



**UNIVERSIDADE ESTADUAL DA PARAÍBA
CAMPUS I
CENTRO DE CIÊNCIAS JURÍDICAS (CCJ)
DEPARTAMENTO DE DIREITO PRIVADO (DDPR)
CURSO DE GRADUAÇÃO EM DIREITO**

MICAELLE ANDRADE GURJÃO COUTINHO FAUSTINO

**PROTEÇÃO DE DADOS DO CONSUMIDOR: UMA ANÁLISE SOBRE A
LEGISLAÇÃO BRASILEIRA E SUA EVOLUÇÃO**

**CAMPINA GRANDE - PARAÍBA
2019**

MICAELLE ANDRADE GURJÃO COUTINHO FAUSTINO

**PROTEÇÃO DE DADOS DO CONSUMIDOR: UMA ANÁLISE SOBRE A
LEGISLAÇÃO BRASILEIRA E SUA EVOLUÇÃO**

Trabalho de Conclusão de Curso apresentado a Coordenação do Centro de Ciências Jurídicas da Universidade Estadual da Paraíba, como requisito parcial à obtenção do título de bacharela em Direito.

Área de concentração: Direito do consumidor.

Orientador: Prof. Me. Antônio Ricardo Rocha de Albuquerque.

**CAMPINA GRANDE - PARAÍBA
2019**

É expressamente proibido a comercialização deste documento, tanto na forma impressa como eletrônica. Sua reprodução total ou parcial é permitida exclusivamente para fins acadêmicos e científicos, desde que na reprodução figure a identificação do autor, título, instituição e ano do trabalho.

F268p Faustino, Micaelle Andrade Gurjao Coutinho.
Proteção de dados do consumidor [manuscrito] : uma análise sobre a legislação brasileira e sua evolução / Micaelle Andrade Gurjao Coutinho Faustino. - 2019.
58 p. : il. colorido.
Digitado.
Trabalho de Conclusão de Curso (Graduação em Direito) - Universidade Estadual da Paraíba, Centro de Ciências Jurídicas , 2019.
"Orientação : Prof. Me. Antônio Ricardo Rocha de Albuquerque , Coordenação do Curso de Direito - CCJ."
1. Direito à privacidade. 2. Proteção de dados. 3. Direito fundamental. 4. Relações de consumo. I. Título
21. ed. CDD 343.071

MICAELE ANDRADE GURJÃO COUTINHO FAUSTINO


PROTEÇÃO DE DADOS DO CONSUMIDOR: UMA ANÁLISE SOBRE A
LEGISLAÇÃO BRASILEIRA E SUA EVOLUÇÃO

Trabalho de Conclusão de Curso apresentado a
Coordenação do Centro de Ciências Jurídicas da
Universidade Estadual da Paraíba, como requisito
parcial à obtenção do título de bacharela em
Direito.

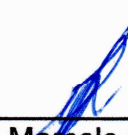
Área de concentração: Direito do consumidor.

Aprovada em: 19 / 06 / 2019.

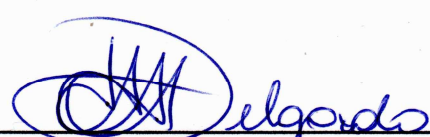
BANCA EXAMINADORA



Prof. Me. Antônio Ricardo Rocha de Albuquerque (Orientador)
Universidade Estadual da Paraíba (UEPB)



Prof. Dr. Marcelo D'Angelo Lara
Universidade Estadual da Paraíba (UEPB)



Profa. Ma. Herteide Herculano Delgado
Universidade Estadual da Paraíba (UEPB)

Aos meus pais, Valdenice Andrade Gurjão
Coutinho e José de Ribamar Gurjão
Coutinho (*In Memoriam*), DEDICO.

AGRADECIMENTOS

À DEUS, por seu amor incondicional.

Aos meu pais, por todo o cuidado e dedicação ao longo dos anos, ensinamentos, companheirismo e, especialmente, pelo amor e amizade.

Ao meu irmão Júnior por sua amizade, carinho e auxílio sempre que necessito.

À Paulo Faustino por seu companheirismo, apoio e amor.

Ao professor Antônio Ricardo Rocha de Albuquerque por sua orientação e dedicação.

Aos professores Marcelo D'Angelo Lara e Herleide Herculano Delgado por aceitarem participar da Banca Examinadora.

Aos professores do Curso de Graduação em Direito da UEPB, que contribuíram ao longo desses anos, por meio das disciplinas, debates e ensinamentos para o nosso desenvolvimento profissional e pessoal.

Aos funcionários da UEPB, pela presteza e atendimento quando nos foi necessário.

Aos colegas de turma pelos momentos de amizade e apoio.

Bem-aventurados os que observam o direito, o que pratica a justiça em todos os tempos.

Bíblia Sagrada (SALMOS, 106:3)

RESUMO

A Lei nº 13.709, de 14 de agosto de 2018, denominada Lei Geral de Proteção de Dados (LGPD) representa um marco na proteção de dados pessoais no País, alinhando o ordenamento jurídico pátrio a uma tendência internacional. O presente trabalho tem como objetivo central discutir e refletir a respeito da conexão entre os direitos dos consumidores e da proteção e privacidade dos dados pessoais nas relações de consumo no Brasil. Para tanto, analisa a proteção dos dados pessoais segundo a legislação brasileira, à luz do direito consumerista, considerando as alterações introduzidas pela Lei nº 13.709/2018, com especial enfoque nos dados do consumidor. Percorre, inicialmente, tópicos introdutórios a respeito da privacidade e da autodeterminação informativa; da proteção de dados como um direito fundamental, e do desenvolvimento das leis de proteção de dados; em seguida, versa sobre a proteção de dados do consumidor, sob a ótica do ordenamento jurídico nacional e, posteriormente, busca apresentar as principais inovações estabelecidas pela nova regulamentação; por fim, realiza-se uma breve análise sobre possíveis formas de comercialização de dados e violações aos direitos da personalidade, o tratamento de dados à luz da nova legislação, e suas respectivas sanções.

Palavras-Chave: Direito à privacidade. Proteção de dados. Direito fundamental. Relações de consumo.

ABSTRACT

Law N° 13,709, from August 14th, 2018, was called General law of Data protection (LGPD) that represents a milestone on protection of personal data in the country and it aligns the legal order in the country on an international trend. This paper aims to discuss and reflect about the connection between the consumers' rights, protection and privacy of the personal data in relation to consumption relations in Brazil. Therefore, it analyses the protection on personal data according to Brazilian legislation in the sense of consumer rights, regarding the changes introduced by law 13709/2018, that focuses specially on consumer data. It courses initially introductory topics in relation to the privacy and informational self-determination on protection of data as a fundamental right, and the development of laws on protection of data and then deals about the protection on data of consumer from the perspective of national legal order and, subsequently, seeks to present the main innovations established by new regulations; at last, occurs a brief analyses about possible ways of commercialization of data and offense to the rights of the personality, the treatment of data on the perspective of the new legislation, and its respective sanction.

Keywords: Right to privacy. Protection of data. Fundamental rights. Consumer relations.

LISTA DE ILUSTRAÇÕES

Figura 1 – Projetos e Leis de Proteção de Dados no mundo em 2016 e 2018.....	22
--	----

SUMÁRIO

1	INTRODUÇÃO	10
2	BREVE CONTEXTO HISTÓRICO	12
2.1	DA PRIVACIDADE À AUTODETERMINAÇÃO INFORMATIVA	12
2.2	A PROTEÇÃO DE DADOS COMO UM DIREITO FUNDAMENTAL	15
2.3	DESENVOLVIMENTO DAS LEIS DE PROTEÇÃO DE DADOS.....	18
3	PROTEÇÃO DE DADOS DO CONSUMIDOR SOB A ÓTICA DA LEGISLAÇÃO BRASILEIRA	24
4	PRINCIPAIS INOVAÇÕES DA LEI Nº 13.709, DE 14 DE AGOSTO DE 2018 (LGPD)	31
5	A UTILIZAÇÃO DOS DADOS DOS CONSUMIDORES E SEUS RISCOS	42
5.1	COMERCIALIZAÇÃO DE DADOS PESSOAIS E VIOLAÇÕES AOS DIREITOS DA PERSONALIDADE.....	42
5.2	TRATAMENTO DE DADOS PESSOAIS À LUZ DA NOVA LEI.....	46
5.3	SANÇÕES	50
6	CONSIDERAÇÕES FINAIS	53
	REFERÊNCIAS	55

1 INTRODUÇÃO

O presente trabalho, intitulado “Proteção de dados do consumidor: Uma análise sobre a legislação brasileira e sua evolução”, tem como objetivo central discutir e refletir a respeito da conexão entre os direitos dos consumidores e da proteção e privacidade dos dados pessoais nas relações de consumo no Brasil. Para tal, questiona-se quais instrumentos normativos são oferecidos, quanto à proteção e privacidade dos dados pessoais, à luz do direito consumerista; bem como, a importância da Lei nº 13.709, de 14 de agosto de 2018 (LGPD), na proteção de dados do consumidor.

Com os avanços tecnológicos, os dados pessoais, sobretudo os dados dos consumidores, passaram a ser cada vez mais atraentes ao mercado, utilizados que são para diversos fins, entretanto, o inadequado tratamento desses dados resulta em riscos aos consumidores.

Até então, a proteção dos dados pessoais em solo brasileiro tem ocorrido de forma indireta, através da aplicação de dispositivos constitucionais e regulamentações setoriais que não tratam de forma efetiva sobre o tema; o que coloca o País em posição de atraso legislativo, se comparado até mesmo aos países latinos. De fato, uma nova legislação específica demonstrou-se como indispensável para a resolução da situação de hipossuficiência técnica e jurídica em que se encontram os consumidores brasileiros, quanto à proteção e privacidade de seus dados pessoais.

Nesse contexto, compreende-se que a recente aprovação da Lei nº 13.709/2018, que entrará em vigor em 2020, representa um marco na Legislação do País, trazendo inovações importantes para proteção de dados do consumidor; e mais segurança jurídica dentro do mercado de consumo.

A partir de pesquisas desenvolvidas sob a perspectiva do método de abordagem dedutivo, com base em bibliografias e estudos existentes sobre o tema, bem como na legislação nacional e internacional, o presente trabalho se propõe a analisar a utilização dos dados dos consumidores nas situações em que o inadequado tratamento dos dados pessoais pode resultar num desequilíbrio das relações comerciais; ou em violações aos direitos subjetivos inerentes ao indivíduo, tais como a privacidade e a intimidade, bem como ponderar as soluções possíveis dentro da perspectiva de que o consumidor, como qualquer cidadão, possui direito à

sua autodeterminação informativa e que na relação de consumo é imperativa a identificação de instrumentos para fazê-la valer.

Nesse intuito, serão abordados, inicialmente, tópicos introdutórios a respeito da privacidade e da autodeterminação informativa, a proteção de dados como um direito fundamental, e o desenvolvimento das Leis de Proteção de Dados. E posteriormente, contextualizando com os instrumentos normativos oferecidos à proteção de dados do consumidor em nosso ordenamento jurídico pátrio, apontando, ainda, as principais inovações trazidas pela Lei nº 13.709, de 14 de agosto de 2018 (LGPD). Por fim, far-se-á uma breve análise sobre possíveis formas de comercialização de dados e violações aos direitos da personalidade, o tratamento de dados à luz da nova legislação, com as respectivas sanções.

2 BREVE CONTEXTO HISTÓRICO

A pesquisa feita a respeito do tema apresentado não teria como ser construída, sem que se apresentasse um breve contexto histórico, que dissesse respeito ao aspecto da privacidade, da autodeterminação informativa e da proteção dos dados como direito fundamental, a justificar o surgimento de legislações nacionais e internacionais que, dispondo sobre o mesmo como direito relevante que é, com a respectiva tutela.

2.1 DA PRIVACIDADE À AUTODETERMINAÇÃO INFORMATIVA

A publicação *The right to privacy*, escrita por Samuel Warren e Louis Brandeis em 1890, na *Harvard Law Review*, originou nos Estados Unidos a discussão sobre o direito à privacidade. A obra justifica a necessidade de proteger a esfera íntima de cada indivíduo, representado pelo direito de ficar só (*right to be let alone*).

Para Doneda, esta concepção foi o marco inicial, logo após, a privacidade passa a ser percebida como prisma fundamental para a realização da pessoa e o desenvolvimento da sua personalidade:

A concepção inicial de privacidade, ligada ao desenvolvimento e reserva do ambiente doméstico, passou a ser ampliada, voltando-se para o interesse do sujeito com relação à 'construção de uma esfera pessoal' baseada na 'liberdade de escolha', viabilizando o desenvolvimento da personalidade do sujeito (DONEDA, 2006, p. 144).

Todavia, o desenvolvimento das tecnologias de informação e comunicação viabilizaram a violação da vida privada e dos direitos subjetivos inerentes à pessoa, ao passo em que se verificava o aumento da tecnologia, dando espaço para as possibilidades de ofensas à privacidade; e sobrevivendo concomitantemente, a necessidade de resguardo.

Na elucidação de Doneda, a noção de privacidade assume um papel voltado para relação do indivíduo com os outros e com o mundo exterior. O sujeito passa a perceber a possibilidade de controlar as informações sobre si, conforme a exposição a seguir:

Atualmente, a noção de privacidade a ser protegida está pautada na relação do sujeito com os outros e com o mundo exterior. Assim, 'vislumbra-se a possibilidade de controle das informações pessoais, a 'determinação de

inserção e de exposição' e, por consequência, o fortalecimento da esfera privada do indivíduo em consonância com o ideal de dignidade da pessoa humana' (DONEDA, 2006, p. 146).

Assim, percebe-se que a noção de privacidade evoluiu a partir do “direito de ficar só”, alcançando a autodeterminação informativa, genuíno exercício da liberdade de escolha do indivíduo, compreendido no direito de controlar as informações sobre si próprio.

