UNIVERSIDADE FRANCISCANA

CAMILA DALCOL DA SILVA

# A LEI GERAL DE PROTEÇÃO DE DADOS NO ÂMBITO BRASILEIRO: UMA ANÁLISE COMPARATIVA EM RELAÇÃO AO REGULAMENTO EUROPEU

SANTA MARIA

2020

CAMILA DALCOL DA SILVA

# A LEI GERAL DE PROTEÇÃO DE DADOS NO ÂMBITO BRASILEIRO: UMA ANÁLISE COMPARATIVA EM RELAÇÃO AO REGULAMENTO EUROPEU

Projeto de Trabalho Final de Graduação
Apresentado à disciplina de TFG II
Área de Ciências Sociais e Aplicadas
Curso de Direito

**Orientadora:** Profª. Carina da Cunha Alvez

**SANTA MARIA**
**2020**

## RESUMO

O principal propósito desse trabalho acadêmico é a avaliação objetiva e factual dos aspectos formais e materiais da implementação da Lei Geral de Proteção de Dados no Brasil que se espelhou nos moldes adotados pela legislação vigente na União Europeia - *General Data Protection Regulation.* Por meio de análise comparativa entre a LGPD e GDPR no que corresponde ao embasamento principiológico vigente na legislação brasileira, a aplicação prática da proteção dos dados processuais e *compliance* exigido pelos entes regulares, visasse estudar o cenário da implementação do marco regulatório da proteção de dados pessoais no Brasil e a fundamental abordagem adotada para a regulação da adoção de boas práticas quanto a proteção tanto na LGPD e GDPR. Por meio de pesquisa doutrinária, análise da legislação, emprego de métodos dedutivos e extensa pesquisa analítica e qualitativa é a pretensão realizar a correlação das temáticas abordadas e a realidade nacional quanto a implementação de um sistema de matéria de grande complexidade, tecnicidade e inovação jurídica. Com um estudo dos mecanismos apresentados pela Lei Geral de Proteção de Dados e os instrumentos regulatórios, intenta-se, a apresentação de uma perspectiva do quadro regulatório nacional. Com o entendimento dessas complexas temáticas, que foram concluídas por meio de estudo analítico e qualitativo da doutrina jurídica, das legislações apresentadas e extensa pesquisa, ao qual aplica-se o método comparativo na abordagem principiológica e teórica dos regulamentos de proteção de dados adotados pela União Europeia e da Legislação brasileira, analisando a realidade comercial e econômica que a implementação desses mecanismos hipoteticamente poderá ocasionar nos aspectos formais e materiais do sistema jurídico brasileiro.

**Palavras-chave:** Dados Pessoais; LGPD; GDPR; Privacidade. Direito Digital. Regulatório.

## ABSTRACT

The main purpose of this academic work is the objective and factual evaluation of the formal and material aspects of the implementation of the General Data Protection Regulation in Brazil, which has been mirrored in the molds adopted by the legislation in force in the European Union. Through a comparative analysis between LGPD and GDPR in what corresponds to the principiological basis in force in the Brazilian legislation, the practical application of procedural data protection and compliance required by regular entities, the aim was to study the scenario of the implementation of the regulatory framework for personal data protection in Brazil and the fundamental approach adopted for the regulation of the adoption of good practices as well as protection in both LGPD and GDPR. Through doctrinal research, legislation analysis, the use of deductive methods and extensive analytical and qualitative research, the purpose is to correlate the approached themes with the national reality as regards the implementation of a highly complex, technical and innovative legal system. With a study of the mechanisms presented by the General Law of Data Protection and the regulatory instruments, it is intended to present a perspective of the national regulatory framework. With the understanding of these complex themes, which were concluded through an analytical and qualitative study of the legal doctrine, the legislation presented and extensive research, to which the comparative method is applied in the principiological and theoretical approach of the data protection regulations adopted by the European Union and the Brazilian legislation, analyzing the commercial and economic reality that the implementation of these mechanisms may hypothetically cause in the formal and material aspects of the Brazilian legal system.


**Keywords:** Personal Data;LGPD; GDPR; Privacy. Digital Law. Regulatory.

## INTRODUÇÃO

Na era digital atual em relação às modernidades, nota-se uma gama de benefícios para a sociedade e o seu desenvolvimento. No entanto, uma das consequências também observada é o fenômeno da falta da privacidade e as constantes violações que este bem, constitucionalmente tutelado, sofre.

São várias as declarações que se alinham à afirmação de que "a privacidade morreu". De fato, não se pode negar que o ritmo acelerado da atualização das tecnologias e sua consequente integração na vida cotidiana das pessoas, seja no âmbito econômico ou pessoal, dificulta uma vigilância rebuscada quanto a coleta de informações pessoais e as finalidades em que estas são empregadas futuramente. Inúmeros casos de vazamentos de dados, vigilâncias obscuras e a divulgação de informações pessoais são relatados frequentemente, e trazem a reflexão de que esse é só mais um dos males da vida moderna.

Dessa forma, se faz necessário uma abordagem sistemática e analítica, do ponto de vista jurídico, dos problemas que a violação da privacidade gera na tentativa do resguardo dessa e a proteção dos dados pessoais no meio digital. Mesmo se tratando de matéria de complexidade alta e multidisciplinar, deve ser realizada uma avaliação dos instrumentos adotados pelos meios regulatórios implementados e sua eficácia no cerceamento do combate a proteção dos direitos individuais e do direito à privacidade.

Portanto, propõe-se no presente trabalho acadêmico, o estudo da construção conceitual jurídica do direito à privacidade e proteção de dados, assim como a aplicação da tutela jurídica apresentado pelos sistemas regulatórios. Trata-se de um estudo comparativo, que tem por objetivos: Analisar comparativamente as legislações de proteção de dados pessoais da União Europeia e Brasileira, por meio de sua construção histórica e principiológica e análise legal de seu real no meio digital é o objetivo demostrar a importância da implementação de sistemas regulatórios estruturados, semelhantes e equilibrados entre si. Dessa forma, analisar os elementos principais da legislação brasileira vigente e as medidas adotadas pela implementação desse sistema emergente na ceara jurídica nacional.

O presente estudo encontra-se inserido na linha de pesquisa do curso de Direito da Universidade Franciscana, Teoria Jurídica, Cidadania e Globalização. Uma vez que representa um tema de grande relevância não apenas no âmbito jurídico, mas também como uma problemática presente na ceara empresarial e de governança nacional, que se faz necessário para o fortalecimento e desenvolvimento econômico do País.

# 1. ABORDAGEM JURIDICA DA PRIVACIDADE E DADOS PESSOAIS NO MEIO DIGITAL

## 1.1. Construção conceitual do direito à privacidade

Na recente história mundial são frequentes os escândalos envolvendo o vazamento de dados pessoais ou o uso ilícito de informações privadas, coletadas por meios digitais para exploração econômica ou política das sociedades. Estas revelações de abusos e as consequências derivadas da exploração da coleta de dados pessoais para fins não declarados por cooperações e entes estatais despertaram na consciência social a necessidade de uma avaliação mais acertada e minuciosa sobre a matéria.

O estabelecimento de uma correlação entre a matéria privacidade na era digital e a exposição constante dos dados pessoais dos usuários do meio tecnológico reforçou a construção do pensamento da necessidade de uma regulamentação sobre o tema. No entanto, para se estabelecer normas gerais e métodos de implementação, fez-se necessário uma construção conceitual dessas duas temáticas interligadas e relacionadas, pelos estudiosos do direito digital.

