UNIVERSIDADE UNIVATES

CENTRO DE CIÊNCIAS HUMANAS E SOCIAIS

CURSO DE DIREITO

PROTEÇÃO GERAL DE DADOS: COMUNIDADE EUROPEIA X BRASIL

Vanessa Junior da Silva

Lajeado, novembro de 2019

Vanessa Junior da Silva

PROTEÇÃO GERAL DE DADOS: COMUNIDADE EUROPEIA X BRASIL

Monografia apresentada na disciplina de Trabalho de Curso II do Curso de Direito, da Universidade do Vale do Taquari – UNIVATES, como parte da exigência para obtenção do título de Bacharel em Direito.

Orientador: Prof. Dra. Thais C. Mueller

Lajeado, novembro de 2019.

AGRADECIMENTOS

Agradeço a Deus, por ter me proporcionado a vida, por me guiar, inspirar, e por sempre estar ao meu lado, me iluminando e renovando minhas forças.

Agradeço à minha filha Julia, por toda paciência e compreensão por nem sempre eu estar presente, você é meu maior amor, obrigada por me acompanhar e apoiar nessa conquista! “Amo você, tigrinha”!

Agradeço ao meu marido Cristiano, que me acompanhou nessa caminhada, com muita paciência, compreensão, esforço e por todos os lanchinhos gostosos. Obrigada por cuidar de tudo durante o tempo dedicado ao presente estudo!

Agradeço minha família por todo apoio, mesmo que de longe, sei que estão torcendo por mim!

Agradeço a minha orientadora Thais C. Muller por ter aceitado ser minha orientadora e ter contribuído com sua experiência e sabedoria para a realização deste trabalho.

Agradeço a todos os amigos, colegas e familiares que acompanharam minha trajetória na graduação e foram essenciais para a concretização deste objetivo.

Enfim, a todos que de alguma forma contribuíram para meu desenvolvimento e formação acadêmica. Muito obrigada!

RESUMO

O presente trabalho tem por objetivo estabelecer um comparativo entre a Proteção de Dados Pessoais, prevista na legislação brasileira (Lei nº 13.709 de 14/08/2018) e legislação da Comunidade Europeia (Regulamento Geral sobre a Proteção de Dados 2016/679), no intuito de revelar as semelhanças e dissonâncias entre as duas legislações, por meio de uma contextualização do desenvolvimento histórico do direito à privacidade, evolução da proteção da privacidade no ciberespaço e reconhecimento do direito à proteção de dados pessoais. Esta pesquisa buscará, através do método indutivo, baseado nas pesquisas bibliográfica e documental, estabelecer benefícios dessa nova legislação, utilizando-se material doutrinário sobre Proteção de Dados Pessoais, além do uso da legislação correspondente ao tema.

Palavras chave: Privacidade, Lei Geral de Proteção de Dados, Princípios, Dados pessoais.

LISTA DE ILUSTRAÇÕES

Lista de Quadros

LISTA DE ABREVIATURAS E SIGLAS

ANPD	Autoridade Nacional de Proteção de Dados
ART	Artigo
CC	Código Civil
CDC	Código de Defesa do Consumidor
CF	Constituição Federal
CJF	Conselho da Justiça Federal
ECA	Estatuto da Criança e do Adolescente
EUA	Estados Unidos
GDPR	Regulamento Geral sobre a Proteção de Dados da União Europeia
IP	Internet Protocol
LAI	Lei de Acesso à Informação
LGPD	Lei Geral de Proteção de Dados
MCI	Marco Civil da Internet
OCDE	Organização para a Cooperação e Desenvolvimento Econômico
ONU	Organização das Nações Unidas
PIPEDA	Personal Information Protection and Eletronics Documents Act
STJ	Superior Tribunal de Justiça
UE	União Europeia

SUMÁRIO

1 INTRODUÇÃO

A história da “Internet” no Brasil é recente, pouco mais de quarenta anos, em 1975, no Brasil, já se realizava transmissão eletrônica de dados (nomeada como telemática), entretanto sofreu e provocou muitas mudanças em todas as esferas da sociedade: para rentabilizar custos com a informática e garantir um serviço de qualidade, em abril de 1975, a Empresa Brasileira de Telecomunicações - Embratel foi incumbida, por determinação do Decreto 301, de instalar/explorar uma rede nacional de transmissão de dados.

Dados da Pesquisa Nacional por Amostra de Domicílio Contínua - PNAD/IBGE 2017 que abrangeu o acesso à internet constatou que, no ano 2017, 68,8% dos homens e 70,7% das mulheres acessavam a internet e o equipamento mais empregado para essa utilização era o celular (97%), seguido pelo microcomputador (56,6%). Sobre a finalidade, 95,5% utilizavam para enviar/receber mensagens de texto/voz/imagens; 83,8% conversavam por chamada de vídeo/voz; 81,8% utilizam para assistir vídeos (programas/séries/filmes); e 66,1% utilizam para enviar e receber e-mail.

Esses números evidenciam a existência de bancos de dados (que centralizam informações sobre usuários). Através desses bancos de dados, elabora-se o perfil de cada usuário e agrupam-se essas informações em grandes grupos de interesse; esses dados passaram a ser comercializados para as mais diversas áreas, que usavam o *Data Mining* para capturar, organizar e armazenar dados com a finalidade de identificar padrões de consumo e guiar as estratégias de *marketing* das empresas.

A preocupação com a gestão dos dados pessoais constantes nesses bancos é assunto relativamente novo e complexo, cujo principal objetivo é tutelar os direitos de personalidade (dados pessoais) que circulam on/off-line ao redor do mundo.

Segundo a Organização para Cooperação e Desenvolvimento Econômico (OCDE), esses dados são utilizados para servir melhor os clientes, tornar eficientes as transações, qualificar os produtos, intensificar macrotendências dos setores como: consumo, segurança, saúde e transporte. Entretanto, destaca no relatório que a ausência de legislação protetiva no tratamento dos dados pessoais, facilita a ocorrência de vazamento de dados em redes sociais para os mais diversos fins.

Diante desse cenário, de massificação do uso da internet para transmissão de dados, e para adequar-se a exigência de proteção no ciberespaço, foi necessária a criação de uma Lei Geral de Proteção de Dados (LGPD) para proteger os cidadãos e a sua privacidade. Entretanto, questiona-se se é suficiente a criação da LGPD para a efetivação da garantia protetiva dos dados pessoais/privacidade dos cidadãos brasileiros?

O presente trabalho buscará contextualizar, historicamente, quando o direito à privacidade começou a ser reconhecido e em que medida, esse direito é afetado em virtude da transmissão de dados no ciberespaço; mapear as principais propostas de regulamento do ciberespaço, desvelando os princípios norteadores desses regulamentos; analisar a evolução da proteção da privacidade no ciberespaço no Brasil como forma de efetivação desse direito; e por fim estabelecer um comparativo entre a Proteção de Dados Pessoais, prevista na legislação do Brasil (Lei nº 13.709 de 14/08/2018) e da Comunidade Europeia (Regulamento Geral sobre a Proteção de Dados 2016/679), no intuito de revelar as semelhanças e dissonâncias das duas legislações.

Adotou-se o método dedutivo, baseado nas pesquisas bibliográfica e documental, utilizando-se material doutrinário sobre Proteção de Dados Pessoais, além do uso da legislação correspondente ao tema. Mezzaroba e Monteiro (2016) destaca que propósito do raciocínio indutivo é chegar a conclusões mais amplas do que o conteúdo estabelecido pelas premissas nas quais está fundamentado, por esta razão, o presente trabalho é composto por três capítulos.

No primeiro capítulo, descreve-se o acerca do histórico mundial da proteção de dados, destacando-se as principais legislações que trataram sobre o assunto. Em seguida, analisa-se os aspectos gerais do desenvolvimento da proteção de dados pessoais no Brasil e por fim, realiza-se um estudo comparativo da proteção de dados pessoais na União Europeia e no Brasil, e considerações finais.

Assim, acredita-se na importância do desenvolvimento deste projeto, pois poderá trazer reflexões pessoais e acadêmicas sobre a tutela deste direito e, a partir desta análise, conscientização acerca da importância deste regulamento para garantir a efetivação da proteção aos dados pessoais adequada e necessária, sobretudo no que concerne à sua privacidade e honra.

2 HISTÓRICO MUNDIAL DA PROTEÇÃO DE DADOS

Pode-se dizer que a preocupação com o direito à privacidade é decorrente da construção doutrinária exposta por Warren e. Brandeis no artigo intitulado *The right to privacy,* publicado em 1890 na Harvard Law Review, defendendo o direito do homem de estar só.

Entretanto, esse direito à privacidade passou a ter uma maior magnitude ao ser reconhecido na Declaração Universal de Direitos do Homem (aprovada em 1948), que diz em seu artigo XII: “Ninguém será sujeito à interferência em sua vida privada, em sua família, em seu lar ou em sua correspondência, nem a ataque à sua honra e reputação. Todo ser humano tem direito à proteção da lei contra tais interferências ou ataques.”

A redação dada por esse regulamento evidencia, a existência de:

a) Sujeito: ser humano enquanto titular de um direito universal;
b) Conteúdo: faculdade jurídica de exigir a proteção e o respeito ao seu direito à vida privada;
c) Objeto da proteção: vida privada do ser humano, da sua família, em seu domicílio, sigilo de correspondência, proteção a sua honra e reputação.

Evidência, também, a possibilidade de manter-se em sigilo todos os atos praticados em âmbito privativo que dizem respeito, exclusivamente ao cidadão/ser humano e sua identidade pessoal e exclusiva, bem como as suas escolhas íntimas. De acordo com Ferraz Jr. (1993), existe uma gradação desses direitos que

compreendem, também, o direito ao nome, à imagem, à reputação, os quais, "...compõem o campo da privacidade" e são "...são exclusivos (próprios), mas perante os outros " e justifica: "... embora sejam de conhecimento dos outros, que deles estão informados, não podem transformar-se em objeto de troca do mercado".

Em razão da compreensão desse direito, em 1950, o Conselho da Europa elaborou a Convenção Europeia dos Direitos do Homem, reafirmando esse direito em seu artigo 8°, mas condicionando a sua proteção à segurança nacional/pública; ao bem-estar, defesa da ordem, prevenção de infrações penais, proteção à saúde, moral e direito de terceiros:

> Art 8º: 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 proteção da saúde ou da moral, ou a proteção dos direitos e das liberdades de terceiros.

Logo, referido direito não é absoluto, e pode sofrer ingerência da autoridade pública em prol dos direitos de terceiros, da sociedade e da manutenção da ordem pública do Estado.

Apesar da grande importância, os diplomas ora citados não garantiam uma proteção adequada à privacidade dos cidadãos, pois não tinham caráter impositivo, e não geravam uma obrigação aos estados-membros de proteger, através de instrumentos regulatórios (garantidores e limitadores), os direitos à privacidade contra seu uso indevido ou abusivo!

Segundo entendimento de Barreto Júnior (2007, p. 62):

> (...)a sociedade contemporânea atravessa uma verdadeira revolução digital em que são dissolvidas as fronteiras entre telecomunicações, meios de comunicação em massa e informática. Convencionou-se nomear esse novo "ciclo histórico" de Sociedade da Informação, cuja principal marca é o surgimento de complexas redes profissionais e tecnológicas voltadas à produção e ao uso da informação (que alcançam, ainda, sua distribuição através do mercado; bem como, a utilização desse bem para gerar conhecimento e riqueza).

Ante aos avanços tecnológicos e os impactos refletidos na dita Sociedade da Informação, fez-se necessário criar regulamentos para garantir direitos universais, como, no caso em análise, o direito à privacidade de usuários do ciberespaço, visando preservar dados de foro íntimo desses usuários.

2.1 *Privacy act* (EUA 1974)

Um dos primeiros instrumentos jurídicos a regulamentar a coleta, manutenção e uso de informações pessoais, mantidos em registros de órgãos federais foi a Lei da Privacidade, promulgada em 31 de dezembro de 1974 nos Estados Unidos,

Este dispositivo trouxe em seu conteúdo o entendimento de que a coleta, tratamento e disseminação de informações pessoais poderiam gerar efeitos danosos na vida dos indivíduos.

Entretanto, esse regulamento tinha seu alcance limitado somente às agências do governo, que usavam tecnologias essenciais para o Estado; mas que poderiam ampliar os riscos de exposição de informações pessoais dos cidadãos cujos dados estavam armazenados nos bancos de dados governamentais.

O *Privacy act* garantiu aos cidadãos norte-americanos uma série de direitos, tais como: acesso aos bancos de dados governamentais, direito à retificação de informações e responsabilização (nas esferas cíveis e criminais), em caso de violação e exposição dessas informações.

2.2 Convenção nº 108 do Conselho da Europa

Durante o início da década de 1980, a Organização para a Cooperação e Desenvolvimento Econômico (OCDE), grupo formado pelos países europeus afetados pela Segunda Guerra Mundial, que tinha por objetivo estabelecer políticas públicas de desenvolvimento econômico e social - instituiu diretrizes acerca da proteção de dados pessoais, que se baseavam em princípios de adesão voluntária, e por terem essa característica, não eram legalmente exigíveis.

Na Europa, a Convenção de Strasbourg nº 108 do Conselho Europeu (1981) foi o primeiro documento que buscou unificar e regulamentar a proteção de dados pessoais. Essa convenção dividia-se em três partes, sendo a primeira relativa aos objetivos, finalidades e princípios fundamentais, a segunda sobre fluxo fronteiriço de dados e a última sobre o acesso e consulta aos bancos de dados.

Em seu preâmbulo apresentava os objetivos do Conselho da Europa, que eram: conseguir uma união mais estreita entre os seus membros, sobretudo no que dizia respeito à supremacia dos direitos do homem e das liberdades fundamentais, ao mesmo tempo, garantir a liberdade de informação transfronteira.

Em seu primeiro artigo apresentava seus objetivos e suas finalidades:

> Artigo 1º - Objectivos e finalidades
>
> A presente Convenção destina-se a garantir, no território de cada Parte, a todas as pessoas singulares, seja qual for a sua nacionalidade ou residência, o respeito pelos seus direitos e liberdades fundamentais, e especialmente pelo seu direito à vida privada, face ao tratamento automatizado dos dados de carácter pessoal que lhes digam respeito («protecção dos dados»)(a Convenção de Strasbourg nº 108 do Conselho Europeu.1981).

Percebe-se que independentemente da sua nacionalidade, os cidadãos europeus tinham garantido o direito à vida privada (devendo-se proteger esses dados no caso de tratamento automatizado).

Em seu artigo 2º apresentava alguns conceitos e definições e finalizava o primeiro capítulo evidenciando que as disposições se aplicavam tanto ao setor público quanto ao privado, para em seguida, apresentar alguns princípios básicos e definições para fluxos transfronteiras de dados.

Doneda (2011) destaca a importância dos documentos supracitados, bem como dos princípios estabelecidos na Convenção nº 108 e nas *Guidelines* da OCDE, a serem aplicados na proteção de dados pessoais. Vale elencar aqui os princípios, tais como citados pelo autor:

> a) Princípio da publicidade (ou da transparência), pelo qual a existência de um banco de dados com dados pessoais deve ser de conhecimento público, seja por meio da exigência de autorização prévia para funcionar, da notificação a uma autoridade sobre sua existência, ou do envio de relatórios

> periódicos;
>
> b) Princípio da exatidão: os dados armazenados devem ser fiéis à realidade, o que compreende a necessidade de que sua coleta e seu tratamento sejam feitos com cuidado e correção, e de que sejam realizadas atualizações periódicas conforme a necessidade;
>
> c) Princípio da finalidade, pelo qual qualquer utilização dos dados pessoais deve obedecer à finalidade comunicada ao interessado antes da coleta de seus dados. Este princípio possui grande relevância prática: com base nele fundamenta-se a restrição da transferência de dados pessoais a terceiros, além do que se pode, a partir dele, estruturar-se um critério para valorar a razoabilidade da utilização de determinados dados para certa finalidade (fora da qual haveria abusividade);
>
> d) Princípio do livre acesso, pelo qual o indivíduo tem acesso ao banco de dados no qual suas informações estão armazenadas, podendo obter cópias desses registros, com a consequente possibilidade de controle desses dados; após este acesso e de acordo com o princípio da exatidão, as informações incorretas poderão ser corrigidas e aquelas obsoletas ou impertinentes poderão ser suprimidas, ou mesmo pode-se proceder a eventuais acréscimos;
>
> e) Princípio da segurança física e lógica, pelo qual os dados devem ser protegidos contra os riscos de seu extravio, destruição, modificação, transmissão ou acesso não autorizado (DONEDA, 2011, texto digital).

Assevera ainda o autor que:

> Estes princípios, mesmo que fracionados, condensados ou adaptados, formam a espinha dorsal das diversas leis, tratados, convenções ou acordos entre privados em matéria de proteção de dados pessoais, formando o núcleo das questões com as quais o ordenamento deve se deparar ao procurar fornecer sua própria solução ao problema da proteção dos dados pessoais (DONEDA, 2011, texto digital).

Resumidamente, o convênio assegura que os dados devem ser obtidos de forma lícita, utilizados para os fins que foram captados, as informações devem ser exatas e devem ser armazenados apenas pelo tempo necessário, de acordo com seus fins.

A Convenção nº 108 entrou em vigor em 1985, sendo o documento propulsor para a regulamentação dessa matéria em muitos países da Europa, porém tratava-se apenas de uma recomendação e referência para que os Estados membros elaborassem suas próprias leis, inclusive com diferentes níveis de proteção.

2.3 Diretiva 95/46/CE

A Diretiva 95/46/CE do Parlamento Europeu e do Conselho Europeu (CE), de 24.10.1995 tinha como objetivo uniformizar a coleta, o tratamento e uso dos dados pessoais pelos estados membros da União Europeia, servindo também como referência para países não membros.

Segundo Limberger (2007, p. 66), a Diretiva 95/46 diferenciava-se do Convênio nº 108 do Conselho Europeu por não se preocupar com “uso incontrolado” dos dados, sendo seu objetivo regular e proteger a livre circulação dos dados pessoais.

