monografia tem o escopo de analisar o instituto do consentimento a partir da Lei Geral de Proteção de dados brasileira. Tem por problema de pesquisa averiguar a sua importância para legitimar o tratamento dos dados pessoais por parte dos agentes de tratamento, bem como de proteger o titular da possível utilização de suas informações sem o seu consentimento expresso, inequívoco e informado, observados os casos em que a norma dispensa o consentimento. Nesse prospecto, o trabalho divide-se em quatro capítulos, nos quais serão retomadas as principais discussões jurídicas para a configuração do direito à privacidade que foi substancial para a construção do direito fundamental à proteção de dados. Por conseguinte, apresenta-se um breve estudo da LGPD, com enfoque nos princípios que regem a norma e os direitos do titular dos dados, bem como da aplicação da norma no sentido de garantir a proteção dos direitos humanos e fundamentais do indivíduo. Por último, analisa-se o instituto do consentimento, tendo como base seu tríplice adjetivo: expresso, inequívoco e informado. O consentimento é um dos elementos fundamentais na proteção de dados, porque devolve ao titular dos dados pessoais a capacidade de decidir sobre o uso das suas informações e o poder de controlá-las. Muito embora a lei preveja casos em que ele é dispensado, o intuito do trabalho é demonstrar que esse elemento é importante para consolidação da autodeterminação informativa, visto que o titular de dados tem o direito de decidir sobre o uso de suas informações pessoais com fulcro em impedir que sejam usadas em seu desfavor ou sem a sua autorização.

Palavras-chave: Lei Geral de Proteção de Dados. Tratamento de dados. Direitos do titular. Consentimento.

RESUMEN

Esta monografía tiene como objetivo analizar la figura del consentimiento a partir de la Ley General de Protección de Datos brasileña. Su problema de investigación es constatar su importancia para legitimar el tratamiento de datos personales por parte de los agentes del tratamiento, así como para proteger al titular del posible uso de su información sin su consentimiento expreso, inequívoco e informado, observando los casos en que la regla prescinde del consentimiento. En este prospecto, el trabajo se divide en cuatro capítulos, en los que se retomarán las principales discusiones jurídicas para la configuración del derecho a la intimidad, que fue sustancial para la construcción del derecho fundamental a la protección de datos. Por ello, se presenta un breve estudio de la LGPD, centrándose en los principios que rigen la norma y los derechos del titular de los datos, así como la aplicación de la norma para garantizar la protección de los derechos humanos y fundamentales de la persona. Finalmente, se analiza el instituto del consentimiento, a partir de su triple adjetivo: expreso, inequívoco e informado. El consentimiento es uno de los elementos fundamentales en la protección de datos, porque otorga al titular de los datos personales la capacidad de decidir sobre el uso de su información y la facultad de controlarlos. Si bien la ley prevé casos en los que se renuncia a ella, el trabajo tiene como objetivo demostrar que este elemento es importante para la consolidación de la autodeterminación informativa, toda vez que el titular de los datos tiene derecho a decidir sobre el uso de su información personal con el fin de evitar que se utilicen en su perjuicio o sin su autorización.

Palabras-clave: Ley General de Protección de Datos. Tratamiento de datos. Derechos del titular. Consentimiento.

SUMÁRIO

1 INTRODUÇÃO

Devido o avanço das tecnologias e o fluxo e uso massivo de dados, as relações sociais, geopolíticas e econômicas sofreram diversas transformações para acompanhar as inovações proporcionadas por essas ferramentas. Apesar de que as tecnologias tenham proporcionado diversos avanços nos campos das ciências e das telecomunicações, é consenso que novos problemas surgiram, sobretudo no âmbito jurídico, em virtude de que os dados pessoais representam o “novo petróleo” que promove o desenvolvimento capital.

Nesse sentido, a proteção de dados nasce como um direito autônomo cujo escopo é tutelar juridicamente os titulares dos dados de caráter pessoal e protegê-los contra qualquer utilização abusiva de suas informações por terceiros, evitando que os direitos humanos e fundamentais sejam objetos de violações. Por essa razão, a Lei de Proteção de Dados – LGPD (Lei n. 13.179/2018) vislumbra inovar na matéria de proteção de dados e dedicar-se somente a esse instituto, tendo em voga as outras normas setoriais que já abordavam este tema, o legislador pretende dedicar o dispositivo específico à tratativa dessa temática.

Destarte, o presente trabalho tem o objetivo de explorar as nuances da Lei Geral de Proteção de Dados, principalmente, no que se refere ao consentimento e suas adjetivações na LGPD, pois o cenário construído pelas tecnologias e o *Big Data* faz com que os dados sejam o novo insumo para o desenvolvimento econômico e vigilância dos cidadãos. Isto não só permite que as estratégias de consumo sejam cada vez mais customizadas, mas acaba por gerar a manipulação e comercialização dessas informações sem trazer benefício algum ao titular e não permite que este tenha o controle sobre o uso dos seus dados.

Ademais, a partir de casos como o da Agência Nacional de Segurança estadunidense (NSA), *Cambridge Analytica*, *Facebook* e dentre outros, pode-se inferir que a ausência de regulação sobre o uso dos dados pessoais pode abrir margem para a vigilância da população e, consequentemente, para a violação de direitos fundamentais. Nessa senda, sabendo que o tratamento de dados pode ser designado ao alcance das finalidades além das consentidas pelo titular de dados, é substancial garantir o uso ético das informações com fulcro em evitar

que o uso inadequado dos dados pelos agentes de tratamento continue a ser praticado pelas instituições públicas e privadas, pois o titular das informações encontra-se em uma posição de hipervulnerabilidade nessas relações e apresenta-se como um instrumento capaz de ampará-lo e dar-lhe o controle de suas informações.

Por isto, o consentimento é um dos pilares da proteção de dados, mesmo que em algumas situações ele seja prescindível, torna-se eficiente a partir do instante que o manejo das informações se limita às finalidades permitidas pelo titular dos dados. Portanto, o consentimento livre, informado e inequívoco está intrinsicamente vinculado ao princípio da autodeterminação informativa, porque o indivíduo, mesmo que de forma não absoluta, pode dispor do acesso e do manejo de suas informações, bem como controlá-las e fiscalizar o uso de seus dados pessoais e contar com o amparo legal que o legitima.

Para tanto, o trabalho divide-se em 4 (quatro) capítulos, aos quais dedicam-se ao estudo da evolução da proteção dos dados pessoais tendo como ponto de partida o *paper* publicado por Samuel Warren e Louis Brandeis, "*The right of privacy",* até a norma de proteção de dados europeia. Por conseguinte, no capítulo 2 (dois) são discutidas as normas setoriais brasileiras que já preparavam o terreno para uma lei de proteção de dados no ordenamento jurídico, como o Código de Defesa do Consumidor (CDC), Marco Civil da Internet (MCI), Lei de Acesso à Informação (LAI) e Lei do Cadastro Positivo.

Sobretudo, o Marco Civil da Internet foi o salto para a chegada da LGPD, porque já vinham à tona os escândalos envolvendo autoridades, o uso indiscriminado dos dados pessoais e os incidentes de vazamento de dados que geravam impactos aos direitos fundamentais. Daí a importância da criação de uma Lei Geral de Proteção de Dados, cujos aspectos são discutidos no capítulo 3 (três), donde são tecidos comentários sobre os princípios que regem a norma, os conceitos elaborados pelo legislador, quais os direitos do titular dos dados e sobre o papel da Autoridade Nacional de Proteção de Dados.

Por último, analisa-se o objeto central deste trabalho, qual seja a figura do consentimento e a sua importância para direcionar o uso ético dos dados pessoais, bem como do acesso às informações claras a despeito do tratamento de dados ao seu titular para que todo o processo seja o mais transparente possível. Disposto no art. 7º, da LGPD, o consentimento evidencia-se como

elemento fundamental para legitimar o tratamento de dados, excetuados aqueles casos em que esse elemento é prescindido. Assim sendo, nos demais casos em que é exigido o consentimento, o legislador dispôs que este deverá ser formalizado, isto é, o titular dos dados deverá expressar o seu consentimento documentalmente para que o tratamento de dados seja realizado para atingir finalidades determinadas.

A metodologia elegida para realização do presente estudo é a de revisão bibliográfica transdisciplinar, com respaldo nas principais doutrinas que discutem a proteção de dados em âmbito nacional, tendo como enfoque a análise de casos reais para que se possa compreender as razões pelas quais a LGPD se funda. Nesse prospecto, o trabalho não tem como objetivo esgotar a temática e tampouco reduzir a sua complexidade, mas abordar alguns dos principais pontos que giram em torno do consentimento e da proteção de dados.

2 A EVOLUÇÃO DO DIREITO À PRIVACIDADE E DA PROTEÇÃO DOS DADOS NO CONTEXTO DAS TECNOLOGIAS DE INFORMAÇÃO E COMUNICAÇÃO NA ERA DO BIG DATA

O Direito, em suas mais diversas acepções, tem como função primordial regular as relações humanas em sociedade, com o propósito de dar a cada sujeito o que lhe é devido e justo e garantir a ordem social. André Franco Montoro (2020) leciona que o Direito é faculdade, justiça, ciência e fato social; não possuindo apenas um sentido unívoco.

Nesse sentido, não à toa é correto afirmar que o Direito se constrói e modifica-se de acordo com as mudanças que ocorrem na sociedade, devendo ajustar-se às novas realidades para gerir os fatos sociais e adequá-los às normas.

O Direito à privacidade vincula-se ao rol dos direitos da personalidade, no qual tem um trajeto histórico bastante instável, tendo em vista que as primeiras articulações em torno dos direitos da personalidade têm fortes influências das concepções patrimonialista e sacralizada, donde tudo se resumia ao caráter econômico, patriarcal e divino.

Consoante Bruno Bioni (2020), com a chegada dos movimentos jusnaturalistas e antropocêntricos, as normas jurídicas passam a centrar sua essência no ser humano, o que também influi na laicização jurídica e estatal.

Por essa razão, incumbe mencionar que de acordo com a cronologia jurídica, o direito à privacidade é recente, pois sua relevância não foi reconhecida até meados da década de 1890, quando Warren e Brandeis publicaram o ensaio sobre o direito à privacidade, diante da emergência da tutela desse direito frente o surgimento das novas tecnologias.

É essencial destacar, ao mesmo passo, que a Segunda Guerra Mundial foi responsável pela “proliferação do princípio da dignidade humana [...], tal como a própria declaração de direitos universais, das Nações Unidas, que se dá uma guinada para que o direito passasse a assegurar os interesses existenciais da pessoa humana” (BIONI, 2020, p. 103).

Atualmente, com a explosão das novas tecnologias e da Internet, a privacidade ganha relevância no contexto jurídico dada a importância das informações que antes eram consideradas “menos importantes” e agora passam

a destacar-se no mercado, pois cada dado obtido a respeito de um indivíduo é precioso para conhecer o sujeito, para garantir o capital das grandes empresas, ou, também, para vigilância e controle social dos cidadãos.

Sem embargo, o fluxo de dados pessoais dos usuários da rede mundial de computadores ocorre de modo descontrolado, já que os indivíduos que baixam aplicativos ou entram em páginas virtuais, ao concordar com os termos de uso sem sequer lê-los, acabam presenteando as grandes corporações digitais com suas informações.

Essas informações, após realizado o tratamento de dados, podem ser utilizadas para perfilamento dos consumidores com o escopo de direcionar ofertas/anúncios de produtos e serviços de acordo com as buscas realizadas pelo usuário do navegador.

Ademais, os dados podem ser utilizados para controlar/monitorar os passos dos indivíduos conectados, bem como manipular seus processos de decisões. São inúmeras as possibilidades de uso dessas informações pessoais por grandes empresas, porque os dados são o novo modelo econômico do capitalismo digitalizado e, por isso, é importante debater a esfera jurídica do direito à privacidade e da sua substancialidade.

O direito a proteção de dados coaduna com outros direitos preexistentes, mas que merece especial tratamento em virtude da nova realidade a que os indivíduos estão inseridos, qual seja da conectividade/digitalização de bens e serviços.

Neste presente capítulo serão apresentados os primeiros debates no mundo jurídico sobre o direito da privacidade, tendo como principal marco a década de 1890. Far-se-á um estudo comparado com outras legislações alienígenas, para, nos capítulos posteriores, serem discutidos os aspectos da legislação brasileira pertinente ao conteúdo e de como contribuiu para a configuração do direito fundamental à proteção de dados.

