



PONTIFÍCIA UNIVERSIDADE CATÓLICA DE GOIÁS
ESCOLA DE DIREITO, COMUNICAÇÃO E NEGÓCIOS
NÚCLEO DE PRÁTICA JURÍDICA
COORDENAÇÃO ADJUNTA DE TRABALHO DE CURSO
TRABALHO DE CONCLUSÃO DE CURSO

**LEI GERAL DE PROTEÇÃO DE DADOS: O IMPORTANTE PAPEL DA
AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS E A BUSCA
PELA DEFESA DO CONSUMIDOR E TITULAR DE DADOS**

ORIENTANDO (A) – ANA LUÍSA GARCÊZ RODRIGUES
ORIENTADOR (A) - Prof. Me. JOSÉ EDUARDO BARBIERI

GOIÂNIA
2021

ANA LUÍSA GARCÊZ RODRIGUES

**LEI GERAL DE PROTEÇÃO DE DADOS: O IMPORTANTE PAPEL DA
AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS E A BUSCA
PELA DEFESA DO CONSUMIDOR E TITULAR DE DADOS**

Projeto de Monografia Jurídica apresentado à disciplina Trabalho de Curso II, da Escola de Direito, Comunicação e Negócios, Curso de Direito, da Pontifícia Universidade Católica de Goiás (PUC GOIÁS).
Prof. (a) Orientador (a) – Me. José Eduardo Barbieri

GOIÂNIA
2021

ANA LUÍSA GARCÊZ RODRIGUES

**LEI GERAL DE PROTEÇÃO DE DADOS: O IMPORTANTE PAPEL DA
AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS E A BUSCA
PELA DEFESA DO CONSUMIDOR E TITULAR DE DADOS**

Data da Defesa: 01 de dezembro de 2021

BANCA EXAMINADORA

Orientador: Prof. Me. José Eduardo Barbieri

Nota

Examinador Convidado: Prof. Dr. Nivaldo dos Santos

Nota

Dedico esse trabalho a minha querida família que tanto admiro, dedico todo o resultado do esforço realizado ao longo dos últimos anos. Dedico também, ao meu avô que faleceu durante a elaboração deste trabalho, mas que está orgulhoso por tê-lo concluído.

Agradeço a Deus por ter me dado força e muita saúde para superar todas as dificuldades. Agradeço ao meu orientador por todo apoio e motivação.

Agradeço aos meus pais, pelo amor incondicional e todo incentivo, bem como a todos que direta ou indiretamente fizeram parte de minha formação.

RESUMO

A referida monografia foi realizada com o intuito de abordar a temática acerca da importância da proteção de dados pessoais, como ocorre a proteção de dados do consumidor e a atuação da Autoridade Nacional de Proteção de Dados (ANPD). Dessa forma, entendeu-se por necessário retratar as condições históricas frente ao atual cenário tecnológico, bem como apresentar conceitos princípios para melhor compreender a importância da proteção de dados pessoais como um direito fundamental. Ainda, compreender o titular de dados com um consumidor e entender a importância e vulnerabilidade desse, e como ocorre a proteção desse. Portanto, destaca a criação da ANPD, sua atuação, função e competência e seu acordo com a Secretaria Nacional do Consumidor (Senacon).

Palavras-chave: Lei Geral de Proteção de Dados; Proteção do Consumidor; Autoridade Nacional de Proteção de Dados

ABSTRACT

This monograph was carried out in order to address the issue of the importance of protecting personal data, such as consumer data protection and the role of the Data Protection Authority (DPA). Thus, it was considered necessary to portray the historical conditions in the current technological scenario, as well as to present principle concepts to better understand the importance of personal data protection as a fundamental right. Also, understand the data subject with a consumer and understand its importance and vulnerability, and how its protection occurs. Therefore, it highlights the creation of DPA, its performance, function and competence and its agreement with the National Consumer Secretariat (Senacon).