Em seu preâmbulo, a Diretiva apresenta 72 considerados, os quais de certa forma, antecipavam o texto da própria lei.

a) eliminação de barreiras entre os Estados pertencentes a mesma comunidade;
b) tratamento de dados observando-se os direitos fundamentais do cidadãos;
c) livre circulação de dados;
d) tratamento adequado dos dados pessoais;
e) fluxo transfronteiras de dados pessoais entre empresas;
f) coordenação de novas redes de telecomunicação para fins de cooperação científica;
g) harmonização da proteção dos direitos e liberdades pessoais entre os Estados membros;
h) equivalência do nível de proteção dos direitos referentes ao tratamento de dados;
i) permissão para os Estados membros especificarem na legislação nacional condições gerais de licitude do tratamento de dados;
j) garantir um elevado nível de proteção para os dados pessoais nas legislações nacionais;
k) ampliar e precisar os princípios da Convenção nº 108;
l) definir a quem se aplica o tratamento de dados pessoais;
m) estabelecer casos (segurança nacional) em que o tratamento de dados pessoais não é abrangido pela diretiva;
n) estabelecer as técnicas que se submetem a diretiva (captação, transmissão, manipulação, graduação, conservação, etc.);

o) necessidade de autorização, controle e acesso facilitado aos dados pessoais;
p) estabelecer a responsabilidade pelo tratamento dos dados em caso de filiais de empresas e em casos de empresas situadas fora da comunidade;
q) estabelece o âmbito da proteção (incluindo o tratamento manual/automatizado);
r) exigir o tratamento leal e lícito dos dados;
s) exigir que a pessoa seja informada sobre o motivo da recolha dos dados.

São os objetos dessa Diretiva, garantir “proteção dos direitos e liberdades fundamentais das pessoas singulares e, em particular, o seu direito à privacidade no que diz respeito ao tratamento de dados pessoais” (art. 1º, 1, da Diretiva 95/46/CE).

E para que todos os Estados membros partam do mesmo pressuposto, a diretiva define no artigo 2º os dados pessoais: “qualquer informação relativa a uma pessoa singular identificada ou identificável”, ou seja, pessoa singular que pode ser identificada, direta ou indiretamente, em particular por referência a um número de identificação ou a um ou mais fatores específicos à sua identidade física, fisiológica, mental, econômica, cultural ou social (art. 2º, a, da Diretiva 95/46/CE).

Sobre o tratamento de dados pessoais, considera-se qualquer operação ou conjunto de operações executadas com base em dados pessoais, ainda que não sejam feitos de forma automatizada, tais como coleta, organização, armazenamento, adaptação ou alteração, consulta, uso, divulgação, disseminação ou disponibilização, alinhamento ou combinação, bloqueio, apagamento ou destruição (art. 2º, b, da Diretiva 95/46/CE).

Para o tratamento leal e lícito, exige-se o consentimento para o tratamento de dados: “qualquer manifestação de vontade, livre, específica e informada, pela qual a pessoa em causa aceita que dados pessoais que lhe dizem respeito sejam objeto de tratamento” (art. 2º, h, da Diretiva 95/46/CE).

Quem quer que realize o tratamento e utilização dos dados pessoais, deve obedecer aos princípios elencados no artigo 6, da Diretiva 95/76/CE:

> a) processados de forma justa e legal;
>
> b) recolhidos para finalidades especificadas, explícitas e legítimas e não tratados posteriormente de forma incompatível com essas finalidades. O tratamento posterior de dados para fins históricos, estatísticos ou científicos

> não será considerado incompatível, desde que os Estados-Membros forneçam garantias adequadas;
>
> c) adequados, relevantes e não excessivos em relação aos fins para os quais são coletados e / ou processados posteriormente;
>
> d) precisas e, quando necessário, atualizadas; devem ser tomadas todas as medidas razoáveis para garantir que os dados imprecisos ou incompletos, tendo em conta as finalidades para as quais foram coletados ou para os quais são posteriormente processados, sejam apagados ou retificados;
>
> e) Mantidos de forma a permitir a identificação dos titulares dos dados por um período não superior ao necessário para os fins para os quais os dados foram coletados ou para os quais são posteriormente tratados. Os Estados-Membros devem estabelecer salvaguardas adequadas para os dados pessoais armazenados por períodos mais longos, para uso histórico, estatístico ou científico (Diretiva 95/76/CE, 1976).

Além dos princípios listados, para ser lícito o tratamento dos dados necessita o consentimento inequívoco do titular dos dados, bem como o tratamento deve ser necessário para a execução de um contrato do qual o titular dos dados é parte ou tenha solicitado; ou cumprir uma obrigação legal a que o responsável pelo tratamento está sujeito; ou para proteger os interesses vitais do titular dos dados; ou para a execução de uma tarefa realizada no interesse público ou no exercício da autoridade oficial investida no responsável pelo tratamento ou em um terceiro a quem os dados são divulgados; ou para fins dos interesses legítimos do controlador ou de terceiros ou terceiros a quem os dados são divulgados, desde que esses interesses não infrinjam direitos e liberdades fundamentais do titular dos dados (art. 7º, h, da Diretiva 95/46/CE).

Para garantir a proteção dos direitos e liberdades das pessoas, o artigo 8º prevê que “os Estados-Membros devem proibir o tratamento de dados pessoais que revelem origem racial ou étnica, opiniões políticas, crenças religiosas ou filosóficas, participação em sindicatos e o tratamento de dados relativos à saúde ou vida sexual”. Importa destacar que, para casos previstos nesse artigo há a possibilidade de tratamento excepcional, necessário para proteger os interesses vitais do titular dos dados, ou se este der o consentimento (art. 8º da Diretiva 95/46/CE).

Os titulares dos dados tem o *Direito de acesso* (a todos os titulares de dados é garantido o direito de obter do responsável pelo tratamento dos dados informações tais como: origem, objetivos, destinação e retificação; essas informações devem ser

prestadas em um prazo razoável e sem custo excessivo) e o *Direito de se opor ao tratamento dos dados* (gratuitamente, por motivos legítimos e particulares; devendo-se comunicar ao titular, antes que os dados pessoais sejam divulgados à terceiros) para permitir que ele se oponha à essa comunicação (caso queira).

No artigo 22 há garantia do "direito de todas as pessoas a um recurso judicial por qualquer violação dos direitos garantidos pela lei nacional aplicável ao tratamento em questão", logo, se não forem protegidos adequadamente os dados, os titulares (que tiveram algum tipo de abuso) poderão responsabilizar aqueles que violaram seus direitos.

Ao tratar da livre circulação de dados, a Diretiva da Comissão Européia, em seu artigo 27, estabelecia que a transferência de dados pessoais para países não pertencentes à União Européia dependia da criação de normas que atendiam ao padrão de "adequação" da União Europeia (UE) para proteção da privacidade, o que exigiu, de todos os países que mantinham algum tipo de relação com países da comunidade europeia, um *enforcement* da legislação (para fins de proteger adequadamente os dados pessoais que obtinham e tratavam). Quando o nível de proteção fosse considerado inadequado, os Estados-Membros deveriam tomar medidas para impedir qualquer transferência de dados para o país terceiro.

Em seu artigo 32, foi estabelecido um prazo máximo de três anos para que os Estados-membros adotassem disposições legislativas, regulamentares e administrativas necessárias para dar cumprimento à diretiva.

2.4 Regulamento geral sobre a proteção de dados

Em 2016, a União Europeia, ao aprovar o Regulamento Geral sobre a Proteção de Dados, incorporou os seguintes "*considerados*" acerca da Diretiva 95/46/CE em seu preâmbulo:

> (...)
>
> (3) A Diretiva 95/46/CE do Parlamento Europeu e do Conselho visa harmonizar a defesa dos direitos e das liberdades fundamentais das pessoas singulares em relação às atividades de tratamento de dados e assegurar a livre circulação de dados pessoais entre os Estados-Membros.

> (...)
>
> (9) Os objetivos e os princípios da Diretiva 95/46/CE continuam a ser válidos, mas não evitaram a fragmentação da aplicação da proteção dos dados ao nível da União, nem a insegurança jurídica ou o sentimento generalizado da opinião pública de que subsistem riscos significativos para a proteção das pessoas singulares, nomeadamente no que diz respeito às atividades por via eletrônica. As diferenças no nível de proteção dos direitos e das pessoas singulares, nomeadamente do direito à proteção dos dados pessoais no contexto do tratamento desses dados nos Estados-Membros, podem impedir a livre circulação de dados pessoais na União. Essas diferenças podem, por conseguinte, constituir um obstáculo ao exercício das atividades económicas a nível da União, distorcer a concorrência e impedir as autoridades de cumprirem as obrigações que lhes incumbem por força do direito da União. Essas diferenças entre os níveis de proteção devem-se à existência de disparidades na execução e aplicação da Diretiva 95/46/CE.

O considerando nº 10 refere que o novo regulamento visa “assegurar um nível de proteção coerente e elevado das pessoas singulares e eliminar os obstáculos à circulação de dados pessoais na União”, bem como instituir uma “determinação mais precisa das condições em que é lícito o tratamento de dados pessoais”. Isso foi necessário porque a Diretiva 95/46 CE, de 1995, mesmo com atualizações, já não correspondia aos avanços tecnológicos e comerciais:

> (10) A fim de assegurar um nível de proteção coerente e elevado das pessoas singulares e eliminar os obstáculos à circulação de dados pessoais na União, o nível de proteção dos direitos e liberdades das pessoas singulares relativamente ao tratamento desses dados deverá ser equivalente em todos os Estados-Membros. É conveniente assegurar em toda a União a aplicação coerente e homogénea das regras de defesa dos direitos e das liberdades fundamentais das pessoas singulares no que diz respeito ao tratamento de dados pessoais. No que diz respeito ao tratamento de dados pessoais para cumprimento de uma obrigação jurídica, para o exercício de funções de interesse público ou o exercício da autoridade pública de que está investido o responsável pelo tratamento, os Estados-Membros deverão poder manter ou aprovar disposições nacionais para especificar a aplicação das regras do presente regulamento. Em conjugação com a legislação geral e horizontal sobre proteção de dados que dá aplicação à Diretiva 95/46/CE, os Estados-Membros dispõem de várias leis setoriais em domínios que necessitam de disposições mais específicas. O presente regulamento também dá aos Estados-Membros margem de manobra para especificarem as suas regras, inclusive em matéria de tratamento de categorias especiais de dados pessoais («dados sensíveis»). Nessa medida, o presente regulamento não exclui o direito dos Estados-Membros que define as circunstâncias de situações específicas de tratamento, incluindo a determinação mais precisa das condições em que é lícito o tratamento de dados pessoais.
>
> (...)

Em virtude desse regulamento, o responsável pelo tratamento de dados deveria garantir a segurança dos dados pessoais, visando coibir a “destruição ou

perda acidental ou ilegal, alteração, divulgação ou acesso não autorizado, em especial nos casos em que o processamento envolva a transmissão de dados através de uma rede, e contra todas as outras formas ilegais de processamento" (art. 17,1, da Diretiva 95/46/CE); bem como deve informar esse tratamento para as autoridades de controle:

> (89) A Diretiva 95/46/CE estabelece uma obrigação geral de notificação do tratamento de dados pessoais às autoridades de controle. Além de esta obrigação originar encargos administrativos e financeiros, nem sempre contribuiu para a melhoria da proteção dos dados pessoais. Tais obrigações gerais e indiscriminadas de notificação deverão, por isso, ser suprimidas e substituídas por regras e procedimentos eficazes mais centrados nos tipos de operações de tratamento suscetíveis de resultar num elevado risco para os direitos e liberdades das pessoas singulares, devido à sua natureza, âmbito, contexto e finalidades. (...)

Em 25 de maio de 2018 o Regulamento Geral sobre a Proteção de Dados entrou em vigor na União Europeia, revogando a Diretiva 95/46/CE conforme se depreende da leitura do considerando abaixo transcrito:

> (171) **A Diretiva 95/46/CE deverá ser revogada pelo presente regulamento.** Os tratamentos de dados que se encontrem já em curso à data de aplicação do presente regulamento deverão passar a cumprir as suas disposições no prazo de dois anos após a data de entrada em vigor. Se o tratamento dos dados se basear no consentimento dado nos termos do disposto na Diretiva 95/46/CE, não será necessário obter uma vez mais o consentimento do titular dos dados, se a forma pela qual o consentimento foi dado cumprir as condições previstas no presente regulamento, para que o responsável pelo tratamento prossiga essa atividade após a data de aplicação do presente regulamento. As decisões da Comissão que tenham sido adotadas e as autorizações que tenham emitidas pelas autoridades de controle com base na Diretiva 95/46/CE, permanecem em vigor até ao momento em que sejam alteradas, substituídas ou revogadas (**grifo nosso**).

Por todo o exposto, pode-se dizer que, a Diretiva 95/46/CE foi de suma importância para a regulamentação e harmonização do assunto, sendo o documento propulsor de diversas leis, tanto de Estados-membros da União Europeia, quanto de estados terceiros.

2.5 *Safe Harbor* e *Privacy Shield* (EUA)

Para atender as exigências da diretiva europeia, surge nos Estados Unidos o *Safe Harbor*. Trata-se de um acordo político firmado entre os Estados Unidos da

América (EUA) e a União Europeia (UE), organizado em forma de princípios, sem natureza normativa e que, conforme entendimento de Alcântara (2017), objetivava a manutenção do fluxo internacional de dados de cidadãos europeus, visto que a Diretiva Europeia não permitia que os dados pessoais fossem transferidos para países que não se encontrassem dentro dos padrões de “adequação da proteção de dados”.

Ao assinar o tratado *Safe Harbor,* empresas como o Google, Facebook, Oracle, etc. (aproximadamente quatro mil empresas norte americanas), obtiveram a certificação necessária para acessar e tratar dados dos cidadãos europeus, tanto no bloco da União Européia, quanto nos EUA.

Segundo Murphy (2005), essas empresas comercializam dados sobre seus clientes no setor industrial, por isso o interesse em assinar esse tratado.

Logo, se os EUA quisessem manter o fluxo de dados, tratar e comercializar esses dados deveria adequar-se ao nível de proteção exigido pela Diretiva 95/46/CE.

Pelo mesmo motivo, o Canadá a criou a *Personal Information Protection and Eletronics Documents Act* - PIPEDA/2000 estabelecendo os seguintes princípios:

a) Responsabilidade pela informação pessoal a qual acedeu;
b) identificação dos fins para os quais as informações serão coletadas/armazenadas;
c) autorização do titular dos dados pessoais para a coleta, uso e divulgação desses dados;
d) limitação da coleta ao indispensável para atingir os fins identificados pela empresa;
e) limitação do uso, divulgação e armazenamento aos fins identificados e pelo tempo necessário para atingir esses fins;
f) exatidão, completude e atualização dos dados para atender a finalidade informada pela empresa;
g) *Safeguards* para proteger os dados tendo em vista a sensibilidade da informação coletada e armazenada;
h) transparência sobre suas práticas/políticas para o tratamento dos dados;

i) acesso para o titular dos dados retificar os seus dados pessoais e saber sobre a existência, uso, divulgação e armazenamento de seus dados;
j) possibilidade de o titular dos dados pessoais questionar a empresa sobre o cumprimento dos princípios legais.

A estrutura normativa do Safe Harbor estava alicerçada nos seguintes princípios:

a) Aviso prévio: as organizações deveriam notificar os indivíduos sobre as finalidades da coleta dos dados pessoais, informando como contatar a organização em caso de dúvidas ou reclamações sobre os tipos de terceiros aos quais divulgaria as informações. Também deveria informar os meios que a organização utilizaria para limitar o uso e divulgação indevidos.
b) escolha: os indivíduos deveriam ter a oportunidade de escolher desativar suas informações pessoais, impedindo que as mesmas fossem divulgadas a terceiros ou usadas para um propósito incompatível com a finalidade para a qual foram originalmente coletadas. Para informações sigilosas, o titular dos dados teria que autorizar que sua informação fosse divulgada a terceiros ou utilizada para um propósito diferente do propósito original ou autorizado.
c) transferência subsequente (transferências para terceiros): Para transferir informações a terceiros, as organizações deveriam aplicar os princípios de aviso e escolha. Quando uma organização quisesse transferir informações para um terceiro, ela poderia fazê-lo se cumprisse os Princípios de Privacidade do *Safe Harbor* ou as exigências da Diretiva.
d) acesso: os titulares dos dados deveriam ter acesso às informações pessoais que sobre eles uma organização detivesse e deveriam ter a possibilidade de corrigir, alterar ou excluir essas informações (quando estiverem imprecisas), exceto quando a despesa de acesso fosse desproporcional aos riscos à privacidade do indivíduo.
e) segurança: as organizações deveriam proteger os dados pessoais coletados contra perda, uso indevido, acesso não autorizado, divulgação, alteração e destruição.
f) integridade de dados: os dados pessoais deveriam ser relevantes para os propósitos para os quais seriam usados, garantindo-se que os dados fossem

confiáveis, precisos, completos e atuais e empregados apenas para o uso pretendido.

g) execução: A fim de assegurar a conformidade com os princípios de segurança, deveriam haver mecanismos independentes disponíveis para que as queixas e disputas fossem investigadas, resolvidas e fossem concedidas indenizações pelo vazamento de dados sempre que a legislação permitisse. Também deveriam haver procedimentos para verificar se os compromissos assumidos pelas empresas para aderir aos princípios do “porto seguro” foram implementados; e obrigações de resolver problemas decorrentes do descumprimento desses princípios.

Em outubro de 2015, o Tribunal Europeu de Justiça emitiu uma sentença declarando “inválida” a Decisão 2000/520/CE da Comissão Europeia “sobre a adequação da proteção fornecida pelos princípios de privacidade do *Safe Harbor* emitidas pelo Departamento de Comércio dos EUA”, no Acórdão C‑362/14 (Maximillian Schrems contra Comissário de Proteção de Dados).

Como resultado dessa decisão, o *Safe Harbor* deixou de ser um mecanismo válido para cumprir os requisitos de proteção de dados da União Europeia, e foi necessário criar-se outro acordo entre a União Europeia e os Estados Unidos: *Privacy Shield,* o qual realizou um *enforcement* do acordo anterior salvaguardando os dados privados dos cidadãos europeus, e estabelecendo sanções mais rígidas, reestabelecendo a confiança nas relações comerciais entre UE e EUA.