Desta forma, incumbe ressaltar que direito à privacidade e direito fundamental à proteção de dados não se confundem, vez que a proteção de dados adquiriu status de direito autônomo cujo objeto de proteção é amplo e não se limita apenas ao direito à privacidade. Conforme leciona Doneda *et.al* (2021), sua extensão é ampla porque engloba outros direitos fundamentais, como da dignidade humana e outros direitos inerentes à personalidade humana. Desse

modo, os impactos causados pelo uso indiscriminado dos dados pessoais e os possíveis abusos realizados pelos agentes de tratamento podem impactar os direitos fundamentais e por isto não se limita a um único direito.

2.1 A década de 1890 como marco do regime jurídico da tutela da privacidade

É consenso na doutrina que o marco que inicia o debate sobre a privacidade advém da contribuição dos estadunidenses Samuel Warren e Louis Brandeis, com a publicação do ensaio acadêmico "*The right of privacy*" (em tradução livre, "O direito à privacidade"), em 1890. Neste ensaio, os dois juristas analisam diversos julgamentos nos quais discutem o que seria o direito de estar só, ou, de não ser incomodado.

Ao longo do *paper*, ambos em tom crítico, explicam que os novos modelos de negócios e invenções estão utilizando as informações sobre a vida privada das pessoas, suas imagens, etc; para obter lucro.

Como exemplos, os autores citam os jornais e periódicos da época ultrapassavam os limites do tolerável, à medida que expunham as pessoas em suas publicações, baseadas em fofocas sobre as relações dos indivíduos no âmbito privado, com o objetivo de tornar a intimidade do outro exposta ao público. Nesse sentido, manifestam-se favoráveis à proteção da intimidade e privacidade dos indivíduos para que lhe seja garantido o "direito a estar só".

Nesse prospecto, o consentimento também passa a ser fundamental para o direito à privacidade, pois somente mediante a aquiescência da pessoa, terceiros poderão gerir as suas informações privadas. Dessa forma, com a positivação do direito à privacidade, o sistema jurídico garante a proteção à intimidade do indivíduo, bem como a sua autonomia, a inviolabilidade da dignidade humana e o controle de suas informações (WARREN; BRANDEIS, 1890).

Cabe destacar que neste *paper* também subsiste uma hierarquização do direito à privacidade, levando em consideração o contexto burguês estadunidense da época, e o caráter patrimonialista e individualista, posto que somente quem tivesse condições socioeconômicas suficientes para judicializar

as ações pertinentes poderiam ter esse direito preservado, porque não se tratava de um direito universalizado (DONEDA, 2021).

Por essa razão, o jurista italiano Stefano Rodotà (2008) afirma que o direito à privacidade nasce do privilégio das classes dominantes, pois estas não queriam ter suas intimidades expostas por terceiros, e pretendiam afastar qualquer possibilidade de invasão por pessoas não autorizadas às suas intimidades.

> Foi com base naquele primeiro conteúdo que em 1890, os Justices da *Supreme Court* americana, Warren e Brandeis, determinaram a necessidade de tutela dessa esfera existencial. À época, a interpretação que se dava ao direito à privacidade era restrita e se aplicava a casos em que existia a atuação de terceiros contra aquela esfera. Isto é, a interpretação que se dava a este direito restringia-se a tutelar a esfera privada de uma pessoa, impedindo que outros pudessem nela ingressar sem sua autorização. Associada à ideia de casa, moradia, este princípio foi primeiramente utilizado para proteger a vida privada das pessoas, dentro de seu próprio lar (MULHOLLAND, 2018, p. 172).

Apesar de ser um marco importante para a delimitação das primeiras acepções sobre o direito à privacidade, Doneda (2021) e Mulholland (2018) concordam no sentido de que o direito à privacidade não se resume apenas ao âmbito privado, como também se trata de um direito fundamental que se relaciona com outros direitos da personalidade, inerentes ao desenvolvimento humano.

2.2 Declaração Americana dos Direitos e Deveres do Homem de 1948 (Bogotá)

O direito à privacidade foi instituído no rol de direitos fundamentais da Declaração Americana dos Direitos e Deveres do Homem, realizada em Bogotá, na Colômbia. Essa norma nasceu na mesma conferência que fundou a Organização dos Estados Americanos (OEA) e tem sua razão de ser na instituição dos direitos fundamentais e humanos como pilares de todos os Estados americanos.

De acordo com os artigos V, IX e X, do referido instrumento, o direito à privacidade assegura que:

> Artigo V. Toda pessoa tem direito à proteção da lei contra os ataques abusivos à sua honra, à sua reputação e à sua vida particular e familiar; Artigo IX. Toda pessoa tem direito à inviolabilidade do seu domicílio. Artigo X. Toda pessoa tem o direito à inviolabilidade e circulação da sua correspondência (OEA, 1948).

Além do enfoque universalista, a Declaração oficializa um novo marco dos Estados americanos, vez que institui o princípio da dignidade humana como pilar do Estado Democrático de Direito e de todas as demais instituições jurídico-políticas das nações americanas, com fulcro de alcançar a finalidade teleológica do Estado e garantir a paz entre os povos.

2.3 A privacidade na Declaração Universal dos Direitos Humanos

A Declaração Universal dos Direitos Humanos tem a sua origem vinculada à necessidade dos Estados soberanos de proteger a dignidade e integridade humana de seus povos, em virtude das tragédias que resultaram da Segunda Guerra Mundial. Consoante os ensinamentos de Norberto Bobbio (2004), em seu livro intitulado “A Era dos Direitos”, trata-se de um marco importante na positivação dos direitos substanciais para a humanidade, já que são direitos históricos caracterizados pelas lutas em defesa das liberdades e em oposição aos velhos poderes.

Ainda em consonância com o referido autor, as consequências ocasionadas pela Segunda Guerra Mundial evidenciaram a urgência da positivação dos direitos garantissem a preservação do mínimo existencial, como a dignidade humana e o direito à vida, com fulcro em proteger os indivíduos das perversidades de regimes autoritários que, em virtude de ideologias extremistas e da necropolítica, vitimaram milhares de indivíduos.

Dito isto, a privacidade foi instituída também como um direito elementar para o ser humano, posto que, conforme o art. 12º: “Ninguém sofrerá intromissões arbitrárias na sua vida privada, na sua família, no seu domicílio ou na sua correspondência, nem ataques à sua honra e reputação (ONU, 1948).

2.4 Convenção Europeia para a Proteção dos Direitos do Homem e das Liberdades Fundamentais de 1950

A Convenção Europeia para a Proteção dos Direitos do Homem e das Liberdades Fundamentais, de 1950, também fora instituída com o objetivo de instaurar uma rede internacional de proteção, com fulcro em assegurar que os direitos por ela instituídos fossem respeitados por aqueles países signatários da convenção. Em se tratando disso, o direito à privacidade figura como direito fundamental em seu art. 8º, o qual anuncia que:

> Art. 8° Direito ao respeito pela vida privada e familiar.
> 1. Qualquer pessoa tem direito ao respeito da sua vida privada e familiar, do seu domicílio e da sua correspondência.
> 2. Não pode haver ingerência da autoridade pública no exercício deste direito senão quando esta ingerência estiver prevista na lei e constituir uma providência que, numa sociedade democrática, seja necessária para a segurança nacional, para a segurança pública, para o bem – estar económico do país, a defesa da ordem e a prevenção das infracções penais, a protecção da saúde ou da moral, ou a protecção dos direitos e das liberdades de terceiros (COUNCIL OF EUROPE, 1950).

Para Bioni (2020), todo esse movimento é resultado da experiência vivenciada pela Segunda Guerra, posto que o Estado considera os dados pessoais da população como fonte fundamental para coordenar e planejar o seu funcionamento.

Contudo, o direito à privacidade emerge como um sistema de freio que permite o indivíduo controlar as suas próprias informações, bem como mitigar riscos de terceiros utilizarem seus dados sem o seu consentimento, já que podem ser utilizados para fins perversos, mesmo com o consentimento[1] –

[1] Aqui é importante abrir um parênteses, pois mesmo com o consentimento do usuário, os seus dados podem ser objeto de tratamento indiscriminado, abrindo margem para a manipulação de suas decisões para satisfazer os interesses. Os chamados *Dark Patterns* (padrões obscuros, traduzindo do inglês) são as interfaces responsáveis pela interação do usuário em webs, aplicativos, redes sociais e outras plataformas digitais; que se aproveitam do consentimento dos usuários – que aceitam cookies e as políticas de privacidade – para manipular a sua interação na internet e prejudicar a tomada de decisões. O comitê europeu fez uma consulta pública em 2022 para averiguar as práticas adotadas pelos *Dark Patterns*. De acordo com as Diretrizes 3/2022, do Comitê Europeu de Proteção de Dados (*European Data Protection Board*), os *Dark Patterns* podem classificar-se em: 1)*Overloading*: criam-se obstáculos que geram o cansaço do usuário no momento de tomar as decisões sobre suas informações pessoais, a partir da criação de sucessivas perguntas e labirintos com fulcro em obter o consentimento imediato do usuário, que aceita as políticas de privacidade para livrar-se das inúmeras perguntas e ter acesso ao serviço; 2) *Skipping*: interface desenhada com o intuito de fazer o usuário não reflita sobre a proteção de seus dados; 3*) Stirring*: faz uso de apelos emocionais/visuais para obter o

resultando na vulnerabilidade/violação dos direitos fundamentais. Mesmo que não seja um direito absoluto, como será visto adiante nos casos em que a LGPD dispensa o consentimento para o tratamento de dados, o consentimento é um dos elementos fundamentais para validar o tratamento de dados.

2.5 Convenção Americana sobre Direitos Humanos de 1969 (Pacto de San José da Costa Rica)

O respaldo à privacidade também se faz presente no Pacto de San José da Costa Rica. A referida Convenção foi responsável por inaugurar o sistema americano de direitos humanos, cujos países signatários também fazem parte da Organização dos Estados Americanos (OEA). No art. 11º, da Convenção Americana sobre Direitos Humanos (CADH), de 1969, a privacidade é um direito fundamental, posto que todo ser humano tem direito ao respeito de sua honra e dignidade.

Nesse prospecto, ninguém pode ter a sua vida privada, familiar, o seu domicílio ou correspondência violados por qualquer ingerência arbitrária ou abusiva, tampouco, ser ofendido. Assim sendo, a própria norma estabelece que contra quaisquer arbitrariedades, o indivíduo tem a proteção da lei (OEA, 1969).

2.6 Da Convenção 108 ao *General Data Protection Regulation* (GDPR)

A Convenção 108, do Conselho da Europa para a Proteção das Pessoas Singulares no que diz respeito ao Tratamento Automatizado de Dados Pessoais, foi realizada em janeiro de 1981, em Estrasburgo. A norma tem como enfoque a proteção de dados, tratando-se do primeiro instrumento jurídico internacional vinculante a tutelar a matéria relativa ao tratamento automatizado de dados.

Nessa esteira, a Convenção reforça o controle dos dados pessoais ao titular dessas informações. A norma estabelece os conceitos básicos sobre

consentimento do usuário; 4) *Hidering*: dificulta ao usuário a possibilidade de ajustar as políticas de privacidade ou complica o seu acesso; 5) *Fickle*: interface instável que impede o usuário de realizar determinadas ações; 6) *Left in the Dark*: as configurações de privacidade estão ocultas ou são difíceis de serem encontradas, em que se utilizam de informação obscura, pouco clara e até mesmo errônea (EPDB, 2022).

dados pessoais, os quais foram substanciais para a configuração do GDPR europeu.

A Convenção 108, ademais, institui os princípios básicos da proteção de dados, quais sejam: a) deveres das partes; b) qualidade dos dados; c) necessidade; d) segurança dos dados; e) finalidade. Doneda (2021) explica que apesar da proteção dos dados fazer-se presente, em linhas iniciais, na Declaração Universal de Direitos Humanos (DUDH) e na Convenção Europeia dos Direitos do Homem, de 1950; somente com a Convenção 108 a matéria foi cuidada expressamente. O autor ainda leciona que somente com o surgimento da Carta dos Direitos Fundamentais da União Europeia é que a proteção de dados é concebida como direito fundamental autônomo (DONEDA, 2021).

O direito à proteção de dados como direito autônomo agrega, segundo Doneda (2019), valor positivo ao estado da arte no Brasil, porque recebe *status* de direito fundamental implícito no regime jurídico constitucional, assumindo os limites formais às reformas constitucionais e vincula todas as demais normas relativas à proteção de dados.