A privacidade possui várias vertentes interpretativas, quando norteada pelo contexto social na qual avaliada. Para o pesquisador sobre direito digital Danilo Doneda, o conceito de privacidade tem como característica a mutabilidade e a variabilidade de sua definição quando analisado o contexto temporal e social na qual foi apresentado, tornando a discussão de problemas reais e práticos em delongadas explanações acadêmicas sem um fim previsto. (DONEDA; ALMEIDA, 2015)

Com a dificuldade de se estabelecer um conceito homogêneo para a temática no direito civil e constitucional das nações, constitui-se então a necessidade de buscar as bases, histórias e conceitos passados para a construção do pensamento atual. Hoje, com a ideia das garantias fundamentais e seu consequente individualismo, como base sagrada nos direitos fundamentais, a privacidade é notada como aspecto fundamental para a percepção de um Estado democrático de direito. Percepção essa, que reflete em outras garantias fundamentais, como o da propriedade privada e toma status de ascensão às ideias liberais burgueses (DONEDA,2006).

Grande foi a produção acadêmica a respeito do tema no decorrer da construção da sociedade moderna. Porém, a que se notar que o direito à privacidade está além de apenas a declaração da não intervenção na vida de alheio desenvolvido nos Estados Unidos no séc.

XX. Deve-se adequá-la ao surgimento de novas tecnologias e suas formas de atuação em sociedade, como a frequente exposição em redes sociais e meios de comunicação, o que remete não só a ideia de preservação da propriedade privada, mas também da personalidade do indivíduo (DONEDA; ALMEIDA, 2015).

Com a verificação das novas situações fáticas frente às novidades relacionadas à matéria desde o século anterior, constata-se a distinção do emprego dela nos mais variados ramos do mundo jurídico e nos níveis de proteção que esse estabelece para a personalidade do indivíduo. Com o advento da internet, a tutela jurídica estatal começou a se estender para se fazer valer nas novas ocorrências e necessidades da vida moderna, passando a se associar a uma perspectiva de proteção de dados pessoais tanto quanto a proteção da personalidade. Surge, dessa forma, o questionamento de como surgiu esse processo de aplicação da privacidade no meio digital e, consequentemente, como se desenvolveu o elo jurídico entre os dados pessoais e o direito digital. É o que se pretende demonstra a seguir.

## 1.2. Direito a privacidade no meio digital e a proteção de dados

A última década foi cenário de uma grande mudança na forma como os indivíduos interagem entre si e a forma como essa interação se dá. A transmissão de informações passou para um ritmo imediato e alarmante no que concerne ao resguardo de dados e na eficácia de sua transmissão. A velocidade com que surgiam novas tecnologias e a complexidade e especificidade da área de gestão do meio digital impossibilitou a implementação de um desenvolvimento de todo seguro para o cidadão.

As particularidades dos métodos utilizados para a transmissão de informação e o fluxo em crescimento constante tiveram um impacto gigantesco na forma de prática econômica que se estabeleceu nos moldes da sociedade moderna. Surge uma nova era capitalista, e com ela um novo modelo econômico, onde a informação é moeda de troca e seu processamento “ação de conhecimento” imediato é sinônimo de produtividade (CASTELLS, 1999). De acordo com Manuel Castells, mesmo que toda forma de desenvolvimento social é atingida quando se implementa novos métodos de processamento de informação e sua consequente absorção, esse modelo econômico informacionalista, característico da era digital, se diferencia pela forma como essa matriz é tratada e gerida dentro do escopo de suas possibilidades de autorreferência, ou seja, a informação é processada de modo que essa, consequentemente, melhore a própria tecnologia que a manuseia (CASTELLS, 1999).

Portanto, a informação se transformou em uma fonte, que se bem gerenciada, pode ser facilmente armazenada, coletada e recuperada. Daí o surgimento de um maior incentivo para a capitalização desse bem que hoje tem valor socioeconômico reconhecida na sociedade, e que é cada vez mais explorado, tanto em sua fonte quanto em formato de dados coletados em grande escala.

Cabe aqui, portanto, para melhor compreensão da temática tratada, fazer algumas distinções quanto aos termos dados e informações, muitas vezes usados como sinônimos de forma equivocada. No que se refere a determinado fato real, situação imaterial e sem carga energética, porém provido de sentido denominamos informação. Já os dados são essas informações fragmentados e compartimentalizados, de forma que se de uma melhor processamento e gerenciamento por parte do instrumento tecnológico utilizado para o gerenciamento dessa informação. Os dados tem uma base primitiva e uma natureza de estado potencial de ser, já a informação representa uma situação completa com sentido, dessa forma, cognitiva (DONEDA, 2010). Sendo assim, aqui apresenta-se o vínculo entre a relação da informação pessoal e o indivíduo, portanto a necessária proteção dos dados pessoais que a ele concede-se.

> O vínculo da informação pessoal com o seu titular deve ser de tal natureza a revelar diretamente algo concreto sobre esta pessoa. Assim, a informação pessoal refere-se às suas características ou ações, atribuíveis à pessoa em conformidade com a lei, como no caso do nome civil ou do domicílio, ou então informações diretamente provenientes de seus atos, como os dados referentes ao seu consumo, informações referentes às suas manifestações, como opiniões que manifesta, e tantas outras (DONEDA, 2010).

Fica demonstrada a correlação do indivíduo e a informação pessoal de qual tem como fonte sua personalidade, emitidas por ele próprio. Como visto, é a este elo que se oferece tutela jurisdicional, pois se configura a ligação entre os direitos e garantias da personalidade humana e os dados e informações pessoais que esta gera. Tópicos que possuem guarda constitucional e grande relevância acadêmica e prática no mundo jurídico.

Em âmbito econômico, este cenário se torna ainda mais dotado de urgência, pois, como já demonstrado, atualmente a informação é uma moeda de troca e tem grande valor de mercado, se deixada desprotegida para ser explorada, coletada e armazenada de forma discriminada, incorre-se em violações das garantias que são asseguradas ao cidadão pela Constituição Federal. Como pontuado, são estes os pontos que atraem a tutela jurisdicional sobre o tema, pois nota-se que “o estatuto jurídico destes dados se torne um dos pontos

centrais que vão definir a própria autonomia, identidade e liberdade do cidadão contemporâneo" (DONEDA, 2010).

Acrescenta-se, a título de esclarecimento, que à proteção de dados pessoais é tópico de estudo e investigação de muitas outras áreas de conhecimento: nas ciências sociais, tecnológicas, entre outras. No entanto, nesta explanação analisa-se apenas os aspectos jurídicos aplicados ao tema.

A regulação dos dados pessoais não pode ser incluída na dualidade do bem ou mal, mas sim, como as demais tecnologias desenvolvidas para a o desenvolvimento econômico e social da humanidade, o fluxo e trato de dados pessoais deve ser abordado com a tecnicidade e complexidade exigida pela matéria. Levando em consideração as bases formadoras dos princípios que norteiam as ferramentas adotadas para se garantir a autonomia informacional por parte do indivíduo e segurança jurídica pretendida.

## 2. ANÁLISE COMPARATIVA DO QUANDO REGULATÓRIO EUROPEU E BRASILEIRO SOBRE PROTEÇÃO DE DADOS

### 2.1. Natureza geral das legislações de proteções de dados

Como anteriormente tratado, a tutela jurisdicional da proteção dos dados deriva da abordagem objetiva, já que nada mais são que indícios deixados pela identidade do indivíduo, ou seja, rastros externos e subjetivos, protegidos pela garantia constitucional conferida a personalidade humana.