Keywords: General Data Protection Law; Consumer Protection; National Data Protection Authority

SUMÁRIO

INTRODUÇÃO.....	8
1 PRIVACIDADE E A PROTEÇÃO DE DADOS PESSOAIS.....	12
1.1 A EVOLUÇÃO DO CONCEITO DE PRIVACIDADE.....	12
1.2 PROTEÇÃO DE DADOS NO BRASIL.....	14
1.3 OS PRINCÍPIOS DA LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS.....	17
1.4 PROTEÇÃO DE DADOS PESSOAIS: UM DIREITO FUNDAMENTAL.....	18
2 A AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD).....	21
2.1 A NECESSIDADE DE UMA AUTORIDADE PARA PROTEÇÃO DE DADOS.....	21
2.2 CRIAÇÃO DA AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS.....	23
2.3 ESTRUTURA, NATUREZA E FUNCIONAMENTO DA ANPD.....	25
3 AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS E A DEFESA DO CONSUMIDOR	28
3.1 O CONSUMIDOR QUE A PROTEÇÃO DE DADOS TUTELA.....	28
3.1.1 VULNERABILIDADE DO CONSUMIDOR E A HIPERVULNERABILIDADE NO AMBIENTE DIGITAL.....	29
3.2 O PROTAGONISMO DA BASE LEGAL DO CONSENTIMENTO.....	31
3.3 ACORDO DA AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS E A SECRETARIA NACIONAL DO CONSUMIDOR (SENACON).....	34
CONCLUSÃO	37
REFERÊNCIAS	40

INTRODUÇÃO

A preocupação com a privacidade, não é recente, pode ser encontrada em variadas épocas do desenvolvimento da sociedade. Acontece que, a privacidade começou a ser abordada de forma concreta no final do século XIX, para enfim, assumir forma na atualidade.

O Estado, com a intenção de desenvolver uma administração pública eficiente, considerando a necessidade de conhecer sua população, usou de informações exclusivas coletadas por meio da realização de censos e pesquisas, que possibilitaram o acesso aos dados pessoais. (DONEDA, 2019)

Entretanto, para a atividade privada, nunca foi atraente a coleta de informações, devido ao alto custo para se conseguir os dados e para tratá-los. No entanto, o desenvolvimento da tecnologia possibilitou que o tratamento de dados para as empresas, o custo tornou-se mais barato e facilitou a coleta dos dados pessoais, conclui-se que à medida que a tecnologia se desenvolve mais importante se torna os dados. (DONEDA, 2019)

No mesmo raciocínio, depreende-se que o direito a proteção dos dados pessoais é algo básico, e tornou-se de caráter fundamental à vida humana. A hodierna necessidade do mercado, converge com essa concepção. O avanço da sociedade e por conseguinte o surgimento de novas tecnologias, mudou o foco das empresas, para uma visão chamada de “orientação para marketing” (KOTLER, 2012), com isso possibilitou o uso irrestrito de técnicas de *data mining* (mineração de dados), coleta e tratamento de dados para a melhor compreensão, sendo mais incisiva a respeito do comportamento do consumidor.

O uso dessas técnicas, garantiu e possibilitou uma maior coleta de dados possíveis de clientes para que sejam elaborados os *Costumer Relationship Management* (CRM), com maior variedade e quantidade de informações sólidas possíveis. (SILVA, 2002). Permitindo assim as instituições observarem e traçarem com maior precisão o comportamento de seus consumidores, assim, as empresas e instituições se tornaram capazes de gerenciar e observar com qualidade sua evolução no mercado e compreender as necessidades do público.

É possível afirmar que o uso indevido de dados pessoais existe, e por mais interessante que seja para o público, torna-se necessário questionar: “qual é o limite do uso dos dados pessoais?”. Nesse contexto, possui grandes escândalos de

vazamentos e compartilhamentos de dados como o caso Facebook (540 MILHÕES, 2019), *Cambridge Analytica* (CASO, 2019) e a brasileira *Dataprev* (INSTITUTO, 2019).

Esses acontecimentos citados, foram precursores para dar início a discussões sobre privacidade e proteção de dados. Para os órgãos internacionais, demonstrou-se se um assunto de grande relevância e importância para os indivíduos, atentando-se que a violação aos dados pessoais se configura na perda individual da autonomia, individualidade e liberdade. Para tanto, depreende-se que a privacidade, incluindo a dos dados pessoais, é reconhecida como direito fundamental pois trata-se dos indicativos da nossa personalidade, portanto merece a proteção do direito.