> Assim, uma compreensão/interpretação/aplicação constitucionalmente adequada do direito fundamental à proteção de dados deverá ser sempre pautada por uma perspectiva sistemática, que, a despeito do caráter autônomo (sempre parcial) desse direito, não pode prescindir do diálogo e da interação (por vezes marcada por concorrências, tensões e colisões) com outros princípios e direitos fundamentais que, dentre outros pontos a considerar, auxiliam na determinação do seu âmbito de proteção, inclusive mediante o estabelecimento de limites diretos e indiretos (DONEDA, et.al., 2021, p. 97).

Nessa toada, em 24 de outubro de 1995, o Parlamento Europeu aprova a "*Directiva 95/46/CE – Relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados*". Essa normativa dá um passo importante na proteção dos dados pessoais, uma vez que acompanha a evolução das tecnologias e da relevância da tutela dos direitos fundamentais e humano no âmbito do ciberespaço e estabelece as bases para garantia da privacidade e segurança dos dados.

Sem embargo, a referida Diretiva foi revogada pelo atual Regulamento 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, e que institui a proteção dos dados pessoais e a livre circulação desses dados,

revogando a Diretiva 95/46/CE e estabelecendo o novo regime do GDPR europeu.

O novo modelo europeu de proteção de dados instituído pelo GDPR 2016/679 não deixa de se inspirar na Diretiva 95/46/CE, posto que ressalta que a proteção de dados é substancial, em virtude do tratamento de dados frequente exercido pelas atividades econômicas e sociais, inclusive, pelos Estados-soberanos; em que cresce consideravelmente à medida que as tecnologias da informação e comunicação facilitam e aceleram essa troca de informações.

Ainda que o enfoque do presente trabalho não seja a abordagem minuciosa do atual GDPR europeu, insta mencionar que a referida norma delimita conceitos como dados pessoais e sensíveis, agentes de tratamento, terceiros, consentimento; bem como define os princípios basilares da proteção de dados (tais como da transparência, lealdade, finalidade, adequação, exatidão), os quais também serviram de inspiração para o modelo brasileiro.

Em suma, o atual GDPR europeu traz consigo o arcabouço de definições e princípios herdados do Tratado sobre o Funcionamento da União Europeia (1957); da Diretiva 97/66/CE (1997), da Carta dos Direitos Fundamentais da União Europeia (2000) e da Diretiva 2002/58/CE (2002).

3 OS MARCOS REGULATÓRIOS DA PROTEÇÃO DOS DADOS PESSOAIS NO CONTEXTO BRASILEIRO ANTERIORES À LGPD

A Lei Geral de Proteção de Dados (Lei n. 13.709/2018) representa um marco jurídico em matéria de regulação do uso de dados pessoais no território nacional e inaugura um novo modelo jurídico que vislumbra regular as relações entre os titulares de informações pessoais e os agentes que fazem o uso de dados para suas atividades. Não obstante, o ordenamento jurídico brasileiro já evidenciava a sua preocupação na garantia do direito à privacidade dos seus cidadãos.

Neste capítulo será analisado o instituto do direito à privacidade no ordenamento jurídico brasileiro *praevius* ao Marco Civil da Internet e da Lei Geral de Proteção de Dados, com enfoque no que está previsto na Constituição da República Federativa de 1988 (CFRB/88), Código Civil de 2002 e Código de Defesa do Consumidor.

3.1 Antecedentes legais

O direito fundamental à proteção de dados, como fora visto nos tópicos anteriores, tem uma jornada histórica que começa com o *paper* de Warren e Brandeis, em 1880, acerca do direito à privacidade e vai ganhando contorno com os debates incisivos oriundos das tensões provocadas pela Segunda Guerra Mundial e pela Guerra Fria, bem como pelo avanço rápido das Tecnologias de Informação e Comunicação. Contudo, a partir da contribuição de outras normas alienígenas que o concebem como um direito autônomo, pode-se inferir como esse direito já se revelava de forma explícita na Lei Maior brasileira.

No contexto brasileiro e dada a recente redemocratização do país que se inaugura com a consolidação da Constituição Federal de 1988, a privacidade também se encontra no rol de direitos fundamentais como um princípio implícito. Tal princípio aparece no art. 5º, incisos X, XI e XII, da Magna Carta, em que o Constituinte garante a inviolabilidade da intimidade, da honra e imagem das pessoas; do domicílio e das comunicações – excetuados nos casos estipulados pela norma em que esses direitos poderão ser sobrepostos.

> Art. 5º.....
> X – 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;
> XI – a casa é asilo inviolável do indivíduo, ninguém nela podendo penetrar sem consentimento do morador, salvo em caso de flagrante delito ou desastre, ou para prestar socorro, ou, durante o dia, por determinação judicial;
> XII – é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal (BRASIL, 1988).

De acordo com Ingo Wolfgang Sarlet (2021), embora seja um direito fundamental implícito na Constituição Federal, o fato de o Constituinte positivar formalmente esse direito e atribuí-lo um *status* superior em relação às demais normas infraconstitucionais torna-o um direito fundamental autônomo.

Além disso, Sarlet (2021) explica que o direito fundamental, por ter *status* superior na pirâmide normativa, não pode ser suprimido e nem abolido, *vide* as cláusulas pétreas do art. 60, §§ 1º a 4º, da CF, que limitam formalmente as reformas constitucionais. Ademais, o próprio Constituinte determina que a aplicação dos Direitos e Garantias Fundamentais, previstos em seu art. 5º, terão aplicação imediata (Art. 5º, § 1º, da CF).

Nessa senda, no âmbito infraconstitucional, o Código Civil de 2002 determina, em seu art. 21, que a intimidade é um direito da personalidade, pois "toda pessoa natural é inviolável, e o juiz, a requerimento do interessado, adotará as providências necessárias para impedir ou fazer cessar ato contrário a esta norma" (BRASIL, 2002). Consoante as lições de Flávio Tartuce (2021), trata-se de um direito que não é absoluto, como supracitado no art. 5º, da CF, donde constam as limitações do Constituinte.

Sem embargo, Tartuce (2021) explica que a dificuldade em garantir o direito à privacidade não está na sua afirmação, mas na sua efetividade, em vista às inúmeras situações cotidianas que permitem a sua violação. Por exemplo, quando o usuário de aplicativos da Internet fornecesse suas informações pessoais às plataformas virtuais para acessar os serviços ou realizar compras e, posteriormente, tem os seus dados compartilhados, sem o seu consentimento,

às outras empresas que lhe enviam publicidades constantes, ou, até ligações telefônicas[2].

O Código de Defesa do Consumidor (Lei n. 8.078, de 11 de setembro de 1990) também vela pela proteção de dados dos consumidores. No *caput* do art. 43, do CDC, o legislador dispõe que o consumidor tem direito ao acesso às informações existentes nos bancos de dados que armazenem informações sobre ele.

Por conseguinte, nos respectivos parágrafos do art. 43º, a lei determina que os cadastros e dados dos consumidores deverão ser "*objetivos, claros, verdadeiros e em linguagem de fácil compreensão, não podendo conter informações negativas referentes a período superior a cinco anos*" (BRASIL, 1990, *grifo da autora*).

Ademais, a abertura de qualquer registro de dados em nome do consumidor deverá ser comunicada quando não solicitada por ele e os dados, a pedido do consumidor, deverão ser corrigidos sempre que apresentarem inexatidão (BRASIL, 1990). Consoante a doutrina de Tepedino, Frazão e Oliva (2019) a partir da leitura do art. 43, do CDC, é possível extrair 5 princípios da proteção de dados: direito de acesso, qualidade dos dados, transparência, direito de retificação e cancelamento; e direito ao esquecimento.

Nessa mesma direção, a Lei do Cadastro Positivo (Lei n. 12,414, de 9 de junho de 2011) também disciplina em matéria de proteção de dados, pois dispõe sobre a formação e a consulta a bancos de dados relativos às informações de adimplemento das pessoas físicas e jurídicas para fins de elaboração do histórico de crédito.

O principal escopo dessa norma é constituir um perfil para os bons pagadores, de modo que as empresas saibam quem são os bons pagadores, respeitando os limites da privacidade dos dados. A Lei do Cadastro Positivo permite o consumidor a retificar os seus dados, cancelar o registro, solicitar a revisão de decisões automatizadas e estabelece que não deverão ser feitas anotações de dados sensíveis dos consumidores (BRASIL, 2011).

---

[2] GOVERNO FEDERAL. **Consumidores poderão denunciar chamadas abusivas de telemarketing**. In: Governo Federal, Ministério da Justiça e Segurança Pública, Publicado em 20/07/2022. Disponível em: https://www.gov.br/mj/pt-br/assuntos/noticias/consumidores-poderao-denunciar-chamadas-abusivas-de-telemarketing. Acesso em: 08 de fev. de 2023.

Importante mencionar que tanto o Código do Consumidor, quanto a Lei do Cadastro Positivo, reforçam a responsabilidade objetiva e solidária nos casos em que o consumidor seja lesado em virtude do descumprimento das normas pelos agentes responsáveis pelo uso desses dados.

Sem embargo, Bruno Bioni (2020) assevera que antes da Lei Geral de Proteção de Dados, o Brasil não tinha uma estrutura normativa de leis setoriais que não passassem se uma "colcha de retalhos". Segundo o jurista, a falta de unicidade no ordenamento e de uma norma que regulasse o tratamento de dados pessoais fez com que os setores da economia ficassem inseguros em relação ao compartilhamento de dados para desenvolvimento de novos modelos de negócio, bem como para a própria formulação de políticas público-privadas.

Muito embora foram inúmeras as inovações jurídicas trazidas pelas normas já comentadas e por outras como a Lei do *Habeas Data* (Lei n. 9.057/1997), Lei do Acesso à Informação (Lei n. 12.527/2011) e Lei de Arquivos Públicos (Lei n. 8.159/1991); é importante afirmar que a LGPD é substancial, já que se dedica prioritariamente à proteção dos dados pessoais e garantir que os titulares das informações tenham o controle suas informações, pois é notório que está vinculado diretamente aos direitos fundamentais.

3.2 Marco Civil da Internet

Outra lei responsável pelo estabelecimento dos pilares da proteção dos dados no Brasil é o Marco Civil da Internet, Lei n. 12.965, de 23 de abril de 2014. Apesar da aludida norma centrar-se em estabelecer os princípios, garantias, direitos e deveres do bom uso da internet no país, é certo que a mesma contribuiu para a construção de um cenário democrático e mais seguro no âmbito do ciberespaço.

> O MCI se pretendeu como a "Constituição da Internet" no Brasil e salvaguardou diversos princípios e direitos fundamentais. A proteção da privacidade, dos dados pessoais e da liberdade de expressão são expressamente previstas no Marco Civil da Internet representando um grande avanço face ao cenário anterior ao diploma, que levava a uma quantidade maior de abusos e violações de direitos. Além disso, suas disposições são fundamentais para um ambiente saudável e seguro tanto para IoT quanto para AI, tendo em vista a necessidade, nesses cenários, de direitos como acessibilidade, segurança dos dados, privacidade, entre outros previstos no MCI (MAGRANI, 2019, p. 74).

A importância do Marco Civil da Internet se consubstancia na preocupação do legislador em garantir a proteção dos direitos humanos e fundamentais no âmbito virtual, em virtude de que a internet ganhava terreno e novas modalidades de violações de direitos e crimes começaram a ocorrer nesse espaço.

Consoante Carlos Affonso de Souza e Ronaldo Lemos (2016), o MCI foi preciso na formulação dos direitos e obrigações na internet apresentando-se como uma excelente ferramenta no combate dos cibercrimes, uma vez que obriga que os logs de conexão dos usuários sejam guardados pelo prazo de 1 ano e 6 meses. Os autores enfatizam que essa medida auxilia às investigações criminais e civis no combate aos delitos virtuais, posto que demonstra que a internet não é uma terra sem lei.

Nessa senda, estabelece a norma os seus fundamentos no art. 2º e seus incisos, que se constituem pelo: i) reconhecimento da rede mundial de computadores; ii) dos direitos humanos, do desenvolvimento da personalidade e do exercício da cidadania nos meios digitais; iii) pluralidade e diversidade no ciberespaço; iv) a internet é um espaço aberto e colaborativo que se fortalece numa comunidade virtual; v) da livre iniciativa, da concorrência e da defesa do direito do consumidor e; vi) da finalidade social da internet (BRASIL, 2014).

Apesar de não ser o objeto deste trabalho a análise minuciosa do MCI, convém ressaltar os seus princípios basilares que estão elencados nos incisos do art. 3º, da aludida norma, os quais constituem-se na: i) garantia da liberdade de expressão, comunicação e manifestação do pensamento; ii) privacidade; iii) proteção dos dados pessoais; iv) neutralidade de rede; v) preservação da rede; vi) responsabilidade dos agentes; vii) natureza participativa da rede; viii) liberdade dos modelos de negócios virtuais.