Contudo, atualmente o fluxo de informações pessoais se dá de forma a abranger a realidade jurídica estabelecida em diversos países, impossibilitando um trato homogêneo às questões do meio digital. O Autor Colin Bennett frisa que a uniformidade nos padrões de abordagem técnica adotados por um conjunto de países tem a tendência a se espelhar, justamente pela necessidade de se estabelecer relações econômicas internacionais de forma equilibrada, e que contenham um núcleo estrutural, principiológico e regulamentador padronizado. (BENNETT, 1992)

Usualmente observa-se uma harmonização nas legislações nacionais quando se trata do desenvolvimento de padrões e fluxos, a utilização de tecnologias e implementação de práticas fundamentadas nos mesmos princípios legais. No entanto, mesmo semelhantes, legislações que partem de realidades sociais e culturais diferentes podem apresentar sistemas de proteção de dados bastante distintos. Como é verificado na disparidade de equilíbrio entre as partes interessadas que compõe a questão, sendo elas o indivíduo, o Estado e as pessoas jurídicas. A

parcela de participação estatal na atuação da mitigação dos danos ou na fiscalização e implementação de medidas protetivas reforça a ideia de que a regulamentação tem por objetivo garantir a efetiva tutela jurisdicional para todos, mesmo que com limitações do efetivo exercício da autonomia informacional. Um conjunto de fatores principiológicos, culturais, e legais do país são os fundamentos para a implementação de um marco regulatório de proteção de dados, contendo às imposições que os controladores e operadores de dados pessoais serão submetidos, estabelecendo os direitos dos usuários de dados e os mecanismos de fiscalização determinações impostas em lei.

Em meados da década de 1960 surgiu a discussão da possibilidade da criação de um banco de dados central com os dados dos cidadãos Estado Unidense, a partir dessa idealização teórica foi constituído um comitê consultivo no Departamento de Saúde, Educação e Bem-Estar Americano, denominado *Secretary's Advisory Committee on Automated Personal Data Systems* (SOLOVE,2004), que posteriormente publicou o relatório de Registros, Computadores e os Direitos dos Cidadãos, com as seguintes determinações quanto à proteção de dados pessoais a ser empregada na coleta, armazenamento, transmissão e tratamento destes:

> - "Não deve existir um sistema de armazenamento de informações pessoais cuja existência seja mantida em segredo.
> - Deve existir um meio para um indivíduo descobrir quais informações a seu respeito estão contidas em um registro e de qual forma ela é utilizada.
> - Deve existir um meio para um indivíduo evitar que a informação a seu respeito colhido para um determinado fim seja utilizada ou disponibilizada para outros propósitos sem o seu conhecimento.
> - Deve existir um meio para um indivíduo corrigir ou retificar um registro de informações a seu respeito.
> - Toda organização que estruture, mantenha, utilize ou divulgue registros com dados pessoais deve garantir a confiabilidade destes dados para os fins pretendidos e deve tomar as devidas precauções para evitar o mau uso destes dados (ESTADOS UNIDOS, 1973, apud DONEDA, 2010)

Os regulamentos emitidos pelo comitê, como enunciados, foram incorporados a base principiológica do documento *Fair Information Practice Principles* e utilizados como norte na elaboração das leis gerais de proteção de dados pessoais mundialmente, ao qual, com o passar do tempo foram adicionados novos princípios em seu rol, de acordo com a realidade de cada Estado, no entanto, nunca entrando em discordância com os pilares já preestabelecidos.

Neste contexto se faz necessária uma breve abordagem conceitual envolvendo os princípios basilares que compõe a formação das legislações que visam a proteção de dados pessoais universalmente, sendo eles (DONEDA, 2010):

A) O **princípio da transparência** determina que o titular dos dados pessoais tratados deve ser comunicado de todas as especificidades nas quais o tratamento dos dados transcorre.

B) O **princípio da qualidade** assegura a veracidade e atualidade das informações apresentadas nos bancos de dados pessoais autorizados, com a aplicação de atualização periódica da informação para que esta não se torne obsoleta.

C) O **princípio da finalidade**, considerado pelos controladores de dados um desafio e complexa premissa que deve ser empregada em situações práticas. Determina que todo dado pessoal coletado deve ter uma finalidade específica para que se dê a guarda, tratamento e manutenção deste, devendo ser sempre informado ao titular. Aqui se determina o sistema de valor e a hierarquia dos dados pessoais, assim como a proibição do repasse dessa informação a terceiro não autorizado pelo titular.

D) O **princípio do livre acesso**, pelo qual é resguardado o direito de o titular acessar livremente as informações sobre ele tratadas e armazenadas nos bancos de dados, assegurando ainda a atualização, cancelamento, suprimento e acréscimo destes dados conforme a discricionariedade do titular.

E) O **princípio da segurança física e lógica** determina que a guarda e tratamento dos dados deve ser realizada em ambiente adequado a prevenção do extravio, transmissão não autorizada ou corrompimento dos dados pessoais.

O rol de princípios apresentado acima é considerado a base formadora de uma legislação protetiva dos dados pessoais, ou seja, esclarece os direitos individuais do indivíduo quando ao tratamento, guarda e utilização de dados pessoais coletados em meio digital, pelas organizações cumpridores da lei e estabelecendo limites que, se ultrapassados, geram obrigações de reparo.

No entanto, faz-se necessário o destaque do equilíbrio do aspecto protetivo dos dados pessoais com a necessidade do manuseio e tratamentos destes por seu valor econômico agregado. Dessa forma, é essencial a observância da necessidade de assegurar a natureza dual e intrínseca na construção dos meios regulatórios e legislações aplicadas ao tema.

## 2.2. Legislação regulatória da proteção de dados pessoais adotada pela União Europeia - GDPR

A União Europeia (UE) apresenta uma maior maturidade legislativa quando se trata da matéria de proteção de dados e as regulamentações associadas com o tema, em relação a maioria dos países detentores de grande atividade econômica internacional e relevância. Atualmente a UE é considerada referência na implementação de medidas protetivas para resguardo do indivíduo e sua privacidade nos meios digitais. A convenção para a Proteção das Pessoas Relativamente ao Tratamento Automatizado de Dados de Caráter Pessoal – Convenção 108/CE foi aprovada em meados do ano 1981, trazendo elementos que embasaram a posterior aprovação da Diretiva 95/46/CE no ano de 1995, laçando raízes profundas no aspecto protetivo dos dados pessoais do indivíduo no sistema jurídico praticado entre os entes internacionais participantes. (MADGE, 2018)

O propósito do relacionado é proporcionar, por meio das diretrizes adotadas, a proteção dos direitos fundamentais do indivíduo e a privacidade ao mesmo tempo incentivando o desenvolvimento econômico-social e a aplicação comercial do tratamento dos dados pessoais, ~~e~~ bem como a transferência das informações com os países participantes da União Europeia. Portanto, com o desenvolvimento de um grande tráfico no fluxo de dados nas comunicações eletrônicas foi aprovada a Diretiva 2006/24/CE, para acompanhar o novo contexto que surgia a época. (MONTEIRO, 2019)