A Organização Nacional das Nações Unidas (ONU), em 1948, na sua Declaração Universal dos Direitos Humanos, estabeleceu o direito à vida privada no artigo XII. Ainda, essa proteção, se tratando da individualidade da pessoa humana, trouxe à tona o princípio básico da dignidade da pessoa humana, no qual norteia a Constituição da República Federativa do Brasil de 1988, pois considera-se o poder de escolha e omissão do particular.

O reconhecimento da privacidade como direito, incluindo a proteção de dados pessoais, foi importante, pois permitiu que se estabelecesse a confiança econômica entre empresas e os titulares de dados pessoais. Para tanto, as instituições precisam firmar e garantir o compromisso com os indivíduos, pois atualmente os dados são informações que geram poder e influência sobre os consumidores, e por isso, devem ser protegidos.

Nesse ínterim, após os escândalos envolvendo o mau tratamento de dados, a União Europeia promulgou o Regulamento Geral de Proteção de Dados Pessoais (GDPR), em abril de 2016. Surtindo um efeito dominó, demais países como o Brasil, com intuito de manter as relações econômicas, políticas e sociais, desenvolveu a Lei nº 13.709/2018, a Lei Geral de Proteção de Dados Pessoais (LGPD), aprovada em agosto de 2018.

A Lei Geral de Proteção de Dados Pessoais (LGPD), tem como intuito regulamentar a proteção de dados pessoais e garantir os direitos dos titulares dos dados. Além disso, percebendo-se que a lei não se propagaria de maneira de autônoma e entendendo a proteção de dados como uma mudança sociocultural, requisitando a criação de uma instituição, a Autoridade Nacional de Proteção de Dados (ANPD), que atuará perante a sociedade, empresas e o setor público, com a

finalidade de orientar e sancionar, bem como realizar as interpretações das lacunas presentes na lei, para um entendimento uniforme e eficaz atuação. (PECK, 2020)

Entende-se, é necessário estudar profundamente a LGPD, pois essa trará impactos no Brasil, para os diversos setores das *Startups*, pequenas e grandes empresas e o setor público.

Tornou-se necessário que a lei não apenas penalize, mas capacite e eduque. Consequentemente, Autoridade Nacional de Proteção de Dados (ANPD), deve estabelecer efeito orientador, para que haja mudança no comportamento em relação a proteção dos dados.

Ainda, a ANPD tem papel fundamental, foi criada com intuito de estabelecer segurança e estabilidade para a aplicação da LGPD. Sabe-se, nesse sentido, que a ANPD inspirará sua atuação, conforme as autoridades de proteção de dados de outros países, que costumam assumir um perfil orientativo/fiscalizatório ou punitivo/arrecadatório. Então, cabe questionar, qual será o papel, função e desafios enfrentados pela ANPD para com a proteção dos titulares de dados pessoais, segundo a LGPD?

Ademais, quem é o consumidor tutelado pela LGPD? Ressalta-se as inúmeras semelhanças entre o Código de Defesa do Consumidor (CDC) e a Lei Geral de Proteção de dados (LGPD), é necessário o entendimento consolidado que o consumidor, que também é titular de dados, é extremamente vulnerável e por isso precisa de proteção.

Realiza-se o apontamento, de grade ressalva, que o desenvolvimento uniformizado de interpretações de ambos os agentes regulatórios de risco, ou seja, a cooperação técnica entre a ANPD e a Senacon, para desenvolvimento eficiente legislações, fiscalizações e sancionamentos.

Dessa forma, o presente trabalho terá como elemento central a análise da regulamentação brasileira, que entrou em vigor em setembro de 2020. Além disso, será realizado um estudo do surgimento da preocupação com a privacidade e proteção de dados, o reconhecimento da proteção de dados como direito fundamental, o surgimento da LGPD no Brasil e os princípios que regem a legislação, que são fundamentais para a aplicação.