Convém mencionar o entendimento de Mota Pinto quanto a autodeterminação informativa:

A Autodeterminação informativa é entendida como controlo sobre informação relativa à pessoa. Consiste no interesse em impedir ou em controlar a tomada de conhecimento, à divulgação ou, simplesmente, à circulação de informações sobre a pessoa, isto é, sobre factos, comunicações ou situações relativas (ou próximo) ao indivíduo, e que previsivelmente ele considere como íntimos, confidenciais ou reservados (MOTA PINTO, 2000, p.164).

Em 1983, o Tribunal Federal Constitucional Alemão utilizou a denominação “autodeterminação informativa” no âmbito de um processo relativo à coleta de informações pessoais pelo Poder Público durante o censo. Por conseguinte, tal Tribunal declarou a existência desse direito como emanado dos princípios da dignidade da pessoa humana e do livre desenvolvimento da personalidade.

Esta decisão é comentada por Ricard Martínez Martínez:

Como resulta sobradamente conocido –y sinperjuicio de iniciativas legislativas de muy diversa índole, cuyo objetivo era regular el uso de la informática–, el llamado derecho a la autodeterminación informativa nace en la República Federal Alemana con la sentencia dictada por el Tribunal Constitucional Federal Alemán (TCFA) en la sentencia sobre la Ley del Censo. El TCFA afirma en la sentencia que el derecho general de la personalidad comporta la atribución al individuo de la capacidad de decidir, en el ejercicio de su autodeterminación, qué extremos desea revelar de su propia vida. Para el TCFA:

«la autodeterminación del individuo presupone –también en las condiciones de las técnicas modernas de tratamiento de la información– que se conceda al individuo la libertad de decisión sobre las acciones que vaya a realizar o, en su caso, a omitir, incluy en dol a posibilidad de obrar de hecho en forma conseqüente con la decisión adoptada. Esta libertad de decisión, de control, supone además que el individuo tenga la posibilidad de acceder a sus datos personales, que pueda, no sólo tener conocimiento de que otros procesan informaciones relativas a su persona, sino también someter el uso de éstas a un control, ya que, de lo contrario, se limitará su libertad de decidir por autodeterminación».

La consecuencia de este razonamiento es el reconocimiento jurisprudencial de un derecho fundamental a la autodeterminación informativa basado en el derecho general de la personalidad y que ofrece protección frente a la recogida, el almacenamiento, la utilización y la transmisión ilimitada de los

datos de carácter personal y «garantiza la facultad del individuo de decidir básicamente por sí mismo sobre la difusión y la utilización de sus datos personales» (MARTÍNEZ, 2007, p.47).

Portanto, este direito fundamental garante a capacidade do indivíduo para determinar sobre a divulgação e o uso de seus dados pessoais, limitando-se, apenas, em caso de interesse público primordial.

Como visto, a partir da autodeterminação informativa, a privacidade passa a ser percebida além de sua esfera íntima, alcançando as relações interpessoais do indivíduo; caracterizando-se, também, pela necessidade de controle das informações sobre si.

Desta maneira, a percepção do direito à privacidade está avançando, sobretudo no que concerne ao direito do consumidor, porquanto não se compreende apenas a privacidade em seu resguardo íntimo, mas, igualmente, em que o consumidor pode determinar a quem se permitirá o acesso a seus dados, bem como os limites ao uso por terceiros.

Rizzatto Nunes (2011) define, como consumidor, pessoa física ou jurídica; e explica que existem situações distintas para a sua caracterização, regulamentadas pela Lei nº 8.078, de 11 de setembro de 1990, denominada Código de Defesa do Consumidor (CDC).

Em relação ao conceito de consumidor o referido autor elucida:

A definição de consumidor do CDC começa no individual, mais concreto (art. 2º, caput), e termina no geral, mais abstrato (art. 29). Isto porque, logicamente falando, o caput do art. 2º aponta para aquele consumidor real que adquire concretamente um produto ou um serviço, e o art. 29 indica o consumidor do tipo ideal, um ente abstrato, uma espécie de conceito difuso, na medida em que a norma fala da potencialidade, do consumidor que presumivelmente existia, ainda que possa não ser determinado (NUNES, 2011, p. 117).

Destarte, o CDC não limita a configuração de consumidor somente ao adquirente do produto ou serviço tal como prevê o artigo 2º, consoante define o artigo 29, da referida norma, o qual dispõe que “equiparam-se aos consumidores todas as pessoas determináveis ou não, expostas às práticas nele previstas”. Desta maneira, nivela a mesma figura a todos aqueles que ficam expostos às práticas comerciais.

É de se ressaltar a distinção apresentada por Doneda, em relação a privacidade e a proteção de dados, em especial no que se refere ao consumidor:

O aspecto do controle efetivo ao consumidor sobre seus próprios dados, tão caro à proteção de dados, é o ponto que a distingue com maior nitidez da tutela da privacidade propriamente dita - posto que a proteção de dados não se destina meramente à tutela de uma liberdade negativa, de não se expor, porém se realiza ao garantir a cada um a liberdade efetiva de escolher o que será feito com suas próprias informações pessoais. No caso do consumidor, o favorecimento desta liberdade é tão mais importante ao se perceber que o tratamento de dados pessoais, lícito, leal e transparente, pode ser de interesse do próprio consumidor, à medida em que reflete em uma variedade maior de opções ou no desenvolvimento de produtos e serviços a partir de suas reais necessidades, por exemplo. E é justamente nesse sentido que, aliás, o próprio Código de Defesa do Consumidor, em seu art. 4º, III, prevê a necessidade de "(...) harmonização dos interesses dos participantes das relações de consumo e compatibilização da proteção do consumidor com a necessidade de desenvolvimento econômico e tecnológico (...)" (DONEDA, 2010, p. 12).

Dessa forma, destaca-se a relevância da proteção aos dados pessoais, a qual permite ao consumidor decidir sobre o uso de seus dados e traz mais segurança jurídica para o mercado de consumo, que se configura pela utilização de técnicas e estratégias cada vez mais avançadas no tratamento de dados dos consumidores para ofertar serviços, personalizar produtos; ou em ações de marketing, por exemplo.

2.2 A PROTEÇÃO DE DADOS PESSOAIS COMO UM DIREITO FUNDAMENTAL

Os avanços tecnológicos, o fácil acesso a dispositivos fixos e móveis, conectados globalmente através da internet, transformaram o papel dos dados pessoais na economia e na sociedade. Hoje há um grande volume e uso de múltiplos dados pessoais, resultantes da facilidade desde a coleta, o processamento, a transferência de enormes quantidades de dados.

Em linhas gerais, o conceito de dados refere-se a representações que não apresentam significado isoladamente, isto é, são simples observações sobre algo, como corrobora a exposição de Filipe Cassapo, no artigo *O que entendemos exatamente por Conhecimento Tácito e Conhecimento Explícito*, publicado no Portal da Sociedade Brasileira de Gestão do Conhecimento – (SBGC):

O dado é proposto como a entidade elementar e essencial da comunicação: um dado é algo físico, que pode ser isolado e medido, e que, por si só, não faz sentido. O dado é independente do ser cognitivo (CASSAPO, s. d., p. 4).

Cabe ressaltar o entendimento dos autores Davenport & Prusak (1988, p.2), no qual, “Dados são um conjunto de fatos distintos e objetivos, relativos a eventos. Num contexto organizacional, dados são utilitariamente descritos como registros estruturados de transações”.

Os referidos autores (1988, p.3), acrescentam que, “os dados são importantes para as organizações – em grande medida, certamente, porque são matéria-prima essencial para a criação da informação”.

Nessa perspectiva, a informação é percebida como proveniente dos dados, ou seja, é resultado de uma análise contextualizada e categorizada. Trata-se de dados aos quais se dotou de significado e contexto, como mencionado pelos autores:

[...] são os dados que fazem a diferença. O significado original da palavra ‘informar’ é ‘dar forma a’, sendo que a informação visa a modelar a pessoa que a recebe no sentido de fazer alguma diferença em sua perspectiva ou insight (DAVENPORT & PRUSAK, 1988, p.4).

Interessante, também, saber o que o sociólogo Manuel Castells (2008, p. 64-65) entende como “sociedade informacional”. Para ele, esta indica uma forma específica de sociedade, na qual a “geração, o processamento e a transmissão da informação tornam-se as fontes fundamentais de produtividade e poder devido às novas condições tecnológicas surgidas nesse período histórico”.

Nesse sentido, compreende-se a sociedade informacional como uma organização social na qual a produção, o processamento e a transmissão da informação se tornam indispensáveis para a produtividade e o exercício do poder, resultado de uma evolução social que provém do uso e da capitalização, mediante as tecnologias de informação e de comunicação; ou seja, quanto mais relevante é a informação e mais avançada está a capacidade de retenção, transporte e uso, mais oportuno será a sua inclusão na rede.

As redes sociais, por exemplo, revolucionaram as formas de comunicação. Tais modificações tem se evidenciado na história social, econômica, cultural e política da humanidade, abrangendo as mais diversas relações, como a interação com outros usuários, o consumo, entre outras variáveis, as quais vão se reconfigurando consoante os proveitos e os benefícios que trazem para os integrantes da sociedade.

Em suma, o processo de comunicação no ciberespaço opera como uma extensão do espaço geográfico, através da capacidade de interligar diversos pontos e lugares do mundo, abrangendo novas formas de interação social.

Nesse contexto, as novas tecnologias consubstanciadas na criação e utilização da Internet, passaram a ser cada vez mais determinantes nas relações estabelecidas dentro dos mais diversos contextos; e, gradativamente, vieram substituir muitos meios e mecanismos de funcionamento dessas relações, com destaque para as relações de consumo.

O aumento significativo da importância das informações no mercado atual, associado à velocidade e à capacidade das novas tecnologias, acabaram por facilitar a coleta, o armazenamento, o processamento e a difusão dessas informações, que após coletadas, passam a influenciar as práticas comerciais, possibilitando verificar desde aspectos relativos ao preço, à qualidade dos produtos, ou à concorrência, como consumidores em potencial, por exemplo.

A partir desse prisma, ressalta-se a questão do tratamento das informações pessoais, conforme aponta Doneda:

A informação pessoal é definida comumente como a informação referente a uma pessoa determinada ou determinável, apresentando uma ligação concreta com a pessoa. Esta modalidade de informação vem se tornando constantemente mais disponível para uma miríade de utilizações, basicamente por conta da facilidade e do baixo custo de sua coleta e armazenamento com os meios digitais hoje disponíveis. O vínculo da informação pessoal com o seu titular deve ser de tal natureza a revelar diretamente algo concreto sobre esta pessoa. Assim, a informação pessoal refere-se às suas características ou ações, atribuíveis à pessoa em conformidade com a lei, como no caso do nome civil ou do domicílio, ou então informações diretamente provenientes de seus atos, como os dados referentes ao seu consumo, informações referentes às suas manifestações, como opiniões que manifesta, e tantas outras (DONEDA, 2010, p. 20).

Ante o exposto, desponta a necessidade de proteção do titular dos dados, sobretudo porque o tratamento inadequado aos dados pessoais, incluindo, os dados sensíveis, pode violar a privacidade, a intimidade e outros direitos fundamentais do indivíduo.

Dado pessoal e dado sensível são definidos pela Lei nº 13.709, de 14 de agosto de 2018 (LGPD), em seu artigo 5º, incisos I e II:

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. (BRASIL, 2018).

Nesse contexto, a proteção de dados diz respeito ao reequilíbrio entre controlador, “pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais”, e o titular, “pessoa natural a quem se referem os dados pessoais que são objeto de tratamento”, que muitas vezes desconhece como se dá o tratamento de dados, suas finalidades ou os seus possíveis riscos. Assim, controlador e titular são definidos pela Lei nº 13.709, de 14 de agosto de 2018 (LGPD), em seu artigo 5º, incisos VI e V, respectivamente.

Em suma, a legislação brasileira já avançou significativamente em relação ao tema com a Lei nº 13.709, de 14 de agosto de 2018, conhecida como Lei Geral de Proteção de Dados (LGPD), no entanto, segundo à recente Proposta de Emenda à Constituição (PEC), no sentido de conferir maior proteção ao tratamento de dados pessoais é necessário prever tal garantia no texto constitucional.

A Comissão de Constituição, Justiça e Cidadania do Senado Federal (SF), no dia 22 de maio de 2019, aprovou a Proposta de Emenda à Constituição Nº 17, que estabelece a proteção de dados pessoais, inclusive nos meios digitais, como direito individual a todos os brasileiros e estrangeiros residentes no país. O texto será analisado pelo Plenário do Senado para, em seguida, ser apreciado pela Câmara dos Deputados.

Dessa forma, a PEC nº 17/2019 acrescenta o inciso XII-A, ao art. 5º e o inciso XXX, ao art. 22, da Constituição da República Federativa do Brasil (CRFB), de 1988, para incluir a proteção de dados pessoais entre os direitos fundamentais do cidadão e fixar a competência privativa da União para legislar sobre a matéria.

Nessa perspectiva, a legislação brasileira segue avançando com a proposta de inclusão da proteção de dados pessoais no rol das garantias individuais, ao lado de direitos fundamentais consagrados pela CRFB, de 1988.

2.3 DESENVOLVIMENTO DAS LEIS DE PROTEÇÃO DE DADOS

As primeiras normas vinculadas à proteção de dados pessoais tiveram sua origem nas décadas de 1960 e 1970, influenciadas pelo desenvolvimento tecnológico, especialmente da informática. Doneda ilustra que:

A mudança do enfoque dado à proteção de dados neste período pode ser entrevisto na classificação evolutiva das leis de proteção de dados pessoais realizada por Viktor Mayer-Scönberger, que vislumbra diferentes gerações de leis que partem desde um enfoque mais técnico e restrito até a abertura a técnicas mais específicas, aplicáveis às tecnologias adotadas para o tratamento de dados (DONEDA, 2010, p. 41).