Com o advento de tecnologias de comunicação cada vez mais em alta e a disseminação e acesso a dispositivos tecnológicos portáteis, a realidade da vivência e exposição nas redes sociais foram o cenário que deram origem a necessidade de uma legislação mais abrangente que a diretriz estabelecida em 2006. No âmbito comercial e econômico europeu percebeu-se a falta de instrumentos necessários para acompanhar o tratamento e uso adequado dos dados do cidadão comum pelas grandes corporações e entes estatais com intenções cerceadoras de algumas liberdades garantidas pela vigilância da observância da privacidade da personalidade do indivíduo, no que se considera espaço privado em meio digital (BURGESS, 2018). Neste cenário surge o quadro regulatório em vigência atualmente, o *General Dada Protection Regulation* – GDPR, Regulamento 2016/679 aprovado pelo Parlamento Europeu. (UNIÃO EUROPÉIA, 2016)

Nos mesmos moldes principiológicos que a Diretriz 95/46/CE, revogada pela GDPR, esta continuou com o incentivo ao livre fluxo de informação com o objetivo de incentivo econômico e comercial dentro das fronteiras Europeias e a natureza protetiva das garantias individuais da privacidade no trato dos dados pessoais. Foi estipulada no corpo inicial do texto legislativo a garantia da promoção de uma proteção coerente e equivalente às exigências

observadas como necessárias, mantendo o incentivo ao desenvolvimento do ambiente digital e a evolução econômica e negocial intrínseca em sua natureza. (UNIÃO EUROPÉIA, 2016)

Em um mundo onde se consegue valorar a coleta de informações pessoais de forma precisa a União Europeia se consolidou como um sistema de tutela da proteção da privacidade individual, com a implementação eficaz de atuação de agentes reguladores no cumprimento dos preceitos legais. (MONTEIRO, 2019) O artigo 29 da GDPR estabelece a atuação do *Working Party* no auxílio da fiscalização no trato dos dados pessoais, fazendo concessões e análises de casos práticos com a emissão de pareces técnicos sobre matéria discutida. A tutela jurisdicional europeia também se faz presente no papel de cerceamento da violação das diretrizes legais.

O GDPR é um Regulamento extenso e bem formulado composto por 11 capítulos e 99 artigos de força normativa em todos os Estados-membros da União Europeia, tornando incongruente a implantação de legislação própria por parte de cada ente estatal europeu. Uma das características inovadoras incorporada no texto legislativo é a possibilidade da aplicação de multas de valor substancial que pode chegar até o € 20.000.000,00 ou até 4% do volume do negócio acumulado no exercício financeiro no ano anterior da empresa que incorrer em violação. (POLIDO, 2018)

Outra novidade incorporada no quadro protetivo do texto regulatório europeu foi a possibilidade de o indivíduo exercer ~~a~~ o "direito ao esquecimento" que tem como objetivo assegurar a possibilidade de o titular do dado pessoal escolher a exclusão ou extinção deste dos meios digitais aos quais encontra-se vinculado, desde que comprovada a falta de finalidade justificada e relevante na guarda e manutenção da informação pelo ente detentor. (UNIÃO EUROPÉIA, 2016) Essa avaliação passou a ser realizada pelo Comitê Europeu para a Proteção de Dados – EDPB, instituído como órgão independente de personalidade jurídica desvinculada dos entes estatais e grupos econômicos.

Interessante, neste momento, realizar a análise da construção do quadro regulatório brasileiro para a posterior construção de estudo comparativo e espelhamento de aplicabilidade dos instrumentos sancionados nos textos legislativos de ambos os entes Estatais.

## 2.3. Regulatório da proteção de dados pessoais adotada pelo sistema jurídico brasileiro – Lei Geral de Proteção de Dados

Conforme já referido anteriormente, a matéria que enseja na proteção dos dados pessoais possui um vínculo quanto a sua natureza jurídica com a defesa da garantia fundamental que é o direito à privacidade do indivíduo. Demonstra-se o reconhecimento do respectivo direito, no momento em que o tema é concatenado no rol de garantias e direitos fundamentais do ser humano disposto na Constituição Federal de 1988.

A lacuna apresentada quanto à falta da nomenclatura utilizada em um contexto tecnológico não descoberta a garantia de uma intenção legislativa expressa em texto constitucional. O art. 5º, incisos X e XII da CF/881 que tratam da inviolabilidade da privacidade formal e material da personalidade do indivíduo e sua propriedade servem de base para se assegurar a proteção constitucional à matéria da proteção de dados pessoais em meios digitais.

Outra garantia estipulada como remédio constitucional, pela Carta Magna é possibilidade de o indivíduo utilizar o instrumento habeas data para efetivar o acesso às informações da qual é titular ou a ele envolve de maneira pessoal, armazenadas nos bacos de dados públicos.

No entanto, além da proteção constitucional conferida à matéria, deve-se fazer notar que o Brasil é signatário de tratados internacionais que versam sobre a privacidade como garantia fundamental de maneira extensa e aprofundada, e por sua vez, reconhecem que a proteção de dados em meio digital diz respeito à intimidade e privacidade do indivíduo, dessa forma, inviolável. Cita-se como exemplo a Declaração de Santa Cruz de La Sierra, que em seu documento final XIII, dispõe no art. 45 sobre a proteção de dados pessoais como garantia fundamental em si:

> Estamos também conscientes de que a proteção de dados pessoais é um direito fundamental das pessoas e destacamos a importância das iniciativas reguladoras ibero-americanas para proteger a privacidade dos cidadãos, contidas na Declaração de Antigua, pela qual se cria a Rede Ibero-Americana de Proteção de Dados, aberta a todos os países da nossa Comunidade. (BOLÍVIA, 2003)

A legislação brasileira não se detém a abordagem do tema apenas na esfera constitucional, na esfera infraconstitucional destaca-se a Lei nº 8.078/1990 - Código de Defesa do Consumidor, que aborda a temática quando abrange os bancos de dados com informações dos consumidores; a Lei nº 12.414/2011 – Lei do Cadastro Positivo, na regulação de formação de banco de dados com informações de inadimplentes e crédito bancário; a Lei nº 12.527/2011 – Lei de Acesso à Informação Pública, que apresenta as diretrizes nas quais as informações pessoais devem ser tratadas pelos agentes públicos e a administração pública.

Não dizendo respeito à especificidade tratada no direito digital, as legislações citadas no parágrafo anterior não se relacionam materialmente, no entanto pode-se destacar a mesma base principiológica utilizada para a construção do raciocínio jurídico que tutela a proteção de dados pessoais, como o princípio da finalidade, o princípio do livre acesso, entre outros.

Outra fonte legal no que diz respeito ao tema privacidade, em convergência com o direito digital, é o Marco Civil da Internet – MCI, sancionado em 2014, veio regular os direitos e deveres dos usuários da Internet em âmbito nacional. Nota-se o espelhamento da legislação Europeia quando a normativa do MCI, no rol de garantias apresentado em seu artigo 3º destaca como bens autônomos a proteção da privacidade e a proteção de dados pessoais, pois é dessa forma que se dá abordagem da temática pela GDPR. (BRASIL,2018) Com a massiva evolução tecnológica e o grande número de denúncia de abusividade no uso dos dados pessoais por parte de grupos econômicos e entes estatais, foi proposta e aprovada em 14 de agosto de 2018 o projeto da Lei Geral de Proteção de Dados, com requerimento de urgência. Esta foi o resultado de longas tratativas parlamentares que teve início em 2016.

A Lei Geral de Proteção de Dados tem como objetivo estabelecer diretrizes no trato, armazenamento e transmissão dos dados pessoais, estabelecer o direito de garantia fundamental da privacidade no meio digital e estipular deveres e obrigações para os agentes responsáveis pelo manuseio das informações privadas de titulares. Ademais, estabeleceu ainda, o novo modelo de procedimentos a ser adotado como base negocial na ceara digital, onde a informação por si só é o produto comercializado.