O programa *Privacy Shield*, atualmente em vigor, exige que as empresas afiliadas assegurem direitos aos titulares dos dados que são tratados, além de exigir o cumprimento de alguns princípios básicos de proteção de dados, tais como: manutenção da integridade dos dados, limitação de objetivos, sigilo, segurança dos dados, plataforma para reclamações, responsabilidade pela transferência dos dados e transparência. A adesão ao programa *Privacy Shield* é voluntária, porém é requisito obrigatório para operações que envolvam transferência de dados entre Estados Unidos e União Europeia.

Uma vez feita a adesão ao programa, o cumprimento a seus requisitos torna-se obrigatório e exigível pela lei local norte-americana, caso a empresa venha se

desvincular do programa, deverá garantir proteção "adequada" para as informações adquiridas durante o período de vinculação ao programa, devendo anualmente renovar seu compromisso.

3 ASPECTOS GERAIS DA PROTEÇÃO DE DADOS PESSOAIS NO BRASIL

No Brasil, a proteção geral de dados pessoais está prevista na Lei 13.709/2018, a qual tem como objetivo proteger os direitos fundamentais de liberdade, privacidade e o livre desenvolvimento da personalidade da pessoa natural. De acordo com o disposto nessa lei, o dado pessoal está relacionado com informação referente a pessoa identificada; por isso, Pinheiro (2018, p. 26), diz que os dados incluem, além do nome, sobrenome e documentos, também: “dados de localização, placas de automóvel, perfis de compras, número de *Internet Protocol* (IP), dados acadêmicos, histórico de compras, entre outros. ”

Conforme visto no capítulo anterior, os princípios fundamentais para a proteção dos dados pessoais são: o respeito à privacidade; direito à autodeterminação informativa; a liberdade de expressão, de informação, de comunicação e de opinião; a inviolabilidade da intimidade, da honra e da imagem; o desenvolvimento econômico e tecnológico e a inovação; a livre iniciativa, a livre concorrência e a defesa do consumidor; os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.

A regulamentação específica da proteção dos dados pessoais no Brasil se deu de forma gradual, porém o direito à privacidade possuía amparo na Constituição Federal, no Código Civil, no Código de Defesa do Consumidor, no Marco Civil da Internet e em outros diplomas legais como se verá a seguir.

3.1 A proteção de dados pessoais como um direito fundamental

O direito à proteção de dados pessoais emana do direito à intimidade e privacidade, assegurado na Declaração Universal de Direitos Humanos de 1948 como um direito humano. Pérez-Luño (1998, p. 48) descreve esses direitos como "...conjunto de faculdades e instituições que, em cada momento histórico, concretizam as exigências da dignidade, da liberdade e da igualdade [...]" que deveriam ser efetivados pelo Estado através dos direitos fundamentais dos cidadãos como "direitos humanos reconhecidos e positivados em determinada ordem constitucional (1998, p. 48) ". De acordo com Bobbio (2004, p. 9), os direitos fundamentais representam uma construção histórica, e por mais fundamentais que pareçam, são construídos através de lutas em defesa do reconhecimento de direitos, sendo constituídos gradualmente como novas gerações de direitos.

O reconhecimento dessas gerações de direitos está relacionado com a implementação do princípio da dignidade da pessoa que pressupõe, dentre outros, o direito à privacidade.

Por isso, o artigo 12 da Declaração Universal de Direitos Humanos (1948) prevê: "Ninguém será sujeito à interferência em sua vida privada, em sua família, em seu lar ou em sua correspondência, nem a ataque à sua honra e reputação. Todo ser humano tem direito à proteção da lei contra, tais interferências ou ataques. "

Reconhecido como direito fundamental, esse direito necessita de proteção por parte do Estado, o qual deve positivar os direitos naturais e inatos dos indivíduos. O Brasil, positivou vários desses direitos na Constituição Federal de 1988, eis que a dignidade da pessoa humana é corolária da República Federativa do Brasil:

> CF/88, Art. 1º A República Federativa do Brasil, formada pela união indissolúvel dos Estados e Municípios e do Distrito Federal, constitui-se em Estado Democrático de Direito e tem como fundamentos:
>
> I - a soberania;
>
> II - a cidadania
>
> III - a dignidade da pessoa humana;

> IV - os valores sociais do trabalho e da livre iniciativa;
>
> V - o pluralismo político.
>
> Parágrafo único. Todo o poder emana do povo, que o exerce por meio de representantes eleitos ou diretamente, nos termos desta Constituição (BRASIL, 1988).

Enquanto corolário da República Federativa do Brasil, a dignidade pressupõe salvaguarda, respeito e incentivo para efetivação dos direitos fundamentais, protegendo, inclusive, os direitos de personalidade das pessoas.

Por esse motivo, no artigo 5º, incisos X e XII, da CF, protege-se a privacidade do cidadão, como se depreende da leitura da transcrição:

> Art. 5º, CF/88,
>
> 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”;
>
> 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);

Mendes (2014) entende que reconhecer a proteção de dados como um direito fundamental não é apenas uma possibilidade, “trata-se de uma necessidade para tornar efetivos os fundamentos e princípios do Estado Democrático de Direito, na sociedade contemporânea da informação, conforme determina a Constituição Federal”.

Gilmar Mendes (2019, p. 287, livro digital) entende que “No âmago do direito à privacidade está o controle de informações sobre si mesmo”, por esse motivo e no que tange a esfera digital (com o crescente uso de redes sociais, sites de pesquisas e compras, transações bancárias *on-line)*, faz-se necessário ponderar, conforme Alcantara (2017, texto digital), “a privacidade é algo que deve ser preservada, não só por quem fornece os serviços, mas também por quem oferece os dados”, ela explica que ao divulgar qualquer informação na internet, a pessoa pode comprometer seu

futuro pessoal, ou praticar algum crime previsto no ordenamento jurídico. Segundo a autora, o que se posta na internet molda os cidadãos, revelando quem são.

Nesse sentido, aduz Mendes (2014) que:

> A disciplina da proteção de dados pessoais emerge no âmbito da sociedade de informação, como uma possibilidade de tutelar a personalidade do indivíduo, contra os potenciais riscos a serem causados pelo tratamento de dados pessoais. A sua função não é a de proteger os dados per se, mas a pessoa que é titular desses dados (MENDES, p. 32, texto digital).

A autora afirma ainda, que essa é a sociedade que mais gerou dados pessoais na história da humanidade:

> Por diversas razões, tais como a ampliação da complexidade do sistema industrial, a burocratização dos setores público e privado e a transformação das ciências sociais, **o certo é que nos tornamos a sociedade que mais gerou dados pessoais na história da humanidade**, o que pode ser demonstrado pelas dezenas de bancos de dados nos mais variados setores: registros de nascimento e casamento, registros escolares, dados do censo, registros militares, dados de passaporte, registros de empregados e de servidores públicos, registros do serviço de saúde, registros da defesa civil, registros de seguros, registros financeiros, registros de dados telefônicos, entre outros (MENDES, 2014, p. 32, texto digital, grifo nosso).

Conforme entendimento de Danilo Doneda (2011), por meio da proteção de dados pessoais, garantias a princípio relacionadas à privacidade passam a ser vistas em uma ótica mais abrangente, pela qual outros interesses devem ser considerados, abrangendo as diversas formas de controle tornadas possíveis com a manipulação de dados pessoais.

3.2 Código de defesa do consumidor - LEI Nº 8.078/1990.

O Código de Defesa do Consumidor é um conjunto de normas que visam a proteção do consumidor. Essa lei provocou inúmeras mudanças no ordenamento jurídico brasileiro, Venosa (2007, p. 225) apresenta, de forma resumida, a abrangência dessa lei:

> Seu caráter é interdisciplinar, daí porque se diz que criou um microssistema jurídico. Nele há normas de direito civil, direito comercial, direito administrativo, direito processual, direito penal. Seus princípios abarcam direito privado e o direito público, formando um terceiro gênero que a doutrina denomina direito social.

Esse código reconhece a vulnerabilidade do consumidor e estabelece a boa-fé como princípio basilar das relações de consumo; também, estabelece princípios básicos como: a proteção à vida, saúde e segurança, a educação para o consumo, o direito à informação clara, precisa e adequada, a proteção contra a publicidade enganosa e abusiva (a fim de promover equilíbrio nas relações de consumo).

Com isso, assegurou um melhor direito para os consumidores, entendidos no artigo 2º como: “toda pessoa física ou jurídica que adquire ou utiliza produto ou serviço como destinatário final”. Ressalta-se que, ao se examinar o tratamento de dados pessoais realizado no âmbito da relação de consumo identifica-se a vulnerabilidade do consumidor, isso porque os dados pessoais (assim como as demais informações extraídas a partir deles), constituem uma representação virtual da pessoa perante a sociedade, ampliando ou reduzindo as suas oportunidades no mercado. O consumidor (que tem os seus dados coletados e processados) pode ser vítima de discriminação no mercado de consumo. Isso acaba por afetar expressivamente o seu acesso a bens e serviços e as suas oportunidades sociais (MENDES, 2014, p. 197).

Os princípios basilares, que norteiam as relações de consumos estão listados no artigo 4º, e são:

> Art. 4º A Política Nacional das Relações de Consumo tem por objetivo o atendimento das necessidades dos consumidores, o respeito à sua dignidade, saúde e segurança, a proteção de seus interesses econômicos, a melhoria da sua qualidade de vida, bem como a transparência e harmonia das relações de consumo, atendidos os seguintes princípios:
>
> I - reconhecimento da vulnerabilidade do consumidor no mercado de consumo;
>
> II - ação governamental no sentido de proteger efetivamente o consumidor: a) por iniciativa direta; b) por incentivos à criação e desenvolvimento de associações representativas; c) pela presença do Estado no mercado de consumo; d) pela garantia dos produtos e serviços com padrões adequados de qualidade, segurança, durabilidade e desempenho.
>
> III - harmonização dos interesses dos participantes das relações de consumo e compatibilização da proteção do consumidor com a necessidade de desenvolvimento econômico e tecnológico, de modo a viabilizar os princípios nos quais se funda a ordem econômica (art. 170, da Constituição Federal), sempre com base na boa-fé e equilíbrio nas relações entre consumidores e fornecedores;
>
> IV - educação e informação de fornecedores e consumidores, quanto aos seus direitos e deveres, com vistas à melhoria do mercado de consumo;

> V - incentivo à criação pelos fornecedores de meios eficientes de controle de qualidade e segurança de produtos e serviços, assim como de mecanismos alternativos de solução de conflitos de consumo;
>
> VI - coibição e repressão eficientes de todos os abusos praticados no mercado de consumo, inclusive a concorrência desleal e utilização indevida de inventos e criações industriais das marcas e nomes comerciais e signos distintivos, que possam causar prejuízos aos consumidores;
>
> VII - racionalização e melhoria dos serviços públicos;
>
> VIII - estudo constante das modificações do mercado de consumo (BRASIL, 1990).

O rol de princípios não é taxativo, mas meramente exemplificativo, tal como os exemplos abaixo listados:

a) princípio da vulnerabilidade (art. 4, I, do CDC): O CDC reconhece o consumidor como pessoa vulnerável, não elencando critérios de distinção (poderio econômico, técnico ou intelectual);
b) princípio da equidade e da confiança (arts. 8, 9,10, 30, 31 e 54, §3, do CDC: O princípio da confiança diz respeito a confiança do consumidor para com o fornecedor.
c) princípio da boa -fé objetiva (art. 4, III, do CDC; art. 3º, I da CF): este princípio diz respeito ao deveres dos contratantes, que devem agir com respeito, responsabilidade, transparência e honestidade.
d) princípio da isonomia (art. 5º, XXXII, da CF e art. 4, I, do CDC): Trata-se de um princípio constitucional, que garante a todos o direito de ser tratados sem que haja tratamento desigual entre os consumidores.
e) princípio da função social do contrato (art. 51, §2, do CDC; art. 1º da CF e art. 421, CC): O art. 421 do novo Código Civil (CC) estabelece: “a liberdade de contratar será exercida em razão e nos limites da função social do contrato”
f) princípio do dever governamental (art. 4, II, VI e VII, do CDC): O CDC reconhece o consumidor como parte hipossuficiente da relação de consumo, e por esse motivo, determina que haja “ação governamental” para proteger o consumidor.

g) princípio da informação e da transparência (art 4, IV e VIII): trata-se do direito adquirido pelo consumidor de receber informações claras e precisas sobre o produto a ser adquirido.

A regulamentação dos bancos de dados encontra-se no artigo 43, Código de Defesa do Consumidor e regula os bancos de dados e cadastros de consumidores, trazendo a seguinte redação:

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

Filomeno (2014, p. 326), relembra que o CDC foi escrito “no contexto dos anos 90”, e naquele período, a preocupação era “disciplinar o banco de dados do consumidor relativo às suas informações creditícias, de caráter negativo, a exemplo daquelas geridas pelos servicos de proteção ao crédito”. Quanto aos direitos supracitados, Bioni (2019, p. 125) destaca que o consumidor é a figura central na relação de consumo:

> Tais direitos (acesso, retificação e cancelamento) e princípios (transparência, qualidade [exatidão] e limitação temporal) gravitam em torno da figura do consumidor, para que ele, na condição de titular dos dados pessoais, exerça

> controle sobre suas informações pessoais. Em suma, o Código de Defesa de Consumidor buscou conferir a autodeterminação informacional o que perpassa desde regras para garantir a exatidão dos dados até limitações temporais para o seu armazenamento (BIONI, 2019, p. 125).

Pode-se considerar bastante frágil a proteção dada aos dados pessoais nas relações de consumo, principalmente porque os dados coletados são usados para elaborar o perfil do consumidor, podendo acarretar tratamento discriminatório. Nesse sentido, Mendes (2014) declara que:

> Ao se examinar o tratamento de dados pessoais realizado no âmbito da relação de consumo, é fundamental se considerar a vulnerabilidade do consumidor nesse processo. Isso porque os dados pessoais, assim como as demais informações extraídas a partir deles, constituem-se em uma representação virtual da pessoa perante a sociedade, ampliando ou reduzindo as suas oportunidades no mercado, conforme a sua utilização. O risco ao consumidor que tem os seus dados coletados e processados ocorre, principalmente, quando o tratamento dos dados é realizado de forma equivocada ou discriminatória, acarretando a sua classificação e discriminação no mercado de consumo. Isso acaba por afetar expressivamente o seu acesso a bens e serviços e as suas oportunidades sociais (MENDES, 2014, p. 198, livro digital).

Contudo, pela redação da norma, é possível verificar a intenção do legislador de garantir aos consumidores a maior proteção possível.

3.3 *Habeas Data* - LEI Nº 9.507/1997

O instituto da *habeas data* está previsto na Constituição Federal de 1988, no artigo 5º, LXXII.

> Art. 5º; LXXII - conceder-se-á *habeas data:*
>
> a) para assegurar o conhecimento de informações relativas à pessoa do impetrante, constantes de registros ou bancos de dados de entidades governamentais ou de caráter público;
>
> b) para a retificação de dados, quando não se prefira fazê-lo por processo sigiloso, judicial ou administrativo;

Analisando-se o artigo é possível verificar:

a) o objeto da Habeas: informações relativas à pessoa do impetrante;

b) a legitimidade para pedir: o interessado deve ser titular das informações pessoais/registros de dados;
c) o jus facultas agendi: é assegurado o direito ao conhecimento de informações e retificação;
d) publicidade do processo, sempre que o titular não prefira fazê-lo por processo sigiloso, judicial ou administrativo.

Canotilho et al. (2018, p. 520) entendem que “o *habeas data* pode ser dividido em 02 etapas: uma extrajudicial, que não se precisa recorrer às vias judiciais, e outra judicial, por ainda persistir a afronta a direito protegido constitucionalmente”.

Os autores explicam o trâmite da seguinte forma:

> O requerimento para o pedido de informações será apresentado ao órgão ou entidade depositária do registro ou banco de dados e será deferido ou indeferido no prazo de quarenta e oito horas (art. 2o, caput, da Lei n. 9.507/97). A decisão do pedido de informações deve ser comunicada ao requerente dentro de prazo de vinte e quatro horas e, em caso de deferimento, será marcado dia e hora para o requerente tomar conhecimento das informações.
>
> Constatada a inexatidão da informação, o interessado pode apresentar explicação sobre o mesmo, justificando suas colocações. Mesmo se não se constatar inexatidão de dado, se o interessado apresentar explicação ou contestação sobre o mesmo, tal explicação será anotada em seu cadastro (art. 4o, § 2o, da Lei n. 9.507/97). Sendo o pedido de retificação acolhido, ela será realizada em, no máximo, dez dias após a entrada do requerimento, devendo a entidade ou órgão depositário dar ciência ao interessado.
>
> Acaso não puder ser a demanda resolvida na esfera extrajudicial, urge recorrer-se às vias judiciais para o cerceamento do gravame. A petição inicial deve atender todos os requisitos dos arts. 319 a 321 do Código de Processo Civil, apresentada em duas vias. Não há citação e sim sua notificação, uma vez que não há defesa e sim informações, haja vista a inexistência de lide no sentido de oposição de interesses e de sucumbência (CANOTILHO et al., 2018, p. 520, livro digital).

Trata-se de um instrumento de elevada importância, tendo prioridade sobre todos os atos judiciais para seu processamento, à exceção de trâmite de *habeas corpus* e *mandado de segurança.*

Conforme entendimento de Canotilho et al. (2018), o *habeas data*, apresenta uma única limitação:

> A única limitação ao habeas data, em razão do caráter sistêmico da Constituição, em que suas normas precisam ser interpretadas em correlação,

> é que o acesso a informações de órgãos públicos não abrange aquelas cujo sigilo seja imprescindível à segurança da sociedade e do Estado (art. 5o, XXXIII, da CF). Nessa hipótese, dada a aparente aporia, prevalece o interesse geral em detrimento do interesse individual. Ressalte-se que o Poder Judiciário deve analisar com cuidado esses casos de interesse à segurança da sociedade e do Estado para que entes governamentais não utilizem esses conceitos indeterminados de forma abusiva (CANOTILHO et al., 2018, p. 520, livro digital).