Em linhas gerais, o desenvolvimento das leis de proteção de dados remonta à preocupação com as informações pessoais constantes em bancos de dados governamentais no século XX. Nesse sentido, segundo Doneda:

A primeira destas gerações de leis pretendia regular um cenário no qual centros de processamento de dados, de grande porte, concentrariam a coleta e gestão dos dados pessoais. O núcleo destas leis girava em torno da concessão de autorizações para a criação destes bancos de dados e do seu controle *a posteriori* por órgãos públicos. Estas leis também enfatizavam o controle do uso de informações pessoais pelo Estado e pelas suas estruturas administrativas, que eram o destinatário principal (quando não o único) destas normas. [...] Exemplo destas leis de primeira geração são a Lei do Land alemão de Hesse, de 1970; a primeira lei nacional de proteção de dados, sueca, que foi o Estatuto para bancos de dados de 1973 – Data Legen 289, ou Datalag, além do Privacy Act norte-americano de 1974 (DONEDA, 2010, p. 41).

Não obstante o direito à privacidade ter se destacado na jurisprudência e doutrina norte-americanas, foi na Europa que se desenvolveram os principais conjuntos de leis sobre proteção de dados pessoais, que emergiram nessas décadas.

Em 1970, o Estado alemão de *Hesse* editou a primeira lei sobre essa matéria; posteriormente, em 11 de maio de 1973, surgiu a Lei nº 289 (*Data Legen*) na Suécia. Em 1974 foi aprovado o Estatuto de Proteção de Dados do Estado Alemão de *Rheinland-Pfalz*. E nesse mesmo período, nos Estados Unidos da América (EUA), o *Fair Credit Reporting Act*, em 1970, com foco na regulação dos relatórios de crédito dos consumidores, e o *Privacy Act*, em 1974, aplicável à administração pública.

A intensificação e a vulnerabilidade no controle e processamento de dados desencadearam a demanda por legislações mais específicas para regular a coleta e o manuseio de informações pessoais, conforme explica Doneda:

Estas leis de proteção de dados de primeira geração não demoraram muito a se tornarem ultrapassadas, diante da multiplicação dos centros de processamento de dados, que inviabilizou o controle baseado em um regime de autorizações. A segunda geração de leis sobre a matéria surgiu no final da década de 1970, já com a consciência da “diáspora” dos bancos de dados informatizados. Pode-se dizer que o seu primeiro grande exemplo foi a lei francesa de proteção de dados pessoais de 1978, intitulada

Informatique et Libertées. A característica básica que diferencia tais leis das anteriores é que sua estrutura não está mais fixada em torno do fenômeno computacional em si, mas se baseia na consideração da privacidade e na proteção dos dados pessoais como uma liberdade negativa, a ser exercida pelo próprio cidadão.[...] Como representante desta geração de leis, podemos mencionar também a lei austríaca (Datenschutzgesetz (DSG), Lei de 18 de outubro de 1978, nº 565/1978); além de que as constituições portuguesa e espanhola apontam neste sentido, mesmo que as leis de proteção de dados destes países tenham surgido somente um pouco mais tarde (DONEDA, 2010, p. 41-42).

Nessa esteira se enquadra a Lei Federal de Proteção de Uso dos Dados Pessoais da Alemanha de 1977; na França, como mencionado pelo autor, viu-se surgir a Lei 78-17, de 06 de janeiro de 1978, concernente à Tecnologia da Informação, arquivos de dados e liberdades civis, que resguarda o direito à informação sobre o tipo de processamento, o direito de acesso e correção, assim como o direito a se opor, por motivos legítimos, ao processamento dos seus dados; a Dinamarca regulamentou a questão da proteção de dados com as Leis 243 e 244, ambas de 08 de julho de 1978, que estenderam a proteção também para as pessoas jurídicas; e a Áustria, com a Lei 565, de 18 de outubro de 1978.

A Constituição de Portugal de 1976, em seu artigo 35, contemplou a previsão do direito do cidadão de conhecer os dados que lhe são concernentes, de que esses dados sejam utilizados de acordo com a finalidade para o qual foram recolhidos e, ainda, de retificá-los, em caso de erro, ou atualizá-los, conforme exposto a seguir:

Artigo 35.º (Utilização da informática)

1. Todos os cidadãos têm o direito de acesso aos dados informatizados que lhes digam respeito, podendo exigir a sua rectificação e actualização, e o direito de conhecer a finalidade a que se destinam, nos termos da lei.
2. A lei define o conceito de dados pessoais, bem como as condições aplicáveis ao seu tratamento automatizado, conexão, transmissão e utilização, e garante a sua protecção, designadamente através de entidade administrativa independente.
3. A informática não pode ser utilizada para tratamento de dados referentes a convicções filosóficas ou políticas, filiação partidária ou sindical, fé religiosa, vida privada e origem étnica, salvo mediante consentimento expresso do titular, autorização prevista por lei com garantias de não discriminação ou para processamento de dados estatísticos não individualmente identificáveis.
4. É proibido o acesso a dados pessoais de terceiros, salvo em casos excepcionais previstos na lei.
5. É proibida a atribuição de um número nacional único aos cidadãos.
6. A todos é garantido livre acesso às redes informáticas de uso público, definindo a lei o regime aplicável aos fluxos de dados transfronteiras e as formas adequadas de protecção de dados pessoais e de outros cuja salvaguarda se justifique por razões de interesse nacional.

7. Os dados pessoais constantes de ficheiros manuais gozam de protecção idêntica à prevista nos números anteriores, nos termos da lei (PORTUGAL, 1976).

Por sua vez, na Espanha, peculiarmente, passou a ter uma regra constitucional determinando a regulamentação da proteção da privacidade contra invasões da atividade informática, consoante previsão do artigo 18, § 4º, da Constituição Espanhola de 1978, o qual dispõe que, “La Ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos”. Além disso, o artigo 105, b, da referida norma, previu a possibilidade de acesso aos arquivos e registros administrativos, ressalvadas as exceções previstas na lei, como em casos que possam interferir na segurança e defesa do Estado, ou afetem a intimidade das pessoas, por exemplo.

Atualmente, os membros da União Europeia contam com uma moderna legislação sobre a proteção de dados pessoais, conhecido como Regulamento Geral de Proteção de Dados (RGPD), nº 679/2016. Esse regulamento veio substituir a Diretiva 95/46/CE, de 1995.

O RGPD entrou em vigor em 25 de maio de 2018, gerando um impacto de nível global, sobretudo no mercado europeu, nas relações comerciais de países europeus com outras nações, incluindo o Brasil.

Os Estados Unidos também são referência mundial no tema, possuindo uma legislação fragmentada. Rony Vainzof, em artigo publicado em julho de 2018, na Revista Conceito Jurídico, destaca algumas leis referentes ao assunto no país:

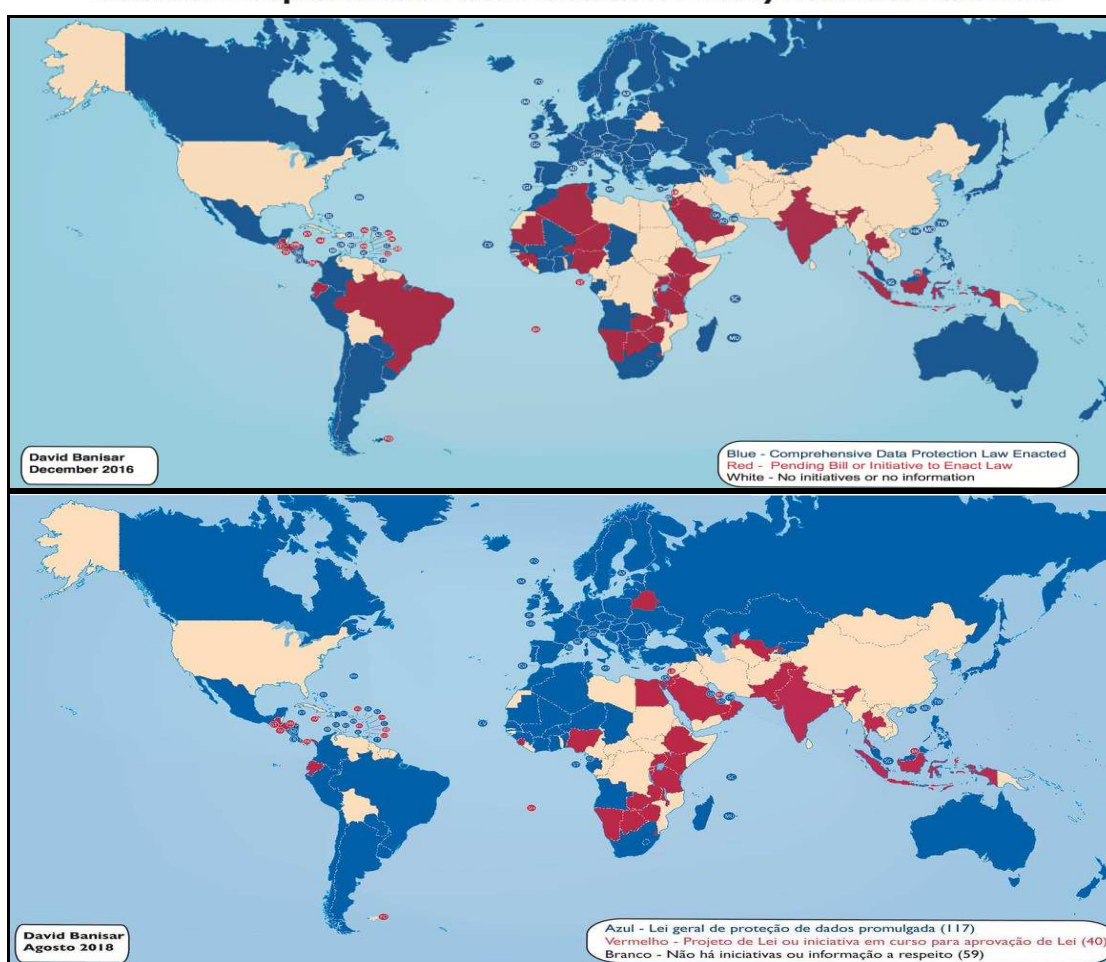
Nos EUA, há leis federais setoriais, todas com mais de 20 anos, como o Health Insurance Portability and Accountability Act (1996), o Electronic Communications Privacy Act (1986), o Video Privacy Protection Act (1988), o Children’s Online Privacy Protection Act (1998), com a relevância do Federal Trade Commission Act, que na sua sessão 5 proíbe atividades comerciais desleais ou enganosas e impõe notificações e práticas razoáveis de segurança da informação, sendo a FTC o órgão federal fiscalizador e sancionador (VAINZOF, 2018, p. 25).

Avançando na temática, foi aprovado o *California Consumer Privacy Act of 2018* (CCPA), no dia 28 de junho de 2018, oficialmente denominado de AB – 375, o qual foi implementado através de uma iniciativa em âmbito estadual na Califórnia, aumentando os direitos a privacidade e a proteção dos consumidores no estado.

Conforme estudo publicado por Daniel Banisar, atualmente há mais de 100 (cem) países que possuem legislações sobre a proteção de dados em vigência, e outros mais de 40 (quarenta) com projetos ou iniciativas pendentes, sendo a maioria embasados em legislações mencionadas, como o RGPD.

Os seguintes mapas elaborados pelo pesquisador, permitem observar (em azul) os países que contam com leis específicas de proteção de dados, muitos deles na América Latina, bem como o desenvolvimento legislativo referente aos anos de 2016 e 2018, respectivamente:

Figura 1 – Projetos e Leis de Proteção de Dados no mundo em 2016 e 2018
National Comprehensive Data Protection/Privacy Laws and Bills 2016



Fonte: BANISAR, Daniel (2018, com adaptações).

Nesse sentido, Demócrito Reinaldo Filho (2018, p. 40) afirma que o Brasil chegou tarde na regulamentação da proteção de dados pessoais. Segundo ele, “muitos países na América do Sul já contavam com leis que protegem a intimidade e a privacidade das pessoas contra coleta e processamento indevidos de dados individuais”, por exemplo:

A Argentina tem leis de proteção de dados pessoais em vigor desde 1994. A lei chilena é de 1999 e o Peru criou sua legislação de proteção de dados em 2011. No Uruguai o direito à proteção de dados está previsto em lei editada em 2008. A Colômbia aprovou sua lei de proteção de dados em 2010 (REINALDO FILHO, 2018, p. 41).

Maria de Lourdes Zamudio Salinas, menciona a evolução legislativa da proteção de dados na América Latina, bem como a criação de autoridades de controle responsáveis pela fiscalização das respectivas leis nos diversos países:

La regulación sobre la protección de datos personales en América Latina ha evolucionado significativamente en los años que van corridos en este nuevo milenio, traduciendo se esto, de manera particular, en la aprobación de leyes de carácter general con autoridades de controlen cinco países: Argentina (2000), Uruguay (2008), México (2010), Perú (2011), Costa Rica (2011) y Nicaragua (2012) (SALINAS, 2012, p. 19).

Seguindo a tendência mundial, foi aprovada a Lei nº 13.709, de 14 de agosto de 2018, conhecida como Lei Geral de Proteção de Dados brasileira (LGPD), que disciplina a proteção dos dados pessoais e define as situações em que podem ser coletados e tratados tanto por empresas quanto pelo Poder Público, por conseguinte, o Brasil se junta a diversos países do mundo que já possuíam regulamentações específicas sobre o tema, inclusive, muitos deles na América Latina.

3 PROTEÇÃO DE DADOS DO CONSUMIDOR SOB A ÓTICA DA LEGISLAÇÃO BRASILEIRA

Até o advento da Lei nº 13.709, de 14 de agosto de 2018 (LGPD), o Ordenamento Jurídico Brasileiro abordava o tratamento de dados pessoais de maneira vaga e esparsa, de modo que, a nova lei criou um marco legal para a proteção de informações pessoais no Brasil.