Com embasamento lógico, formal e material, muito semelhante ao adotado pela GDPR, a legislação brasileira apresenta uma estrutura textual composta de 65 artigos de lei que objetivam regulamentar todos os entes responsáveis pelo tratamento de dados pessoais, em meio digital ou físico. Aos coletadores e tratadores destes estipula-se deveres e obrigações específicas a serem observadas sob pena de multas pecuniárias extravagantes, assim como na GDPR, além de sansões administrativas a serem impostas pela Autoridade Nacional de Proteção de Dados - ANPD, órgão público exclusivamente criado para regulamentação e aplicação do disposto no texto legal.

Contudo, a legislação brasileira estipulou uma série de atribuições quanto à fiscalização e capacidade punitiva para a ANPD. No entanto, nota-se a falta de recursos econômicos e estruturais para o bom desenvolvimento destas atividades por parte da Agência Reguladora. A LGPD entrou em vigor recentemente, especificamente no dia 18 de agosto de

2020, portanto, pouco tempo ~~se~~ transcorreu para se emitir uma análise da atuação já realizada pela ANPD.

Dessa forma, será realizada a análise das diretrizes estabelecidas na Lei Geral de Proteção de Dados e sua fundamentação principiológica e estrutural com relação à ~~a~~ legislação europeia - General Dada Protetion Regulatory, por meio do estudo dos conceitos centrais estabelecidos, sendo estes: dados pessoais, privacidade e consentimento.

## 3. ANÁLISE COMPARATIVA ENTRE A GDPR E LGPD

Tendo a criação da Lei Geral de Proteção de Dados brasileira sido inspirada no *General Data Protection Regulation* europeu, guardam entre si diversas semelhanças na abordagem principiológica e regulamentar, como, por exemplo, o conceito de consentimento. Em ambas o entendimento desse tópico essencial a proteção de dados demonstra a importância do poder de decisão, autonomia e controle do titular sobre suas informações. No entanto, ao se analisar as diretrizes estipuladas, ambas as legislações possuem diferenças notórias e importantes na quando da implicação da proteção de dados pessoais.

A LGPD é uma lei, sendo assim, possui uma linguagem subjetiva e abrangente, estipulado determinações legais abertas a interpretação jurisprudencial e regulamentação posterior da Autoridade Nacional de Proteção de Dados (ANPD). A GDPR, por outro lado, é um regulamento, que estipula diretrizes diretas e objetivas em suas cláusulas, onde estipula regras claras e específicas.

No entanto, o modelo de aplicabilidade adotado por ambas legislações se enquadra no de lei geral, buscando construir um sistema regulatório consolidando a proteção de dados com política pública de implementação obrigatória, composto por instrumentos estatutários e sancionatórios disponíveis a um órgão administrativo, responsável para implementação e fiscalização das diretrizes determinadas em lei. (CAVALCANTI & SANTOS, 2018).

Todas as empresas que possem atuação na União Europeia, sem importar a localização fixa utilizada, mas que manipulem dados de pessoas naturais europeias são passiveis da aplicação da GDPR. Estão sujeitos a aplicação da LGPD pessoas jurídicas de direito privado e público que tratarem os dados em território nacional, na atividade de tratamento que tem como objetivo a oferta de bens e serviços ou realize o tratamento de dados de indivíduos em território nacional. (CAVALCANTI & SANTOS, 2018).

Quanto as bases legais utilizadas para o tratamento de dados privados, a LGPD adicionou quatro outros requisitos no rol especificado na GDPR. A legislação europeia determina que seja verificado: o (a) consentimento explícito; (b) a necessidade contratual; (c) a execução de políticas públicas; (d) o interesse vital; (e) a obrigação legal; e (f) o legitimo interesse. A LGPD acresceu qautro outros requisitos a esse rol, são ele: (a) a proteção da saúde em um procedimento realizado por profissionais de saúde; (b) realização de estudos por um órgão de pesquisa; (c) exercício de direitos em processos judiciais; e (d) a proteção ao crédito. (IRAMINA, 2020).

Dessa forma, passa-se a explanar sobre a abordagem utilizada pela lei brasileira e o regulamento Europeu ao conceito de dados pessoais, em suas singularidades, através de estudo comparativo.

## 3.1. Abordagem do conceito de dados pessoais na LGPD e GDPR

Como o próprio termo sugere, dados pessoais referem-se a fragmentos compostos por informações de um agente humano. Tais informações refletem a identidade do indivíduo. Considerando a possibilidade de classificar um dado pessoal, verificasse o confronto com duas definições: expansionistas ou reducionistas. (BIONI, 2016)

A definição reducionista baseia-se nos dados referentes a um único, conhecido, identificado indivíduo, não se permitindo a associação de tais dados com informações de terceiros. (BIONI, 2018) Os dados oferecem clara e inquestionável evidência de estarem associados a um indivíduo específico, como por exemplo, os dados apresentados na extração de certidões de nascimento, passaportes ou registros gerais.

Contrapondo-se à definição vista acima, tem-se a visão expansionista, onde reza a não necessidade de clareza na identificação de um indivíduo. Exemplo desta modalidade são as datas de aniversário que, num âmbito limitado de família e colegas próximos de trabalho podem identificar um indivíduo, mas, quando expandida essa observação para um contexto do território de uma cidade, país ou até o mundo, essas informações perdem a sua capacidade de identificar um determinado indivíduo, uma vez que compartilham esse dado com vários outros, ou seja, não é titular exclusivo dessa informação.

Pode-se afirmar que, no Brasil, encontra-se em voga o modelo expansionista vigente na Lei Geral de Proteção de Dados, assim como na GDPR. Ambas as legislações compartilham o conceito adotado para dados pessoais.

## 3.2. Classificação dos dados sensíveis, anônimos e os anonimizados

Importante se faz perceber e considerar o que vem a ser classificado como categorias de dados sensíveis e anônimos. Primeiro se faz referência às informações que necessitam de alto nível de proteção. Tais informações podem trazer em seu escopo princípios que desencadeariam ações de discriminação e/ou preconceito direcionado ao indivíduo.

Segundo Danilo Doneda, tal modalidade não foi elaborada sem contrapontos, levantando o argumento que é possível antecipar os efeitos advindos do manejo de uma informação, seja ela qual for. Entretanto, essa definição leva em consideração os danos advindos indevido dos dados. (DONEDA, 2010)

A LGPD determina que, dentro dos aspectos dos dados sensíveis, apenas o indivíduo, de maneira consciente e voluntária, pode consentir e autorizar o manejo dos dados dos quais é titular. Abrem-se exceções para o cumprimento de obrigações legais determinadas em lei ou regulamentos, sendo vetado o compartilhamento ou comunicação de dados pessoais sensíveis que redundem em ganho econômico, segundo o parágrafo 4º do artigo 11 da LGPD.

Outras duas modalidades consideradas no âmbito da classificação dos dados, são os anônimos e os anonimizados. Os dados anônimos não são protegidos por lei, já os anonimizados, dependendo da tecnicidade da informação, têm o seu potencial de informação restringido.

Há vários motivos para se anonimizados dados pessoais, no entanto destaca-se uma intenção de diminuição de risco na manipulação ou transmissão destes dados. Considera-se um fator relevante dentro da anonimação: a inviolabilidade da identidade do indivíduo titular das informações. O processo para reidentificação deve ser inviabilizado até mesmo o controlador ou aquela figura que manuseia e trata os dados, mesmo tal processo não oferecendo garantia total. (BIONI, 2016)

A Lei Geral de Proteção de Dados, em seu artigo 5º, inciso III, dispõe que “o dado anonimizado é correspondente ao dado relativo ao titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião do tratamento.”