Logo, a importância da criação da ANPD para a eficácia da LGPD, ainda as funções, estrutura, competências da ANPD, os desafios de sua criação, ademais,

qual o titular tutelado pela LGPD, a hipervulnerabilidade do titular e os desafios do consentimento, e como a ANPD auxiliará na proteção desses titulares.

1 – A PRIVACIDADE E PROTEÇÃO DE DADOS

Para o desenvolvimento do presente trabalho, há a necessidade de realizar breve análise histórica, para que haja uma compreensão objetiva de como surgiu-se o direito à privacidade, ainda quais foram as implicações dos avanços tecnológicos perante a proteção de dados pessoais, fazendo com que o direito à proteção de dados seja reconhecido como um direito fundamental, o que possibilitou a elaboração da Lei de Geral de Proteção de Dado Pessoais – LGPD.

1.1 – A EVOLUÇÃO DO CONCEITO DE PRIVACIDADE

Em 1890, Warren e Brandeis (1890, p. 196), publicaram o artigo referência do direito à privacidade, *The right to privacy*, tornando-os precursores no assunto, no qual a partir da leitura do texto entende-se o desenvolvimento da privacidade, em que os juristas sugerem tutelar a privacidade como um direito protagonista e independente. Os autores descrevem como motivação para necessidade da privacidade da pessoa humana, pela invasão realizada pela imprensa na vida doméstica, expondo imagens e relatando escândalos íntimos, ainda salientam o quão essencial se tornou a privacidade e a solidão.

Assim surgiu a necessidade de proteger a privacidade, e cunhou o princípio bem conhecido como *right to be let alone* (direito a ser deixado só). Nesse sentido, que Danilo Doneda (2019, p.30) destaca que a privacidade se trata de um aspecto intrínseco a qualquer pessoa humana no desenvolvimento da personalidade, ou seja, trata-se de um direito fundamental.

Reconhecidos como modernos “fundadores” do direito à privacidade, Brandeis e Warren, inseriram o assunto em pela grande quantidade informações que passou a circular, sendo o fundamentando da construção da doutrina nos moldes da sociedade norte-americana no final do século XIX. (DONEDA, 2019, p. 31)

Dessa maneira, depreende-se que falar sobre privacidade não é algo recente, e desde o final do século XIX, quando a mesma começou ser discutida para assumir o conceito atual, trouxe uma série de alterações de valores e percepções, já que quando fala-se de privacidade, refere-se as informações como os dados pessoais, consequentemente é sobre novas tecnologias, um território impenetrável e desconhecido,

em que questiona-se como é possível enfrentar o paradigma para estabelecer-se uma vida privada e ainda cumprir com o papel de social.

Sendo assim, hodiernamente com o rápido desenvolvimento tecnológico e a consolidação de espaços virtuais, fortaleceu-se o fluxo informacional, possibilitando nas últimas décadas o debate sobre a privacidade e a proteção de dados.

Com o acelerado desenvolvimento tecnológico e a consolidação de espaços públicos virtuais, a gestão da informação sobre si próprio tornou-se expressão fundamental do indivíduo. Por conseguinte, revela-se impossível cogitar de proteção integral à liberdade, à privacidade e ao desenvolvimento da pessoa natural sem que se lhe garanta eficaz defesa e controle de seus próprios dados (...) (ABILIO, FRAZÃO, OLIVA, 2019, p, 677 e 678)

Ao tratar da privacidade, não há que se falar de forma isolada, pois essa refere-se a busca por diversas urgências no qual a humanidade tem lutado por tanto tempo, como liberdade, igualdade e personalidade de cada indivíduo. (DONEDA, 2019, p. 29)

Nesse sentido, percebe-se que o paradigma da privacidade se refere as informações, os dados, como parte na construção da personalidade dos indivíduos. Por isso a proteção de dados ganhou tanto destaque sob o olhar de Alan Westin, que estabeleceu que uma das ameaças da natureza tecnológica à privacidade é a vigilância dos dados pessoais. (WESTIN, p. 34 *apud* DONEDA, 2019, p.42)

O Tribunal Constitucional Alemão, em 1982, realizou uma decisão histórica ao julgar a “Lei do Recenseamento de População, Profissão, Moradia e Trabalho”, na qual estabeleceu que o moderno tratamento de dados pessoais resultaria em séria ameaça ao direito de personalidade do indivíduo. Nessa perspectiva, a privacidade organizou-se em torno de dados pessoais, ainda, possibilitando a tutela da personalidade do indivíduo, evidenciando os riscos causados pelo tratamento dos dados pessoais.