A preocupação com a proteção de dados pessoais no País, remonta à década de 1980, quando aprovada a Lei nº 7.232, em 29 de outubro de 1984, que estabeleceu a Política Nacional de Informática, atendendo aos princípios previstos no artigo 2º, incisos VIII e IX, conforme exposto:

Art. 2º. A Política Nacional de Informática tem por objetivo a capacitação nacional nas atividades de informática, em proveito do desenvolvimento social, cultural, político, tecnológico e econômico da sociedade brasileira, atendidos os seguintes princípios: VIII - estabelecimento de mecanismos e instrumentos legais e técnicos para a proteção do sigilo dos dados armazenados, processados e veiculados, do interesse da privacidade e de segurança das pessoas físicas e jurídicas, privadas e públicas; IX - estabelecimento de mecanismos e instrumentos para assegurar a todo cidadão o direito ao acesso e à retificação de informações sobre ele existentes em bases de dados públicas ou privadas (BRASIL, 1984).

De fato, o avanço tecnológico influenciou no desenvolvimento da legislação pátria, posto que, diante do crescimento de ameaças à privacidade, bem como a outros direitos subjetivos inerentes ao indivíduo, sobrevém também a necessidade de mecanismos que possibilitem à referida proteção, conforme elucida Luiz Alberto David Araújo:

Os direitos da personalidade, como direitos autônomos, garantidos de forma específica, se constituem em novidades do texto de 1988. A razão para tal proteção encontra-se no desenvolvimento tecnológico e na ameaça de bens como a imagem, a vida privada, a intimidade e a honra das pessoas. Com o desenvolvimento tecnológico, bens como a imagem, a privacidade e a intimidade sofreram maior ameaça, merecendo o cuidado do constituinte. (ARAÚJO, 1996, p. 259).

É inegável, sobretudo, que a proteção aos dados pessoais constitui valor integrante e implícito ao direito à privacidade e encontra guarida no rol dos direitos fundamentais da Constituição da República Federativa do Brasil de 1988, nos termos do artigo 5º, inciso X, o qual dispõe que, “são invioláveis a intimidade, a vida

privada, a honra e a imagem das pessoas, assegurado o direito à indenização pelo dano material ou moral decorrente de sua violação”.

A proteção normativa em relação à privacidade do indivíduo se estabelece de duas formas, conforme ressalta Araújo:

Com efeito, a vida social do indivíduo divide-se em duas esferas: a pública e a privada. Por privacidade, de conseguinte, deve-se entender os níveis de relacionamento social que o indivíduo habitualmente mantém oculto ao público em geral, dentre eles: a vida familiar, as aventuras amorosas, o lazer e os segredos do negócio. Assim, dentro dessa esfera teríamos demarcado o território próprio da privacidade, formado por relações marcadas pela confidencialidade. Entretanto, como se disse, no território da privacidade é que se desenvolvem, por exemplo, as relações conjugais, as relações entre pai e filho, irmãos, namorados, etc., que são peculiarizadas exatamente pela interpessoalidade. Assim, havendo mais de uma pessoa envolvida, existe, por evidente, espaço para violação de direitos, e é nessa porção dos relacionamentos sociais – a chamada “tirania da vida privada” – que ganha importância o conceito de intimidade (ARAÚJO, 2005, p. 239).

Como exposto, percebe-se a distinção constitucional entre intimidade e vida privada, de modo que, em linhas gerais, a primeira seria de conteúdo menos abrangente, ligada às relações subjetivas da pessoa, relaciona-se a fatos mais reservados e pessoais, abrangendo aspectos como orientação sexual, segredos íntimos; por sua vez, a segunda abarcaria o conceito da primeira, incluindo, também, todos os relacionamentos objetivos, por exemplo, as relações comerciais.

Na mesma orientação segue a exposição de Eduardo Molina Quiroga:

A fundamentação jurídica do direito à proteção de dados pessoais, sem dúvida pode e deve relacionar-se com o tradicional direito à intimidade, mas o transcende já que reflete mais que uma idéia individualista de proteção à intimidade, uma tutela dos interesses de um grupo social contra o processamento, armazenamento e coleta de informação, especialmente se admitirmos a vinculação com práticas discriminatórias, ainda quando dito direito esteja entrelaçado com uma parte importante do direito individual à intimidade, que é a que faz referência à proteção dos dados pessoais da esfera privada (QUIROGA, 2000, p. 9).

Assim, a Constituição da República Federativa do Brasil de 1988, prevê o direito à privacidade (art. 5º, inciso X), incluindo a inviolabilidade do sigilo de comunicações, de dados e comunicações telefônicas (art. 5º, inciso XII), bem como a garantia de acesso a informações pessoais, e de retificação de dados, constantes de bancos de dados públicos por meio do Habeas Data (art. 5º, inciso LXXII), este regulado pela Lei nº 9.507, de 1997.

Quanto ao Habeas Data, esclarece o doutrinador Alexandre de Moraes sobre tal instrumento jurídico:

O habeas data é uma ação constitucional, de caráter civil, conteúdo e rito sumário, que tem por objeto a proteção do direito líquido e certo do impetrante em conhecer todas as informações e registros relativos à sua pessoa e constantes de repartições públicas ou particulares acessíveis ao público, para eventual retificação de seus dados pessoais (MORAES, 2018, p. 225).

Dada a sua importância, cabe mencionar em quais situações pode ser concedido: para assegurar o conhecimento de informações relativas à pessoa do impetrante ou para a retificação de dados, quando não se prefira fazê-lo por processo sigiloso, judicial ou administrativo; ademais, tal instituto pode ser impetrado por qualquer pessoa, física ou jurídica, em face de órgãos públicos ou instituições privadas que prestem serviço para a esfera pública ou de interesse público.

Sobretudo para que ocorra a efetivação do direito de proteção aos dados pessoais, compete ao Estado não intervir nas informações pessoais dos indivíduos constantes em bancos de dados públicos ou privados, salvo quando a lei o autorizar, como nos casos das possibilidades de quebra de sigilo de dados (Lei Complementar nº 105/2001), quebra de sigilo das comunicações (artigo 5º, inciso XII, da CF/88 e Lei nº 9.296/96), e nos casos excepcionais, destacados na Lei de Acesso à Informação Pública (artigo 31, da Lei nº 12.527/2011).

Os direitos da personalidade também encontram proteção na Lei nº 10.406, de 10 de janeiro de 2002, o Código Civil, conforme dispõe o artigo 20:

Art. 20. Salvo se autorizadas, ou se necessárias à administração da justiça ou à manutenção da ordem pública, a divulgação de escritos, a transmissão da palavra, ou a publicação, a exposição ou a utilização da imagem de uma pessoa poderão ser proibidas, a seu requerimento e sem prejuízo da indenização que couber, se lhe atingirem a honra, a boa fama ou a respeitabilidade, ou se se destinarem a fins comerciais. Parágrafo único. Em se tratando de morto ou de ausente, são partes legítimas para requerer essa proteção o cônjuge, os ascendentes ou os descendentes (BRASIL, 2002).

Ademais, o art. 21 do referido código, regulamenta o direito à privacidade com o intuito de proteger o resguardo pessoal, dispondo que a vida privada da pessoa natural é inviolável.

Resta clara, igual influência dos direitos de personalidade no direito consumerista, no qual cabe o entendimento de Eduardo Bittar:

Os direitos do consumidor são a concretização de direitos de personalidade. Prova disso é a extensa previsão legal existente, que garante ao consumidor a salvaguarda dos valores que o cercam na situação de consumo, todos protegidos legalmente (direito à vida, à saúde, à higidez física, à honra) e devidamente instrumentalizados (ação de reparação por danos materiais e morais, ações coletivas para proteção de direitos difusos, procedimentos administrativos) (BITTAR, 2002. p.149-150).

No Ordenamento Jurídico Brasileiro, a proteção às informações pessoais deve incidir, até mesmo, quando o indivíduo desenvolve sua personalidade nos meios eletrônicos, uma vez que a tecnologia passou a estar cada vez mais presente, seja na esfera de relações pessoais ou profissionais praticadas nesse meio, sobretudo nas relações de consumo.

O Código de Defesa do Consumidor – CDC (Lei nº 8.078/90), trata da questão do acesso por parte do consumidor aos dados pessoais que estejam arquivados, conforme exposto em seu artigo 43:

O consumidor, sem prejuízo do disposto no art. 86, terá acesso às informações existentes em cadastros, fichas, registros e dados pessoais e de consumo arquivados sobre ele, bem como sobre as suas respectivas fontes. § 1º 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. § 2º A abertura de cadastro, ficha, registro e dados pessoais e de consumo deverá ser comunicada por escrito ao consumidor, quando não solicitada por ele. § 3º 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 (BRASIL, 1990).

Consta, que uma das formas mais frequentes de violação da privacidade decorrente do avanço da tecnologia está no âmbito das relações de consumo e nas práticas comerciais; podendo se caracterizar pela utilização inadequada dos arquivos de consumo, por exemplo.

Ao regular os arquivos de consumo, o CDC expressamente estabeleceu o direito de acesso do consumidor a esses cadastros e bancos de dados com informações a seu respeito e às respectivas fontes, determinando o dever de clareza, retificação de informações incorretas e notificação ao consumidor sobre a coleta e o uso de seus dados. Além disso, o armazenamento foi estipulado por um período máximo de cinco anos. O Decreto nº 7.962 de 2013, que regulamentou o CDC para dispor sobre o comércio eletrônico, trouxe ainda em seu artigo 4º, inciso VI, que “o fornecedor deverá utilizar mecanismos de segurança eficazes para o tratamento de dados do consumidor”.

A Lei nº 12.414, de 09 de junho de 2011, conhecida como Lei do Cadastro Positivo, passou a disciplinar a formação e consulta a bancos de dados com informações de adimplemento, de pessoas naturais ou de pessoas jurídicas, para formação de histórico de crédito, respeitadas as disposições previstas no CDC.

O Cadastro Positivo, inicialmente criado pela referida Lei, trata em linhas gerais, da formação de bancos de dados com informações positivas ou adimplidas pelo consumidor.

Em 8 de abril de 2019, foi sancionada a Lei Complementar 166, que estabelece mudanças no funcionamento do Cadastro Positivo, com as alterações. A adesão aos bancos de dados do Sistema do Cadastro Positivo passou a ser automática a todos que não se opuserem expressamente; o Cadastro vai incorporar informações de todos os cidadãos, automaticamente, no entanto, a exclusão poderá ser solicitada a qualquer momento.

O Cadastro Positivo, contudo, não afeta o sigilo bancário; saldo da conta ou detalhes da fatura do cartão, por exemplo, devem ser resguardados, bem como informações pessoais que não estiverem vinculadas à análise de risco de crédito, como consta nas informações divulgadas pelo Banco Central do Brasil:

O Cadastro Positivo existe desde 2011, mas a adesão dos consumidores era voluntária. Com a sanção presidencial da nova lei, a expectativa é que o banco de dados receba informações de mais de 110 milhões de pessoas. Atualmente, o sistema contém os dados de aproximadamente seis milhões de clientes. Integram o Cadastro Positivo informações sobre operações de crédito quitadas ou em andamento – inclusive cartão de crédito, cheque especial e financiamentos. O banco de dados não pode reunir informações pessoais e que não estiverem vinculadas à análise de risco de crédito (BANCO CENTRAL DO BRASIL, 2019).

Atente-se também que a Lei nº 12.527, de 18 de novembro de 2011, denominada Lei de Acesso à Informação (LAI), entrou em vigor em 16 de maio de 2012, possibilitando a qualquer pessoa, física ou jurídica, sem necessidade de apresentar motivo, o recebimento de informações públicas dos órgãos e entidades.

Esta norma é válida para os três Poderes da União, Estados, Distrito Federal e Municípios, inclusive aos Tribunais de Conta e Ministério Público, bem como as entidades privadas sem fins lucrativos, que são obrigadas a dar publicidade a informações referentes ao recebimento e à destinação dos recursos públicos por elas recebidos.

A LAI tem por escopo que todas as informações produzidas ou sob guarda do poder público são públicas e, portanto, acessíveis a todos os cidadãos, sobretudo, resguarda que o tratamento das informações pessoais deve ser feito de forma transparente e com respeito aos direitos fundamentais constitucionalmente estabelecidos. O artigo 31 da referida lei, esclarece o acesso às informações pessoais, bem como prevê tais restrições:

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.

§ 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.

§ 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. (BRASIL, 2011).

Necessário se faz, da mesma forma, mencionar, a Lei nº 12.965, de 23 de abril de 2014, conhecida por Marco Civil da Internet, que estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil, no âmbito da União, dos Estados, do Distrito Federal e dos Municípios.

O Marco Civil da Internet, reconheceu as relações jurídico-virtuais e seus efeitos no ordenamento, prevendo, por exemplo, disposições referentes aos crimes cibernéticos. No entanto, tal norma deveria prever as possibilidades técnicas e jurídicas de viabilização da proteção às informações pessoais, as quais estão expostas a práticas não totalmente transparentes nos serviços de internet, ao passo que se coloca como legislação de defesa dos usuários, mas não aponta os caminhos necessários para a implementação dos direitos e deveres que transcreve.

Diante disso, existe uma grande lacuna na questão da proteção de dados pessoais que são totalmente ignoradas pela referida lei. Destarte, apesar de caracterizar um avanço na legislação sobre o tema, o Marco Civil da Internet não conseguiu suprir às lacunas normativas acerca da proteção de dados pessoais.

Consoante o crescente desenvolvimento tecnológico, bem como a dificuldade que o legislador se depara para acompanhar estas alterações, não se confere uma efetiva proteção das informações pessoais na legislação nacional, sobretudo, a respeito dos dados dos consumidores.

Como visto, o Código de Defesa do Consumidor e a Lei do Cadastro Positivo regulamentam o direito à proteção de dados pessoais nas relações de consumo, mas essa proteção setorial é insuficiente.

Na verdade, percebe-se que os instrumentos normativos de proteção consumerista não se apresentam satisfatórios. Daí a importância de previsões capazes de expandir esses direitos para contextos mais variados, online e off-line, envolvendo o uso de dados pessoais.

Para esse fim, foi promulgada a Lei nº 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados do Brasil (LGPD), que transplanta o sistema setorial de proteção nacional para um geral, e abrange o tratamento de dados pessoais, independente do contexto, setor e mercado, trazendo inovações marcantes e gerando impactos na sociedade, o que demanda adaptação às novas regulamentações.