Ainda abordando o tema da anonimização, temos os dados pseudoanonimizados que se caracterizam pelas ligações realizadas com pseudônimos, com o propósito de se classificar a originalidade do seu conteúdo. Isso acontece quando, por exemplo, os dígitos do CPF são

aleatoriamente trocados ou codificados para fins de elevação do nível de segurança estabelecido para a guarda daquela informação. Essa definição foi disposta no caput do artigo 3º e § 4º da LGPD, conforme segue:

> Art. 13. Na realização de estudos em saúde pública, os órgãos de pesquisa poderão ter acesso a bases de dados pessoais, que serão tratados exclusivamente dentro do órgão e estritamente para a finalidade de realização de estudos e pesquisas e mantidos em ambiente controlado e seguro, conforme práticas de segurança previstas em regulamento específico e que incluam, sempre que possível, a anonimização ou pseudonimização dos dados, bem como considerem os devidos padrões éticos relacionados a estudos e pesquisas.
> [...]
> § 4º Para os efeitos deste artigo, a pseudonimização é o tratamento por meio do qual um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo, senão pelo uso de informação adicional mantida separadamente pelo controlador em ambiente controlado e seguro. (BRASIL, 2018)

Contudo a GDPR, ao abordar o tema da classificação dos dados pessoais, não faz menção aos dados anonimizados, trata, no entanto, sobre os pseudonimizados, mesmo que com uma abordagem diferenciada do que a constatada pela LGPD. Relevante ressaltar novamente que por todas as suas similaridades ou disparidades no trato da temática discutida os quadros regulatórios discutidos neste texto possuem a mesma base principiológica e intenção legislativa. Ambos buscam proporcionar a tutela protetiva do estado aos dados pessoais, sem deixar de observar a relevância e valor econômico que estão agregados a estes no mercado.

### 3.3. Necessidade de consentimento no trato dos dados pessoais

O consentimento é um elemento considerável na proteção de dados. É por meio dele que a pessoa expressa sua concordância com a coleta e tratamento dos dados pessoais.

No artigo 5º, XII da LGPD fica definido o consentimento como “manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada.” Pressupõe, portanto, que o indivíduo tenha ciência da operação, bem como das informações. Ao individuo titular dos dados, repousa a decisão consciente e livre de manifestar-se sobre o manejo das suas informações.

Ainda no âmbito da liberdade de escolha o Grupo de Proteção de Dados – GDP, normativa participante da legislação europeia e componente do texto do GDPR, em seu artigo 29 expõe a importância das condições de análise da liberdade de escolha quando do consentimento. (DATA PROTECTION WORKING PARTY, 2016) A legislação brasileira reconhece que:

> "Art. 9º
>
> (...)
>
> § 3º Quando o tratamento de dados pessoais for condição para o fornecimento de produto ou de serviço ou para o exercício de direito, o titular será informado com destaque sobre esse fato e sobre os meios pelos quais poderá exercer os direitos do titular elencados no art. 18 desta Lei." (BRASIL, 2018)

Ainda se faz necessário salientar as submodalidades dentro das diretrizes do manejo dos dados pessoais, destacando-se a granularidade que se apresenta próxima a condicionalidade. Como granularidade compreende-se na prática que, quando da autorização do uso de dados por parte do sujeito, tal ato permitirá vários tipos de uso das informações. Lavrando mão do seguinte exemplo: uma empresa recebe o consentimento do seu cliente para ser adicionado a sua listagem de e-mail e contatos telefônicos com o fim determinado de repassar informações publicitárias, mas, também, de compartilhar esses mesmos dados do cliente com outras empresas que sejam ligados ao grupo econômico de que é participante. Diante deste cenário, percebe-se uma atitude estratégica que burla a liberdade de escolha do indivíduo, uma vez que ao mesmo foi negada a informação quanto às duas formas de uso às quais seus dados pessoais serão expostos.

Segundo o *caput* do artigo 8º da LGPD, o consentimento por parte do indivíduo deverá ser realizado de forma escrita ou por meio de outro mecanismo automatizado, desde que demonstre de maneira clara a inequívoca vontade do titular.

Merece destaque no âmbito de compartilhamento de dados, um fenômeno recorrente que gera um "cansaço" no cliente quando, no contexto digital exige-se a necessidade de repetidas ações para expressar o seu consentimento, baseadas em "cliques". Assim, por estresse, o cliente deixa de ler todos os termos que norteiam e caracterizam o consentimento. Para o GDPR é função obrigatória dos controladores e desenvolvedores, o estabelecimento de mecanismos necessários a fim de combater tal prática.

Como já mencionado, há outras maneiras legais que autorizam o manejo de dados, em destaque, o próprio interesse legítimo do controlador dos dados, quando reconhece violada a proteção de dados do titular, bem como assegurar todos os direitos que a estes beneficiam.

## 4. LEI Nº 13.709/2018 – LEI GERAL DE PROTEÇÃO DE DADOS BRASILEIRA

Existem 120 países e territórios autônomos que oferecem um marco regulatório voltado à proteção de dados pessoais. (BANISAR, 2018) Com a sanção da Lei Geral de Proteção de Dados, o Brasil se uniu a estes países fazendo com que discussões que se estendiam há oito anos no âmbito institucional fossem por fim sucedidas por um marco que confrontou perspectivas.

A base da LGPF, bem como da GDPR, é construída em cima de princípios, o que facilita a sua resistência à passagem do tempo e consequente evolução tecnológica. Além dos princípios, a Lei traz as definições de dados pessoais, dados sensíveis, controladores e operadores, consentimento etc., que servem para direcionar o uso da Lei na sociedade brasileira, bem como para estabelecer obrigações a quem irá dispor de dados pessoais, bem como fiscalizar o cumprimento das disposições legais. Em relação à fiscalização, se faz extremamente necessária a existência de uma entidade fiscalizadora, imparcial, que utilizará dos meios públicos e da legislação em si para fazer valer cada artigo.

Ocorre que a ausência do órgão regulador coloca em risco a fiscalização e efetividade da norma. A autoridade nacional corresponde a um "pilar de sustentação, sem o qual todo o arcabouço normativo e principiológico vem a ruir". Essa inefetividade da norma frente a ausência de órgão fiscalizador é tão iminente que dentre os 120 países que possuem um marco próprio quanto à proteção de dados, apenas 12 não possuem a entidade em questão. (DONEDA, MENDES, 2018).

É importante mencionar que há uma atuação pluralista das autoridades nacionais em relação à proteção de dados. Prova-se tal situação ao observar os artigos vetados da LGPD, que demonstram que as responsabilidades da ANDP vão além da fiscalização e aplicação de sanção. Ou seja, é muito importante que haja a autoridade reguladora para que o sistema de proteção de dados se fortaleça e se fixe além da normatividade, como também na área consultiva, educativa, representativa etc.

Como resultado da observação da implementação de um sistema de proteção de dados em outros países, manter como pilar da ANPD seu aspecto consultivo e orientador na implementação das melhores práticas de trato de dados, promovendo a disseminação de informações e o auxilio do quadro mercadológico e econômico nacional, aumenta o envolvimento do cenário acadêmico e empresarial, já que se estabelece como órgão regulador de diretrizes, não figura principal no cenário da proteção de dados.