Em síntese, cabe *Habeas Datas*, para a retificação de informações, bem como a explicação ou contestação sobre dado verdadeiro, porém, justificável, que esteja sob pendência administrativa ou judicial, porém este dispositivo contempla apenas informações armazenadas nos bancos de registros públicos. Sendo necessário para a propositura do Habeas Datas o indeferimento do requerimento nas vias administrativas, ou o descumprimento nos casos deferidos, provando que a informação pretendida fora negada.

Trata-se de uma criação brasileira, criada para assegurar o conhecimento de informações relativas à pessoa do impetrante, constantes de registros ou bancos de dados de entidades governamentais ou de caráter público e para a retificação de dados, quando não se prefira fazê-lo por processo sigiloso, judicial ou administrativo.

Aduz Canotilho et al. (2018) que:

> O bem jurídico tutelado é de natureza individual, que cada um dos cidadãos pode dispor na medida em que não cause lesão a outros. Consiste em um direito à autonomia pessoal, que afeta predicativos reconhecidos legalmente, como intimidade, vida privada, honra, imagem, produzindo eficácia erga omnes. Igualmente faz parte do objeto tutelado a proteção da identidade informática, que decorre na prerrogativa de conhecer, retificar e assentar dados constantes em quaisquer fichários eletrônicos (CANOTILHO et al. 2018, p. 520, livro digital).

Trata-se de um remédio constitucional, que visa garantir ao cidadão o acesso de informações pessoais e a retificação, se necessária, sendo o exercício desse direito exercido de forma extrajudicial. A regulamentação do *habeas data (*expressão latina que significa “que tenhas os dados”) se deu através da Lei no 9.507, de 12 de novembro de 1997.

Conceder-se-á *habeas data* nos casos listados no artigo 7º da referida lei:

> Art. 7° Conceder-se-á *habeas data*:

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

Em julgado do Supremo Tribunal Federal sobre esse tema, o relator do caso, Ministro Celso de Mello, ao fundamentar as razões de seu voto, reitera a importância deste remédio constitucional:

> E M E N T A: RECURSO EXTRAORDINÁRIO – "HABEAS DATA" (CF, ART. 5º, LXXII) – PETROBRAS – SISPAT – REGISTROS DE NATUREZA PÚBLICA – LEGITIMIDADE PASSIVA "AD CAUSAM" DESSA SOCIEDADE DE ECONOMIA MISTA – CABIMENTO DA AÇÃO CONSTITUCIONAL – INCORPORAÇÃO, AO ACÓRDÃO, DAS RAZÕES EXPOSTAS PELO MINISTÉRIO PÚBLICO FEDERAL – MOTIVAÇÃO "PER RELATIONEM" – LEGITIMIDADE JURÍDICO- -CONSTITUCIONAL DESSA TÉCNICA DE FUNDAMENTAÇÃO – RECURSO DE AGRAVO IMPROVIDO. O Supremo Tribunal Federal, ao tratar da garantia constitucional de acesso a informações de caráter pessoal registradas em órgãos do Estado, reconheceu que esse tema envolve um dos aspectos mais expressivos da tutela jurídica dos direitos da personalidade, proferindo, então, em 1991, decisão consubstanciada em acórdão assim ementado: "- A Carta Federal, ao proclamar os direitos e deveres individuais e coletivos, enunciou preceitos básicos, cuja compreensão é essencial à caracterização da ordem democrática como um regime do poder visível. - O modelo político-jurídico, plasmado na nova ordem constitucional, rejeita o poder que oculta e não tolera o poder que se oculta. Com essa vedação, pretendeu o constituinte tornar efetivamente legítima, em face dos destinatários do poder, a prática das instituições do Estado. - O 'habeas data' configura remédio jurídico-processual, de natureza constitucional, que se destina a garantir, em favor da pessoa interessada, o exercício de pretensão jurídica discernível em seu tríplice aspecto: (a) direito de acesso aos registros; (b) direito de retificação dos registros e (c) direito de complementação dos registros. - Trata-se de relevante instrumento de ativação da jurisdição constitucional das liberdades, que representa, no plano institucional, a mais expressiva reação jurídica do Estado às situações que lesem, efetiva ou potencialmente, os direitos fundamentais da pessoa, quaisquer que sejam as dimensões em que estes se projetem. (...). " (RTJ 162/805-806, Rel. p/ o acórdão Min. CELSO DE MELLO, Pleno) (STF, RE 742701 AgR / PE, Rel. Min. CELSO DE MELLO, Julgamento em 24/09/2013).

Logo, o habeas data goza de um status de garantia constitucional servindo como mecanismo jurídico cuja finalidade é proteger os direitos fundamentais de privacidade (autodeterminação informativa) como o direito de "manter o controle sobre as próprias informações e de determinar as modalidades de construção da própria

esfera privativa...pode ser identificado no patrimônio informativo atual ou potencial de um sujeito” Rodotá (2008, p. 109).

Isso significa que trata-se de uma garantia de caráter instrumental para a privacidade dos dados pessoais que depende:

a) do direito à informação;
b) da liberdade de acesso para o titular dos dados;
c) notificação do titular;
d) da possibilidade de retificação, cancelamento e, bloqueio dos dados.

3.4 Direito Civil

Com a promulgação do Código Civil de 2002 percebeu-se uma alteração da estrutura privatista desse ramo do direito, como explica Lôbo (2014, p. 19):

> Se eu pudesse dizer em uma palavra qual o objeto central do Direito Civil Constitucional, no momento em que vivemos hoje no Brasil, diria que é “humanismo”, ou seja, ter a pessoa humana como foco central da investigação da aprendizagem, e da aplicação do Direito Civil.

Essa “humanização” do Direito Civil originou uma cláusula geral da personalidade a qual foi ratificada na IV Jornada de Direito Civil, no enunciado nº 274 do CJF/STJ:

> Os direitos da personalidade, regulados de maneira não-exaustiva pelo Código Civil, são expressões da cláusula geral de tutela da pessoa humana, contida no art. 1º, inc. III, da Constituição (princípio da dignidade da pessoa humana). Em caso de colisão entre eles, como nenhum pode sobrelevar os demais, deve-se aplicar a técnica da ponderação.

Ressalta-se que enquanto cláusula geral de tutela humana, os direitos de personalidade são “projeções da pessoa humana e da dignidade que lhe é inerente” (GODINHO; GUERRA, 2013, p. 180).

Nesse diapasão, leciona Bittar (2014, p.35), que os direitos da personalidade são aqueles inerentes à pessoa em função da estruturação física, mental e moral que lhes são próprias; e por isso, seriam dotados de características peculiares que lhe

conferem o status da singularidade na seara do direito privado, sobretudo quanto aos aspectos da intransmissibilidade e da sua irrenunciabilidade, que se projetam em garantias contra a ação lesivas aos dados do titular dos direitos.

Nesta esteira, entende Godinho (2014, p. 40) “a tutela da personalidade e da dignidade humana em nada recua ou se torna insuficiente quando se reconhece a elasticidade do rol dos direitos da personalidade”, segundo o autor, esses direitos ”se expandem tanto quanto seja necessário para resguardar a pessoa e seus valores existenciais”.

3.5 Lei Carolina Dieckmann - LEI Nº 12.737/ 2012

Em 30 de novembro de 2012 foi sancionada a Lei nº 12.737; a referida lei ficou conhecida popularmente como “Lei Carolina Dieckmann” (a lei ganhou esse apelido porque a atriz citada teve sua conta de *e-mail* atacada e fotos íntimas vazadas no mesmo ano de sancionamento da lei), foi criada para estabelecer a tipificação criminal de delitos informáticos, conforme transcrição do artigo:

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

> Supremo Tribunal Federal; III - Presidente da Câmara dos Deputados, do Senado Federal, de Assembleia Legislativa de Estado, da Câmara Legislativa do Distrito Federal ou de Câmara Municipal; ou IV - dirigente máximo da administração direta e indireta federal, estadual, municipal ou do Distrito Federal.

Antes da lei entrar em vigor não havia tipificação de crimes cibernéticos, com este diploma, invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita, tornou-se passível de prisão e multa.

3.6 Cadastro Positivo - LEI Nº 12.414/ 2011.

O Cadastro Positivo é um banco de dados, com informações relativas às operações de créditos de pessoas físicas e jurídicas, regulamentado pela Lei nº 12.414/11, que estabelece regras sobre o compartilhamento de dados, quais empresas são aptas a operar e receber os dados positivos, bem como a forma que a informação será usada.

Mendes (2014, p. 117) explica que “diante da importância que o conhecimento sobre os consumidores adquiriu na economia atual, os dados pessoais tornaram-se capital essencial para o sucesso de inúmeros negócios”.

Essa explicação se justifica, pois com as informações do Cadastro Positivo, comerciantes, bancos, financeiras e prestadores de serviços em geral elaboram um histórico de crédito dos consumidores, definindo assim condições comerciais, preços e taxas ajustados ao perfil de cada consumidor. Quanto mais dados referentes ao consumidor, mais eficiente será a análise econômica para fornecimento de crédito e risco do inadimplemento. Tecnicamente, o objetivo do Cadastro Positivo é beneficiar o consumidor. O Art. 3º, § 1º da lei prevê que “Para a formação do banco de dados, somente poderão ser armazenadas informações objetivas, claras, verdadeiras e de fácil compreensão, que sejam necessárias para avaliar a situação econômica do cadastrado”.

De acordo com o descrito no artigo supra, o cadastro positivo funciona como uma indicação (com base nas informações dos dados pessoais) mais segura para o tomador de créditos sobre risco do consumidor.

Segundo Grinover et al. (2019), os bancos de dados dos consumidores transformaram-se numa necessidade de mercado, principalmente os bancos de cadastros positivos:

> Na sociedade de consumo como a conhecemos, o consumidor não existe sem crédito; dele destituído, é um nada. Um bom histórico creditício é um patrimônio tão valioso quanto um currículo exemplar, no momento em que se procura emprego. Irrecusável que a influência dessas informações cadastrais nos destinos da vida do consumidor é poderosíssima, não tendo ele praticamente nenhum controle pessoal sobre onde e como seus antecedentes são fixados por terceiros, que desconhece (GRINOVER et al., 2019, p. 430).

Bancos de dados, com informações relativas às operações de créditos de pessoas físicas e jurídicas, já existiam antes da criação dessa lei de cadastros positivos, porém normalmente registravam-se apenas informações negativas. Sobre o tema, disserta Bessa (2014, texto digital):

> A grande maioria das informações registradas é denominada negativa: referem-se a dívidas vencidas e não pagas. Por se tratar de informação que enseja, invariavelmente, avaliação desfavorável quanto à concessão de crédito a alguém, cunhou-se o termo negativar e suas derivações: o consumidor não é registrado ou inscrito nos bancos de dados, ele é negativado (BESSA, 2014, texto digital).

O artigo 4º da lei determina que a abertura de cadastro requer autorização prévia do potencial cadastrado mediante consentimento informado por meio de assinatura em instrumento específico ou em cláusula apartada, e o artigo 5º, traz as prerrogativas do cadastrado:

> Art. 5º São direitos do cadastrado:
>
> I - obter o cancelamento do cadastro quando solicitado;
>
> II - acessar gratuitamente as informações sobre ele existentes no banco de dados, inclusive o seu histórico, cabendo ao gestor manter sistemas seguros, por telefone ou por meio eletrônico, de consulta para informar as informações de adimplemento;
>
> III - solicitar impugnação de qualquer informação sobre ele erroneamente anotada em banco de dados e ter, em até 7 (sete) dias, sua correção ou cancelamento e comunicação aos bancos de dados com os quais ele

> compartilhou a informação;
>
> IV - conhecer os principais elementos e critérios considerados para a análise de risco, resguardado o segredo empresarial;
>
> V - ser informado previamente sobre o armazenamento, a identidade do gestor do banco de dados, o objetivo do tratamento dos dados pessoais e os destinatários dos dados em caso de compartilhamento;
>
> VI - solicitar ao consulente a revisão de decisão realizada exclusivamente por meios automatizados; e
>
> VII - ter os seus dados pessoais utilizados somente de acordo com a finalidade para a qual eles foram coletados (BRASIL, 2011).

A partir desse cadastro, histórico de operações de créditos, tais como pagamentos realizados ou que venha a realizar, serão disponibilizados às instituições financeiras, sendo que essas informações deverão ser utilizadas, única e exclusivamente, para análise de eventual concessão de crédito.

A proteção do consumidor deve prevalecer, pois trata-se de uma garantia constitucional, nesse sentido, é oportuna a transcrição de Grinover et al. (2019, p. 529) “A acumulação de dados sobre o consumidor, por mais singela e útil que seja, não deixa de ser uma invasão de sua privacidade”.

Leonardo Roscoe Bessa (2014, texto digital) faz uma ressalva importante o tratamento de dessas informações:

> O tratamento de informações – positivas ou negativas – pelas entidades de proteção ao crédito é atividade potencialmente ofensiva a direitos da personalidade do consumidor (privacidade e honra). Embora relevantes para o mercado e para o consumidor, as entidades de proteção ao crédito devem observar rigorosamente os limites e requisitos estabelecidos pela lei, sob pena de ofensa a direitos da personalidade e, consequentemente, surgimento do dever de indenizar os danos morais e materiais causados aos consumidores (BESSA, 2014, texto digital).

A lei prevê ainda o direito de cancelamento do cadastro a qualquer momento, possibilidade de acessar gratuitamente as informações constantes nos bancos de dados, bem como a possibilidade de impugnar qualquer informação erroneamente anotada nos bancos de dados.

Referido cadastro gerou alguns efeitos, a saber:

a) melhoria na avaliação do tomador de crédito;
b) melhoria na taxa de juros dos consumidores considerados bons pagadores;
c) incentivo para consumidor quitar as dívidas;
d) diminuiu a inadimplência;
e) permitiu a expansão do mercado creditício;
f) contribuiu para viabilização do desenvolvimento econômico;
g) aumentou a transparência no mercado de crédito.

Nesse caso, os dados pessoais geram informações capazes de nortear o mercado creditício.

3.7 Lei de Acesso à Informação - LEI Nº 12.527/2011

A Lei de Acesso à Informação regulamentou o artigo 5º, XXXIII, CF, e determina que Poder Público tem a obrigação de disponibilizar o acesso à todas as informações de caráter público, de natureza contábil (financeira, orçamentária); operacional e patrimonial, com objetivo de concretizar a transparência pública relacionada com a gestão. Essa lei criou mecanismos que possibilitam qualquer pessoa, física ou jurídica (sem necessidade de apresentar motivo), obter informações públicas de órgãos e entidades.

Para garantir o acesso à informação pública, um conjunto de requisitos devem ser observados, com base nos seguintes princípios: o acesso é a regra; a solicitação não precisa ser motivada; o fornecimento é gratuito; as hipóteses de sigilo são limitadas e legalmente estabelecidas; e, o acesso deve ser facilitado atendendo o interesse coletivo e geral.

Não se pode olvidar que o acesso à informação é direito constitucional, previsto no artigo 5º, inciso XXXIII, que assegura a todos o direito a receber dos órgãos públicos informações de seu interesse particular, ou de interesse coletivo ou geral, que devem ser prestadas no prazo da lei, sob pena de responsabilização, ressalvadas aquelas cujo sigilo seja imprescindível à segurança da sociedade e do Estado. As hipóteses de sigilo que se refere esta lei são aquelas que tratam de acesso os dados

pessoais, as informações classificadas por autoridades como sigilosas e as informações sigilosas com base em outras leis.

Por isso, a lei de acesso à informação prevê em seu artigo 8, § 1 e incisos, a obrigação do Estado a disponibilizar documentos e informações nos canais de informação dos entes públicos.

Entretanto, o tratamento das informações pessoais deve ser restrito para proteger à intimidade, vida privada, honra e imagem das pessoas, bem como às liberdades e garantias individuais.

> Art. 31. O tratamento das informações pessoais deve ser feito de forma transparente e com respeito à intimidade, vida privada, honra e imagem das pessoas, bem como às liberdades e garantias individuais.
>
> § 1º As informações pessoais, a que se refere este artigo, relativas à intimidade, vida privada, honra e imagem:
>
> I - terão seu acesso restrito, independentemente de classificação de sigilo e pelo prazo máximo de 100 (cem) anos a contar da sua data de produção, a agentes públicos legalmente autorizados e à pessoa a que elas se referirem; e
>
> II - poderão ter autorizada sua divulgação ou acesso por terceiros diante de previsão legal ou consentimento expresso da pessoa a que elas se referirem.
>
> § 2º Aquele que obtiver acesso às informações de que trata este artigo será responsabilizado por seu uso indevido (BRASIL, 2011).

Logo, as informações pessoais, relativas à intimidade, vida privada, honra e à imagem (independentemente de classificação de sigilo), terão seu acesso restrito. Somente poderão ser acessadas pelos próprios indivíduos e, por terceiros, outorgados, mas esse acesso ocorrerá em casos excepcionais previstos na Lei.

> § 4º A restrição de acesso à informação relativa à vida privada, honra e imagem de pessoa não poderá ser invocada com o intuito de prejudicar processo de apuração de irregularidades em que o titular das informações estiver envolvido, bem como em ações voltadas para a recuperação de fatos históricos de maior relevância.
>
> § 5º Regulamento disporá sobre os procedimentos para tratamento de informação pessoal (BRASIL, 2011).

Quando as informações de dados pessoais forem necessárias para o interesse público, dispensa-se o consentimento expresso do titular dos dados, de acordo com previsão taxativa do artigo 31, § 3º, o qual estabelece:

> § 3º O consentimento referido no inciso II do § 1º não será exigido quando as informações forem necessárias:
>
> I - à prevenção e diagnóstico médico, quando a pessoa estiver física ou legalmente incapaz, e para utilização única e exclusivamente para o tratamento médico;
>
> II - à realização de estatísticas e pesquisas científicas de evidente interesse público ou geral, previstos em lei, sendo vedada a identificação da pessoa a que as informações se referirem;
>
> III - ao cumprimento de ordem judicial;
>
> IV - à defesa de direitos humanos; ou
>
> V - à proteção do interesse público e geral preponderante (BRASIL, 2011).