Consoante Doneda (2021), o MCI foi importante para o salto na proteção de dados porque preparou o terreno para a chegada da Lei Geral de Proteção de Dados, já que em estado germinal cuidou dos riscos dos impactos que seriam provocados pelo vazamento de dados e pela discriminação algorítmica.

Segundo Ricardo Villas Bôas Cuevas (2021), o MCI consagrou a reserva de jurisdição ao Poder Judiciário no que concerne à determinação da remoção de conteúdo ilícito disponibilizado na rede mundial, não sendo responsabilizado

o provedor do serviço pelo conteúdo publicado por terceiros, mas somente nos casos de descumprimento das ordens judiciais[3].

[3] Em um caso recente e para fins didáticos, um youtuber brasileiro conhecido como Bruno Aiub (Monark) teve sua conta do Youtube suspensa por determinação judicial do Tribunal Superior Eleitoral (TSE), em virtude da difusão de fake news relativas às eleições de 2022, pois alegava fraude na contagem dos votos. Além disso, a conta também foi denunciada pelos usuários da rede em razão do discurso proferido pelo youtuber ao defender a criação de um partido nazista no Brasil, durante a gravação de um *podcast* que contava com a participação da deputada Thabata Amaral e do deputado Kim Kataguiri. (Para mais detalhes, acessar: MAGALHÃES, Thais; TORTELLA, Tiago. Youtube bloqueia canal de Monark no Brasil. In: CNN, Publicado em 09 de novembro de 2022. Disponível em: https://www.cnnbrasil.com.br/politica/youtube-bloqueia-canal-de-monark-no-brasil/. Acesso em: 08/02/2023).

4 LEI GERAL DE PROTEÇÃO DE DADOS (LEI N. 13.709/2018)

A Lei Geral de Proteção de Dados - LGPD (Lei n. 13.709, de 14 de agosto de 2018) representa um marco legal importante para a proteção dos dados pessoais, pois a lei se reserva especialmente para tratar desse instituto. Esse movimento global da proteção de dados pessoais culminou à medida em que as tecnologias de informação e comunicação ganharam terreno e os dados pessoais se tornam a base da nova economia.

Consoante Tepedino, Frazão e Oliva (2019) os dados são substanciais na economia atual0 porque são o próprio objeto que impulsiona o mercado, porque é a partir dessa matéria que o mercado formula suas estratégias e gera capital. Os autores ainda mencionam que, em se tratando dos aspectos sociais, o uso dos dados pelos agentes de tratamento também modifica as relações sociopolíticas, quer seja positiva ou negativamente.

Um exemplo famoso sobre esse impacto nas relações sociopolíticas é o escândalo envolvendo a empresa *Cambridge Analytica* (CA). Em 2016, a qual atuava como mineradora de dados para campanhas eleitorais e foi responsável pela coleta de mais de 87 milhões de dados de usuários da rede social *Facebook* (atualmente denominada META) para beneficiar a campanha eleitoral de Donald Trump.

As estratégias da CA foram descobertas quando o ex-funcionário Christopher Wylie denunciou os métodos da empresa para obtenção desses dados e como essas informações eram utilizadas para construir a estratégia eleitoral de Donald Trump (KANG, 2018).

Tratava-se de um teste de personalidade disponibilizado pela plataforma Facebook, na qual os usuários que acediam para realizar o teste forneciam informações potenciais, como nome, localização, idade, gênero, etc; e, a partir dos vasculhamentos realizados nas redes sociais dessas pessoas, a empresa conseguia mapear as posições políticas de cada usuário, descartando os que não seriam potenciais eleitores de Donald Trump.

Por sua vez, até os amigos das pessoas que fizeram o teste tiveram seus perfis invadidos sem o consentimento/conhecimento, com fulcro em alcançar prováveis eleitores do candidato estadunidense. Os mesmos métodos também

foram utilizados para alavancar a campanha do Brexit, o qual resultou na saída do Reino Unido da União Europeia[4].

O caso da *Cambridge Analytica* não é o único escândalo[5] envolvendo o uso de dados pessoais de milhões de cidadãos para finalidades adversas, mas um dos principais acontecimentos que serviu de alerta para os perigos do uso indiscriminado dos dados pessoais e de como eles podem ser utilizados para finalidades adversas e antidemocráticas.

> Dados considerados "irrelevantes" ou "públicos" como idade, altura, nacionalidade, os locais de moradia e de trabalho podem servir de insumo para correlações, predições e ranqueamentos acerca da personalidade do titular dos dados pessoais ou de determinados grupos sociais. Essas decisões têm a capacidade prática de determinar "a vida das pessoas: desde a seleção de currículos para uma vaga de emprego, chegando até os seguros, acesso ao crédito e serviços do governo". Em suma, a criação de detalhados perfis a respeito dos cidadãos pode criar sérios riscos à sua personalidade na medida em que essas representações virtuais têm o condão de diminuir ou de aumentar oportunidades sociais "em aspectos centrais da vida humana", como "emprego, moradia, crédito, justiça criminal", justamente de acordo com a classificação ou o score conferido ao seu perfil. Dessa maneira, dados inexatos ou incompletos e vieses do programador do algoritmo, por exemplo, podem gerar predições, inferências e interpretações verdadeiramente discriminatórias acerca de um indivíduo ou de um segmento social (DONEDA *et.al*., 2021, 172-173).

Por essa razão, o art. 1º, da LGPD, anuncia que o principal escopo da lei é proteger os direitos fundamentais de liberdade, de privacidade e o livre desenvolvimento da pessoa humana quando os seus dados pessoais forem objeto de tratamento por pessoa natural/jurídica. Os pilares da LGPD se sustentam no respeito à privacidade, autodeterminação informativa, dos direitos humanos, das liberdades de expressão, desenvolvimento econômico e tecnológico e do direito do consumidor, conforme a leitura do art. 2º e incisos, da LGPD (BRASIL, 2018).

---

[4] KANG, Cecilia. **Facebook admite que Cambridge Analytica accedió a los datos de 87 millones de usuarios**. In: The New York Tomes, Publicado em 4 de abril de 2018. Disponível em: https://www.nytimes.com/es/2018/04/04/espanol/facebook-cambridge-analytica-87-millones.html. Acesso em: 18 de fev. de 2023.

[5] O caso mais conhecido sobre invasão da privacidade para fins de espionagem envolve a Agência Nacional de Segurança (NSA – National Security Agency) estadunidense, donde foi revelado pelo ex-funcionário Edward Snowden que Washington espionava os líderes soberanos de diversos países.

Segundo Caitlin Mulholland (2020), a autodeterminação informativa é um direito fundamental e está diretamente vinculada à proteção de dados pessoais porque se trata de uma defesa e prevenção do indivíduo ou da coletividade contra os desvios de finalidade nos atos de captação, tratamento e comunicação dos dados pessoais.

Ademais, a mesma advém do art. 21 do Código Civil, em conjunto com os artigos que tratam dos princípios do consentimento e da confiança, bem como da cláusula geral de responsabilidade objetiva (*Idem,* 2020).

No que concerne à aplicação da norma, o art. 3º e seus incisos, da LGPD, determinam que a mesma incide em todo território nacional e fora dele, quando os dados forem coletados/tratados em território nacional, ou, o tratamento desses dados for realizado para prestar bens ou serviços aos titulares que se encontram em território brasileiro (BRASIL, 2018). Diametralmente, o legislador também elencou no art. 4º quais os casos em que a LGPD não será aplicada, quando o tratamento dos dados pessoais for:

a) realizado por pessoa natural para fins particulares e não econômicos;

b) realizados para fins jornalísticos, artísticos ou acadêmicos;

c) realizado para fins de segurança pública, defesa nacional, segurança do Estado ou para investigação penal;

d) proveniente do território nacional e que não seja objeto de comunicação ou compartilhamento aos agentes de tratamento brasileiros ou com de outro país de onde esses dados não provém (BRASIL, 2018).

Importante ressaltar que para que o inciso III seja aplicado corretamente, deverá subsistir uma lei específica para estabelecer as medidas proporcionais e estritamente necessárias para atender o interesse público, observando toda a principiologia que rege os direitos fundamentais e do devido processo legal, conforme o previsto no parágrafo 1º, do art. 4º, da LGPD.

Por conseguinte, o legislador estabelece que o tratamento dos dados do inciso III, do art. 4º, da LGPD, não poderão ser utilizados por pessoa de direito privado quando os dados pessoais não estiverem sob tutela de direito público.

Também é importante destacar que a Autoridade Nacional de Proteção de Dados (ANPD) poderá emitir opiniões técnicas e recomendações para o uso

ético dos dados nos casos previstos no inciso referido anteriormente e solicitar aos agentes de tratamento o Relatório de Impacto à Proteção dos Dados Pessoais (RIPD) (Art. 4º, parágrafos 3º e 4º, da LGPD).

4.1 Base principiológica da proteção dos dados

Os princípios são as bases que norteiam as regras que conduzem a criação, interpretação e aplicação das leis. Não à toa, refletem-se constantemente, na medida em que o legislador os integra no corpo da norma para reafirmar o compromisso do Estado Democrático de Direito que se erige com base neles.

> Os princípios enunciam as diretrizes do ordenamento jurídico e, por conseguinte, fundamentam as regras criadas pelo aplicador do direito. São princípios cardeais de todo o direito à justiça e à equidade. Sua aplicação às situações jurídicas concretas dá-se por meio da incidência de um sem número de regras, como as relativas à responsabilidade civil (art. 187 e 927 do Código Civil), ou à redução da cláusula penal excessiva (art. 413 do Código Civil). Estas são normas que concretizam os princípios embora com eles não se confundam. Os princípios são tão fortes que, sequer, há necessidade de serem enunciados pelo legislador para que possam ser aplicados. Não raro, as normas postas na legislação simplesmente sobrepõem sua existência, sem que haja referência expressa. Há também princípios aplicáveis à parte do direito, como por exemplo, aqueles que regem a atuação da Administração Pública (art. 37 da Constituição Federal) ou mesmo princípios constitucionais, aplicáveis nas relações contratuais, como o princípio da dignidade da pessoa humana e da ordem econômica (AQUINO, 2021, p.59).

Nessa toada, a LGPD traz em seu bojo os princípios que deverão guiar os agentes de tratamento para assegurar a proteção de dados pessoais, quais sejam:

> 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 (BRASIL, 2018).

O princípio da finalidade constitui-se no tratamento de dados cujos fins deverão ser legítimos, específicos, explícitos e informados, e posteriormente, não poderão ser utilizados para finalidades incompatíveis com as finalidades anteriores. Esse dispositivo é semelhante ao da Diretiva 95/46/CE da União Europeia.

Por conseguinte, o princípio da adequação corresponde à compatibilidade do tratamento dos dados com as finalidades informadas ao titular, não devendo extrapolar/exceder esses limites.

Nesse prospecto, e em acordo com Tepedino, Frazão e Oliva (2019); o princípio da finalidade, da adequação e da necessidade estão atrelados, porque em todos os casos o tratamento dos dados deverá ocorrer com o consentimento prévio e informado do titular dos dados pessoais.

Assim, o princípio da necessidade consubstancia-se na minimização do uso dos dados, os quais estão limitados somente para atingir as suas finalidades de modo proporcional e não excessivo (BRASIL, 2018).

Em se tratando do princípio do livre acesso, Mulholland (2020) aduz que a lei garante o acesso pelos titulares aos seus próprios dados, sendo a consulta facilitada e de forma gratuita. O objetivo é assegurar que o titular possa averiguar se suas informações estão sendo usadas de acordo com suas finalidades e se os mesmos estão corretos e atualizados. É nesse mesmo sentido que se dirige

o princípio da qualidade, posto que os dados deverão estar atualizados, ser exatos, claros, cumprindo com os outros requisitos para o alcance da finalidade.

Por sua vez, a LGPD também dispõe sobre a transparência, a qual também se correlaciona com os outros princípios e tem o condão de assegurar que os titulares dos dados poderão obter as informações relativas ao tratamento de forma clara, precisa e facilmente acessíveis, desde já, resguardando os segredos comercial e de indústria.

Doneda (2021) explica que o objetivo é reduzir a assimetria que há no fluxo informacional e estabelecer uma relação mais sincera e menos danosa no trânsito de dados pessoais, com fulcro em tornar o processo menos obscuro.

Preocupando-se com a segurança desses dados, o legislador também insculpiu no rol de princípios da LGPD a segurança dos dados, com o escopo de garantir o controle de acesso e impedir vazamentos ou perda de dados (TEPEDINO; FRAZÃO; OLIVA, 2019).