Assim, conferindo liberdade para que a temática alcance uma abrangência multidisciplinar e um nível de tecnicidade que só se é verificado longe das barreiras estatais

impostas pela burocracia e o passo da vivência pública. Dessa forma, poderá mitigar, de forma benéfica, a autonomia da autoridade supervisora. Pois, abrindo espaço para atuação do mercado como impositor das diretrizes exigidas, resulta-se como consequência dos benefícios econômicos auferidos, o cumpridor espontâneo da lei.

No entanto, a ausência do órgão fiscalizador traz prejuízos além dos que aqui foram mencionados até o presente momento. O Brasil manifestou seu interesse em participar da OCDE (Organização para a Cooperação e Desenvolvimento Econômico) em 2018, porém um dos requisitos exigidos para ingresso é a adequada proteção dos dados pessoais por meio de um órgão autônomo de acordo com a autoridade nacional.

Ademais, o pré-requisito para que países terceiros ofereçam um nível adequado de proteção de dados pessoais, é um controle efetivo independente das proteções. Isso se dá para que haja o livre fluxo de dados com os países da União Europeia, de acordo com exigências da GDPR. (UNIÃO EUROPEIA, 2016)

## 4.1. Características da Regulamentação de Risco e a prática da cooregulmentação

É importante observar a abordagem dos riscos envolvendo as operações com dados pessoais. O avanço do modelo econômico centrado em dados nos remete ao fato de que a proteção de dados pessoais está além da tutela à privacidade e se relaciona, também, à proteção de várias liberdades e direitos individuais. A prática da perfilização, que é a definição de um perfil de comportamento para o titular de dados em franca expansão, é o exemplo apto a demonstrar o aqui referido. Essa expansão pode gerar discriminação e inibição do exercício de liberdades.

Assim sendo, é possível chegar à conclusão de que a proteção de dados não está relacionada apenas à dimensão do indivíduo junto a sua privacidade e sim também aos valores coletivos de forma mais ampla. (BENETT; RABB, 2018)

O fato descrito acima, que tem como característica as ameaças causadas pelo tratamento de dados aperfeiçoa a ascensão dos riscos na proteção de dados pessoais. A regulação do risco tem como principal objetivo detectar um prejuízo futuro e que após análise de probabilidade haja desenvolvimento de medidas para antecipar a configuração do malefício, aniquilando-o na raiz e não permitindo que configure de fato o prejuízo.

Como aqui mencionado, tanto a LGPD quanto a GDPR reconhecem que operações que envolvem dados pessoais geram riscos às liberdades civis e aos direitos fundamentais e como

forma de prevenção está o papel do controlador de dados que elaborará um documento chamado relatório de impacto à privacidade. Neste documento, que é um estudo de impacto à privacidade, devem ser registrados os processos de tratamento de dados que representem ameaça considerável às garantias individuais, além de haver apontamento de ferramentas capazes de mitigar os riscos.

Ou seja, o papel desempenhado pelos responsáveis pela mitigação de riscos mostra uma dinâmica corregulatória em relação aos quadros legais. Assim sendo, sejam os atuantes públicos ou privados, são corresponsáveis pela promoção da proteção de dados pessoais por meio do poder de agência que exercem nas estruturas organizacionais que integram.

Tanto na GDPR, em seus artigos 40, 41 e 42; quanto na LGPD, no *caput* do artigo 50, há obrigatoriedade dos agentes de tratamento desenvolverem tais medidas desde que sejam apropriadas no sentido de observar as prescrições da Lei, como por exemplo as regras de boas práticas e de governança, diretrizes internas para processar dados, ações educativas, mecanismos internos de mitigação de riscos, dentre várias outras.

De acordo Rafael Zanatta, a proteção de dados pessoais baseada num modelo de regulação do risco conta com os seguintes elementos:

> (i) instrumentos de tutela coletiva e participação de entidades civis no diálogo preventivo com autoridades independentes de proteção de dados pessoais, (ii) obrigações e instrumentos de regulação ex ante atribuídas aos controladores para identificação de riscos a direitos e liberdades fundamentais, (iii) disseminação e metodologias de "gestão de risco" e calibragem entre riscos gerados pelo tratamento e uso de dados pessoais e imunidades jurídicas construídas pela discussão ética sobre os limites do progresso técnico. (ZANATTA, 2017)

Levando em consideração o primeiro ponto, interessa mencionar que tanto a legislação europeia quanto a brasileira trazem a possibilidade de adjudicação de demandas judiciais por organizações coletivas em relação à proteção de dados pessoais, sinalizando a crescente perspectiva que leva em consideração o interesse coletivo da matéria.

De forma resumida, é observado que existe uma convergência teleológica e estrutural entre os dois exemplos acima mencionados. Mas se levarmos em consideração apenas a prática, a União Europeia conta com um sistema de proteção de dados bem-desenvolvido e consolidado, resultado de uma evolução de décadas. Desde 1981 observa-se a matéria sendo abordada na legislação local da União. São pioneiros e isso permitiu a sintonia da evolução com os novos desafios trazidos pelas inovações tecnológicas que sucedem por meio dos anos.

Para que o Brasil chegue neste nível de desenvolvimento é preciso avançar na matéria, desenvolver um sistema nacional bem-sucedido por meio da criação de uma autoridade

nacional. A pluralidade de situações e questões que envolvem a proteção de dados e os desafios vivenciados bem como os futuros, tendo em vista o avanço tecnológico cada vez mais iminente, somente será superada e enfrentada por meio da participação eficaz da referida autoridade.

## CONCLUSÃO

Parte-se da premissa resultante da observação das evidências que se avolumam no que se refere à privacidade, a constatação de que, tanto a garantia como a proteção da mesma, são elementos fundamentalmente necessários ao conhecimento público.

Faz parte do senso comum a ideia que o direito caminha vagarosamente quando se trata das inovações ligadas à tecnologia. Assim, a legalidade própria dos reguladores dos fenômenos factuais que são, por sua vez, o produto das ações tecnológicas, incorre à necessidade de tornarem-se específicas, já que, em curto espaço de tempo, já estão obsoletas.

A proteção de dados pessoais está cimentada na necessidade de garantir à personalidade humana a tutela sobre a sua individualidade em todas as suas manifestações. Assim, quando se fala em proteger dados, torna-se imperativa a compreensão de que, intrinsecamente, indivíduos são protegidos, garantindo-lhes a segurança das suas manifestações a fim de assegurar-lhes que suas liberdades, sejam elas pessoais ou públicas, serão resguardadas. É de importância inquestionável assegurar que, a partir do momento em que essas liberdades são violadas, as consequências podem expandir-se, não sendo apenas sentidas no âmbito pessoal, como atingindo um corpo social.

Assim, percebe-se um agravante desta violação que, como elemento da matéria, infringe a ética e seus valores. Como consequência desse nexo de causalidade, as prerrogativas sobre as quais assenta-se o modelo de proteção de dados, baseiam-se na promoção de ações regulatórias bem elaboradas e dissociadas, até certo ponto, da atual situação tecnológica.

Há que haver uma ampliação da importância do assunto a nível social, uma vez que tal programa tem a faculdade de legislar sobre a defesa dos dados do elemento humano, seja ele independe e individual ou esteja inserido em grupos. A chancela sobre a publicidade de dados restringe-se ao detentor dos mesmos, cabendo a este ter consciência e controle sobre as informações que deseja serem públicas ou não

Nos anos subsequentes, é importante desenhar-se a possibilidade de ações gradativas que levarão à construção de um regime de proteção de dados pessoais com amola possibilidade de sucesso. Outro tópico a ser observado será quanto ao campo da ação predominante: seria este pessoal ou coletivo, uma vez que há intrínseca ligação entre ambos os polos.