Será restringido o acesso às informações classificadas como sigilosas, ou seja, aquelas cuja divulgação possa colocar em risco a segurança da sociedade (vida, segurança, saúde da população) ou do Estado (soberania nacional, relações internacionais, atividades de inteligência). Por isso, apesar de serem públicas, o acesso a elas deve ser restringido por meio da classificação da autoridade competente.

Conforme o risco que a divulgação pode proporcionar à sociedade ou ao Estado, a informação pública pode ser classificada como ultrassecreta (25 anos), secreta (15 anos) e reservada (5 anos).

O legislador preocupou-se também em listar de forma específica e exaustiva quais informações podem ser consideradas sigilosas:

> Art. 23. “São consideradas imprescindíveis à segurança da sociedade ou do Estado e, portanto, passíveis de classificação as informações cuja divulgação ou acesso irrestrito possam:
>
> I - pôr em risco a defesa e a soberania nacionais ou a integridade do território nacional;
>
> II - prejudicar ou pôr em risco a condução de negociações ou as relações internacionais do País, ou as que tenham sido fornecidas em caráter sigiloso por outros Estados e organismos internacionais;
>
> III - pôr em risco a vida, a segurança ou a saúde da população;
>
> IV - oferecer elevado risco à estabilidade financeira, econômica ou monetária do País;

> V - prejudicar ou causar risco a planos ou operações estratégicos das Forças Armadas;
>
> VI - prejudicar ou causar risco a projetos de pesquisa e desenvolvimento científico ou tecnológico, assim como a sistemas, bens, instalações ou áreas de interesse estratégico nacional;
>
> VII - pôr em risco a segurança de instituições ou de altas autoridades nacionais ou estrangeiras e seus familiares; ou
>
> VIII - comprometer atividades de inteligência, bem como de investigação ou fiscalização em andamento, relacionadas com a prevenção ou repressão de infrações".

Há ainda, outras informações classificadas como informações sigilosas, que são protegidas por outras legislações, tais como os sigilos bancário, fiscal e industrial.

Haja vista a classificação dessas informações, não serão atendidos os pedidos que forem considerados genéricos, desproporcionais ou desarrazoados. A Controladoria Geral da União (CGU) no documento "Aplicação da Lei de Acesso à Informação em recursos da CGU", define tais conceitos da seguinte forma:

> Genérico: É aquele que não é específico, ou seja, não descreve de forma delimitada (quantidade, período temporal, localização, sujeito, recorte temático, formato, etc.) o objeto do pedido de acesso à informação, o que impossibilita a identificação e a compreensão do objeto da solicitação[...](CGU, 2015, p.33).
>
> Desproporcional: Analisa-se a adequabilidade do pedido de modo que seu atendimento não comprometa significativamente a realização das atividades rotineiras da instituição requerida, acarretando prejuízo injustificado aos direitos de outros solicitantes. O órgão deve indicar as razões de fato ou de direito da recusa total ou parcial da demanda, apresentando o nexo entre o pedido e os impactos negativos ao órgão (CGU, 2015, p.36).
>
> Desarrazoado: É aquele que não encontra amparo para a concessão de acesso solicitado nos objetivos da Lei de Acesso à Informação e tampouco nos seus dispositivos legais, nem nas garantias fundamentais previstas na Constituição. É um pedido que se caracteriza pela desconformidade com os interesses públicos do Estado em prol da sociedade, como a segurança pública, a celeridade e a economicidade da administração pública (CGU, 2015, p.37).

Esta lei é válida para os três Poderes da União, Estados, Distrito Federal e Municípios, inclusive aos Tribunais de Contas e Ministério Público. Entidades privadas sem fins lucrativos também são obrigadas a dar publicidade a informações referentes ao recebimento e à destinação dos recursos públicos por elas recebidos.

3.8 Marco Civil da Internet - Lei nº 12.965/2014

O Marco Civil da Internet (Lei n° 12.965, de 23 de abril de 2014) foi o primeiro marco regulatório brasileiro específico para proteção dos direitos fundamentais da intimidade e da liberdade de expressão no uso da internet, no entanto, restringe sua eficácia apenas às relações jurídicas realizadas pela internet, entre provedores e usuários; por isso sua divisão foi em cinco capítulos: disposições preliminares, direitos e garantias dos usuários, da provisão de conexão e de aplicações de internet, da atuação do poder público e, por fim, as disposições finais, com normas de transição.

De acordo com Lemos (2014, p. 10), “a situação pré - Marco Civil era de completa ausência de regulamentação civil da internet no país”.

Dentre os direitos tutelados pelo Marco Civil da Internet, está o direito de acesso à internet. Em 2011, Assembleia Geral da ONU determinou que o direito de acesso à internet é um direito humano fundamental:

> Os Estados têm a obrigação de promover o acesso universal à internet para garantir o gozo efetivo do direito à liberdade de expressão. O acesso à internet também é necessário para assegurar o respeito a outros direitos, como o direito à educação, à saúde e ao trabalho, ao direito de reunião e associação, e ao direito a eleições livres (ONU, 2011).

Sobre o direito de acesso à internet, Gonçalves (2017, p. 79) faz uma importante consideração:

> O direito de acesso à internet somente será pleno quando os usuários puderem se apropriar dos direitos e da tecnologia de forma clara e transparente. O direito de acesso à internet, num primeiro momento, independe da privacidade e da liberdade de expressão, o usuário deve possuir condições econômicas, sociais, históricas e culturais para se incluir digitalmente. E principalmente, o usuário tem de ser agraciado com políticas públicas que distribuam as infraestruturas de telecomunicações a todos de forma igualitária, o que não acontece no Brasil atualmente (2017, p. 79).

Antes do Marco Civil, no Brasil não havia nenhuma lei específica que tratasse do uso da internet, direitos e garantias dos usuários e deveres dos provedores, por isso se diz que o Marco Civil da Internet trouxe segurança jurídica, para as relações entre provedores e usuários de internet.

Em seus primeiros artigos, o Marco Civil da Internet estabelece os princípios e as garantias, os direitos e os deveres para o uso da internet no Brasil e estabelece as regras para atuação da União, dos Estados, do Distrito Federal e dos Municípios em relação à matéria.

Acerca das regras de proteção de dados pessoais, o MCI prevê os seguintes princípios:

a) Consentimento - O MCI determina que, como regra geral, não haverá fornecimento dos dados pessoais coletados pelos provedores de conexão e de aplicação de internet, contudo, traz a previsão do “consentimento livre, expresso e informado ou nas hipóteses previstas em lei”, tais exceções estão previstas nos artigos 7, VII e IX e 16, I do MCI; e
b) Transparência - O art. 7, VI, do MCI traz a determinação de que as informações constantes dos contratos de prestação de serviços devem ser claras e completas, com detalhamento sobre o regime de proteção aos registros de conexão e aos registros de acesso a aplicações de internet, bem como sobre práticas de gerenciamento da rede que possam afetar sua qualidade; no inciso XI, traz a garantia que deve haver clareza e publicidade de eventuais políticas de uso dos provedores de conexão à internet e de aplicações de internet. O princípio da transparência também está previsto no Código de Defesa do Consumidor, em seu art. 6º, inc. III que considera um “direito básico do consumidor a informação adequada e clara sobre os diferentes produtos e serviços, com especificação correta de quantidade, características, composição, qualidade, tributos incidentes e preço, bem como sobre os riscos que apresentem”; e
c) Proteção contra discriminação - Conforme art. 4, III do MCI, “a disciplina do uso da internet no Brasil tem por objetivo a promoção da inovação e do fomento à ampla difusão de novas tecnologias e modelos de uso e acesso”, nessa mesma perspectiva, o art. 6, II do CDC prevê que “a educação e divulgação sobre o consumo adequado dos produtos e serviços, asseguradas a liberdade de escolha e a igualdade nas contratações” são direitos básicos do consumidor. O Estado deve criar políticas públicas de inovação, promovendo o acesso à

educação e a cultura, deve também se empenhar para reduzir a exclusão social e digital; e

d) Comunicação em caso de vazamento - Antes da criação do Marco Civil da Internet, o Código de Defesa do Consumidor já garantia certa proteção nas relações de consumo, essa proteção estava prevista no artigo 10, § 1° da seguinte forma: “o fornecedor de produtos e serviços que, posteriormente à sua introdução no mercado de consumo, tiver conhecimento da periculosidade que apresentem, deverá comunicar o fato imediatamente às autoridades competentes e aos consumidores, mediante anúncios publicitários”. Com propósito de garantir a segurança jurídica nas relações de consumo, era imprescindível manter tal aplicação, sendo assim, ficou estabelecido no art. 7, XIII do MCI, que “o acesso à internet é essencial ao exercício da cidadania, e aos usuários são assegurados a aplicação das normas de proteção e defesa do consumidor nas relações de consumo realizadas na internet”; e
e) Segurança da informação e dos sistemas - O MCI, no artigo 10, diz que “A guarda e a disponibilização dos registros de conexão e de acesso a aplicações de internet, bem como de dados pessoais e do conteúdo de comunicações privadas, devem atender à preservação da intimidade, da vida privada, da honra e da imagem das partes direta ou indiretamente envolvidas. Ainda nesse artigo, no § 4º, declara que “as medidas e os procedimentos de segurança e de sigilo devem ser informados pelo responsável pela provisão de serviços de forma clara e atender a padrões definidos em regulamento, respeitado seu direito de confidencialidade quanto a segredos empresariais”. Neste caso, Gonçalves (2017, p. 101, livro digital) entende que “o Marco Civil não deixou nítido se as políticas de segurança de informação são integrantes dos contratos realizados entre os usuários e os provedores”, porém, ao analisar sob a “lógica da proteção dos dados pessoais”, a falta de clareza, bem como a ausência das políticas de segurança de informação tornam-se provas contra os próprios provedores de aplicações de internet”; e
f) Respeito ao contexto - Conforme artigo 7, VIII do MCI, as informações sobre coleta, uso, armazenamento, tratamento e proteção de seus dados pessoais devem ser claras e completas, somente poderão ser utilizados para finalidades que se a coleta for justificada, prevista em lei e que estejam especificadas nos contratos de prestação de serviços ou nos termos de uso de aplicações de

internet. Essa redação visa ampliar a proteção do usuário, no entendimento de Gonçalves (2017, p. 67, livro digital), “pela forma que os incisos foram escritos, os requisitos são cumulativos e não alternativos”.

Além dos princípios citados, o Marco Civil da Internet apresenta ainda importantes fundamentos que devem ser considerados, tais como: o respeito à liberdade de expressão, os direitos humanos, o desenvolvimento da personalidade e o exercício da cidadania em meios digitais, a pluralidade e a diversidade, a livre iniciativa, a livre concorrência e a defesa do consumidor e a finalidade social da rede.

Em seu artigo terceiro, disciplina os princípios, dentre eles o direito à privacidade e à proteção de dados pessoais, porém, sem os devidos enfrentamentos.

> Art. 3º A disciplina do uso da internet no Brasil tem os seguintes princípios:
>
> I - garantia da liberdade de expressão, comunicação e manifestação de pensamento, nos termos da Constituição Federal;
>
> II - proteção da privacidade;
>
> III - proteção dos dados pessoais, na forma da lei;
>
> IV - preservação e garantia da neutralidade de rede;
>
> V - preservação da estabilidade, segurança e funcionalidade da rede, por meio de medidas técnicas compatíveis com os padrões internacionais e pelo estímulo ao uso de boas práticas;
>
> VI - responsabilização dos agentes de acordo com suas atividades, nos termos da lei;
>
> VII - preservação da natureza participativa da rede;
>
> VIII - liberdade dos modelos de negócios promovidos na internet, desde que não conflitem com os demais princípios estabelecidos nesta Lei.
>
> Parágrafo único. Os princípios expressos nesta Lei não excluem outros previstos no ordenamento jurídico pátrio relacionados à matéria ou nos tratados internacionais em que a República Federativa do Brasil seja parte (BRASIL, 2014).

Dentre os princípios, há três que se destacam, que são os princípios da neutralidade da rede, da privacidade e da liberdade de expressão.

A neutralidade da rede está prevista no artigo terceiro, tendo sua definição no enunciado do artigo 9º, o qual apresenta a seguinte redação:

> Art. 9º O responsável pela transmissão, comutação ou roteamento tem o dever de tratar de forma isonômica quaisquer pacotes de dados, sem distinção por conteúdo, origem e destino, serviço, terminal ou aplicação (BRASIL, 2014).

O princípio da neutralidade da rede visa garantir tratamento isonômico, sem distinção por conteúdo, origem e destino, serviço, terminal ou aplicação, a fim de coibir o abuso de poder por parte do provedor.

No que diz respeito à privacidade, o Marco Civil da Internet garante aos internautas, nas comunicações por provedores de conexão e de aplicações de internet, proteção em qualquer operação de coleta, armazenamento, guarda e tratamento de registros, de dados pessoais, o fornecimento de registros depende de autorização judicial.

O Marco Civil da Internet trouxe também algumas regras inovadoras, que são:

a) controle de práticas abusivas: uso e compartilhamento de dados de forma abusiva (incompatibilidade com as finalidades do contrato inicial);
b) garantia da confidencialidade da comunicação: (independente da natureza do provedor do serviço);
c) garantia da confidencialidade do armazenamento;
d) nulidade de cláusulas contratuais: art. 8, do MCI;
e) Vedação da guarda e registros de acesso à serviços de internet para provedores de conexão: art. 14, do MCI.

Havendo violação da intimidade, da vida privada e do sigilo do fluxo das comunicações via internet, a lei prevê indenização pelo dano material ou moral sofrido, salvo a violação for decorrente de ordem judicial fundamentada, na forma da lei.

Sobre essa indenização, o Código Civil assegura em seu artigo 927 que “aquele que, por ato ilícito, causar dano a outrem, fica obrigado a repará-lo”, o valor da

indenização será fixado conforme artigo 944, desse mesmo código “a indenização mede-se pela extensão do dano (BRASIL, 2002)”.

Importante lembrar que, nos moldes o princípio da proporcionalidade, havendo necessidade de violação do direito à intimidade, à privacidade, ou do direito à proteção de dados pessoais, deve prevalecer o interesse da administração, da justiça e da ordem social, garantindo a harmonia entre normas, as regras e os princípios.

Para Gonçalves (2017, p. 7), “o Marco Civil consagrou a liberdade de expressão como fundamento principal do uso da internet no Brasil”. A proteção da liberdade de expressão na Internet foi um avanço do Marco Civil da Internet, regulamentar e assegurar a liberdade de expressão, a qual está prevista na Constituição de 1988, fez com que a Internet se tornasse um ambiente mais democrático, aberto e livre, e ao mesmo tempo, contempla e protege a intimidade e a vida privada.

Contudo, o MCI se absteve de regulamentar a proteção dos dados pessoais, o texto da lei fala apenas que tal proteção se dará na forma da lei.

4 A PROTEÇÃO DE DADOS PESSOAIS NA UNIÃO EUROPEIA E NO BRASIL

O Regulamento Geral sobre a Proteção de Dados da União Europeia (*European General Data Privacy Regulation*- GDPR, em inglês), que entrou em vigor em maio de 2018. Versa sobre a proteção de dados pessoais dos cidadãos da União Europeia. Começou a ser idealizado em 2012, sendo aprovado em 2016, substituindo assim a Diretiva 95/46 CE, de 1995, a qual mesmo com atualizações, já não correspondia aos avanços tecnológicos e comerciais.

Em virtude desse regulamento, estão protegidos os dados pessoais de qualquer pessoa na União Europeia, mesmo os não cidadãos, e se aplica a qualquer empresa que preste serviços a esses consumidores. Nesse sentido, Patrícia Peck Pinheiro (2018, p.18) explica a urgência do Brasil em tutelar a proteção de dados pessoais:

> [...] O Regulamento trouxe a previsão de dois anos de prazo de adequação, até 25 de maio de 2018, quando se iniciou a aplicação das penalidades.
>
> Este, por sua vez, ocasionou um “efeito dominó”, visto que passou a exigir que os demais países e as empresas que buscassem manter relações comerciais com a UE também deveriam ter uma legislação de mesmo nível que o GDPR. Isso porque o Estado que não possuísse lei de mesmo nível passaria a poder sofrer algum tipo de barreira econômica ou dificuldade de fazer negócios com os países da UE. Considerando o contexto econômico atual, esse é um luxo que a maioria das nações, especialmente as da América Latina, não poderia se dar (PINHEIRO, 2018, p.18).

Para adequar-se ao Regulamento Europeu, a Lei Geral de Proteção de Dados Pessoais do Brasil, foi sancionada dia 14 de agosto de 2018, que entrará em vigor em agosto de 2020. Pinheiro (2018, p.15) a classifica da seguinte forma: “É uma legislação extremamente técnica, que reúne uma série de itens de controle para assegurar o cumprimento das garantias previstas cujo lastro se funda na proteção dos direitos humanos. ”

Cabe esclarecer que o objetivo deste capítulo não é remontar toda a linha cronológica acerca dessa matéria, mas sim analisar, de forma comparativa, a Lei Geral de Proteção de Dados Pessoais do Brasil e o Regulamento Geral sobre a Proteção de Dados da União Europeia.

4.1 A proteção de dados pessoais na União Europeia

Conforme narrado, o Regulamento Geral sobre a Proteção de Dados da União Europeia (GDPR) é uma legislação protetiva para dados pessoais dos cidadãos da União Europeia, e está em vigor desde maio de 2018.

O regulamento europeu estabelece as regras relativas à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados, também defende os direitos e as liberdades fundamentais dessas pessoas.

Quanto a sua aplicabilidade material, o presente regulamento contempla o tratamento de dados pessoais (por meios totais ou parcialmente automatizados), bem como ao tratamento por meios não automatizados de dados pessoais contidos em ficheiros ou a eles destinados.

No que diz respeito à territorialidade, o artigo 3º determina que o presente regulamento se aplica ao tratamento de dados pessoais de titulares residentes no território da União Europeia, efetuado por um responsável pelo tratamento ou subcontratante situado no território da União, independentemente de o tratamento ocorrer dentro ou fora da União.