Para tanto, os agentes de tratamento estarão obrigados a adotar medidas de segurança, técnicas e administrativas para proteção dos dados pessoais; e prevenir os incidentes de vazamento de dados (com base no art. 46º e seus respectivos parágrafos, da LGPD). O art. 47º, da LGPD, reforça essa obrigação dos agentes de tratamento, inclusive, de quaisquer que intervenha no processo de tratamento de garantir a segurança da informação[6].

No instante que o tratamento de dados não observar o disposto na LGPD, ou, quando não fornecer a segurança que o titular das informações espera, será considerado irregular (art. 44º, LGPD/2018). Em qualquer ocorrência de incidentes que afetem a segurança dos dados, o controlador deverá comunicá-los à ANPD e ao titular dos dados, conforme o art. 48º (BRASIL, 2018)[7]. Por esse motivo, o inciso VIII, do art. 6º, da LGPD, apregoa o princípio da prevenção, que corresponde à adoção de mecanismos para prevenir os incidentes que coloquem em risco a proteção dos dados pessoais.

---

[6] Trata-se da noção de *privacy by design*, a qual consiste na segurança e sigilo em todas as operações de tratamento de dados, que não se limitam apenas à implementação de medidas de segurança ou cumprimento dos parâmetros regulatórios, como também da própria conscientização do agente de tratamento de dados sobre o impacto de sua atividade (TEPEDINO; FRAZÃO; OLIVA, 2019).

[7] É válido ressaltar que o princípio da segurança dos dados já se fazia presente no Capítulo III, do Marco Civil da Internet.

A não discriminação se institui como um dos princípios basilares da proteção de dados pessoais, presente no inciso IX, do art. 6º, da LGPD. Insta mencionar que o art. 5º, da CRFB/1988, já estabeleceu que ninguém deverá ser objeto de discriminação. Então, nas operações de tratamento de dados não seria diferente, porque tanto o Constituinte, quanto o legislador infraconstitucional rechaçam a possibilidade do uso de dados pessoais para fins discriminatórios ilícitos ou abusivos.

Não obstante, o uso de dados que gerem alguma diferenciação, mas que sejam lícitos, isto é, estejam previstos em lei, poderão ser admitidos (vide art. 7º e 11º, da LGPD/2018). Nessa senda, Bioni (2020) explica que o uso de dados para fins lícitos para segmentação de riscos de créditos ou securitários podem ser admitidos, por exemplo, respeitadas as normas legais.

> Na medida em que a lei afirma que são vedadas práticas discriminatórias cujas finalidades sejam abusivas ou ilícitas, compreende-se que práticas discriminatórias que não tenham tais finalidades são consideradas permitidas. Esse entendimento é plenamente coerente com o que foi exposto anteriormente, e torna-se mais palatável na medida em que compreendemos que a natureza da discriminação é, na realidade, o estabelecimento de correlações, que geralmente incluem generalizações, algo absolutamente comum em nosso ordenamento jurídico. Ademais, é igualmente razoável supor que há uma diferença entre abusividade e ilicitude, caso contrário a lei não traria ambas as expressões. Necessário, portanto, definir cada um dos conceitos e buscar um caminho que possibilite a diferenciação dessas ideias. É o que se passa a fazer (BIONI, 2020, p. 761).

Na sociedade atual, a utilização de sistemas artificiais de decisões automatizadas tornou-se recorrente. O uso de Inteligência Artificial para tomada de decisões tem o objetivo de agilizar os serviços e facilitar a vida dos seus indivíduos, resolver problemas do cotidiano e movimentar o novo modelo econômico digital. A partir da análise de grandes volumes de dados (*Big Data*), as máquinas conseguem desenvolver o seu aprendizado por reforço e, mediante erros e acertos, chegar às decisões mais precisas.

No entanto, conforme aborda Frank Pasquale, em seu livro "*The Black Box Society: the secret algorithms that control money and information*", as decisões automatizadas implicam, muitas vezes, em decisões discriminatórias e enviesadas. Embora tenha enormes potenciais para o desenvolvimento socioeconômico, humano e político, o *Big Data* e sua aplicação em mecanismos

de Inteligência Artificial pode ampliar as desigualdades, principalmente, quando as decisões automatizadas resultam em violações dos direitos humanos[8] e fundamentais[9] (PASQUALE, 2015; BECK, 2021; BIONI, 2021; MULHOLAND, 2020).

Assim sendo, toda a estrutura principiológica da LGPD está vinculada. O inciso X, do art. 6º, da LGPD, traz consigo o princípio da responsabilização e prestação de contas (*accountability*). A tendência das normas de regulação da proteção de dados baseia-se nas noções de risco e de *accountability*, pois a responsabilidade da proteção dos dados pessoais é de todos os atores envolvidos no tratamento de dados, não devendo recair a responsabilidade somente no titular das informações que fornece o seu consentimento para o tratamento de dados.

Por isto, devem coexistir medidas de segurança capazes de mitigar os riscos das operações de tratamento de dados e análise dos possíveis impactos que podem advir em virtude de incidentes para garantir a segurança dos dados (BIONI, 2021).

4.2 Definições

A LGPD traz consigo algumas definições importantes para a proteção de dados. O art. 5º e seus incisos abarcam os principais conceitos para auxiliar o operador do direito na aplicação correta da norma. Alguns dos conceitos dispostos pela lei que são importantes para serem abordados são: dados pessoais, banco de dados, titular de dados, agentes de tratamento (controlador

[8] Vide o caso *State Wisconsin vs Loomis*, donde são denunciados o racismo e discriminação algorítmicos de raça, gênero, condição socioeconômica, entre outros; pelo uso do algoritmo de inteligência artificial *COMPAS - Correctional Offender Management Profiling for Alternative Sanctions*, o qual é usado para determinar a probabilidade de reincidência criminal das pessoas apenadas.

[9] O Projeto de Lei n. 21/2020, proposto pelo Deputado Federal Eduardo Bismarck (PDT-CE), tem como objetivo regular o uso da Inteligência Artificial no Brasil, estabelecendo os princípios, direitos e deveres para o seu uso. Segundo o projeto de lei, (o qual conceitua inteligência artificial como sistema computacional que tem objetivos definidos e faz previsões, recomendações ou toma decisões que impactam no mundo real e virtual) os princípios da igualdade e a não discriminação deverão ser garantidos quando se faça uso de IA nos processos decisórios que impactam na vida dos seres humanos e o seu uso deverá ser direcionado pela ética e pelo direito (CÂMARA DOS DEPUTADOS, 2020).

e operador), tratamento de dados, consentimento e o relatório de impacto à proteção dos dados pessoais (RIPD).

Segundo a definição atribuída pelo art. 5º, I e II, da LGPD, dado pessoal é qualquer informação que torne uma pessoa identificada ou identificável. Por outro lado, quando este dado compreende qualquer informação pessoal de caráter racial ou étnico, religioso, político, filiação a sindicato ou organização de caráter religioso, filosófico ou político; de saúde, sexual, genético ou biométrico; tem-se o que a lei denomina como dado sensível (BRASIL, 2018).

Dado sensível é qualquer informação que permita discriminar uma pessoa e implica riscos maiores ao titular, por isso merece uma proteção mais rígida (DONEDA *et.al*, 2021). Logo no inciso III, do art. 5º, o legislador traz o conceito de dado anonimizado, considerando como qualquer dado que não permita a identificação do seu titular com os métodos aplicados no seu tratamento.

Essas informações são armazenadas em banco de dados que, de acordo com o inciso IV, do art. 5º, é todo o conjunto de dados estruturados em um ou vários locais que podem ter suporte eletrônico ou físico. Longe de elaborar um estudo aprofundado em ciência de dados, um banco de dados compreende a "entrada (*inputs*) e processamento de dados e a saída (*output*) de uma informação [...] com o gerenciamento manual ou automatizado [...] para que seja extraído algum conhecimento" (BIONI, 2020, p. 57).

Em se tratando do titular dos dados, a lei refere-se à pessoal natural cujos dados são o objeto de tratamento. Segundo Doneda *et.al* (2021), titular de dados não se limita apenas às pessoas naturais identificadas ou identificáveis, porque se trata de um direito humano disposto no art. 5º, da CRFB/88.

Nesta senda, o constituinte alude que a titularidade possui diversas posições jurídicas subjetivas possíveis, variando de acordo com os critérios de cidadania, idade, eventual incapacidade por força de deficiência, etc. Nesse prospecto, o jurista explica que a CF/88 cuidou expressamente em tutelar os direitos fundamentais a toda e qualquer pessoa brasileira ou estrangeira que resida no país, porque também é um direito humano universal a todos (DONEDA *et.al,* 2021).

Prosseguindo nas definições, o legislador estabeleceu as duas figuras que podem ser consideradas como agente de tratamentos de dados. Consoante o inciso IX, do art. 5º, os agentes de tratamento podem ser tanto controladores

quanto operadores. Não obstante, traz a diferença de cada um desses atores, pois hierarquicamente se distinguem. Controlador é toda pessoa natural ou jurídica, de direito público ou privado, responsável pelas decisões referentes ao tratamento de dados; conquanto o operador é a pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados e é subordinado ao controlador (Art. 5º, incisos VI e VII, da LGPD, 2018).

Tepedino, Frazão e Oliva (2019) advertem que a titularidade dos dados não se transfere a nenhum dos agentes de tratamento, pois essas informações são personalíssimas e intransmissíveis, sendo elementos inerentes à pessoa humana e, portanto, que pertencem ao titular dos dados.

Com efeito, o tratamento de dados é qualquer operação com dados pessoais que objetiva coletar, produzir, armazenar, recepcionar, classificar, acessar, reproduzir, transmitir, distribuir, processar, arquivar, armazenar, eliminar, avaliar ou controlar as informações; bem como modificar, comunicar, transferir, difundir ou extraí-las (Art. 5º, inciso X, LGPD, 2018).

Para Bioni (2020), essa lista de ações expostas pelo legislador revela a preocupação pela mitigação dos riscos que essa atividade implica aos direitos do titular, porque quanto maior o volume de dados muito maiores são as chances de as informações serem utilizadas sem um processo de anonimização[10], por exemplo, ou, facilitar a extração de dados sensíveis, como saúde, geolocalização, financeiro, etc.

Por sua vez, o legislador também traz a definição do consentimento, objeto deste estudo, como a manifestação livre, informada e inequívoca do titular, a qual confirma que este permite o tratamento de seus dados pelo agente de tratamento para atingir uma finalidade determinada (BRASIL, 2018).

Doneda *et.al* (2021, p. 238) explica que o consentimento, nesta linguagem do legislador, revela que “o titular do dado tem de ter ao seu dispor as informações necessárias e suficientes para avaliar corretamente a situação e a forma como seus dados serão tratados”.

[10] O processo de anonimização, em acordo com o art. 5º, XI, da LGPD; consiste na utilização de meios técnicos adequados que permitem impossibilitar a identificação do titular dos dados, direta e indiretamente. Muito embora existam métodos que tornam possível a identificação do indivíduo a partir de dados aleatórios anonimizados, a pretensão do legislador é justamente dificultar essa possibilidade, porque existe essa chance de todo o processo de anonimização ser revertido (BIONI, 2020).

Tendo isso em vista, para assegurar a proteção dos dados pessoais dos titulares e mitigar os possíveis impactos pelo tratamento de suas informações pelos agentes de tratamento, a LGPD define, em seu art. 5º, XVII, o Relatório de Impacto à Proteção dos Dados Pessoais (RIPD) como instrumento comprobatório que descreva quais os processos e técnicas foram adotados pelos agentes durante o tratamento dos dados pessoais (BRASIL, 2018).

O referido artigo revela que a função primordial do RIPD é esboçar os processos utilizados pelos agentes de tratamento durante o tratamento das informações que podem gerar prejuízos às liberdades e direitos fundamentais dos titulares, de modo a apresentar quais são os mecanismos aplicados para mitigação desses danos.

Doravante, o art. 38º, da LGPD, indica que a ANPD – Autoridade Nacional de Proteção de Dados tem o poder de determinar a elaboração do RIPD ao controlador, inclusive os dados sensíveis, respeitando os limites do segredo comercial e industrial (BRASIL, 2018). A ANPD é definida no art. 5º, XIX, da LGPD; como órgão da administração pública encarregado de zelar, implementar 0e fiscalizar o cumprimento da LGPD no território nacional.