4 PRINCIPAIS INOVAÇÕES DA LEI Nº 13.709, DE 14 DE AGOSTO DE 2018

A Lei nº 13.709, de 14 de agosto de 2018, conhecida como Lei Geral de Proteção de Dados Pessoais (LGPD), foi inspirada em leis internacionais, em evidência, no Regulamento Geral sobre a Proteção de Dados nº 679/2016 (*General Data Protection Regulation* – “GDPR”), regulamento europeu que entrou em vigor em 2018 e possui abrangência extraterritorial.

Destaca-se a importância da nova legislação brasileira, resultado do empenho de vários setores da sociedade em busca de um avanço legislativo referente ao tema no país, conforme elucida Rony Vainzof:

No Brasil, além da nossa Constituição Federal, já tínhamos ao menos 30 (trinta) legislações setoriais que permeavam o assunto, como o Código de Defesa do Consumidor, o Código Civil, a Lei do Cadastro Positivo, o Marco Civil da Internet, apenas para citar alguns exemplos. Porém, mesmo diante de tantas leis setoriais, há anos se discutia no Brasil um marco legal em proteção de dados pessoais, diante da sua relevância para o nosso país, principalmente para trazer maior segurança jurídica mediante a harmonização de conceitos, elevando a proteção aos direitos individuais das pessoas e ao fomento da economia digital, bem como, com um nível de legislação compatível com outros países, da facilitação ao fluxo de transferência internacional de dados (VAINZOF, 2018, p. 26).

O processo público e legislativo começou em 2010, com a abertura de uma consulta pública sobre o tema, promovida pelo Ministério da Justiça, que resultou, posteriormente, na propositura do Projeto de Lei 5.276/2016, anexado ao PL 4.060/2012, perante a Câmara dos Deputados.

No dia 10 de julho de 2018, foi aprovado no plenário do Senado Federal o Projeto de Lei Complementar 53/2018, o qual dispõe sobre a proteção de dados pessoais e altera a Lei 12.965/14, conhecida como Marco Civil da Internet.

Após dois anos de trâmite no Congresso Nacional, duas consultas públicas, mais de 2.500 contribuições, inúmeros eventos e interações com vários atores nacionais e internacionais de todos os setores, a lei foi sancionada em 14 de agosto de 2018, publicada no Diário Oficial da União (DOU) em 15 de agosto de 2018, e republicada parcialmente no mesmo dia em edição extra.

O projeto sofreu vetos de Michel Temer, o qual vetou a criação da Autoridade Nacional de Proteção de Dados (ANPD) que seria o órgão independente que faria a fiscalização da aplicação da lei.

Entretanto, a Medida Provisória nº 869, de 27 de dezembro de 2018, estabeleceu a criação da Autoridade Nacional de Proteção de Dados Brasileira, bem como estendeu o prazo legal para a lei entrar em vigor para vinte e quatro meses.

A Lei Geral de Proteção de Dados (LGPD) apresenta-se de forma inovadora, portanto, fundamental para a sua compreensão é o conhecimento sobre alguns pontos destacados, mesmo que sintenticamente, quais sejam: a abrangência da lei; a aplicação extraterritorial; os direitos dos titulares de dados; a autorização para o tratamento de dados; os princípios de tratamento; as regras específicas no que concerne ao tratamento de dados, em especial os sensíveis, de crianças e adolescentes e a transferência internacional de dados; o mapeamento do tratamento de dados; a avaliação de impacto à proteção de dados; o *Data protection officer* (DPO); as notificações obrigatórias; bem como a criação de uma autoridade nacional de controle.

A LGPD aplica-se ao tratamento de dados pessoais, inclusive nos meios digitais, por empresas privadas ou órgãos públicos, no intuito de resguardar a pessoa física e natural, como esclarece seu artigo 1º:

Art. 1º Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural (BRASIL, 2018).

A sua aplicação é extraterritorial, ou seja, afeta qualquer operação de tratamento realizada por pessoa natural ou por pessoa jurídica de direito público ou privado, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados, desta maneira, define situações, tais como: o tratamento de dados realizado no Brasil; o tratamento de dados para ofertar produtos ou serviços, ou relacionado com indivíduos localizados no Brasil; ou os dados que tenham sido coletados no Brasil, isto é, de pessoas que estejam no país no momento da coleta.

Todavia, nos termos do artigo 4º, da LGPD não se aplicará ao tratamento de dados pessoais quando realizados nas seguintes hipóteses:

Art. 4º Esta Lei não se aplica ao tratamento de dados pessoais: I - realizado por pessoa natural para fins exclusivamente particulares e não econômicos; II - realizado para fins exclusivamente: a) jornalístico e artísticos; ou b) acadêmicos; III - realizado para fins exclusivos de: a) segurança pública; b) defesa nacional; c) segurança do Estado; ou d) atividades de investigação e

repressão de infrações penais; ou IV - provenientes de fora do território nacional e que não sejam objeto de comunicação, uso compartilhado de dados com agentes de tratamento brasileiros ou objeto de transferência internacional de dados com outro país que não o de proveniência, desde que o país de proveniência proporcione grau de proteção de dados pessoais adequado ao previsto nesta Lei (BRASIL, 2018).

A LGPD garante ao titular dos dados, além dos direitos de informação, acesso, correção e revogação do consentimento, o direito de requerer a portabilidade dos dados pessoais, isto é, de solicitar a transferência de seus dados pessoais a outro fornecedor de serviço ou produto, mediante requisição expressa; possibilita ao titular a oposição ao tratamento dos dados quando realizados nas hipóteses de dispensa de consentimento, dado o descumprimento da norma; bem como a anonimização ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com a legislação.

Ao titular dos dados, também foi assegurado o direito de solicitar a revisão, bem como a disponibilização de informações claras e adequadas a respeito dos critérios e dos procedimentos utilizados quando tal tratamento for baseado exclusivamente em decisões automatizadas, conforme disposição do artigo 20 da LGPD:

Art. 20. O titular dos dados tem direito a solicitar a revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, incluídas as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade (BRASIL, 2018).

Neste ensejo, com o advento do novo texto legislativo, os usuários podem obter informações sobre os dados coletados, saber a quem e com qual finalidade estes dados foram repassados, e pedir alteração caso estejam incompletos, inexatos ou desatualizados, também passa a ser possível a exclusão, ressalvadas as exceções previstas em lei, como é o caso das informações para fins de pesquisa, que devem ser realizadas preferencialmente em anonimato, dentre outros.

Em relação ao tratamento dos dados pessoais, a LGPD estabelece dez hipóteses, incluindo, além do consentimento, o interesse legítimo do controlador ou de terceiro, a necessidade de cumprimento de contrato ou de obrigação legal ou regulatória. O artigo 7º da referida norma, prevê de forma taxativa, em quais hipóteses é possível a realização do tratamento de dados pessoais:

Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:

- I - mediante o fornecimento de consentimento pelo titular;
- II - para o cumprimento de obrigação legal ou regulatória pelo controlador;
- III - pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei;
- IV - para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;
- V - quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados;
- VI - para o exercício regular de direitos em processo judicial, administrativo ou arbitral, esse último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem);
- VII - para a proteção da vida ou da incolumidade física do titular ou de terceiro;
- VIII - para a tutela da saúde, em procedimento realizado por profissionais da área da saúde ou por entidades sanitárias;
- IX - quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais; ou
- X - para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente (BRASIL, 2018).

Quanto a obtenção do consentimento, a partir da nova legislação, o consentimento é compreendido como uma manifestação livre, informada e inequívoca que autoriza o tratamento de dados pessoais para uma finalidade determinada, por isso, autorizações genéricas, que não têm como escopo uma finalidade específica, explícita e informada serão nulas.

Por conseguinte, o consentimento deverá ser fornecido por escrito em cláusula destacada ou por qualquer outra ação afirmativa que demonstre a vontade do titular dos dados, não se admitindo hipóteses com consentimento implícito, podendo, ainda, ser revogado a qualquer momento pelo titular, por procedimento gratuito e facilitado, considerado assim como uma autorização temporária. Dessa forma, ocorrendo alterações na finalidade para a qual o consentimento do titular foi obtido, tornando-se esta incompatível com a autorização originalmente dada para o tratamento dos dados pessoais, deverá o titular ser previamente informado sobre tal mudança.

Em caso de dados tornados manifestamente públicos pelo próprio titular, a obtenção ao consentimento para o tratamento de dados passa a ser dispensável, observada sua finalidade originária, de modo que permanecem vigentes os demais direitos do titular e princípios estabelecidos na LGPD.

No caso de tratamento de dados pessoais com fundamento no interesse legítimo do controlador ou de terceiro, somente os dados estritamente necessários, considerando a finalidade pretendida, poderão ser utilizados, desde que tal tratamento não viole os direitos e liberdades fundamentais do titular dos dados e que sejam adotadas medidas para garantir sua transparência.

O direito a proteção de dados pessoais requer para sua configuração, a adoção de determinadas garantias e princípios que devem ser estabelecidos a todo o tratamento dos dados, desde o momento da coleta; a observação dos princípios é a garantia de um tratamento adequado as informações pessoais. Nesse sentido, a LGPD em seu artigo 6º, consagra os seguintes princípios:

Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:

I - finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;

II - adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;

III - necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;

IV - livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;

V - qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;

VI - transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;

VII - segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;

VIII - prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;

IX - não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;

X - responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas (BRASIL, 2018).

Dos princípios previstos, destaca-se como de especial relevância quando do tratamento de dados, sobretudo dos dados sensíveis, o princípio da finalidade e o da não discriminação. Pelo princípio da finalidade, os dados devem ser tratados para propósitos específicos, previamente informados a seu titular de maneira explícita,

sem que seja possível a sua utilização posterior para outra aplicação, na qual haveria abusividade, esclarece Doneda que:

Este princípio possui grande relevância prática: com base nele fundamenta-se a restrição da transferência de dados pessoais a terceiros, além do que é possível a estipulação de um critério para valorar a razoabilidade da utilização de determinados dados para uma certa finalidade (DONEDA, 2006, p. 216).

Em relação ao princípio da não discriminação, conforme visto no art. 6º, inciso IX, a lei veda a utilização dos dados pessoais para fins discriminatórios ilícitos ou abusivos, não impedindo, porém, a possibilidade de tratamentos diferenciados de dados. Nesse sentido, Rodotà menciona que:

[...] coletar dados sensíveis e perfis sociais e individuais pode levar à discriminação; logo, a privacidade deve ser vista como “a proteção de escolhas de vida contra qualquer forma de controle público e estigma social” (L. M. Friedman), como a “reivindicação dos limites que protegem o direito de cada indivíduo a não ser simplificado, objetivado, e avaliado fora de contexto” (J. Rosen) (RODOTÀ, 2008, p.12).

Logo, se questiona se esse tratamento segregado, desde que lícito e não abusivo, pode ser realizado também quando considerados os dados pessoais sensíveis, na medida em que eles possuem características personalíssimas, que devem ser tuteladas prioritariamente, portanto, torna-se necessário verificar quais as restrições impostas na lei para seu tratamento.

Para fins de regulação das atividades de tratamento de dados, a Lei Geral de Proteção de Dados Brasileira (LGPD) categoriza e tutela de forma diferenciada os dados pessoais, dados pessoais sensíveis, e dado anonimizado, conforme dispõe o art. 5º:

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 (BRASIL, 2018).

O conceito de dado pessoal é bastante abrangente, isto é, um dado é considerado pessoal quando ele permite a identificação da pessoa natural, direta ou indiretamente, tais como: nome, sobrenome, data de nascimento, CPF, RG,

endereço residencial ou comercial, telefone, e-mail, cookies, endereço IP, dentre outros. A referida lei também definiu os dados pessoais sensíveis, visto que são aqueles que apresentam maior potencial lesivo, dadas as características personalíssimas do indivíduo, devendo-se observar regras mais rígidas para tal tratamento, a exemplo do artigo 11 da norma, em que o consentimento deve ser fornecido de forma específica e destacada, para finalidades específicas.

No entanto, a lei dispõe que o tratamento pode ser possível sem o fornecimento do consentimento, quando for indispensável para o cumprimento de obrigação legal ou regulatória pelo controlador dos dados, para o exercício regular de direitos em processo judicial, administrativo ou arbitral ou necessário para a execução de contrato, entre outras hipóteses, nos termos do art. 11, II.

Dadas tais peculiaridades dos dados sensíveis, destaca-se, por exemplo, a vedação aos controladores de comunicação ou compartilhamento destes dados no intuito de auferir lucro, consoante previsão do art. 11, §3º, o que caberá a autoridade de controle regulamentar a questão, conforme a seguir:

A comunicação ou o uso compartilhado de dados pessoais sensíveis entre controladores com objetivo de obter vantagem econômica poderá ser objeto de vedação ou regulamentação por parte de autoridade nacional, ouvidos os órgãos setoriais do Poder Público, no âmbito de suas competências (BRASIL, 2018).

Em relação aos dados anonimizados, estes estão excluídos do escopo de aplicação da lei, uma vez que não permitam a identificação de forma direta ou indireta do seu titular. Para fins do referido texto normativo, a “anonimização” é um procedimento por meio do qual um dado perde a possibilidade de identificar o indivíduo, a qual deve ser utilizada sempre que possível, como no caso de estudos em saúde pública e por órgãos de pesquisas, por exemplo; bem como, é um dos direitos assegurados ao titular dos dados, quando estes forem utilizados de forma excessiva, desnecessária ou em desacordo com a lei.

Entretanto, ressalta-se que a linha divisória entre dados pessoais e dados anonimizados é bastante tênue, a exemplo, a LGPD em seu artigo 12, § 2º, dispõe que, “poderão ser igualmente considerados como dados pessoais, para os fins desta Lei, aqueles utilizados para formação do perfil comportamental de determinada pessoa natural, se identificada”. A utilização de determinadas técnicas de tratamento de dados, dispensa a necessidade da precisa identificação da pessoa natural

relacionada aos dados tratados, como o *data-profiling*, que visa a segregação de indivíduos em determinadas categorias, sem que seja necessária a identificação precisa destes para a obtenção de informações comercialmente valiosas, em suma, tal aplicação permite a identificação de grupos de indivíduos, aos quais podem ser dirigidas propagandas relacionadas aos seus perfis. Em tais situações, informações como nome, sobrenome ou CPF tornam-se irrelevantes, ocasionando a impressão de que a anonimização estaria assegurada.