Os princípios garantidos pelo Regulamento Geral de Proteção de Dados são:

1) Princípio da legalidade, justiça e transparência**:** O processamento somente será legal se contemplar pelo menos um requisito, previstos no regulamento, que são:

a) necessidade de consentimento para o tratamento dos seus dados pessoais para um ou mais fins específicos; ou
b) necessidade do processamento para a execução de um contrato do qual o titular dos dados é parte ou para tomar medidas a pedido do titular dos dados antes de celebrar um contrato; ou
c) necessidade decorrente de uma obrigação legal a que o responsável pelo tratamento está sujeito; ou
d) quando houver necessidade de proteger os interesses vitais do titular dos dados ou de outra pessoa singular; ou
e) quando houver necessidade de execução do processamento para atender o interesse público ou no exercício da autoridade oficial investida no responsável pelo tratamento;
f) processamento é necessário para fins dos interesses legítimos prosseguidos pelo responsável pelo tratamento ou por terceiros, exceto quando esses interesses forem substituídos pelos interesses ou direitos e liberdades fundamentais do titular dos dados que exijam proteção de dados pessoais, em particular quando os dados sujeito é uma criança.

Os princípios supracitados estão previstos nos “considerados” que antecedem a lei.

> Considerando nº 39: Qualquer processamento de dados pessoais deve ser legal e justo. Deverá ser transparente para as pessoas físicas que os dados pessoais referentes a elas sejam coletados, usados, consultados ou processados de outra forma e até que ponto os dados pessoais serão ou serão processados. O princípio da transparência exige que qualquer informação e comunicação relacionada ao processamento desses dados pessoais seja facilmente acessível e fácil de entender, e que seja usada uma linguagem clara e clara. Este princípio refere-se, em particular, a informação aos titulares dos dados sobre a identidade do responsável pelo tratamento e os objetivos do tratamento, bem como informações complementares para garantir um tratamento justo e transparente em relação às pessoas singulares em causa e o seu direito de obter confirmação e comunicação de informações. Dados pessoais relativos aos que estão sendo processados. As pessoas singulares devem estar cientes dos riscos, regras, salvaguardas e direitos em relação ao processamento de dados pessoais e de como exercer seus direitos em relação a esse processamento. Em particular, os propósitos específicos para os quais os dados pessoais são processados devem ser explícitos, legítimos e determinados no momento da coleta dos dados

> pessoais. Os dados pessoais devem ser adequados, relevantes e limitados ao necessário para os fins para os quais são processados. Isso requer, em particular, garantir que o período durante o qual os dados pessoais sejam armazenados seja limitado a um mínimo estrito. Os dados pessoais devem ser processados apenas se o objetivo do processamento não puder ser razoavelmente cumprido por outros meios. Para garantir que os dados pessoais não sejam mantidos por mais tempo que o necessário, os prazos devem ser estabelecidos pelo controlador para apagamento ou para uma revisão periódica. Todas as medidas razoáveis devem ser tomadas para garantir que dados pessoais imprecisos sejam retificados ou excluídos. Os dados pessoais devem ser processados de maneira a garantir a segurança e confidencialidade adequadas dos dados pessoais, inclusive para impedir o acesso não autorizado ou o uso de dados pessoais e do equipamento usado para o processamento (GDPR, 2016).

2) Princípio da adequação e limitação da finalidade: Os dados pessoais devem ser adequados, relevantes e limitados ao necessário para os fins para os quais são coletados e processados.

3) Princípio da transparência: exige que qualquer informação e comunicação relacionada ao processamento desses dados pessoais seja facilmente acessível e fácil de entender, e que seja usada uma linguagem fácil e clara.

4) Princípio da qualidade dos dados ou exatidão: Este princípio visa assegurar que os dados serão exatos e completos, devendo respeitar a finalidade para os quais foram coletados, bem como a conservação deverá permanecer apenas durante o tempo necessário para que atenda a sua finalidade.

5) Princípio da limitação da conservação: Para garantir que os dados pessoais não sejam mantidos por mais tempo que o necessário, os prazos devem ser estabelecidos pelo controlador para apagamento ou para uma revisão periódica.

6) Princípio da segurança, integridade e confidencialidade: A segurança, integridade e confidencialidade nos tratamentos dos dados caberá ao responsável pelo tratamento, que deverá implantar “medidas técnicas” a fim de garantir que não haverá vazamento de dados ou outro tratamento ilícito.

7) Princípio da prestação de contas ou responsabilização: Os responsáveis pela proteção de dados devem trabalhar para garantir o cumprimento de todas as leis relevantes de proteção de dados, bem como realizar avaliações de impacto na proteção de dados, aumentar a conscientização dos funcionários quanto à proteção de dados e treiná-los adequadamente, além de colaborar com as autoridades de supervisão.

Percebe-se que os princípios estão interligados entre si e complementam-se. Caso haja conflito entre esses princípios, Tartuce (2019, p. 167, livro digital) recomenda que “o aplicador do Direito deve fazer uso da *técnica de ponderação* [...], que nada mais é do que a solução do caso concreto de acordo com a máxima da proporcionalidade”.

4.2 A proteção de dados pessoais no Brasil

O tratamento de dados pessoais por parte de empresas e de órgãos públicos é uma realidade cada vez mais presente na vida dos cidadãos devido ao rápido desenvolvimento tecnológico, o qual eleva o grau de coleta e compartilhamento desses dados, trazendo desafios para a proteção desses dados.

Diante desse contexto, torna-se imprescindível assegurar tratamento adequado aos dados pessoais, principalmente no que concerne aos dados sensíveis, definidos como aqueles que podem ensejar discriminação social, como os relativos à orientação religiosa, política ou sexual.

A relevância da proteção desses dados é evidente, sobretudo, no âmbito das relações de consumo. A falta de confiança dos consumidores na manutenção do sigilo de seus dados gera hesitação quando da aquisição de mercadorias e serviços, principalmente no ambiente on-line (comprometendo-se o próprio desenvolvimento econômico do país).

Patrícia Peck Pinheiro (2018) define a Lei Geral de Proteção de Dados da seguinte forma:

> A Lei n. 13.709/2018 é um novo marco legal brasileiro de grande impacto, tanto para as instituições privadas como para as públicas, por tratar da proteção dos dados pessoais dos indivíduos em qualquer relação que envolva o tratamento de informações classificadas como dados pessoais, por qualquer meio, seja por pessoa natural, seja por pessoa jurídica. É uma regulamentação que traz princípios, direitos e obrigações relacionados ao uso de um dos ativos mais valiosos da sociedade digital, que são as bases de dados relacionados às pessoas (PINHEIRO, 2018, p. 15).

Ainda, segundo Patrícia Peck Pinheiro (2018):

> O espírito da lei foi proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural, trazendo a premissa da boa-fé para todo o tipo de tratamento de dados pessoais, que passa a ter que cumprir uma série de princípios, de um lado, e de itens de controles técnicos para governança da segurança das informações, de outro lado, dentro do ciclo de vida do uso da informação que identifique ou possa identificar uma pessoa e esteja relacionada a ela, incluindo a categoria de dados sensíveis(PINHEIRO, 2018, p. 16).

Essa lei determina que, todas as atividades que envolvem o tratamento de dados pessoais deverão observar além do princípio da boa-fé e os seguintes princípios:

a) Princípio da Finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;
b) Princípio da Adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;
c) Princípio da 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;
d) Princípio do 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;
e) Princípio da 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;
f) Princípio da Transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;
g) Princípio da 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;
h) Princípio da Prevenção**:** adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;

i) Princípio da Não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;
j) Princípio da 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.

Segundo Geraldo Ataliba *apud* Tartuce (2019, p. 30) os princípios “são as linhas mestras orientadoras do ordenamento jurídico, que apontam os rumos a serem seguidos por toda a sociedade e obrigatoriamente seguidos pelos órgãos do governo”. Observa-se que, os princípios desempenham importante papel para a efetivação e concretização dos direitos dos titulares dos dados.

4.3 Estudo comparativo das proteções

A proteção dos dados pessoais passou a ser de suma importância ante ao rápido desenvolvimento tecnológico, bem como gerou uma necessidade de criação de leis para garantir a proteção dos titulares dos dados.

Para garantir que o Brasil se enquadrasse nas exigências estabelecidas pelo regulamento europeu, pois, os Estados que não incorporassem em seus ordenamentos internos, normas de proteção de dados pessoais, poderiam sofrer penalidades, tais como barreiras econômicas e impossibilidade de transações financeiras com os países membros da união europeia, foi criada a legislação brasileira.

Tanto o regulamento europeu, quanto o regulamento brasileiro, preocuparam-se em trazer logo nos primeiros capítulos alguns conceitos e definições essenciais, os quais serão a seguir apresentados.

a) Definição e diferenciação do que são dados pessoais:

Quadro 1 - Definição e diferenciação do que são dados pessoais

LGPD - BRASIL	**GDPR - UNIÃO EUROPEIA**
Art. 5º Para os fins desta Lei, considera-se: I - dado pessoal: informação relacionada a pessoa natural identificada ou identificável; II - dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural; III - dado anonimizado: dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento;	Art. 4. Para efeitos do presente regulamento: 1. Dados pessoais: qualquer informação relativa a uma pessoa singular identificada ou identificável (titular dos dados); uma pessoa singular identificável é aquela que pode ser identificada, direta ou indiretamente, em particular por referência a um identificador, como nome, número de identificação, dados de localização, identificador on-line ou a um ou mais fatores específicos de natureza física, fisiológica, identidade genética, mental, econômica, cultural ou social dessa pessoa natural; 13. Dados genéticos: dados pessoais relacionados com as características genéticas herdadas ou adquiridas de uma pessoa singular que fornecem informações únicas sobre a fisiologia ou a saúde dessa pessoa singular e que resultam, em particular, de uma análise de uma amostra biológica da natureza natural pessoa em questão; 14. Dados biométricos: dados pessoais resultantes de processos técnicos específicos relacionados com as características físicas, fisiológicas ou comportamentais de uma pessoa singular, que permitem ou confirmam a identificação única dessa pessoa singular, como imagens faciais ou dados dactiloscópicos; 15. Dados relativos à saúde: dados pessoais relacionados com a saúde física ou mental de uma pessoa singular, incluindo a prestação de serviços de saúde, que revelam informações sobre o seu estado de saúde;

Fonte: Da autora, (2019) com base nos dados da Lei.

Conforme se observa, ambas legislações fazem distinção entre dados pessoais e dados pessoais sensíveis, porém o regulamento europeu foi um pouco além, garantindo proteção aos dados genéticos, biométricos e dados relativos à saúde.

b) Dados pessoais de crianças e de adolescentes:

Quadro 2 - Dados pessoais de crianças e de adolescentes

LGPD - BRASIL	**GDPR - UNIÃO EUROPEIA**
Art. 14. O tratamento de dados pessoais de crianças e de adolescentes deverá ser realizado em seu melhor interesse, nos termos deste artigo e da legislação pertinente. § 1º O tratamento de dados pessoais de crianças deverá ser realizado com o consentimento específico e em destaque dado por pelo menos um dos pais ou pelo responsável legal. § 2º No tratamento de dados de que trata o § 1º deste artigo, os controladores deverão manter pública a informação sobre os tipos de dados coletados, a forma de sua utilização e os procedimentos para o exercício dos direitos a que se refere o art. 18 desta Lei. § 3º Poderão ser coletados dados pessoais de crianças sem o consentimento a que se refere o § 1º deste artigo quando a coleta for necessária para contatar os pais ou o responsável legal, utilizados uma única vez e sem armazenamento, ou para sua proteção, e em nenhum caso poderão ser repassados a terceiro sem o consentimento de que trata o § 1º deste artigo. § 4º Os controladores não deverão condicionar a participação dos titulares de que trata o § 1º deste artigo em jogos, aplicações de internet ou outras atividades ao fornecimento de informações pessoais além das estritamente necessárias à atividade. § 5º O controlador deve realizar todos os esforços razoáveis para verificar que o consentimento a que se refere o § 1º deste artigo foi dado pelo responsável pela criança, consideradas as tecnologias disponíveis. § 6º As informações sobre o tratamento de dados referidas neste artigo deverão ser fornecidas de maneira simples, clara e acessível, consideradas as características físico-motoras, perceptivas, sensoriais, intelectuais e mentais do usuário, com uso de recursos audiovisuais quando adequado, de forma a proporcionar a informação necessária aos pais ou ao responsável legal e adequada ao entendimento da criança.	Art. 8. Condições GDPR aplicáveis ao consentimento da criança em relação aos serviços da sociedade da informação 1. Quando se aplica o artigo 6.º, n. º 1, alínea a), em relação à oferta de serviços da sociedade da informação diretamente a uma criança, o tratamento dos dados pessoais de uma criança é legal quando a criança tiver pelo menos 16 anos de idade. 2. Quando a criança tiver menos de 16 anos de idade, esse processamento será legal somente se e na medida em que o consentimento for dado ou autorizado pelo titular da responsabilidade dos pais sobre a criança. 3. Os Estados-Membros podem prever por lei uma idade inferior para esses fins, desde que essa idade inferior não seja inferior a 13 anos. O responsável pelo tratamento deve fazer esforços razoáveis para verificar nos casos em que o consentimento é dado ou autorizado pelo detentor da responsabilidade dos pais sobre a criança, levando em consideração a tecnologia disponível. O n.º 1 não afeta o direito contratual geral dos Estados-Membros, como as regras relativas à validade, formação ou efeito de um contrato em relação a uma criança.

Fonte: Da autora, (2019) com base nos dados da Lei.

Nos termos do Estatuto da Criança e do Adolescente (ECA), considera-se criança a pessoa até doze anos de idade incompletos e, adolescente, aquela entre doze e dezoito anos de idade. No artigo 1º do ECA, está previsto o princípio da proteção integral, ou seja, “toda criança e adolescente são merecedores de direitos próprios e especiais que, em razão de sua condição específica de pessoas em desenvolvimento, estão a necessitar de uma proteção especializada, diferenciada e integral” (VERONESE, 2018, p. 49, texto digital), por este motivo, os dados pessoais de crianças e adolescentes devem receber tratamento diferenciado, devendo obedecer aos princípios da transparência e da finalidade. A LGPD determina que deverá haver o consentimento do responsável pela criança ou o adolescente até que este atinja a maioridade.

No regulamento europeu, diferentemente da lei brasileira, é possível que o adolescente com 16 anos completos (relativamente incapaz), mediante anuência de um dos responsáveis legais, conceda este consentimento.

c) Definição e diferenciação do que são bancos de dados:

Quadro 3 - Definição e diferenciação do que são bancos de dados

LGPD - BRASIL	**GDPR - UNIÃO EUROPEIA**
Art. 5, IV - banco de dados: conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico;	Art. 4. 6. Sistema de arquivamento: qualquer conjunto estruturado de dados pessoais que sejam acessíveis de acordo com critérios específicos, centralizados, descentralizados ou dispersos com base funcional ou geográfica;

Fonte: Da autora, (2019) com base nos dados da Lei.

Ambas legislações se preocuparam em definir o conceito de banco de dados, o qual é considerado como “conjunto estruturado de dados pessoais”, podendo ser eletrônico ou físico.

Logo no primeiro artigo, a LGPD, traz em seu texto a seguinte expressão “Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais (…) ”. Apesar das constantes revoluções digitais, onde o meio mais utilizado para transações é o ciberespaço, é importante destacar que a LGPD serve também para a “papelada”,

ou seja, a lei aplica-se às informações coletadas, não importando o meio (físico/digital/*on-off line*).

d) Definição e importância do consentimento:

Quadro 4 - Definição e importância do consentimento

LGPD - BRASIL	**GDPR - UNIÃO EUROPEIA**
Art. 5º, XII - consentimento: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada;	Art. 4º. 11. consentimento do titular dos dados: qualquer indicação dada livremente, específica, informada e inequívoca dos desejos do titular dos dados pelos quais ele ou ela, por uma declaração ou por uma ação afirmativa clara, significam concordância com o tratamento de dados pessoais relacionados a ele ou ela**;**

Fonte: Da autora, (2019) com base nos dados da Lei.

Além da definição do termo “consentimento”, tanto a lei brasileira, quanto o regulamento europeu, incluíram princípios e regras para disciplinar o tratamento dos dados, impondo limitações ao responsável pelo tratamento.

O artigo 8º da LGPD dispõe sobre a forma empregada para obtenção do consentimento, sendo vedado o tratamento de dados pessoais com vícios de consentimento, bem como sendo consideradas nulas as “autorizações genéricas”.

Ainda, o consentimento deverá atender à finalidade pré-determinada e, havendo necessidade de alterações nos termos do consentimento, o titular, quando informado, revogá-lo. O direito à revogação do consentimento poderá ser exercido a qualquer tempo, e deverá ser possibilitado de forma acessível, por procedimento gratuito e facilitado, mediante manifestação expressa do titular, nos termos da legislação:

> Art. 8º O consentimento previsto no inciso I do art. 7º desta Lei deverá ser fornecido por escrito ou por outro meio que demonstre a manifestação de vontade do titular.
>
> § 1º Caso o consentimento seja fornecido por escrito, esse deverá constar de cláusula destacada das demais cláusulas contratuais.
>
> § 2º Cabe ao controlador o ônus da prova de que o consentimento foi obtido

> em conformidade com o disposto nesta Lei.
>
> § 3º É vedado o tratamento de dados pessoais mediante vício de consentimento.
>
> § 4º O consentimento deverá referir-se a finalidades determinadas, e as autorizações genéricas para o tratamento de dados pessoais serão nulas.
>
> § 5º O consentimento pode ser revogado a qualquer momento mediante manifestação expressa do titular, por procedimento gratuito e facilitado, ratificados os tratamentos realizados sob amparo do consentimento anteriormente manifestado enquanto não houver requerimento de eliminação, nos termos do inciso VI do caput do art. 18 desta Lei.
>
> § 6º Em caso de alteração de informação referida nos incisos I, II, III ou V do art. 9º desta Lei, o controlador deverá informar ao titular, com destaque de forma específica do teor das alterações, podendo o titular, nos casos em que o seu consentimento é exigido, revogá-lo caso discorde da alteração(LGPD, 2018).