É no parágrafo único, do art. 38º, que o legislador determina quais as informações mínimas que deverão constar no RIPD, quais sejam: i) descrição dos dados coletados, ii) metodologia aplicada para coleta, iii) metodologia aplicada para garantia da segurança das informações, iv) análise do controlador relativas às medidas e salvaguardas aplicadas para mitigar os riscos adotados (*Idem*, 2018).

Consoante Bruno Bioni (2020), o Relatório de Impacto possibilita ao titular dos dados pessoais o controle de suas informações, além de garantir que este seja o tomador da decisão para se opor ao tratamento de seus dados. Isso revela que o principal objetivo é assegurar os princípios da transparência, minimização dos riscos e o legítimo interesse do titular, visto que as atividades podem extrapolar os limites das finalidades e, somente dando poder ao titular, os seus dados poderão ser controlados por este.

Por conseguinte, o tomador deverá aplicar mecanismos que mitiguem os danos com fulcro em efetivar o disposto na lei, por isto, a relevância do RIPD para vigiar as atividades de tratamento de dados e sua conformidade com a norma.

4.3 Direitos dos titulares dos dados pessoais

A LGPD elenca, do art. 17º ao art. 22º, os direitos concernentes ao titular dos dados pessoais. Como já fora mencionado anteriormente, o titular de dados é pessoa natural (tendo em vista o que considera o art. 5º, da CRFB/88, como qualquer pessoa nacional ou estrangeira residente no país).

Para o art. 17º, toda pessoa natural é titular dos dados e serão garantidos os seus direitos fundamentais de liberdade, de intimidade e privacidade (BRASIL, 2018). Nessa esteira, o art. 18º enuncia quais são os direitos que o titular dos dados poderá obter do controlador de dados responsável pelo tratamento de suas informações, *in verbis*:

> Art. 18. O titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição:
> 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;
> 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 (BRASIL, 2018).

A partir da leitura desses dispositivos é possível inferir que o legislador tem o interesse de concretizar e delimitar o âmbito do direito fundamental à proteção de dados, pois “relaciona-se com os direitos fundamentais constitucionalmente tutelados e tem função de direito negativo (defesa) e positivo (prestações)” (DONEDA, *et.al,* 2021, p. 104).

É uma forma de concretizar os princípios da proteção de dados e retomar o controle dos dados ao indivíduo cujas informações são objeto de tratamento (BIONI, 2020). Para tanto, os parágrafos do art. 18º, da LGPD, elucidam que o titular dos dados poderá peticionar em detrimento do controlador perante à ANPD, que é o órgão responsável por fiscalizar o cumprimento da LGPD, inclusive, nos casos em que o consentimento é dispensado. Nesse sentido, em qualquer caso de descumprimento da norma, o titular poderá questionar o tratamento de seus dados e se opor a ele.

Por sua vez, o art. 19º e seus incisos informam que a confirmação de existência ou acesso aos dados pessoais mediante a requisição do titular deverá ser feita de forma simplificada, imediata ou por meio de declaração clara e completa, informando desde a origem dos dados à finalidade do tratamento, resguardados os segredos comercial e industrial. Cabe também a possibilidade de o titular solicitar essas informações tanto pela via eletrônica, quanto pela forma impressa (BRASIL, 2018).

Outro dispositivo que mais se destaca na LGPD é o art. 20º. Nela, o legislador legitima a possibilidade de o titular obter a revisão das decisões automatizadas com base no tratamento de seus dados pessoais, devendo o controlador fornecê-las, resguardados o segredo industrial e comercial.

Insta salientar que um dos principais mecanismos aplicados para a tomadas de decisões automatizadas é a Inteligência Artificial, a qual vem tomando proporções gigantescas, na medida em que a força humana é substituída por máquinas.

Um dos objetivos do uso da inteligência artificial para execução das decisões é aprimorar os serviços e torná-los mais ágeis, contudo, o seu uso vem gerando controvérsia, vez que são inúmeros os casos em que a máquina de IA emana decisões contraditórias e que ferem direitos e garantias fundamentais. Em 2016 a Inteligência Artificial da Microsoft, chamada Tay, desenvolvida para conversar e interagir com humanos através da rede social Twitter, adotou posturas racistas e homofóbicas. O caso imediatamente fez com que a Microsoft viesse à público pedir desculpas e, consequentemente, desativar a IA das redes sociais[11].

[11] VICTOR, Daniel. **Microsoft created a twitter bot to learn from users**. It Quickly became. In: the New York Times, Publicado em 24 de março de 2016. Disponível em:

Um outro caso concreto disso é a aplicação desses sistemas na segurança pública, posto que há um enorme risco de a tecnologia estigmatizar determinada parcela da sociedade pelas características fenotípicas físicas e de condutas, principalmente, das populações socialmente marginalizadas vítimas do racismo estrutural. Foi o que o Ministro Benedito Gonçalves, do Superior Tribunal de Justiça, decidiu em sede de Habeas Corpus, em 2020, no HC: 631298-BA.

Conforme a decisão exarada pelo ministro do Egrégio, o paciente impetrou o remédio constitucional em face do Secretário de Segurança Pública, Comandante da Polícia Militar e do Governador do Estado da Bahia, pelo uso indiscriminado de mecanismos imprecisos de reconhecimento facial nos transportes públicos para o monitoramento da população durante a Pandemia de SARS-COV-2.

De acordo com as alegações, o uso desses instrumentos implica na violação dos direitos fundamentais da população baiana, sobretudo, da população negra e residentes em zonas marginalizadas da Bahia. O paciente ressalta que não há rito para tratamento adequado dos dados pessoais e sensíveis obtidos pela captura de fotos, o que resultaria na abordagem de policiais pelas suas características físicas (pessoa negra, moradora da periferia), vez que o uso de máscaras torna mais difícil a identificação dos usuários de transportes públicos.

Consoante Miriam Wimmer e Danilo Doneda (2021), é importante ressaltar que os sistemas de Inteligência Artificial são propensos às falhas, sobretudo quando as decisões estão enviesadas, isto é, quando se caracterizam por critérios não neutros para a tomada de decisão. Ademais, emerge outro problema quando esses sistemas decisórios são utilizados para substituir decisões humanas, por essa razão, a necessidade de revisão humana com fulcro em intervir nos casos em que não são seguidos os parâmetros éticos e jurídicos.

Assim sendo, o legislador complementa, nos artigos 21º e 22º, que os dados pessoais referentes ao exercício regular de direitos não podem ser utilizados em seu prejuízo e poderá apresentar em juízo a defesa de seus

---

https://www.nytimes.com/2016/03/25/technology/microsoft-created-a-twitter-bot-to-learn-from-users-it-quickly-became-a-racist-jerk.html. Acesso em: 20 de fev. de 2023.

interesses individual ou coletivamente para a defesa dos seus direitos individuais e coletivos (BRASIL, 2018).

5 O CONSENTIMENTO E SUAS ADJETIVAÇÕES COMO PILAR DA PROTEÇÃO DE DADOS PESSOAIS

O consentimento é um dos principais pilares da LGPD, pois legitima o tratamento de dados e coaduna com a autodeterminação informativa, uma vez que empodera o titular dos dados pessoais no controle de suas informações e as finalidades do seu uso.

Segundo a LGPD, no art. 5º, inciso XII, o consentimento é entendido como a manifestação livre, informada e inequívoca do titular dos dados pessoais para o tratamento de suas informações para o alcance de uma finalidade determinada (BRASIL, 2018).

Por conseguinte, o art. 7º, inciso I, da LGPD reforça que o tratamento dos dados pessoais somente poderá ser realizado se o titular fornecer o seu consentimento, devendo constituir-se pelos elementos já mencionados pelo art. 5º, inciso XII.

Sem embargo, não é um direito absoluto, visto que a lei determina as situações em que sua aplicabilidade será dispensada, consoante o art. 4º e incisos, da LGPD. Contudo, isso não desobriga os agentes de tratamento de dados, sejam eles públicos ou privados, a respeitarem os princípios e direitos previstos na norma de proteção de dados, pois:

> [...] foi estabelecido um modelo legislativo no Brasil que privilegia a prevenção de danos à pessoa humana e a segurança no tratamento de dados pessoais, instituindo deveres e responsabilidades específicas aos agentes, além do amplo rol de princípios e direitos aos titulares dos dados. Busca-se antecipar os riscos de violação à privacidade, como também evitar tratamentos abusivos de informações e vazamentos de dados (TEPEDINO; DE TEFFÉ, 2020, p. 88).

Nesse prospecto, o interesse do legislador é de assegurar o uso ético, legítimo, transparente e seguro dos dados do titular, mesmo que este não tenha dado o seu consentimento, nas situações destacadas pela lei. Tal preocupação advém em virtude do ritmo acelerado que os dados pessoais são coletados, dada a relevância dessas informações para o novo modelo econômico atual.

Como bem explica Shoshana Zuboff (2018), no ano de 2018 o mercado mundial de “lares inteligentes” cresceu exponencialmente, podendo chegar aos 153 milhões de dólares em 2023. De acordo com a socióloga, isto se deve porque a coleta dos dados pelo sistema inteligente permite coletar mais informações de outros dispositivos conectados na casa através dos servidores do Google.

Assim, o usuário que aceita os “*Termos e Condições*” para poder fazer uso dos serviços hiperconectados não tem consciência do impacto que o consentimento implica para a proteção de seus dados pessoais genéricos e sensíveis. Zuboff (2018) reitera que se o cliente desses serviços se negar a fornecer essas informações, não poderá desfrutar de um serviço confiável, estando comprometidas as funcionalidades corretas dos dispositivos.

Outras situações que comprometem a validade do consentimento refletem-se nos serviços oferecidos pelas empresas de tecnologia, que não cobram aos seus usuários pelos serviços oferecidos, mas que por trás da gratuidade dos serviços existe o acesso a suas informações privadas, como mensagens de texto, criação de perfis de usuário, acesso aos contatos, geolocalização, etc; para fins de comercialização (TEPEDINO; DE TEFFÉ, 2020).

A gigante *Alphabet*, empresa-mãe do *Google*, está sendo demandada pela Justiça estadunidense pela coleta de dados biométricos dos cidadãos do estado do Texas sem o consentimento dos seus titulares. Segundo a denúncia, a empresa está coletando informações de seus usuários dos serviços do Google Fotos, Assistente de voz do Google e Nest Hub Max (assistente virtual de vídeo que compete com o Echo Show da Amazon)[12]. A empresa Meta (anterior Facebook) também foi acusada de coletar dados biométricos de cerca de 100 milhões de usuários sem o consentimento para fins de comercialização, no ano de 2020, na Califórnia[13].

---

[12] SANTINO, Renato. **Google é acusado de coletar dados biométricos de milhões sem permissão**. In: Terra, Publicado em 21 de out. de 2022. Disponível em: https://www.terra.com.br/byte/google-e-acusado-de-coletar-dados-biometricos-de-milhoes-sem-permissao,42d3d3708b1c6d50a51f42a39eb88587a3wgy5oc.html. Acesso em: 20 de fev. de 2023.

[13] SILVA, Victor Hugo. **Instagram é acusado de coletar dados biométricos sem autorização**. In: Tecnoblog, Publicado em 12 de agosto de 2020. Disponível em: https://tecnoblog.net/noticias/2020/08/12/instagram-e-acusado-de-coletar-dados-biometricos-sem-autorizacao/. Acesso em: 20 de fev. de 2023.

Daí, a importância e o cabimento da LGPD, pois essa troca de informações entre as grandes empresas coloca o usuário em uma posição de hipervulnerabilidade, já que os dados pessoais têm grande potencial no mercado e permite controlar o usuário enquanto consumidor de bens e serviços.

Por essa razão, é fundamental que o indivíduo tenha poder sobre as suas informações e da forma como elas serão utilizadas por outro particular/empresa/Estado, já que corporações gigantescas como Meta, Google, Microsoft, Apple, Alibaba, Amazon, IBM e dentre outras; detêm o monopólio no mercado das tecnologias informáticas e o consumidor acaba sendo sujeito vulnerável ao poder delas.

Na teoria geral dos contratos, o consentimento é base para realização dos negócios jurídicos bilaterais ou plurilaterais, pois a vontade das partes vai na direção de um único objetivo. Desta forma, o consentimento deve ser livre e espontâneo para o negócio jurídico ser válido, sob o risco de ser afetado pelos vícios ou defeitos do negócio jurídico (erro, coação, dolo, estado de perigo, lesão, fraude contra credores) (AQUINO, 2021).

De acordo com o estudo feito pela Fundação Getúlio Vargas (FGV) e o Conselho Europeu de Direitos Humanos para Usuários da Internet, dificilmente os usuários da internet entendem o que está disposto nos termos de serviço das plataformas digitais e acabam consentindo sem pensar nas consequências que as decisões não plenamente informadas aos seus direitos humanos e fundamentais e de como os dados são processados.