Ademais, em um processo chamado “reversão”, a partir de algoritmos complexos, é possível inferir a quem determinado dado anonimizado se refere. Quanto a essa possibilidade, a LGPD não se descuidou estabelecendo que não são anonimizados os dados cujo procedimento puder ser revertido, com esforços razoáveis e por meios próprios, nos termos do artigo 12 da LGPD:

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

Para garantir maior proteção ao procedimento de anonimização dos dados, a LGPD em seu artigo 12, § 3º, prevê que “a autoridade nacional poderá dispor sobre padrões e técnicas utilizados em processos de anonimização e realizar verificações acerca de sua segurança”.

Quanto ao tratamento de dados pessoais de crianças e de adolescentes, estes gozam de proteção diferenciada, posto que tal tratamento deverá ser realizado em seu melhor interesse, com o consentimento específico e por pelo menos um dos pais ou pelo responsável legal. Como exemplo, é o acesso de crianças e adolescentes à plataforma do *Youtube* vinculado ao consentimento de ao menos um dos pais, conforme previsão do artigo 14, §1º, da LGPD, caso este em que deverão ser realizados todos os esforços razoáveis para verificar que o consentimento foi realmente fornecido por um dos ascendentes.

A LGPD permite a coleta de dados pessoais sem o consentimento dos pais ou responsável legal apenas na hipótese em que haja a necessidade de realizar contato com os mesmos. Nesta situação, os dados pessoais coletados sem o prévio consentimento disposto na lei, poderá ser utilizado somente uma vez, sendo vedado o armazenamento, dado que sua única finalidade é a realização do referido contato.

O tratamento de dados pessoais pelas pessoas jurídicas de direito público, também apresenta características peculiares, devendo considerar a finalidade e o interesse público, consoante o artigo 23 da LGPD. Para que tal tratamento seja realizado, a lei estabelece que sejam fornecidas em veículos de fácil acesso, preferencialmente em seus sítios eletrônicos, informações claras e atualizadas sobre a previsão legal, a finalidade, as práticas e os procedimentos que serão utilizados nestas atividades, bem como a indicação de um encarregado, profissional responsável pela proteção aos dados pessoais em tais tratamentos.

Os serviços notariais e de registro exercidos em caráter privado, por delegação do Poder Público, terão o mesmo tratamento dispensado às pessoas jurídicas de direito público, e devem fornecer por meio eletrônico o acesso a tais dados para a administração pública.

Quanto as empresas públicas e as sociedades de economia mista que atuam em regime de concorrência, nos termos do artigo 173 da Constituição da República Federativa do Brasil de 1988, terão o mesmo tratamento dispensado às pessoas jurídicas de direito privado. Por outro lado, se estiverem operacionalizando políticas públicas as quais estejam atuando na execução, terão o mesmo tratamento dispensado aos órgãos e às entidades do Poder Público.

Em matéria de transferência de dados pessoais para outros países, somente será permitida para quem proporcione grau de proteção de dados pessoais adequado ao disposto na LGPD, a qual determina expressamente as hipóteses permitidas, em seu artigo 33:

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 (BRASIL, 2018).

Não obstante o nível de proteção dos dados do país estrangeiro ou do organismo internacional, a Autoridade Nacional de Proteção de Dados avaliará, considerando, dentre outras hipóteses, a adoção de medidas de segurança, a natureza dos dados, bem como as normas gerais e setoriais vigentes no país de destino ou no organismo internacional, consoante disposição do artigo 34, da referida norma.

Quanto ao momento no qual os dados pessoais não sejam mais necessários para o objetivo inicial, o seu tratamento será terminado. Assim, o término do tratamento de dados pessoais deverá ocorrer, nas seguintes situações: depois de atingida a finalidade da coleta do dado pessoal; ao final do período de tratamento; mediante recebimento de comunicação do titular, inclusive no exercício do seu direito de revogação do consentimento; ou por determinação legal. Dessa forma, ao término do tratamento, os dados pessoais devem ser eliminados, exceto se de outra forma o seu armazenamento for autorizado pela referida norma, tal como o emprego de anonimização, por exemplo.

A Lei Geral de Proteção de Dados elegeu algumas medidas que visam assegurar uma maior efetividade a proteção aos dados pessoais, tal como, o mapeamento do tratamento de dados, o qual compreende que as atividades relacionadas a tais tratamentos devem ser mantidas em registros, consoante previsão do artigo 37.

Por sua vez, o artigo 38 da norma, alude sobre a possibilidade de avaliação de impacto à proteção de dados, mediante determinação da autoridade de controle, na qual configura-se em um relatório em que deverá constar, no mínimo, as seguintes informações: descrição dos tipos de dados coletados, a metodologia utilizada para a coleta e para a garantia da segurança das informações, bem como a análise do controlador com relação a essas medidas, salvaguardas e mecanismos de mitigação de riscos adotados.

A figura do *Data Protection Officer* (DPO) também compreende uma significativa inovação da LGPD, nos termos do artigo 41, toda empresa que atua com o tratamento de dados pessoais deverá nomear um encarregado, profissional responsável por assegurar tal proteção.

Outro destaque corresponde a segurança das informações, a lei vislumbra assegurar a integridade dos dados de forma mais intensiva, desta forma, a notificação aos titulares dos dados passará a ser obrigatória em caso de incidentes que possam acarretar-lhes algum risco ou dano relevante, bem como a autoridade de controle deverá ser comunicada, em prazo razoável.

Por fim, uma das grandes inovações previstas na lei refere-se à criação da Autoridade Nacional de Proteção de Dados (ANPD), introduzida pela Medida Provisória nº 869, de 27 de dezembro de 2018, órgão da administração pública federal, integrante da Presidência da República, será responsável por zelar, implementar e fiscalizar o cumprimento da LGPD, além de aplicar as sanções previstas para os casos de descumprimento das exigências legais.

Entre outras competências, está a edição de normas e procedimentos sobre a proteção de dados pessoais, o estímulo a adoção de padrões para serviços e produtos, a elaboração de estudos sobre as práticas de proteção de dados, bem como a promoção de ações de cooperação com autoridades de proteção de dados pessoais de outros países, de natureza internacional ou transnacional, nos termos do artigo 55-J, bem como demais atribuições que visam a correta aplicação da lei.

A agência reguladora será composta por um quadro técnico de 23 profissionais, sendo cinco deles membros do Conselho Diretor do órgão, que serão escolhidos e nomeados pelo presidente da República após aprovação pelo Senado Federal, e ocuparão cargos comissionados.

5. A UTILIZAÇÃO DOS DADOS DOS CONSUMIDORES E SEUS RISCOS

Para auxiliar na compreensão do tema, é imprescindível refletir sobre o uso e abuso no tratamento dos dados pessoais, considerada uma atividade que possibilita riscos aos consumidores, por exemplo, quando na utilização indevida ou abusiva de dados pessoais; na eventualidade destes dados não serem corretos e representarem erroneamente seu titular; ou na utilização por terceiros sem o devido consentimento ou conhecimento do titular, entre outras hipóteses, consoante exposição a seguir.

5.1 COMERCIALIZAÇÃO DE DADOS PESSOAIS E VIOLAÇÕES AOS DIREITOS DA PERSONALIDADE

Têmis Limberger, em sua obra *o Direito à Intimidade na Era da Informática* (2007), analisa com muita propriedade o desafio relacionado a proteção das informações pessoais no âmbito comercial:

O comércio e intercâmbio de informação e de dados são necessários, são quase uma demanda da sociedade atual, e por isso impõe-se a tutela dos direitos fundamentais. A globalização pressupõe uma economia sem fronteiras e sem regulamentação. No entanto, não se pode desprezar anos de construção de direitos fundamentais e mudar tudo isso por uma única lei: a lei do mercado e a ilusão de que o mercado tudo regulará. O grande desafio que se impõe no plano dos direitos fundamentais é como fazer com que não somente o capital e os bens de consumo circulem em todo o mundo, mas também os direitos (LIMBERGER, 2007, p. 33).

Os avanços tecnológicos, bem como a intensificação do uso da internet, aumentaram as possibilidades de obter informações pessoais, no entanto, ressalta-se que estas informações por vezes são utilizadas para fins lucrativos, sem o devido consentimento do titular ou seu conhecimento, podendo ser vendidas a terceiros ou utilizadas pelos próprios responsáveis pelo tratamento no intuito de auferir lucro ou vantagem no mercado, o que pode ensejar em violações aos direitos da personalidade, como destaca Fernanda Mendonça:

Ocorre que, muitas vezes, os cidadãos e especialmente os usuários das novas ferramentas tecnológicas como a internet, têm sua privacidade e intimidade violadas por pessoas físicas ou jurídicas que buscam obter suas informações a todo o custo. Além disso, uma vez armazenada a informação, ela é repassada a terceiros sem o consentimento – ou, pior, sem o conhecimento – dos titulares dos dados. Configura-se, daí uma verdadeira violação ao direito à privacidade dos indivíduos, que ficam à mercê de quem

detém o conhecimento técnico, sem poder ter controle das informações sobre si mesmo, as quais são bens privados de cada um e merecem a devida proteção e respeito. Porém, no que diz respeito ao titular desses dados, muitas vezes a apropriação de tais informações por terceiros gera constrangimento e/ou revolta, por se tratarem de dados privados (MENDONÇA, 2016, p. 283-311).

Paralelo ao desenvolvimento tecnológico, surgem técnicas mais avançadas e eficientes para o tratamento de dados, possibilitando as empresas coletar e analisar um volume cada vez maior, como práticas relativas ao monitoramento dos consumidores, direta ou indiretamente.

Em relação ao tratamento de dados, o estudo será delimitado em etapas, nas quais a autora Laura Schertel Mendes (2008, p. 86), considera que podem acarretar mais riscos à personalidade e à privacidade do consumidor, quais sejam: a coleta, o processamento e à difusão de dados, conforme descritas a seguir:

O momento da coleta pode ser considerado a primeira fase do tratamento dos dados, no qual a empresa ou o controlador do banco de dados necessita obter as informações pessoais do consumidor, o que pode ser realizado a partir do próprio consumidor ou de outras fontes (...) O processamento de dados constitui a segunda fase do tratamento, na qual os dados são submetidos a diversas técnicas necessárias para lapidá-los e transformá-los em informações úteis para a empresa (...) o terceiro momento de tratamento de dados, que corresponde à sua difusão ou cessão. (MENDES, 2008, p. 87).

Tratando-se da utilização dos dados dos consumidores, muitas empresas utilizam estes dados para auferir lucro através da análise do comportamento na internet, a exemplo de redes sociais como o *Facebook*, *Instagram* e *LinkedIn*, além de grandes corporações como o *Google*, inclusive o *Facebook* atualizou sua política de dados em abril de 2018, após escândalos envolvendo violações de informações, em especial o da *Cambridge Analytica*.

Outras vezes, o próprio usuário considera vantagem ao acessar os serviços de determinada empresa de forma gratuita, por meio do preenchimento do cadastro rápido, na verdade, estas empresas estão colhendo os dados do consumidor, para futuramente vender a terceiros.

Há diversas outras empresas, em vários setores, que também realizam práticas semelhantes, como as lojas, supermercados e farmácias que garantem descontos para o cadastramento do CPF do cliente, sem, no entanto, informar que estes dados são repassados para que outras empresas tenham acesso e possam oferecer serviços.

Laura Schertel Mendes menciona diversas formas de apropriação de dados, as quais considera como as principais fontes de dados dos consumidores, conforme a seguir:

As principais fontes de dados dos consumidores são as seguintes: i) transações comerciais, ii) censos e registros públicos; iii) pesquisas de mercado e de estilo de vida e; iv) sorteios e concursos; v) comercialização e cessão de dados; vi) tecnologias de controle na internet; e vii) facilitadores tecnológicos. (MENDES, 2008, p.87 - 88).

Entre as diversas formas de apropriação de dados pessoais, como as mencionadas por Mendes, destaca-se a prática de marketing comportamental no âmbito virtual, a qual segundo Doneda:

A prática do marketing comportamental online é relativamente recente, apesar de já poder ser tratada como um traço estrutural de muitos modelos de negócios baseados na Internet. A necessidade de garantir os direitos do consumidor neste ambiente contra práticas abusivas, bem como de lhe proporcionar a efetiva proteção sobre suas próprias informações pessoais vem sendo, portanto, tema de iniciativas regulatórias em aspectos como, entre outros, a garantia do consentimento livre do consumidor para a atuação destes serviços, a salvaguarda de sua privacidade, a transparência desta atividade e a possibilidade de recusar-se a continuar recebendo publicidade comportamental, entre outros (DONEDA, 2010, p. 96).

Nesse contexto é importante refletir sobre o consentimento do titular, o qual deve ser expresso e com evidente aprovação, não podendo ser genérico, dentro de termos de usos que muitas vezes não são lidos pelos usuários, consoante esclarece Doneda em relação ao consentimento e a necessidade de informação ao consumidor, em casos de publicidade comportamental:

Em relação ao consentimento, um aspecto a ser levado em conta é que a necessidade de informar ao consumidor sobre a publicidade comportamental não se exaure no momento da obtenção do consentimento para a sua realização. A ser tomado desta forma, o consentimento do consumidor mais se assemelharia - e correria o risco de ser tratado - como um objetivo a ser atingido pelo fornecedor em um determinado momento do que uma escolha livre, consciente em relação às opções disponíveis, cujos efeitos prolongam-se no tempo. Para isso, devem ser proporcionadas ao consumidor as condições para perceber e identificar claramente quando uma mensagem publicitária comportamental lhe é dirigida, de forma a distingui-la das demais em situações onde tal dúvida possa ocorrer. Somente desta forma o consumidor poderá dispor de elementos para julgar efetivamente a conveniência do recebimento desta modalidade de publicidade e também para buscar solucionar eventuais abusos (DONEDA, 2010, p. 97).