O consentimento, de forma clara, transparente e adequada, é extremamente importante, assim como a delimitação da finalidade para qual se concede o consentimento, por este motivo, a lei assegurou ao titular dos que, “se houver mudanças da finalidade para o tratamento de dados pessoais, diferentes das que originalmente estava previsto, o controlador deverá informar previamente o titular sobre as mudanças de finalidade, podendo o titular revogar o consentimento, caso discorde das alterações”; como se depreende da leitura do seguinte artigo:

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

> § 1º Na hipótese em que o consentimento é requerido, esse será considerado nulo caso as informações fornecidas ao titular tenham conteúdo enganoso ou abusivo ou não tenham sido apresentadas previamente com transparência, de forma clara e inequívoca.
>
> § 2º Na hipótese em que o consentimento é requerido, se houver mudanças da finalidade para o tratamento de dados pessoais não compatíveis com o consentimento original, o controlador deverá informar previamente o titular sobre as mudanças de finalidade, podendo o titular revogar o consentimento, caso discorde das alterações.
>
> § 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 (LGPD, 2018).

O regulamento europeu considera o consentimento muito importante, tanto que garante aos titulares dos dados que “Deve ser tão fácil retirar-se quanto dar consentimento”, ou seja, o agente responsável pelo tratamento tem o dever legal de conceder ao titular dos dados informações claras e completas, inclusive sobre a possibilidade de revogação do consentimento:

> Art 7, 3. O titular dos dados terá o direito de retirar o seu consentimento a qualquer momento. A retirada do consentimento não afetará a legalidade do processamento com base no consentimento antes de sua retirada. Antes de dar o seu consentimento, o titular dos dados deve ser informado. **Deve ser tão fácil retirar-se quanto dar consentimento (grifo nosso)** (GDPR, 2016)**.**

Nota-se que o consentimento se tornou o núcleo central em ambas normas de proteção, gerando um empoderamento do titular dos dados e zelando pela sua segurança jurídica.

e) Definição e diferenciação acerca dos responsáveis pelo tratamento dos dados:

Quadro 5 - Definição e diferenciação acerca dos responsáveis pelo tratamento dos dados

LGPD - BRASIL	**GDPR - UNIÃO EUROPEIA**
Art 5º, VI - controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais; VII - operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador; VIII - encarregado: pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD); IX - agentes de tratamento: o controlador e o operador;	Art. 4º. 7. Responsável pelo tratamento: a pessoa singular ou coletiva, a autoridade pública, a agência ou outro organismo que, individualmente ou em conjunto com outras, determina as finalidades e os meios de tratamento de dados pessoais; sempre que as finalidades e os meios desse tratamento sejam determinados pelo direito da União ou de um Estado-Membro, o responsável pelo tratamento ou os critérios específicos aplicáveis à sua nomeação podem ser previstos pelo direito da União ou de um Estado-Membro; 8) Subcontratante: uma pessoa singular ou coletiva, a autoridade pública, agência ou outro organismo que trate os dados pessoais por conta do responsável pelo tratamento destes;

Fonte: Da autora, (2019) com base nos dados da Lei.

Como pode-se observar, ambas legislações apresentam nomenclaturas diferentes, porém as atribuições são muito próximas, pois ambos são responsáveis pelo tratamento, pela segurança e pela privacidade dos dados tratados.

f) Possibilidade de alteração e exclusão do dado pessoal:

Quadro 6 - Possibilidade de alteração e exclusão do dado pessoal

LGPD - BRASIL	**GDPR - UNIÃO EUROPEIA**
Art. 16. Os dados pessoais serão eliminados após o término de seu tratamento, no âmbito e nos limites técnicos das atividades, autorizada a conservação para as seguintes finalidades:	Art. 17. 1. O titular tem o direito de obter do responsável pelo tratamento o apagamento dos seus dados pessoais, sem demora injustificada, e este tem a obrigação de apagar os dados pessoais, sem demora injustificada, quando se aplique um dos seguintes motivos:

Continua

I - cumprimento de obrigação legal ou regulatória pelo controlador; sempre que possível, a anonimização dos dados pessoais; III - transferência a terceiro, desde que respeitados os requisitos de tratamento de dados dispostos nesta Lei; ou IV - uso exclusivo do controlador, vedado seu acesso por terceiro, e desde que anonimizados os dados.	Art. 17. 1. O titular tem o direito de obter do responsável pelo tratamento o apagamento dos seus dados pessoais, sem demora injustificada, e este tem a obrigação de apagar os dados pessoais, sem demora injustificada, quando se aplique um dos seguintes motivos: b)O titular retira o consentimento em que se baseia o tratamento dos dados nos termos do artigo 6.o, n.o 1, alínea a), ou do artigo 9.o, n.o 2, alínea a) e se não existir outro fundamento jurídico para o referido tratamento;

Fonte: Da autora, (2019) com base nos dados da Lei.

O GDPR garante ao titular dos dados o chamado “direito a ser esquecido”, tal previsão encontra-se no artigo 17, e determina que o responsável pelo tratamento dos dados deverá apagá-los sempre que, por exemplo, estes deixam de ser necessários para a finalidade que foram recolhidos, quando o consentimento para o tratamento for retirado ou quando os dados forem tratados ilicitamente. Há também a possibilidade do titular dos dados rejeitar o pedido de exclusão (em virtude do exercício do direito à liberdade de expressão e informação; do cumprimento de uma obrigação legal; para atender uma obrigação legal para o desempenho de uma tarefa de interesse público; por razões de interesse público, para fins de investigação científica, histórico ou estatísticos; ou para o exercício ou defesa de um direito num processo judicial).

A lei brasileira também prevê o direito de exclusão (artigos 16 e 17, da LGPD), que deverá acontecer sempre que finalidade para a qual foram coletados os dados chegar ao fim; ou quando titular de os dados solicitar (salvo nos casos previstos em lei), ou se houver a revogação do consentimento; ou ainda, por determinação da autoridade nacional.

Ambas legislações visam evitar que os tratamentos dos dados sejam realizados indiscriminadamente e/ou por tempo indeterminado, e contra a vontade do titular dos dados.

g) Sanções previstas no caso do descumprimento das regras:

Quadro 7 - Sanções previstas no caso do descumprimento das regras

LGPD - BRASIL	**GDPR - UNIÃO EUROPEIA**
Art. 52. Os agentes de tratamento de dados, em razão das infrações cometidas às normas previstas nesta Lei, ficam sujeitos às seguintes sanções administrativas aplicáveis pela autoridade nacional: I - advertência, com indicação de prazo para adoção de medidas corretivas; II - multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R$ 50.000.000,00 (cinquenta milhões de reais) por infração; III - multa diária, observado o limite total a que se refere o inciso II; IV - publicização da infração após devidamente apurada e confirmada a sua ocorrência; V - bloqueio dos dados pessoais a que se refere a infração até a sua regularização; VI - eliminação dos dados pessoais a que se refere a infração; VII - XII - (VETADOS). § 1º As sanções serão aplicadas após procedimento administrativo que possibilite a oportunidade da ampla defesa, de forma gradativa, isolada ou cumulativa, de acordo com as peculiaridades do caso concreto e considerados os seguintes parâmetros e critérios: I - a gravidade e a natureza das infrações e dos direitos pessoais afetados; II - a boa-fé do infrator; III - a vantagem auferida ou pretendida pelo infrator; IV - a condição econômica do infrator; V - a reincidência; VI - o grau do dano; VII - a cooperação do infrator; VIII - a adoção reiterada e demonstrada de mecanismos e procedimentos internos capazes de minimizar o dano, voltados ao tratamento seguro e adequado de dados, em consonância com o disposto no inciso II do § 2º do art. 48 desta Lei; IX - a adoção de política de boas práticas e governança; X - a pronta adoção de medidas corretivas; e XI - a proporcionalidade entre a gravidade da falta e a intensidade da sanção. § 2º O disposto neste artigo não substitui a aplicação de sanções administrativas, civis ou penais definidas na Lei nº 8.078, de 11 de setembro de 1990, e em legislação específica. § 3º O disposto nos incisos I, IV, V, VI, VII, VIII e IX do caput deste artigo poderá ser aplicado às	Art. 83. 1. Cada autoridade de supervisão deve garantir que a aplicação de multas administrativas nos termos do presente artigo em relação às infrações ao presente regulamento referidas nos n.os 4, 5 e 6 seja, em cada caso individual, eficaz, proporcional e dissuasiva. 2. As multas administrativas serão aplicadas, dependendo das circunstâncias de cada caso individual, além das medidas referidas nas alíneas a) ah) ej) do no 2 do artigo 58.o 2 Ao decidir se deve aplicar uma multa administrativa e ao montante da multa administrativa em cada caso individual, deve-se considerar o seguinte: a) A natureza, gravidade e duração da infração, tendo em conta o escopo ou objetivo da natureza do tratamento em causa, bem como o número de titulares de dados afetados e o nível de dano sofrido por elas; b) O caráter intencional ou negligente da infração; c) qualquer ação tomada pelo controlador ou processador para mitigar os danos sofridos pelos titulares dos dados; d) O grau de responsabilidade do responsável pelo tratamento ou processador, tendo em conta as medidas técnicas e organizacionais por eles aplicadas nos termos dos artigos 25. o e 32. o e) Quaisquer infrações anteriores relevantes pelo controlador ou processador; f) O grau de cooperação com a autoridade de supervisão, a fim de remediar a infração e atenuar os possíveis efeitos adversos da infração; g) As categorias de dados pessoais afetados pela infração; h) A maneira pela qual a infração ficou conhecida pela autoridade supervisora, em particular se e em que medida o controlador ou o processador notificou a infração; i) Se as medidas referidas no artigo 58.o, n.o 2, tiverem sido previamente ordenadas contra o responsável pelo tratamento ou o transformador em causa no que diz respeito ao mesmo objeto, o cumprimento dessas medidas; j) Adesão aos códigos de conduta aprovados nos termos do artigo 40. ou aos mecanismos de certificação aprovados nos termos do artigo 42 e k) Qualquer outro fator agravante ou atenuante aplicável às circunstâncias do caso, como benefícios financeiros obtidos ou perdas evitadas, direta ou indiretamente, pela infração. 3. Se um controlador ou processador intencional ou negligentemente, para as mesmas operações de processamento ou vinculadas, infringir várias disposições do presente regulamento, o montante

entidades e aos órgãos públicos, sem prejuízo do disposto na Lei nº 8.112, de 11 de dezembro de 1990 (Estatuto do Servidor Público Federal) , na Lei nº 8.429, de 2 de junho de 1992 (Lei de Improbidade Administrativa) , e na Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação) . § 4º No cálculo do valor da multa de que trata o inciso II do caput deste artigo, a autoridade nacional poderá considerar o faturamento total da empresa ou grupo de empresas, quando não dispuser do valor do faturamento no ramo de atividade empresarial em que ocorreu a infração, definido pela autoridade nacional, ou quando o valor for apresentado de forma incompleta ou não for demonstrado de forma inequívoca e idônea. § 5º O produto da arrecadação das multas aplicadas pela ANPD, inscritas ou não em dívida ativa, será destinado ao Fundo de Defesa de Direitos Difusos de que tratam o art. 13 da Lei nº 7.347, de 24 de julho de 1985, e a Lei nº 9.008, de 21 de março de 1995. § 6º (VETADO). § 7º Os vazamentos individuais ou os acessos não autorizados de que trata o caput do art. 46 desta Lei poderão ser objeto de conciliação direta entre controlador e titular e, caso não haja acordo, o controlador estará sujeito à aplicação das penalidades de que trata este artigo. Art. 53. A autoridade nacional definirá, por meio de regulamento próprio sobre sanções administrativas a infrações a esta Lei, que deverá ser objeto de consulta pública, as metodologias que orientarão o cálculo do valor-base das sanções de multa. § 1º As metodologias a que se refere o caput deste artigo devem ser previamente publicadas, para ciência dos agentes de tratamento, e devem apresentar objetivamente as formas e dosimetrias para o cálculo do valor-base das sanções de multa, que deverão conter fundamentação detalhada de todos os seus elementos, demonstrando a observância dos critérios previstos nesta Lei. § 2º O regulamento de sanções e metodologias correspondentes deve estabelecer as circunstâncias e as condições para a adoção de multa simples ou diária. Art. 54. O valor da sanção de multa diária aplicável às infrações a esta Lei deve observar a gravidade da falta e a extensão do dano ou prejuízo causado e ser fundamentado pela autoridade nacional. Parágrafo único. A intimação da sanção de multa diária deverá conter, no mínimo, a descrição da	total da multa administrativa não deve exceder o montante especificado para a infração mais grave. 4. A infração das disposições a seguir sujeita, em conformidade com o parágrafo 2, a multas administrativas de até 10 000 000 EUR ou, no caso de uma empresa, até 2% do volume de negócios anual global do exercício financeiro anterior, conforme o que ocorrer é maior que: a) As obrigações do responsável pelo tratamento e do transformador nos termos dos artigos 8.o, 11.o, 25.o a 39.o e 42.o e 43.o; b) As obrigações do organismo de certificação nos termos dos artigos 42. e 43. c) As obrigações do organismo de controlo nos termos do artigo 41. 5. As violações das seguintes disposições estão sujeitas a multas administrativas de até 20 000 000 EUR ou, no caso de uma empresa, até 4% do volume de negócios anual mundial do exercício financeiro anterior, consoante o que for. é maior que: a) Os princípios básicos do tratamento, incluindo condições de consentimento, nos termos dos artigos 5.o, 6.o, 7.o e 9.o; b) Os direitos das pessoas em causa nos termos dos artigos 12. o a 22. o c) As transferências de dados pessoais para um destinatário num país terceiro ou organização internacional nos termos dos artigos 44. o a 49. o d) Quaisquer obrigações nos termos da legislação dos Estados-Membros adotadas nos termos do capítulo IX; e) Incumprimento de uma ordem ou limitação temporária ou definitiva no processamento ou suspensão dos fluxos de dados pela autoridade de supervisão nos termos do artigo 58.o, n.o 2, ou falha no fornecimento de acesso, violando o artigo 58.o, n.o 1. 6. O não cumprimento de uma ordem da autoridade de supervisão a que se refere o artigo 58.o, n.o 2, nos termos do n.o 2 do presente artigo, está sujeito a multas administrativas até 20.000.000 EUR ou, no caso de uma empresa, até 4% do faturamento anual total mundial do exercício financeiro anterior, o que for maior. 7. Sem prejuízo dos poderes corretivos das autoridades de supervisão nos termos do artigo 58.o, n.o 2, cada Estado-Membro pode estabelecer as regras sobre se e em que medida podem ser aplicadas coimas administrativas às autoridades e organismos públicos estabelecidos nesse Estado-Membro. 8. O exercício pela autoridade supervisora de seus poderes nos termos do presente artigo estará sujeito a salvaguardas processuais adequadas, em conformidade com o direito da União e dos Estados-Membros, incluindo medidas judiciais eficazes e o devido processo legal. 9. 1. Quando o sistema jurídico do Estado-Membro não preveja multas administrativas, o presente artigo

obrigação imposta, o prazo razoável e estipulado pelo órgão para o seu cumprimento e o valor da multa diária a ser aplicada pelo seu descumprimento.	poderá ser aplicado de forma que a multa seja iniciada pela autoridade supervisora competente e imposta pelos tribunais nacionais competentes, garantindo, ao mesmo tempo, a eficácia desses recursos. e ter um efeito equivalente às multas administrativas impostas pelas autoridades de supervisão. 2. De qualquer forma, as multas aplicadas deverão ser efetivas, proporcionadas e dissuasivas. 3. Esses Estados-Membros devem notificar à Comissão as disposições das suas leis que adotarem nos termos do presente número até 25 de maio de 2018 e, sem demora, qualquer lei ou alteração posterior que as afete.

Fonte: Da autora, (2019) com base nos dados da Lei.

A aplicação de sanções e multas deverá sempre, observar o princípio da proporcionalidade. Os critérios para a aplicação de sanções e multas estão elencados no artigo 52, § 1º e incisos da LGPD, assegurando que a penalidade será proporcional "a gravidade e a natureza das infrações e dos direitos pessoais afetados", assegura também a possibilidade de defesa. O artigo 83.1. do GDPR estabelece que aplicação de multas administrativas será proporcional ao caso individual.

Entretanto, vale destacar a diferença entre os valores previstos de multa; enquanto no Brasil as multas variam entre 2% (dois por cento) do faturamento das empresas e R$ 50.000.000,00 (cinquenta milhões de reais), na União Européia a variação fica entre 4% (quatro por cento) do volume de negócios anual e 20 000 000 EUR (vinte milhões de euros), valor que, convertido pela cotação atual, corresponde a quase o dobro do valor máximo aplicado no Brasil.

h) Fluxo transfronteiriço de dados

Quadro 8 - Fluxo transfronteiriço de dados

LGPD - BRASIL	**GDPR - UNIÃO EUROPEIA**
Art. 33. A transferência internacional de dados pessoais somente é permitida nos seguintes casos: I - para países ou organismos internacionais que proporcionem grau de proteção de dados pessoais adequado ao previsto nesta Lei; II - quando o controlador oferecer e comprovar garantias de cumprimento dos princípios, dos direitos do titular e do regime de proteção de dados previstos nesta Lei, na forma de: a) cláusulas contratuais específicas para determinada transferência; b) cláusulas-padrão contratuais; c) normas corporativas globais; d) selos, certificados e códigos de conduta regularmente emitidos; III - quando a transferência for necessária para a cooperação jurídica internacional entre órgãos públicos de inteligência, de investigação e de persecução, de acordo com os instrumentos de direito internacional; IV - quando a transferência for necessária para a proteção da vida ou da incolumidade física do titular ou de terceiro; V - quando a autoridade nacional autorizar a transferência; VI - quando a transferência resultar em compromisso assumido em acordo de cooperação internacional; VII - quando a transferência for necessária para a execução de política pública ou atribuição legal do serviço público, sendo dada publicidade nos termos do inciso I do caput do art. 23 desta Lei; VIII - quando o titular tiver fornecido o seu consentimento específico e em destaque para a transferência, com informação prévia sobre o caráter internacional da operação, distinguindo claramente esta de outras finalidades; ou IX - quando necessário para atender as hipóteses previstas nos incisos II, V e VI do art. 7º desta Lei. Parágrafo único. Para os fins do inciso I deste artigo, as pessoas jurídicas de direito público referidas no parágrafo único do art. 1º da Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação) , no âmbito de suas competências legais, e responsáveis, no âmbito de suas atividades, poderão requerer à autoridade nacional a avaliação do nível de proteção a dados pessoais conferido por país ou organismo internacional.	Art. 50. Cooperação internacional para a proteção de dados pessoais 1. Em relação a países terceiros e organizações internacionais, a Comissão e as autoridades de supervisão tomam as medidas adequadas para: a) desenvolver mecanismos de cooperação internacional para facilitar a aplicação efetiva da legislação para a proteção de dados pessoais; b) fornecer assistência mútua internacional na aplicação da legislação para a proteção de dados pessoais, inclusive por meio de notificação, encaminhamento de reclamações, assistência investigativa e troca de informações, sujeita às salvaguardas adequadas para a proteção de dados pessoais e outros direitos e liberdades fundamentais; c) envolver as partes interessadas relevantes em discussões e atividades destinadas a promover a cooperação internacional na aplicação da legislação para a proteção de dados pessoais; d) promover o intercâmbio e a documentação da legislação e prática de proteção de dados pessoais, inclusive em conflitos jurisdicionais com países terceiros.