> Cláusulas relacionadas à coleta de dados exigem que os usuários concordem com a coleta de certos tipos de informações – geralmente apenas algumas são especificadas como exemplos – sem detalhar para quais fins elas podem ser usadas. Um exemplo dessa prática é o *Airbnb*, que informa aos usuários que irá coletar, armazenar e processar informações fornecidas durante o cadastro e uso da plataforma, bem como dados coletados automaticamente: recebemos, armazenamos e processamos informações que você nos disponibiliza quando acessa ou usa nossa plataforma. Os exemplos incluem quando você: preenche qualquer formulário na plataforma, como quando você se registra ou atualiza os detalhes de sua conta de usuário; acessar ou usar a plataforma, como pesquisar ou postar serviços de acomodações, fazer ou aceitar reservas, pagar por acomodações, reservar ou pagar por quaisquer serviços associados que possam estar disponíveis (como, mas não limitado a, limpeza), postar comentários ou avaliações, ou se comunicar com outros usuários; […] Também podemos receber, armazenar e processar *log data*, que são informações registradas automaticamente por nossos servidores sempre que você acessa ou usa a plataforma, independentemente de

> você estar registrado no *Airbnb* ou conectado à sua conta do *Airbnb*, como seu endereço IP, a data e a hora em que você acessa ou usa a plataforma, o *hardware* e o *software* que está usando, as páginas e *URLs* de referência e saída, o número de cliques, as páginas visualizadas e a ordem dessas páginas e a quantidade de tempo gasto em páginas específicas. […] Também podemos usar *web beacons* e *URLs* de rastreamento em nossas mensagens para você para determinar se você abriu uma determinada mensagem ou acessou um determinado *link*. Ainda que a coleta desses dados possa ser pensada para oferecer serviços mais personalizados – ou seja, serviços baseados nos interesses dos usuários identificados a partir do tratamento de seus dados pessoais – o texto não especifica como esses dados serão utilizados e o tipo de suposições que podem ser extraídas deles por meio de práticas de criação de perfil, por exemplo. Cláusulas semelhantes podem ser encontradas em várias das plataformas analisadas. Os Termos de Serviço do *Dropbox*, por exemplo, estabelecem que além dos dados cadastrais e de uso, outras informações, inclusive dados de localização, serão coletadas automaticamente quando disponíveis (VENTURINI; LOUZADA; MACIEL; ZINGALES; STYLIANOU; BELLI, 2016, p.61-62)[14].

Doneda *et.al.* (2021) explica que a proteção de dados se torna um direito fundamental porque o poder econômico, social e político exercido pelas grandes corporações produz desequilíbrios entre os atores envolvidos, neste caso, o usuário-indivíduo que se encontra em posição desfavorável. O consentimento do titular/usuário colide com as limitações da autonomia privada, pois o acesso aos bens e serviços depende dos contratos de adesão e, muitas vezes, obriga o

[14] Clauses related to data collection require users to consent with the collection of certain types of information – usually only a few are specified as examples – without detailing for which purposes they may be used. One example of this practice is Airbnb, which informs users that it will collect, store and process information provided during registration and use of the platform, as well as data collected automatically: We receive, store and process information that you make available to us when accessing or using our Platform. Examples include when you: fill in any form on the Platform, such as when you register or update the details of your user account; access or use the Platform, such as to search for or post Accommodations, make or accept bookings, pay for Accommodations, book or pay for any associated services that may be available (such as but not limited to cleaning), post comments or reviews, or communicate with other users; […] We may also receive, store and process Log Data, which is information that is automatically recorded by our servers whenever you access or use the Platform, regardless of whether you are registered with Airbnb or logged in to your Airbnb account, such as your IP Address, the date and time you access or use the Platform, the hardware and software you are using, referring and exit pages and URLs, the number of clicks, pages viewed and the order of those pages, and the amount of time spent on particular pages. […] We may also use web beacons and tracking URLs in our messages to you to determine whether you have opened a certain message or accessed a certain link.
Even though the collection of such data can be designed to off er more personalized services – that is, services based on users' interests identified from the processing of their personal data – the text does not specify how this data will be used and the type of assumptions that can be extracted from them through profiling practices, for example. Similar clauses can be found in several of the analyzed platforms. The Terms of Service of Dropbox, for example, state that besides registration and usage data, other information, including location data will be collected automatically when available (VENTURINI; LOUZADA; MACIEL; ZINGALES; STYLIANOU; BELLI, 2016, p.61-62).

usuário/titular a aceitar as condições para ter o acesso, deste modo, Doneda *et.al.* (2021) afirma que esse comportamento esvazia a autonomia individual e o direito fundamental à autodeterminação informativa e abre margem para a invalidade do consentimento.

> Ocorre que, não raras vezes, o titular dos dados pessoais se encontra em situação de vulnerabilidade nessa relação contratual eletrônica. Primeiro, pois, como já dito, os termos das políticas de privacidade podem ser demasiadamente complexos e abstratos, impossibilitando uma compreensão mais transparente a respeito do concreto emprego dos dados. Segundo, porque vários desses termos negociais se baseiam em uma lógica binária "*take it or leave it*": consentir ou não consentir, sem outras opções. Entretanto, ao não consentir, o custo é o de não desfrutar o serviço almejado, v.g., o uso de uma rede social ou de um aplicativo on-line. Dessa forma, mesmo estando exposto a tamanhos riscos, o titular dos dados pessoais pode acabar realizando seu consentimento com base em proveitos, tais como: a conexão com suas amizades, a disponibilidade de meios de comunicação em tempo real, a possibilidade de ouvir músicas e assistir a filmes etc. Assim, muitas vezes esse consentimento é meramente aparente, sendo questionável sua contribuição para o objetivo de proteger o titular dos dados. Portanto, coloca-se em dúvida o grau concreto pelo qual ele reflete a autonomia decisória desse titular (BIONI, 2020, p. 170-171).

Tendo esses detalhes em vista, a LGPD elucida, no art. 7º, §4º, que o consentimento será dispensado quando os dados se tornarem manifestamente públicos pelo titular, contudo, resguardando os direitos do titular e os princípios que regem a proteção de dados.

Por outro lado, se o controlador dos dados obteve o consentimento do titular e pretende compartilhar essas informações com outros controladores, deverá obter o consentimento específico do titular para essa finalidade, ressalvadas as hipóteses já previstas em lei (BRASIL, 2018).

> Primeiro, por adjetivar extensivamente o consentimento seguindo a linha evolutiva do direito comunitário europeu e da quarta geração de leis de proteção de dados pessoais. O consentimento deve ser livre, informado, inequívoco e dizer respeito a uma finalidade determinada de forma geral e, em alguns casos, deve ser, ainda, específico. Segundo, porque grande parte dos princípios tem todo o seu centro gravitacional no indivíduo: a) de um lado, princípios clássicos, como a transparência, a especificação de propósitos, de acesso e qualidade de dados por meio dos quais o titular do dado deve ser munido com informações claras e completas sobre o tratamento de seus dados e, ainda, ter acesso a eles para, eventualmente, corrigi-los; b) de outro lado, princípios mais "modernos", como adequação e necessidade, em que o tratamento dos dados deve corresponder às legítimas expectativas do seu titular. Isso deve ser perquirido de acordo com a finalidade especificada para o tratamento dos dados, assegurando-se

> que os dados sejam pertinentes, proporcionais e não excessivos (minimização dos dados). Terceiro, porque há uma série de disposições que dão um regramento específico para concretizar, orientar e, em última análise, reforçar o controle dos dados pessoais por meio do consentimento. Por exemplo: a) consentimento deveria ser extraído por meio de “cláusulas contratuais destacadas”; b) autorizações genéricas (sem uma finalidade determinada) seriam nulas; e, principalmente, c) nas hipóteses em que não há consentimento se deveriam observar os direitos e princípios da LGPD, de modo que haja a possibilidade de o titular dos dados pessoais se opor ao tratamento de seus dados (BIONI, 2020, p. 215-216).

Do mesmo modo, o §6º, do art. 7º, da LGPD, reforça que a dispensa da exigência do consentimento não exime os agentes de tratamento no cumprimento das demais obrigações previstas na lei, principalmente os princípios gerais da proteção de dados e os direitos do titular. Assim mesmo, o §7º, do art. 7º, reitera que o tratamento posterior dos dados, ao qual se referem os parágrafos 3º e 4º, só poderá ser realizado para novas finalidades quando os propósitos forem legítimos e específicos e os direitos do titular forem preservados, além da observância de todo o disposto na LGPD (BRASIL, 2018).

Em todos os casos donde o consentimento se exige, deverá ser formalizado por escrito ou outro meio que demonstre a manifestação da vontade do titular, conforme determina o art. 8º, da LGPD. Nos parágrafos do art. 8º, extrai-se não basta o consentimento por escrito, é necessário constar como cláusula destacada das demais cláusulas contratuais. Assim, no caso de que haja dúvida sobre a validade do consentimento, o ônus da prova caberá ao controlador para demonstrar que o consentimento foi obtido nos conformes da lei. Além disso, a lei veda o tratamento de dados quando há vício de consentimento.

Para Aquino (2021), com a globalização das relações jurídicas os contratos foram massificados, em virtude disso, a vontade de contratar deve ser protegida dela mesma quando há vícios do consentimento, prezando pelos princípios da boa-fé, da equivalência das prestações e função social dos contratos, com fulcro em evitar o desequilíbrio das relações jurídicas.

O intuito do legislador é adequar o consentimento à finalidade do tratamento, de acordo com o contexto a que está inserido e observando os parâmetros rígidos quando se tratar de dados sensíveis (DONEDA, 2021). Desta forma, o legislador preocupa-se em nulificar os tratamentos de dados cujas

autorizações genéricas, devendo o consentimento referir-se às finalidades determinadas (art. 8º, parágrafo 4º, LGPD).

O consentimento poderá ser revogado a qualquer momento. A pedido expresso do titular dos dados, por meio gratuito e facilitado, desde que os tratamentos realizados estejam amparados pelo consentimento anteriormente facilitado e quando não houver sido requerida a eliminação dos dados pessoais (Art. 8º, parágrafo 5º, LGPD, 2018).

Salienta-se que a necessidade do consentimento não é um direito absoluto, no entanto, é elemento fundamental para a proteção de dados, uma vez que a circulação dos dados pessoais deve ser limitada ao uso ético e determinado, justamente para não extrapolar os limites e provocar uma assimetria entre titular e agente de tratamento.

Principalmente, o tratamento dos dados não pode ser uma atividade que obste o livre desenvolvimento da personalidade do indivíduo, devendo as relações entre esses atores erigidas pelos princípios da Lei Maior, LGPD e demais normas setoriais, sobretudo, pela boa-fé.

Isto porque no cotidiano, na vida real/analógica, é incomum solenizar todos os atos da vida cotidiana, como, por exemplo, assinar termos de consentimento quando uma pessoa acaba fotografando ou gravando um vídeo de um monumento histórico e registrar, sem querer, o rosto de uma outra pessoa desconhecida; ou, quando blogueiros e *youtubers* gravam vídeos nas ruas sem pedir o consentimento das pessoas que são registradas nos vídeos. Longe de afirmar que o direito não tutela os direitos aqui implicados, o que se pretende afirmar é que se necessita uma cultura engajada na proteção de dados e, sobretudo, no consentimento, porque ele está vinculado à autonomia da vontade do indivíduo que é o titular dos dados.

Nesse prospecto, entende-se que o tratamento dos dados pessoais deve-se guiar pelo uso ético e prescrito em lei, pois o mau uso das informações pode resultar em problemas maiores, como a ampliação das desigualdades socioeconômicas, tensões geopolíticas, de manipulação em massa, vigilância e comercialização dos dados de forma indiscriminada, dentre outros. Além disso, é importante retomar o protagonismo do consentimento, pois ele está intrinsicamente relacionado à autodeterminação informativa e, consequentemente, ao desenvolvimento pleno da personalidade do indivíduo.

Desta forma, o operador do direito, ao interpretar e aplicar a norma, deverá analisar o contexto no qual circunda o consentimento para averiguar se o mesmo será válido ou se subsistem desigualdades que vulneram o titular dos dados pessoais.

6 CONSIDERAÇÕES FINAIS

O presente trabalhou debruçou-se no estudo da Lei Geral de Proteção de Dados, atravessando todo o contexto que gira em torno da privacidade para a construção do que se concebe atualmente como direito fundamental à proteção de dados. Por se tratar de uma temática complexa, transdisciplinar e que perpassa por todos os setores da sociedade; o estudo tem o interesse de demonstrar a importância do consentimento e suas adjetivações e como ele dirige o tratamento dos dados para o seu uso ético.