Em um mundo cada vez mais informatizado, técnicas e ferramentas são desenvolvidas e aprimoradas com fins a obtenção de dados dos consumidores. Mendes destaca algumas técnicas de processamento, bem como menciona em relação aos benefícios e riscos ao consumidor:

Diversas são as técnicas que possibilitam a extração de valiosas informações a partir dos dados coletados, como a *Datawarehousing*, *Data Mining*, *On-Line Analytical Processing (OLAP)*, Construção de Perfil (*Profiling*) e Sistema de avaliação (*Scoring- ou Rating-System*). Essas técnicas trazem benefícios e desafios ao consumidor. De um lado, a personalização de produtos e serviços e a possibilidade de diminuição de publicidade importuna; de outro, riscos à privacidade, à discriminação do consumidor e à sua exclusão do mercado de consumo (MENDES, 2008, 101).

Por processamento, compreende-se de forma singela, o ato de organizar, ou seja, atividades ordenadas e contextualizadas que visam obter um resultado. No contexto do processamento de dados, este será a matéria-prima obtida por uma ou mais fontes, bem como o resultado é a informação, o dado processado.

Em evidência, o processamento de dados pessoais é realizado em diversos setores do mercado, que atuam em vários contextos, como empresas de telefonia, instituições financeiras, lojas, supermercados, farmácias, empresas de marketing direto e de telemarketing, serviços e proteção ao crédito, companhias de seguro, entre outros.

De fato, no mercado atual, as empresas realizam a coleta dos dados dos consumidores em razão dos serviços oferecidos, no entanto, Mendes explica sobre empresas em que a atuação no mercado trata-se unicamente da coleta e do armazenamento de dados pessoais, com o fim de comercialização destes dados:

Assim, ao lado das empresas que coletam dados dos seus clientes em razão da necessidade dos serviços oferecidos, surgem também empresas cuja única finalidade é a coleta e o armazenamento da maior quantidade possível de dados pessoais para a sua comercialização e cessão. ChoicePoint, Acxiom e LexisNexis são três das maiores empresas, nos EUA, cuja única finalidade é a comercialização de dados. Existem muitas outras empresas que compõem esta indústria. A base de dados da indústria fornece dados às empresas de marketing, ao governo, ao setor privado, aos credores para verificações de crédito, e aos empregadores para controle sobre os antecedentes. (MENDES, 2008, p. 110).

A autora também observa em relação a circulação dos dados pessoais na sociedade, segundo a qual, se estes dados forem repassados equivocadamente, podem resultar em violações aos direitos do consumidor, conforme esclarecimento a seguir:

O tema da transferência, cessão, comercialização ou compartilhamento de dados pessoais é complexo e polêmico à luz dos princípios da proteção de dados e do regime de proteção e defesa do consumidor. Isso ocorre porque os riscos advindos da coleta e do processamento de dados indevidos podem se multiplicar infinitamente, caso essas informações sejam repassadas a terceiros. Afinal, se essas informações circulam na sociedade, de forma equivocada, sem se constituir em uma representação fidedigna do consumidor, a sua liberdade e a igualdade de acesso aos bens de consumo estarão sendo gravemente violadas. (MENDES, 2008, p. 110).

Em suma, vários são os problemas que podem ser observados quanto ao tratamento dos dados dos consumidores, são exemplos, o desvio da finalidade na etapa de coleta dos dados, quando a partir da coleta para um determinado fim, aproveita-se estes dados a outras atividades, sem o conhecimento ou autorização do consumidor, ou ainda, quando resulta em discriminação, em que determinados perfis de consumidores são excluídos do mercado de consumo, ao constar equivocadamente, por exemplo, em cadastros negativos de proteção ao crédito.

Desse modo, como inovação legislativa, a Lei Geral de Proteção de Dados Pessoais (LGPD) passará a regulamentar e dificultar essas questões no mercado, visto que, cada vez mais utiliza-se técnicas e estratégias aprimoradas para o tratamento de dados, desde a coleta ao compartilhamento, assim, a lei busca resguardar a privacidade e os dados dos consumidores, delimitando até onde as empresas poderão utilizar estes dados e punindo vendas e vazamentos ilegais de informações pessoais.

5.2 TRATAMENTO DE DADOS PESSOAIS À LUZ DA NOVA LEI

A Lei nº 13.709, de 14 de agosto de 2018, conhecida como Lei Geral de Proteção de Dados Pessoais (LGPD), altera o Marco Civil da Internet, e está prevista para entrar em vigor em agosto de 2020, com o objetivo de aumentar a proteção dos dados pessoais. A legislação chega em um momento propício, o qual foi marcado por grandes vazamentos de informações e escândalos que envolvem justamente o uso indevido de informações pessoais.

Como mencionado anteriormente, a LGPD está prevista para começar a vigorar em agosto de 2020, ou seja, dois anos depois de sua aprovação. Inicialmente o prazo previsto era de dezoito meses, estendido para vinte e quatro meses, pela Medida Provisória nº 869, de 27 de dezembro de 2018. Esse prazo foi estipulado para que as empresas tenham tempo suficiente para se estruturarem e conseguirem colocar em prática as novas exigências de proteção e transparência no tratamento das informações pessoais.

Em decorrência, significativas mudanças estão previstas na forma de tratar os dados pessoais, especialmente nas relações comerciais, pois qualquer empresa que incluir em sua base informações de seus clientes, por mais básicas que sejam, como nome, sobrenome, endereço residencial ou comercial, entre outros, deve seguir os procedimentos previstos na nova lei.

A partir da Lei Geral de Proteção de Dados Pessoais (LGPD), o tratamento de dados pessoais pode ser entendido como qualquer procedimento que envolva a utilização de dados pessoais, conforme define o artigo 5º, inciso X:

Toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração (BRASIL, 2018).

A LGPD dispõe sobre o tratamento de dados de pessoas naturais, tanto por meio físico, quanto por meio digital, reconhecendo a finalidade da tutela desses dados para a proteção da privacidade e de direitos subjetivos inerentes ao indivíduo (art. 2º).

Para se enquadrar nas exigências da nova legislação, tanto o setor público quanto empresas do setor privado, que envolvam atividades relacionadas ao tratamento de dados pessoais, deverão implementar modificações na política interna, bem como direcionadas a estrutura técnica.

No âmbito empresarial, por exemplo, além das estratégias e ferramentas desenvolvidas em áreas como as de Tecnologia da Informação (TI), *compliance/governança* ou jurídica, medidas específicas, incluindo outros setores, tais como os de marketing ou comercial, devem contribuir para a harmonização à lei, bem como para mitigar possíveis riscos de danos e penalidades.

Nesse sentido, Alessandra Borelli ressalta a importância de um programa multidisciplinar nas empresas:

A jornada à LGPD não se restringe a um projeto de TI. Para traçar o planejamento, é preciso saber quais dados pessoais e, eventualmente, sensíveis a empresa possui, onde estão armazenados, como são tratados, quais riscos representam e o que as áreas de negócios pretendem fazer com eles. O objetivo do programa concentra na ideia de que todas as áreas envolvidas trabalhem em paralelo e com o mesmo foco. Além de acelerar o processo e garantir o cumprimento do prazo, essa colaboração faz com que o tripé da conformidade – jurídico, técnico e organizacional – seja abordado de forma integrada, para que se definam prioridades e investimentos com assertividade. O contínuo acompanhamento também permite antecipar os ajustes – uma vez que especialistas de diversas frentes participam de todo o ciclo – evitando retrabalho com medidas técnicas e operacionais necessárias para seu cumprimento. A empresa que encara o processo de implementação como oportunidade para garantir a segurança de seus dados, considerando inclusive um sério trabalho de conscientização, mitiga riscos e ganha diferencial competitivo (BORELLI, 2018).

Entre os primeiros passos destinados ao processo de adequação à LGPD, figura a necessidade de uma avaliação realizada por uma equipe de TI, contendo as análises de risco e de impacto das novas exigências, o que permite a verificação dos principais pontos e setores da empresa que deverão sofrer alterações.

Entre tais modificações, inclui-se, obrigatoriamente, a presença no quadro de funcionários do controlador, operador e encarregado, figuras centrais no processo de tratamento de dados, regulamentadas pelo novo texto normativo. Em linhas gerais, o controlador pode ser pessoa natural ou jurídica, de direito público ou privado, responsável pelas decisões relativas ao tratamento dos dados e suas orientações são colocadas em prática pelo operador, o qual também pode ser pessoa natural ou jurídica, de direito público ou privado, tais profissionais são os chamados agentes de tratamento. Por fim, o encarregado (*Data Protection Officer – DPO*), tem a missão de intermediar as relações entre o controlador, o titular dos dados e a Autoridade Nacional de Proteção de Dados (ANPD).

Consoante o artigo 37 da LGPD, o controlador e o operador devem manter o registro das operações de tratamento de dados pessoais que realizem, podendo a autoridade nacional determinar que seja elaborado relatório de impacto à proteção de dados referente às tais operações. Cabe ao controlador, entre outras atividades, confirmar a existência ou providenciar o acesso a dados pessoais, mediante requisição do titular, bem como provar que o consentimento foi obtido em conformidade com a lei.

A responsabilidade de tais profissionais está regulamentada no artigo 42, da LGPD, conforme a seguir:

Art. 42. O controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo.

§ 1º A fim de assegurar a efetiva indenização ao titular dos dados:

I - o operador responde solidariamente pelos danos causados pelo tratamento quando descumprir as obrigações da legislação de proteção de dados ou quando não tiver seguido as instruções lícitas do controlador, hipótese em que o operador equipara-se ao controlador, salvo nos casos de exclusão previstos no art. 43 desta Lei;

II - os controladores que estiverem diretamente envolvidos no tratamento do qual decorreram danos ao titular dos dados respondem solidariamente, salvo nos casos de exclusão previstos no art. 43 desta Lei (BRASIL, 2018).

Quanto ao encarregado, este será indicado pelo controlador, e terá sua identidade e informações divulgadas publicamente de forma clara e objetiva, preferencialmente no sítio eletrônico da empresa. O artigo 42, § 2º, elenca algumas de suas atividades:

§ 2º As atividades do encarregado consistem em: I - aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências; II - receber comunicações da autoridade nacional e adotar providências; III - orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais; e IV - executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares. (BRASIL, 2018).

A ANPD poderá regulamentar a necessidade de indicação de um encarregado, conforme a natureza e o porte da empresa ou o volume de operações de tratamento de dados.

Após essa estruturação relativa aos funcionários, ressalta-se a importância de investimentos em programas de treinamento sobre a nova legislação e o tratamento de dados, possibilitando as empresas fortalecer a nova política interna e enfrentar esse novo cenário do mercado.

A lei destina um tratamento diferenciado aos dados pessoais, especialmente os considerados sensíveis, coíbe o uso indiscriminado das informações pessoais, e garante ao cidadão o direito de estar ciente sobre como será feito tal tratamento e para qual finalidade específica estas informações serão usadas, destacado o consentimento expresso do titular antes da utilização, assim como para a transferência de informações para outras empresas. Nesse novo contexto legislativo,

assegurado o acesso as respectivas informações do titular, as organizações deverão garantir a autonomia do usuário na realização de operações, como consultas, correções em cadastro ou até mesmo a revogação de consentimento, disponibilizando, por exemplo, canais gratuitos de atendimento.

Além das diversas medidas já citadas, muitas outras podem auxiliar as organizações na adequação à LGPD, no entanto, destaca-se, ainda, a adoção de medidas de segurança com a finalidade de garantir a proteção dos dados pessoais contra acessos não autorizados e situações acidentais ou até mesmo ilícitas. Nesse sentido, é recomendado a atuação em torno da gestão de crises envolvendo a segurança e a privacidade, por meio de um grupo ou comitê responsável pela elaboração de políticas internas, metas e planos de gerenciamento de proteção de dados, assim como planos de emergência.

De fato, as empresas enfrentarão desafios para se adaptar à nova legislação, no entanto, ressalta-se a importância do tema para a segurança jurídica no mercado de consumo, como corrobora o entendimento de Márcio Cots, especialista em *Cyberlaw* (Direito dos Negócios Digitais):

(...) A adaptação à legislação pode ser ou não custosa, mas com certeza será trabalhosa para a grande maioria das empresas, que terão que atuar com diligência nesta mudança de cultura. Há duas formas de ver a legislação que surge sobre fatos jurídicos que antes não eram regulados: a de que a legislação é um empecilho e a de que a legislação é uma segurança para as empresas. Ao olhar o copo meio cheio é possível vislumbrar a possibilidade de novos negócios criados em bases mais sólidas, nos quais não se vive em incertezas e não há ameaças regulatórias num horizonte próximo. (COTS, 2018, p. 24).

Por todo o exposto, a LGPD representa uma garantia da segurança das informações pessoais, ao passo que contribui para o aprimoramento do mercado de consumo.

5.3 SANÇÕES

Além da responsabilidade de indenizar o titular dos dados, a Lei Geral de Proteção de Dados (LGPD) prevê sanções de caráter administrativo na hipótese de seu descumprimento, este tema está regulamentado nos artigos 52 ao 54, da referida norma.

As sanções administrativas aplicáveis pela Autoridade Nacional de Proteção de Dados (ANPD), em razão das infrações a LGPD, vão desde advertência até a imposição de sanções de natureza pecuniária, que podem chegar a 2% do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, limitada a R\$ 50 milhões por infração, com base na gravidade e extensão da violação.

Em razão das infrações às normas da LGPD, os agentes de tratamento de dados estão sujeitos às seguintes penalidades, nos termos do artigo 52:

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 (BRASIL, 2018).

As sanções serão precedidas de um procedimento administrativo que garanta a ampla defesa do infrator, as quais serão aplicadas considerando as particularidades de cada caso e os seguintes parâmetros e critérios, nos termos do artigo 52, § 1º:

- 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;
- XI - a proporcionalidade entre a gravidade da falta e a intensidade da sanção (BRASIL, 2018).