Fonte: Da autora, (2019) com base nos dados da Lei.

Segundo Pinheiro (2018, p. 92), “o Brasil segue o movimento europeu de padronização internacional do fluxo de dados”, a adoção de regras para os fluxos transfronteiriço de dados pessoais visa “garantir que o desenvolvimento tecnológico e econômico possa continuar seu acelerado e complexo processo, sem que com isso direitos e garantias fundamentais sejam relativizados ou violados”.

Em suma, pode-se notar que a legislação brasileira muito se espelhou na legislação europeia, e por ser a primeira lei a tratar do assunto no Brasil, possivelmente ainda sofrerá alguns ajustes, mas o fato é que os direitos fundamentais foram contemplados, pela primeira vez, de forma tão abrangente no país.

5 CONCLUSÃO

Neste trabalho, buscou-se observar o *enforcement* do direito à privacidade e as evoluções sofridas juntamente com as inúmeras e constantes mudanças na sociedade. Ao mesmo tempo, buscou-se estabelecer a evolução, surgimento e reconhecimento do direito à proteção de dados pessoais como como um direito fundamental. Pode-se dizer que as principais mudanças ocorreram após o surgimento (e rápida expansão) da internet, a qual conquistou importante papel nas relações humanas, sendo imprescindível que as legislações acompanhem os avanços tecnológicos. A preocupação com os dados pessoais surge com o reconhecimento do valor comercial dessas informações.

Observou-se que o direito à privacidade passou a ter maior magnitude após ser reconhecido na Declaração Universal de Direitos do Homem (aprovada em 1948), sendo aos poucos incorporadas em legislações norte-americanas e europeias.

Desse modo, essa monografia buscou apresentar no primeiro capítulo o desenvolvimento da proteção dos direitos de personalidade, em especial o direito à privacidade. Foi possível verificar que os maiores esforços aconteceram na União Europeia, em especial com a elaboração da Convenção nº 108 e posteriormente a Diretiva 95/46 CE.

Em seguida, abordou-se a evolução da regulamentação da proteção dos dados pessoais no Brasil, inicialmente o direito à privacidade possuía amparo na Constituição Federal, no Código Civil, no Código de Defesa do Consumidor, no Marco

Civil da Internet e em outros diplomas legais, contudo não havia uma lei específica para tutelar a proteção dos dados pessoais.

No terceiro capítulo, buscou-se estabelecer um comparativo entre Regulamento Geral sobre a Proteção de Dados da União Europeia e a Lei Geral de Proteção de Dados Pessoais do Brasil. O objetivo principal dos diplomas citados é o tratamento dos dados pessoais, bem como a proteção os direitos fundamentais, tais como dignidade, privacidade, intimidade, e a honra. Foi possível verificar que a legislação brasileira muito se espelhou na legislação europeia, porém a legislação europeia é muito mais abrangente.

Quanto ao objetivo principal, que era verificar se a criação da LGPD seria suficiente para a efetivação da garantia protetiva dos dados pessoais/privacidade dos cidadãos brasileiros, pode-se concluir que a criação dessa lei foi extremamente importante, principalmente porque coloca o Brasil em condições jurídicas e comerciais de negociar com os países integrantes do bloco da União Europeia.

Trata-se de um grande avanço, porém, conforme exposto ao longo da monografia, a tecnologia encontra-se no auge do seu desenvolvimento, e, com base nisso, o ordenamento jurídico precisa constantemente estar contato com esta para que possa garantir aos cidadãos brasileiros, a cada dia, uma maior segurança do uso das ferramentas de proteção de dados. Dessa forma, o contato com países com legislações acerca da proteção de dados já estabelecidas, é importante para a implantação e aperfeiçoamento da nossa legislação. Importante também estabelecer parcerias sobre desenvolvimento das novas tecnologias e os riscos que estas podem causar.

Ao longo de toda pesquisa, conclui-se que a proteção de dados no Brasil evoluiu lentamente ao longo dos anos, sendo que muito dessa evolução se deu em decorrência de fatos que, de alguma forma, pressionaram o ordenamento jurídico brasileiro para a elaboração da norma, sendo a aprovação do regulamento europeu (e as sanções econômicas previstas), um dos maiores motivos para o Brasil rapidamente adotar uma normativa de proteção de dados.

REFERÊNCIAS

ALCANTARA, Larissa K. Big Data e IoT. **Desafios da Privacidade e da Proteção de Dados no Direito Digital**. Edição do Kindle. Disponível em: <https://ler.amazon.com.br/?asin=B07577SWTQ. > Acesso em: 31 mai. 2019.

ANACOM. Autoridade Nacional de Comunicações. **Personal Information Protection and Electronic Documents Act**. PIPEDA. Disponível em: < https://laws-lois.justice.gc.ca/eng/acts/P-8.6/index.html >- Acesso em: 14 out. 2019.

BARRETO JUNIOR, Irineu Francisco. **Atualidade do Conceito Sociedade da Informação para a Pesquisa Jurídica**. In: PAESANI, Liliana Minardi (coord.). Direito na Sociedade da Informação. São Paulo: Atlas, 2007

BESSA, Leonardo R. **O consumidor e os limites dos bancos de dados de proteção ao crédito.** São Paulo: Edição Revista dos Tribunais, 2003, v.25. Disponível em: < https://www.revistadostribunais.com.br/maf/app/resultList/document?&src=rl&srguid=i0ad82d9a0000016e5cba198b07cfdeb9&docguid=I853d9430b18c11e38340010000000000&hitguid=I853d9430b18c11e383400100000000000&spos=1&epos=1&td=84&context=100&crumb-action=append&crumb-label=Documento&isDocFG=true&isFromMultiSumm=true&startChunk=1&endChunk=1 >. Acesso em: 11 nov. 2019.

BIONI, Bruno Ricardo**. Proteção de dados pessoais**: Uma função e os limites do consentimento.2019. Disponível em:< https://integrada.minhabiblioteca.com.br/#/books/9788530983291> Acesso em: 11 nov. 2019.

BITTAR, Alberto, C. **Os direitos da personalidade**. 8ª edição. 2014. Disponível em: <https://integrada.minhabiblioteca.com.br/#/books/9788502208292/. > Acesso em: 31 mai. 2019.

BRASIL. **Lei nº 8.078**, de 11 de setembro de 1990. Código de Defesa do

Consumidor. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/l8078.htm >. Acesso em: 10 out. 2019.

_____. **Lei nº 12.414**, de 09 de junho de 2011. Lei do Cadastro Positivo. Disponível em:https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12414.htm>. Acesso em: 25 set. 2019.

_____. **Lei nº 12.527**, de 18 de novembro de 2011. Lei de Acesso Informação. 2011. Disponível em: < http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm> Acesso em: 01 nov. 2019.

_____. **Lei nº 12.737/2012**. 2011. Disponível em:< http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2012/Lei/L12737.htm#art2>. Acesso em: 10 nov. 2019.

_____. **Lei Nº 12.965**, de 23 de abril de 2014. Marco Civil da Internet. Disponível em: < http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm> Acesso em 03 nov. 2019.

_____. Supremo Tribunal Federal**. Recurso Extraordinário 742.701**. Pernambuco. Agravante (S): Petróleo Brasileiro S/ A - Petrobras. Agravado. (A / S): Paulo Sérgio De Souza Lacerda. Relator: Min. Celso De Mello. 24 set. 2013. Disponível em:<http://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=4803420> Acesso em:17 out. 2019.

_____. **LAI para Cidadãos**. Disponível em: < http://www.acessoainformacao.gov.br/assuntos>. Acesso em: 12 out. 2019.

CANOTILHO, J. J. Gomes et al. **Comentários à Constituição do Brasil**. 2. ed. – São Paulo: Saraiva Educação, 2018. (Série IDP) Ebook. Disponível em: <https://integrada.minhabiblioteca.com.br/#/books/9788502212640/cfi/0!/4/4@0.00:9.71 >. Acesso em: 31 out. 2019.

CGU. CONTROLADORIA-GERAL DA UNIÃO. **Aplicação da lei de acesso à informação em recursos à CGU**. 2015 Disponível em: < http://www.acessoainformacao.gov.br/central-de-conteudo/publicacoes/arquivos/aplicacao-da-lai-em-recursos-a-cgu.pdf> Acesso em: 03 nov. 2019.

CHEMIN, Beatris F. **Manual da Univates para trabalhos acadêmicos**: planejamento, elaboração e apresentação. 3. ed. Lajeado: Univates, 2015.

COMISSÃO NACIONAL DE PROTEÇÃO DE DADOS. **Convenção nº 108**. Disponível em: < https://www.cnpd.pt/bin/legis/internacional/Convencao108.htm. > Acesso em: 31 out. 2019.

Directiva 95/46/ce do parlamento europeu e do conselho europeu, de 24 de outubro de 1955. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:31995L0046&from=PT> Acesso em: 31 out. 2019.

DONEDA, Danilo. **A proteção dos dados pessoais como um direito fundamental**. 2011. Disponível em: <https://portalperiodicos.unoesc.edu.br/espacojuridico/article/view/1315/658>. Acesso em: 31 out. 2019.

EUA. PRIVACY ACT OF 1974. (**Lei de Privacidade de 1974**). Disponível em: <https://www.justice.gov/opcl/privacy-act-1974 > Acesso em: 20 ago. 2019

EUA. PRIVACY SHIELD OF 2016. (**Escudo de Privacidade UE -EUA e Suíça-EUA**). 2016. Disponível em: <https://www.privacyshield.gov/Program-Overview> Acesso em: 01 nov. 2019

EUA. Safe Harbor (**Porto Seguro EUA-UE).** 2016. Disponível em:<https://2016.export.gov/safeharbor/ > Acesso em: 20 ago.2019.

FERRAZ Jr, Tércio Sampaio. Sigilo de dados: o direito à privacidade e os limites a função dos fiscalizadores do Estado. 01 jan. 1993. Disponível em: <http://www.periodicos.usp.br/rfdusp/article/view/67231/69841> . Acesso em: 23 out. 2019.

FILOMENO, J. G. B. **Tutela Administrativa do Consumidor:** Atuação dos Procon's, Legislação, Doutrina e Jurisprud. 2014. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788522493289/ >. Acesso em: 06 nov. 2019.

FIORILLO, Celso Pacheco. **O Marco civil da internet e o meio ambiente digital na sociedade da informação** - Comentários à Lei n. 12.965 / 2014, 1ª edição. 2011. Disponível em: <https://integrada.minhabiblioteca.com.br/#/books/9788502627741> Acesso em: 05 nov. 2019.

GODINHO, Adriano M; GUERRA, Gustavo R. A defesa especial dos direitos de personalidade: os instrumentos de tutela previstos no direito brasileiro. In **Revista Jurídica Cesumar**-Mestrado. Maringá: Unicesumar; 2013.

GODINHO, Adriano M. Col. passe em concursos públicos: Nível superior: direito civil, v. 1 - Parte geral e especial. 2014. Disponível em: <https://integrada.minhabiblioteca.com.br/#/books/9788502211308/ > Acesso em 01 nov. 2019.

GONÇALVES, Pereira, V. Marco Civil da Internet Comentado 2017. Disponível em: Disponível em: <https://integrada.minhabiblioteca.com.br/#/books/9788597009514/cfi/6/20!/4@0.00:0.0143> Acesso em 05 out. 2019.

GRINOVER, Ada Pellegrini Grinover et al. **Código Brasileiro de Defesa do Consumidor**: comentado pelos autores do anteprojeto: direito material e processo coletivo: volume único /; colaboração Vicente Gomes de Oliveira Filho e João Ferreira Braga. – 12. ed. – Rio de Janeiro: Forense, 2019. Ebook. Disponível em:< https://integrada.minhabiblioteca.com.br/#/books/9788530982867. > Acesso em: 04 nov. 2019.

IBGE. Instituto Brasileiro De Geografia E Estatística**. Acesso à Internet e a televisão e posse de telefone móvel celular para uso pessoal 2017**. Disponível em: < https://biblioteca.ibge.gov.br/visualizacao/livros/liv101631_informativo.pdf. Acesso em: 23 out. 2019.

LEMOS, Ronaldo (Org). **Marco Civil da Internet.** 1ª ed. São Paulo. Atlas.2014.

LÔBO, Paulo Luiz Neto. **Metodologia do Direito Civil Internacional:** A ressignificação da função dos instintos fundamentais do direito contemporâneo e suas consequências. Florianópolis: conceito editorial 2014.

MENDES, Ferreira, G., BRANCO, Gonet, P. Linha Doutrina - Curso de direito constitucional. Série IDP. 2019. Disponível em: <https://integrada.minhabiblioteca.com.br/#/books/9788553610945/ > Acesso em: 22 out. 2019.

MENDES, Schertel, L. Série IDP - **Linha de pesquisa acadêmica** - Privacidade, proteção de dados e defesa do consumidor. 2014. Disponível em: <https://integrada.minhabiblioteca.com.br/#/books/9788502218987/ >. Acesso em: 31 mai. 2019.

MEZZAROBA, Orides; MONTEIRO, Cláudia S. **Manual de metodologia da pesquisa no Direito.** 6. ed. São Paulo: Saraiva, 2014.

MURPHY, Sean, **United States Practice in International Law:** 2002-2004. Cambridge University Press. 2005. Disponível em: < http://assets.cambridge.org/052175/0717/frontmatter/0521750717_frontmatter.htm> Acesso em: 20 ago. 2019.

OCDE. Organização para Cooperação e Desenvolvimento Econômico. **Diretrizes da OCDE sobre a proteção da privacidade e do fluxo transfronteiriço de dados pessoais.** 2013. Disponível em: < http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm#recommendation> Acesso em 20 set. 2019.

OLIVEIRA, Carlos Eduardo Elias de. **Aspectos Principais Da Lei Nº 12.965**. De 2014, O Marco Civil da Internet: subsídios à comunidade jurídica. 2014. Disponível em: < <http://www1.tjrs.jus.br/export/poder_judiciario/tribunal_de_justica/centro_de_estudos/doutrina/doc/lei_12625_comentarios.pdf > Acesso em: 30 out 2019.

ONU. Organização das Nações Unidas. Relatório do Relator Especial sobre a promoção e proteção do direito à liberdade de opinião e expressão, Frank La Rue. 2011. Disponível em: https://www.oas.org/pt/cidh/expressao/showarticle.asp?artID=849&lID=4> Acesso em: 19 nov. 2019.

PAESANI, Liliana Minardi. **Direito e Internet:** Liberdade de Informação, Privacidade e Responsabilidade Civil, 7ª edição. Atlas, out. 2014. Disponível em: <https://integrada.minhabiblioteca.com.br/#/books/9788522493623> Acesso em: 19

nov. 2019.

PEREZ-LUÑO, Antonio E. **Ciberciudadani@ o ciudadani@.com?** Barcelona: Gedisa, 1998.

PINHEIRO, Peck, P. **Proteção de dados pessoais** - comentários à Lei n. 13.709/2018 LGPD. Disponível em:< https://integrada.minhabiblioteca.com.br/#/books/9788553608324/>. Acesso em: 06 nov. 2019.

PT. **DIRECTIVA 95/46/CE**. Disponível em: https://www.anacom.pt/render.jsp?contentId=965550 . Acesso em: 20 abr.2019.

RGPD. Regulamento Geral sobre a Proteção de Dados. 27 abr. 2016.Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016R0679&from=pt#d1e2012-1-1>. Acesso em: 18 out. 2019.

TARTUCE, Flávio. **Direito civil: lei de introdução e parte geral**. v. 1, 15. ed. Rio de Janeiro: Forense, 2019. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788530984052/epubcfi/6/10[;vnd.vst.idref=copyright]!/4/12/4@0:100 >.Acesso em: 12.10.2019.

VENOSA, Silvio de S. **Direito Civil:** Responsabilidade civil. 7.ed. São Paulo: Atlas, v. 4, 2007.

VERONESE, Josiane Rose Petry. A proteção integral da criança e do adolescente no direito brasileiro. **Revista do Tribunal Superior do Trabalho**, São Paulo, v. 79, n. 1, p. 38-54, jan. /mar. 2013.11/17. Disponível em: < https://juslaboris.tst.jus.br/bitstream/handle/20.500.12178/38644/003_veronese.pdf?sequence=1&isAllowed=y> Acesso em: 10 nov. 2019.

IV Jornada de Direito Civil, **Enunciado 274.** 2006. Disponível em: <https://www.cjf.jus.br/cjf/corregedoria-da-justica-federal/centro-de-estudos-judiciarios-1/publicacoes-1/jornadas-cej/IV%20Jornada%20volume%20I.pdf> Acesso em: 11 nov. 2019.

UNIVATES

R. Avelino Tallini, 171 | Bairro Universitário | Lajeado | RS | Brasil
CEP 95900.000 | Cx. Postal 155 | Fone: (51) 3714.7000
www.univates.br | 0800 7 07 08 09