Para tanto, o trabalho foi desenhado em 4 capítulos que permitem traçar uma linha cronológica, partindo da construção do conceito de privacidade e de como ele foi importante para a configuração da proteção dos dados até a chegada das normas setoriais que já abordavam a temática e abriam margem para o surgimento da LGPD. Destaca-se o Marco Civil da Internet porque fora um dos diferenciais no tratamento de dados, uma vez que já dispunha sobre a importância do consentimento livre, expresso e informado.

No primeiro capítulo destacou-se a evolução do direito à privacidade a partir de uma revisão do *paper* de Warren e Brandeis, os quais trouxeram a primeira definição de privacidade a qual se compreende como "*right to be alone*" (direito de ser deixado só) e representa um marco do regime da proteção de dados. Por sua vez, apresenta-se as principais normas internacionais que já tutelavam o direito à privacidade e o atribuía como um direito humano e universal.

Com a Convenção 108, da União Europeia, deu-se os primeiros passos para a proteção de dados pessoais no tratamento de dados automatizados, importante para o desenvolvimento do *General Data Protection Regulation* europeu. Em se tratando do GDPR, forte inspiração para a LGPD brasileira, o seu arcabouço jurídico definiu o conceito de dados pessoais, tratamento de dados, agentes de tratamento e outras figuras importantes responsáveis pelas operações que fazem uso de dados pessoais. Não obstante, trata-se de uma síntese de todas as outras normas que já tratavam sobre a privacidade e dados pessoais, principalmente, a Diretiva 97/46/CE.

Por conseguinte, o capítulo 2 (dois) explanou os marcos regulatórios nacionais que abriram o caminho para o surgimento da LGPD no ordenamento jurídico pátrio. Como foi visto, o primeiro documento legal a ser revisado trata-se da Constituição Federal de 1988, pois é na Lei Maior que se respalda os principais alicerces da proteção de dados, posto que o Constituinte deixou implícito o direito à proteção de dados pessoais como direito autônomo.

Nessa mesma esteira, do ponto de vista infraconstitucional, tem-se o Marco Civil da Internet, de 2014, o qual foi o divisor de águas, pois estabeleceu os princípios fundamentais para o uso ético da internet e garantia de direitos aos seus usuários, sobretudo, em se tratando da privacidade e fluxo de dados pessoais.

Assim, tendo em vista as normas setoriais e princípios dispersos pelo ordenamento jurídico, o capítulo três abordou o pilar deste trabalho: a Lei Geral de Proteção de Dados. Foram analisadas as bases principiológicas da LGPD, as definições e os direitos dos titulares de dados estabelecidos pelo legislador.

A partir da análise da LGPD, é possível inferir a preocupação do legislador em tutelar os dados pessoais, em virtude de que a sociedade atual é regida pela economia pautada nos dados, tendo estes como principal fonte de capital para os negócios.

Nesse sentido, toda informação é potencial para os agentes de tratamento e, por se tratar de uma fonte de conhecimento sobre as pessoas, merece uma proteção especial. Esse argumento respalda-se em casos muito concretos, como *Cambridge Analytica* em que os dados pessoais podem ser manipulados para benefício de determinados grupos da sociedade, para fins de manipulação, controle e até vigilância.

Por essa razão, o presente trabalho tem como principal objeto a análise do consentimento (capítulo 4), porque é um dos principais elementos que conformam o direito à proteção dos dados. O consentimento relaciona-se com todos os demais princípios tutelados pela LGPD, principalmente, a autodeterminação informativa, posto que permite o titular dos dados ter o controle de sua informação e lhe dá o poder de gerir o tratamento de dados.

Portanto, a figura do consentimento apresenta-se como um dos elementos legais fundamentais para o tratamento de dados, pois a pessoa natural tem o direito a controlar as suas informações, uma vez que todas elas

constituem elementos de sua personalidade e são imprescindíveis para o desenvolvimento da pessoa humana. No entanto, esse direito não é absoluto, como já visto anteriormente, havendo casos em que o consentimento é prescindível.

Contudo, o fato de ser prescindível, não anula a sua importância e necessidade nos demais processos de tratamento. Assim, a LGPD dispõe-se em amparar o titular dos dados pessoais a partir de suas estratégias legais, por meio da rejeição de qualquer tratamento de dados que opere sem o consentimento expresso, inequívoco e informado da pessoa (quando não são respaldados pelos casos em que o consentimento é prescindido). Além disso, o legislador estabeleceu os mecanismos que amparam o titular nas situações em que se vê obrigado a confrontar o agente de tratamento, de possíveis ilegalidades no tratamento de suas informações.

Desse modo, depreende-se que a LGPD não só se dispõe a regular o tratamento de dados e tutelar a proteção dos dados pessoais em matéria específica, como também almeja tutelar toda a gama de direitos fundamentais e humanos que se relacionam com ela a lei. Porque em virtude do contexto em que a sociedade está inserida, o fluxo de informações ocorre de modo acelerado e, muitas vezes, o consentimento acaba perdendo a sua importância e protagonismo, devendo o Direito encarregar-se de regular e equilibrar a balança contra os desequilíbrios das relações socioeconômicas e políticas.

REFERÊNCIAS

AQUINO, Leonardo Gomes de. **Teoria Geral dos contratos**. Belo Horizonte Editora Expert, 2021.

BECK, Cesar Augusto Moacyr Rutowitsch. **O mundo pós-CoVid-19**: a proteção de dados e inteligência artificial à luz das violações dos direitos humanos. Dissertação (Mestrado em Direito), Universidade Regional do Noroeste do Estado do Rio Grande do Sul (Campus Ijuí) – Ijuí, 2021.

BIONI, Bruno Ricardo. **Proteção de dados pessoais**: a função e os limites do consentimento. Rio de Janeiro: Forense, 2020.

BOBBIO, Norberto. **A Era dos Direitos**. 9. ed. Rio de Janeiro: Elsevier, 2004.

BRASIL. **Constituição da República Federativa do Brasil de 1988**. Brasília: Presidência da República, 1988.

BRASIL. Lei n. 12.414, de 9 de junho de 2011. **Disciplina a formação e consulta a bancos de dados com informações de adimplemento, de pessoas naturais ou de pessoas jurídicas, para formação de histórico de crédito**. Brasília: Presidência da República, 2011.

BRASIL. **Lei n. 12.965, de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Presidência da República: Brasília, 2014.

BRASIL. **Lei n. 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados. Brasília: Presidência da República, 2018.

BRASIL. Lei n. 8.078, de 11 de setembro de 1990. **Dispõe sobre a proteção do consumidor e dá outras providências**. Brasília: Presidência da República, 1990.

CÂMARA DOS DEPUTADOS. **Projeto de Lei n. 21/2020**. Estabelece princípios, direitos e deveres para o uso de inteligência artificial no Brasil, e dá outras providências. Câmara dos Deputados: Brasília, 2020. Disponível em: https://www.camara.leg.br/propostas-legislativas/2236340. Acesso em: 20 de fev. de 2023.

CONSELHO EUROPEU. **Convenção para a protecção das pessoas relativamente ao tratamento automatizado de dados de carácter pessoal**. Conselho Europeu: Estrasburgo, 1981.

CUEVAS, Ricardo Villas Bôas. Proteção de dados pessoais e direito ao esquecimento. In: DONEDA, Danilo (coord.). **Tratado de proteção de dados pessoais**. Rio de Janeiro: Forense, 2021.

DONEDA, Danilo *et.al.* (coord.). **Tratado de proteção de dados pessoais**. Rio de Janeiro: Forense, 2021.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**: fundamentos da Lei Geral de Proteção de Dados. 2.ed. São Paulo: Revista dos Tribunais, 2019.

EUROPEAN DATA PROTECTION BOARD. ***Guidelines 3/2022 on Dark patterns in social media platform interfaces****: How to recognise and avoid them*. Disponível em: https://edpb.europa.eu/system/files/2022-03/edpb_03-2022_guidelines_on_dark_patterns_in_social_media_platform_interfaces_en.pdf. Acesso em: 20 de fev. de 2023.

KANG, Cecilia. **Facebook admite que Cambridge Analytica accedió a los datos de 87 millones de usuarios**. In: The New York Tomes, Publicado em 4 de abril de 2018. Disponível em: https://www.nytimes.com/es/2018/04/04/espanol/facebook-cambridge-analytica-87-millones.html. Acesso em: 18 de fev. de 2023.

MAGRANI, Eduardo. **Entre dados e robôs:** ética e privacidade na era da hiperconectividade. 2.ed. Porto Alegre: Arquipélago Editorial, 2019.

MONTORO, André Franco**. Introdução à ciência do Direito**. 34.ed. São Paulo: Revista dos Tribunais, 2020.

MULHOLLAND, Caitlin Sampaio. (org.). **A LGPD e o novo marco normativo no Brasil**. Porto Alegre: Arquipélago, 2020.

MULHOLLAND, Caitlin Sampaio. **Dados pessoais sensíveis e a tutela de direitos fundamentais**: uma análise à luz da Lei Geral de Proteção de Dados (Lei n. 13.709/18). In: Revista de Direitos e Garantias Fundamentais, Vitória, v. 19, n.3, pp. 159-180, set/dez, 2018.

OEA. **Convenção Americana sobre Direitos Humanos:** Assinada na Conferência Especializada Interamericana sobre Direitos Humanos, San José, Costa Rica, em 22 de novembro de 1969. San José: Organização dos Estados Americanos, 1969.

OEA. **Declaração Americana dos Direitos e Deveres do Homem**: Aprovada na Nona Conferência Internacional Americana. Bogotá: Comissão Interamericana de Direitos Humanos, 1948.

ONU. **Declaração Universal dos Direitos Humanos de 1948**. Paris: Organização das Nações Unidas, 1948. Disponível em: https://brasil.un.org/pt-br/91601-declaracao-universal-dos-direitos-humanos. Acesso em: 15 de jan. de 2023.

PASQUALE, Frank. **The black box society**: the secret algorithms that control money and information. Cambridge: Harvard University Press, 2015.

RODOTÀ, Stefano. **A sociedade da vigilância**: a privacidade hoje. Rio de Janeiro: Renovar, 2008.

SARLET, Ingo Wolgang. Fundamentos constitucionais: o direito fundamental à proteção de dados. In: DONEDA, Danilo et.al. (coord.). **Tratado de proteção de dados pessoais**. Rio de Janeiro: Forense, 2021.

SOUZA, Carlos Affonso; LEMOS, Ronaldo. **Marco civil da internet**: construção e aplicação. Juiz de Fora: Editar Editora Associada Ltda, 2016.

SUPERIOR TRIBUNAL DE JUSTIÇA. STJ - HC: 631298 BA 2020/0325153-1, Relator: Ministro Benedito Gonçalves, Data de Publicação: DJ 07/12/2020. Disponível em: https://www.jusbrasil.com.br/jurisprudencia/stj/1385756712/decisao-monocratica-1385756726. Acesso em: Acesso em: 10 de jan. de 2023.

TARTUCE, Flavio. **Manual de Direito Civil**: volume único. 11.ed. Rio de Janeiro, Forense; METODO, 2021.

TEPEDINO; Gustavo; DE TEFFÉ, Chiara Spadaccini. **O consentimento na circulação de dados pessoais**. In: Revista Brasileira de Direito Civil, Belo Horizonte, v. 25, p. 83-116, jul./set., 2020.

TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato. **Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro**. São Paulo: Thomson Reuters Brasil, 2019.

VENTURINI, Jamila; LOUZADA, Luiza; MACIEL, Marilia; ZINGALES, Nicolo; STYLIANOU, Konstantinos; BELLI, Luca. **Terms of service and human rights**: an analysis of online platform contracts. 1. ed. Rio de Janeiro: Revan, 2016.

WARREN, Samuel D.; BRANDEIS, Louis D. **The right to privacy**. In: Harvard Law Review, v. 04, n. 05, 1890.

WIMMER, Miriam. **Os desafios do *enforcement* na LGPD: fiscalização, aplicação de sanções administrativas e coordenação intergovernamental**. In: MENDES, Laura Schertel; DONEDA, Danilo; SARLET, Ingo Wolfgang; RODRIGUES JR., Otavio Luiz. Tratado de proteção de dados pessoais. Rio de Janeiro: Forense, 2021.

ZUBOFF, Shoshana. **The age of surveillance capitalism**: the fight for a human future at the new frontier of power. New York: Hachette USA, 2018.