No cálculo do valor da multa, a ANPD poderá considerar o faturamento total da empresa ou do 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, bem como na sanção de multa diária, a aplicação deverá ser fundamentada observando a gravidade da falta e a extensão do dano ou prejuízo causado.

Em síntese, a Lei Geral de Proteção de Dados estabeleceu severas punições para aqueles que não atendam às disposições exigidas, o que requer a atenção das empresas, bem como de toda a sociedade quanto às novas normas.

6 CONSIDERAÇÕES FINAIS

Este trabalho procurou lançar luz sobre a proteção de dados pessoais, em especial do consumidor, no ordenamento jurídico pátrio. O tema da proteção de dados pessoais ganha enfoque nas relações comerciais, posto que, com o desenvolvimento das tecnologias de informação e comunicação tornou-se cada vez mais frequente a utilização de dados pessoais no mercado, para diversos fins, o que viabilizou a violação da privacidade e dos direitos subjetivos inerentes ao indivíduo, necessitando, portanto, de uma efetiva proteção.

Diante da falta de uma regulamentação específica, o tema era tratado apenas em regulamentações setoriais, deixando o país em posição de atraso legislativo se comparado até mesmo a outros países latinos. Hodiernamente, a proteção dos dados pessoais tem sido debatida no cenário jurídico nacional, principalmente, depois da aprovação da Lei nº 13.709, de 14 de agosto de 2018, conhecida como Lei Geral de Proteção de Dados Pessoais (LGPD).

A Lei nº 13.709/2018, denota a importância que a sociedade confere ao tema, com o prazo de adaptação de dezoito para vinte e quatro meses, estendido pela MP nº 869, de 27 de dezembro de 2018, a norma entrará em vigor em agosto de 2020, e, prevê, mudanças significativas para o mercado de consumo, com benefícios para o cidadão, bem como para toda a sociedade, pois o estabelecimento do marco legal de proteção de dados pessoais gera segurança jurídica, alinhando o ordenamento jurídico brasileiro a uma tendência internacional.

Sustenta-se que a proteção aos dados pessoais deve estar embasada nos princípios constitucionais da dignidade da pessoa humana, do respeito à vida privada e à liberdade do indivíduo, posto que, são informações que dizem respeito à personalidade do indivíduo, portanto, a supremacia da dignidade da pessoa humana obsta o alcance de qualquer regramento jurídico e justifica a existência e a proteção dos direitos da personalidade.

Não é por outra razão, portanto, que neste trabalho buscou-se analisar a proteção de dados do consumidor sob a ótica da legislação brasileira, e por todo o exposto, sugere-se que, para a efetiva proteção de dados do consumidor, é fundamental uma aplicação conjunta entre o Código de Defesa do Consumidor (CDC), além das demais regulamentações presentes em nosso ordenamento pátrio, e a nova Lei Geral de Proteção de Dados Pessoais, à luz de princípios basilares, tais

como a dignidade da pessoa humana, assegurado pela Constituição da República Federativa do Brasil de 1988, bem como o princípio da vulnerabilidade do consumidor, garantido pelo CDC.

A Lei Geral de Proteção de Dados (LGPD) deve atingir praticamente todos os setores da sociedade, em especial as organizações que envolvam atividades relacionadas ao tratamento de dados pessoais, importante premissa da nova legislação. Entre as principais inovações introduzidas pela nova legislação, está a criação da Autoridade Nacional de Proteção de Dados (ANPD), regulamentada pela Medida Provisória nº 869, de 27 de dezembro de 2018, a qual será a responsável por elaborar diretrizes, fiscalizar e aplicar as sanções estabelecidas pela lei.

Como já mencionado, a LGPD está prevista para vigorar em agosto de 2020, em consequência, as organizações tem se preocupado neste momento em se adequar às suas exigências. Para atender aos requisitos definidos no novo texto normativo, significativas mudanças serão necessárias, além de revisão e melhoria dos principais procedimentos e processos internos, bem como na estrutura técnica, investimentos em novas tecnologias e mecanismos de controle são fundamentais a fim de evitar possíveis danos e penalidades.

Em suma, a nova legislação terá um forte impacto na sociedade, uma vez que, como visto, atualmente praticamente toda e qualquer atividade se vale do uso de dados pessoais, nessa esteira, o advento da LGPD abre um leque de discussões sobre a proteção de dados do consumidor, a adaptação das empresas, do poder público e da sociedade em geral até o início de sua vigência, fundamentais para sua efetiva aplicação.

REFERÊNCIAS

ARAÚJO, Luiz Alberto David. Direitos da personalidade na Constituição Federal de 1988. **Revista da Academia Brasileira de Direito Constitucional**, n.3, Curitiba: ABDCnst, p. 259-260, 1996.

_____. Luiz Alberto David; NUNES JÚNIOR, Vidal Serrano. **Curso de direito constitucional**. 9.ed. São Paulo: Saraiva, 2005.

BANCO CENTRAL DO BRASIL. **Lei do Cadastro positivo é sancionada**. Disponível em: <https://www.bcb.gov.br/detalhenoticia/336/noticia>. Acesso em: 06 de maio de 2019.

BANISAR, David. **National Comprehensive Data Protection: Privacy Laws and Bills 2018 (September 4, 2018)**. Disponível em: <https://ssrn.com/abstract=1951416>. Acesso em: 06 de maio de 2019.

BITTAR, Eduardo C. B. **Contribuições para a crítica da consciência consumista e acerca da construção dos direitos do consumidor**. In: CHINELATO, Silmara Juny. Estudos de direito do autor, direito da personalidade, direito do consumidor e danos morais: homenagem ao professor Carlos Alberto Bittar. Rio de Janeiro: Forense Universitária, 2002. p.149-150.

BORELLI, Alessandra. **CYLK e Opice Blum Academy criam programa multidisciplinar sobre LGPD**. Disponível em: <https://cryptoid.com.br/protecao-de-dados/cylk-e-opice-blum-academy-criam-programa-multidisciplinar-sobre-lgpd/>. Acesso em: 07 de maio de 2019.

BRASIL. Constituição (1988). **Constituição**: República Federativa do Brasil. Brasília, DF: Senado Federal, 2016.

_____. Lei nº 7.232, de 29 de outubro 1984. Dispõe sobre a Política Nacional de Informática. **Diário Oficial da União**, Brasília, DF, 30 de outubro de 1984. Disponível em: http://www.planalto.gov.br/ccivil_03/LEIS/L7232.htm. Acesso em: 10 de junho de 2019.

_____. Lei nº 8.078, de 11 de setembro de 1990. Dispõe sobre a proteção do consumidor. **Diário Oficial da União**, Brasília, DF, 12 de setembro de 1990. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8078.htm Acesso em: 10 de junho de 2019.

_____. Lei nº 10.406, de 10 de janeiro de 2002. Institui o Código Civil. **Diário Oficial da União**, Brasília, DF, 11 de janeiro de 2002. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/2002/l10406.htm. Acesso em: 10 de junho de 2019.

_____. Lei nº 12.414, de 09 de junho de 2011. Disciplina a formação e consulta a bancos de dados com informações de adimplemento, de pessoas naturais ou de pessoas jurídicas, para formação de histórico de crédito. **Diário Oficial da União**, Brasília, DF, 10 de junho de 2011. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12414.htm. Acesso em: 10 de junho de 2019.

_____. Lei nº 12.527, de 18 de novembro de 2011. Regula o acesso a informações, e dá outras providências. **Diário Oficial da União**, Brasília, DF, 18 de novembro de 2011. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm. Acesso em: 10 de junho de 2019.

_____. Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. **Diário Oficial da União**, Brasília, DF, 24 de abril de 2014. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 10 de junho de 2019.

_____. Lei nº 13.709, de 14 de agosto de 2018. Dispõe sobre a proteção de dados pessoais. **Diário Oficial da União**, Brasília, DF, n. 157, 15 de agosto de 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm#art65. Acesso em: 10 de junho de 2019.

_____. Senado Federal. Proposta de Emenda à Constituição PEC N. 17/2019. Acrescenta o inciso XII-A, ao art. 5º, e o inciso XXX, ao art. 22, da Constituição Federal para incluir a proteção de dados pessoais entre os direitos fundamentais do cidadão e fixar a competência privativa da União para legislar sobre a matéria. Disponível em: <https://www25.senado.leg.br/web/atividade/materias/-/materia/135594>. Acesso em: 10 de junho de 2019.

CALIFORNIA. Assembly Bill N. 375, June 28, 2018. Privacy: personal information: businesses. Disponível em: https://leginfo.legislature.ca.gov/faces/billtextClient.xhtml?bill_id=201720180AB375. Acesso em: 10 de junho de 2019.

CASSAPO, Filipe Miguel. **O que entendemos exatamente por conhecimento tácito e conhecimento explícito**. Portal SBGC. Disponível em: <https://docplayer.com.br/41279-O-que-entendemos-exatamente-por-conhecimento-tacito-e-conhecimento-explicito.html>. Acesso em: 29 de abril de 2019.

CASTELLS, Manuel. **A sociedade em rede**. A era da informação: economia, sociedade e cultura; v.1. São Paulo: Paz e Terra, 1996.

COTS, Márcio. Impactos da lei geral de proteção de dados. **Revista Conceito Jurídico**, ano II, n. 19, Brasília: Editora Zakarewicz, p. 22-24, jul. 2018.

DONEDA, Danilo. **A proteção de dados pessoais nas relações de consumo**: para além da informação creditícia. Brasília: SDE/DPDC, 2010.

_____. A proteção dos dados pessoais como um direito fundamental. **Revista Espaço Jurídico**. vol. 12. n. 2. Joaçaba: Unoesc, 2011, pp. 91-108. Disponível em: <https://dialnet.unirioja.es/descarga/articulo/4555153.pdf>. Acesso em: 04 de maio de 2019.

_____. **Da privacidade à proteção de dados pessoais**. Rio de Janeiro: Renovar, 2006.

DAVENPORT, Thomas H.; PRUSAK, Laurence. **Conhecimento empresarial**: como as organizações gerenciam o seu capital intelectual. 5. ed. Rio de Janeiro: Campus, 1998.

ESPANHA. Constituição (1978). **Constitución española**. Senado de España, 2018. Disponível em: <http://www.senado.es/web/conocersenado/normas/constitucion/detalheconstitucioncompleta/index.html#t1c2s1>. Acesso em: 23 de maio de 2019.

LIMBERGER, Têmis. **O Direito à Intimidade na Era da Informática**. Porto Alegre: Livraria do Advogado, 2007.

MARTÍNEZ MARTÍNEZ, Ricard. El derecho fundamental a la protección de datos: Perspectivas. **Revista Internet, Derecho y Política**, n. 5, España: Universitat Oberta de Catalunya, p. 47, 2007.

MENDES, Laura Schertel. **Transparência e Privacidade**: Violação e Proteção da Informação Pessoal na Sociedade de Consumo. 2008. Dissertação (Mestrado em Direito) – Faculdade Direito, Universidade de Brasília, Brasília, 2008.

MENDONÇA, Fernanda Graebin. Proteção de Dados Pessoais na Internet: Análises Comparativas da Situação do Direito à Autodeterminação Informativa no Brasil e Em Países Latino-Americanos. **Revista Jurídica da Faculdade de Direito de Santa Maria**, v. 11, n. 1, Santa Maria: FADISMA, p. 283-311, 2016.

MORAES, Alexandre de. **Direito constitucional**. 34. ed. São Paulo: Atlas, 2018.

MOTA PINTO, Paulo Cardoso Correia da. A proteção da vida privada. **Boletim da Faculdade de Direito**, v. LXXVI, Coimbra: Universidade de Coimbra, 2000.

NUNES, Antônio Luis Rizzato. **Curso de Direito do Consumidor**, 6ª ed., São Paulo: Editora Saraiva, 2011.

PORTUGAL. Constituição (1976). **Constituição da República Portuguesa**, de 02 de abril de 1976. Assembleia da República: 2005. Disponível em: <https://www.parlamento.pt/Legislacao/paginas/constituicaorepublicaportuguesa.aspx>. Acesso em: 23 de maio de 2019.

QUIROGA, Eduardo Molina et. al. **Daños. Globalizacion – Estado – Economía**. Buenos Aires: Rubinzal-Culzoni, 2000.

REINALDO FILHO, Demócrito. A Diretiva Europeia sobre proteção de dados pessoais. Uma análise de seus aspectos gerais. **Revista Jus Navigandi**, ano 18, n. 3507, Teresina: Jus Navigandi, 6 fev. 2013. Disponível em: <https://jus.com.br/artigos/23669>. Acesso em: 20 jun. 2019.

REINALDO FILHO, Demócrito. Lei de proteção de dados pessoais aproxima o Brasil dos países civilizados. **Revista Conceito Jurídico**, ano II, n. 19, Brasília: Editora Zakarewicz, p. 39-41, jul. 2018.

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

SALINAS, Maria de Lourdes Zamudio. El marco normativo latino americano y la ley de protección de datos personales del Perú. **Revista Internacional de Protección de Datos Personales**, n. 1, Bogotá: Universidad de los Andes – Facultad de Derecho, p. 19, 2012.

SENADO FEDERAL. Projeto de Lei da Câmara nº 53, de 2018. Disponível em: <https://www25.senado.leg.br/web/atividade/materias/-/materia/133486>. Acesso em: 10 de junho de 2019.

VAINZOF, Rony. Finalmente a Lei Geral de Proteção de Dados (LGPD) – Resumo dos pontos relevantes. **Revista Conceito Jurídico**, ano II, n. 19, Brasília: Editora Zakarewicz, p. 25-36, jul. 2018.

WARREN, Samuel D.; BRANDEIS, Louis D. The Right to Privacy. **Harvard Law Review**, vol. 4, n. 5. (Dec. 15, 1890), p. 193-220. Disponível em: https://www.jstor.org/stable/1321160?seq=1#metadata_info_tab_contents. Acesso em: 23 de maio de 2019.