## REFERÊNCIAS

Article 29 Data Protection Working Party. **Guidelines on consent under Regulation 2016/679**. Disponível em: <http://ec.europa.eu/newsroom/article29/itemdetail.cfm?item_id=623051>. Acesso em: 30/11/2020

BENNETT, Colin J. **Regulating privacy: data protection and public policy in Europe and the United States**. 1. ed. Nova Iorque: Cornell University Press, 1992. BENNETT, Colin; RAAB, Charles D**. Revisiting 'The Governance of Privacy': Contemporary Policy Instruments in Global Perspective**. 2018. Disponível em: <https://ssrn.com/abstract=2972086> Acesso em: 29/11/2020

BIONI, Bruno Ricardo**. Xeque-mate: o tripé da proteção de dados pessoais no jogo de xadrez das iniciativas legislativas no Brasil**. [S.l.: s.n.], 2016. Disponível em: <https://www.researchgate.net/publication/328266374_Xeque-Mate_o_tripe_de_protecao_de_dados_pessoais_no_xadrez_das_iniciativas_legislativas_no_Brasil>. Acesso em 30.11.2020

BIONI, Bruno Ricardo. **De 2010 a 2018: a discussão brasileira sobre uma lei geral de proteção de dados: Próximas semanas serão decisivas e pode não haver melhor momento para que Brasil deixe para trás seu atraso. JOTA**, [S.l.], 02 jul. 2018.

Disponível em: <https://www.jota.info/opiniao-e-analise/colunas/agenda-da-privacidade-e-daprotecaode- dados/de-2010-a-2018-a-discussao-brasileira-sobre-uma-lei-geral-de-protecaodedados- 02072018>. Acesso em 02/12/2020.

BIONI, Bruno Ricardo; MONTEIRO, Renato Leite; GOMES, Maria Cecília Oliveira. **GDPR matchup: Brazil's General Data Protection Law**. 2018. Disponível em: <https://iapp.org/news/a/gdpr-matchup-brazils-general-data-protection-law/>. Acesso em 30/11/2020.

BURGESS, Matt. **What is GDPR? The summary guide to GDPR compliance in the UK**. 20/03/2020. WIRED. Disponível em:< https://www.wired.co.uk/article/what-is-gdpr-uk-eulegislation-compliance-summary-fines-2018 >. Acesso em 01/12/2020.

DONEDA, Danilo Cesar Maganhoto. **A proteção de dados pessoais nas relações deconsumo: para além das informações creditícias**. Brasília: Secretaria de direito econômico / Departamento de proteção e defesa do consumidor, 2010.

DONEDA, Danilo Cesar Maganhoto; ALMEIDA, Virgílio Augusto Fernandes de**. Privacy Governance in Cyberspace.** IEEE Internet Computing, [S.l.], v. 19, n. 3, p. 50- 53, maio. 2015. Disponível em: <https://ieeexplore.ieee.org/document/7111890?reload=true>. Acesso em: 01/12/2020.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. 1. Ed. Rio de Janeiro: Renovar.

IRAMINA, A. **RGPD v. LGPD: Adoção Estratégica da Abordagem Responsiva na Elaboração da Lei Geral de Proteção de Dados do Brasil e do Regulamento Geral de Proteção de Dados da União Europeia.** Revista de Direito, Estado e Telecomunicações, Brasília, v. 12, nº 2, p. 91-117, Outubro de 2020.
DONEDA, Danilo Cesar Maganhoto**. Privacy and Data Protection in the Marco Civil da Internet.** Disponível em: <http://www.privacylatam.com/?p=239> Acesso em 02/12/2020.

DONEDA, Danilo Cesar Maganhoto; MENDES, Laura Schertel. **Lei de proteção de dados não pode morrer na praia: Eventual veto ameaçaria fino equilíbrio alcançado.** Folha de São Paulo, São Paulo, 10 mar. 2018. Opinião, p. 12. Disponível em:<https://www1.folha.uol.com.br/opiniao/2018/07/laura-schertel-mendes-e-danilodonedalei-de-protecao-de-dados-nao-pode-morrer-na-praia.shtml>. Acesso em 02/12/2020.

MONTEIRO, Renato Leite**. Lei Geral de Proteção de Dados do Brasil: análise contextual detalhada.** JOTA, [S.L.], 14 jul. 2018. Disponível em: < https://www.jota.info/opiniao-eanalise/colunas/agenda-da-privacidade-e-da-protecao-de-dados/lgpd-analisedetalhada14072018>. Acesso em 03/12/2020.

PRIVACY INTERNATIONAL. **The Keys to Data Protection:** a guide for policy engagement on data protection. [S.l.: s.n.], 2018. Disponível em: <https://privacyinternational.org/report/2255/data-protection-guide-complete>. Acesso em 01/12/2020.

SOLOVE, Daniel J. **Conceptualizing Privacy.** California Law Review, v. 90, p. 1088- 1156, jul. 2002.

SOLOVE, Daniel J. **I've Got Nothing to Hide and Other Misunderstandings of Privacy**. San Diego Law Review, San Diego, v. 44, p. 745-772, jan. 2007. Disponível em: <https://scholarship.law.gwu.edu/cgi/viewcontent.cgi?referer=https://scholar.google.com/&httpsredir=1&article=1159&context=faculty_publications>. Acesso em 30/11/2020.

ZANATTA, Rafael A. F. **Proteção de dados pessoais como regulação do risco: uma nova moldura teórica? I ENCONTRODA REDE DE PESQUISA EM GOVERNANÇA DA INTERNET**, NOVEMBRO DE 2017. Disponível em: <http://www.redegovernanca.net.br/public/conferences/1/anais/ZANATTA,%20Rafael_2017.pdf >. Acesso em 02/12/2020.

MADGE, Robert. **GDPR's global scope: the long story**. [S.l.: s.n.], 10 de maio de 2018. Disponível em: <https://medium.com/mydata/does-the-gdpr-apply-in-the-us-c670702faf7f>. Acesso em: 05/01/2021.

MOTEIRO, Renato Leite. et al. **Lei Geral de Proteção de Dados e GDPR: Histórico, análise e impactos.** [S.l.: s.n.], Janeiro de 2019. Disponível em: https://baptistaluz.com.br/wp-content/uploads/2019/01/RD-DataProtection-ProvF.pdf. Acesso em: 05/01/2021.

POLIDO, Fabrício B. Pasquot. et al. **GDPR e suas repercussões no direito brasileiro: Primeiras impressões de análise comparativa.** Instituto de Referência em Internet e Sociedade – IRIS. [S.l.]. 07 de Junho de 2018. Disponível em: https://irisbh.com.br/wp-content/uploads/2018/06/GDPR-e-suas-repercuss%c3%b5es-no-direito-brasileiro-Primeiras-impress%c3%b5es-de-an%c3%a1lise-comparativa-PT.pdf . Acessado em 05/01/2021.

CAVALCANTI, N; SANTOS, L**. Lei Geral de Proteção de Dados do Brasil na Era do Big Data**. In: FERNANDES, R; CARVALHO, A. Tecnologia Jurídica & Direito Digital: II Congresso Internacional de Direito, Governo e Tecnologia – 2018, Belo Horizonte: Fórum, 2018. p. 351 - 365