Fundamentando-se a disciplina de proteção de dados e demonstrando que evoluiu, houve certos impulsos relacionados dentro da administração pública no pós-guerra, especificamente na década de 1960, que começou a utilizar largamente informações pessoais, alegando ser para uma administração pública eficiente. (DONEDA, 2019)

Além de tudo, é essencial saber que legislações sobre dados pessoais existem há mais de cinquenta anos. Como as conhecidas como “leis de primeira geração Lei do Land alemão de Hesse (Alemanha, 1970), *Data Legen* ou *Datalag* (Suécia, 1973), também a *Privacy Act* (Estados Unidos da América, 1974). As leis

nacionais foram importantes instrumentos para consolidar o conceito de privacidade ao de proteção de dados pessoais as leis nacionais. (MENDES, 2017)

Entretanto, ao relacionar tais conceitos Rodotá (2008, p.24) aponta que a privacidade não se relaciona apenas a finalidade de “ser deixado só”, mas hoje destaque-se a possibilidade de indivíduos controlarem e exercerem poder baseado em informações disponíveis.

Sendo assim, as leis de quarta geração, as mais recentes legislações se encontram em mais de 120 países, foram desenvolvidas com consciência da existência de uma dificuldade em basear a tutela de dados pessoais na primazia individual. Essas novas leis, têm como fundamento estabelecer autoridade independentes para atuação da lei, estabelecer um padrão coletivo de proteção, e ainda fortalecer o papel do indivíduo perante as entidades que coletam dados.

Conclui-se, que o conceito de privacidade se modificou. No passado, como abordado por Warren e Brandeis, se referia apenas a propriedade privada, envolvia a inviolabilidade das casas e o sigilo de comunicações, mas sofreu alterações em uma perspectiva ampla. Defender a privacidade é lembrar dos seus mais diversos significados, mas discuti-la possibilitou limitar a coleta e acesso de dados ou informações dos indivíduos, sem a devida autorização.

1.2 – PROTEÇÃO DE DADOS NO BRASIL

No Brasil, por volta de 1990 surgiram-se os primeiros instrumentos jurídicos referentes à proteção do uso de dados, começando a romper as primeiras novas concepções sobre os dados pessoais.

Cabe apontar o surgimento do Código de Defesa do Consumidor, instituído com a promulgação da Lei nº 8.078/90, no qual estabeleceu a regulação do uso de banco de dados de consumidores, o mesmo prevê regras sobre o acesso a “informações existentes em cadastros, fichas, registros e dados pessoais e de consumo arquivados sobre ele”, entretanto, permite a correção em caso de obscuridade e, embora não tenha previsto tal consentimento para o recolhimento desses dados, foi reivindicado que o consumidor seja comunicado sobre a abertura do registro.

Logo, em 1996, foi promulgada a Lei de Interceptação Telefônica e Telemática (Lei nº 9.296/96), essa caracterizou o direito à privacidade ao estabelecer o uso do recurso proposto em lei para apurar as possibilidades e sempre sob o amparo de uma ordem judicial.

Já, um ano depois, em 1997, a Lei do *Habeas Data* (Lei nº 9.507/97), foi promulgada, regulando o direito constitucional e o rito de acesso e correção de informações pessoais, contudo, Barroso (1998, p. 212) afirma que tal feito foi meramente simbólico, pois os direitos tutelados eram passíveis de remédio já existente.

Outro ponto sobre a vida privada, foi a menção no Código Civil Brasileiro no artigo 21, sobre os direitos da personalidade, em que aborda a vida privada e concede instrumentos para controlar a violação desse direito, destaca-se o direcionamento gradual do conceito de privacidade como um direito subjetivo ao indivíduo.

No ano de 2011, foi publicada Lei de Acesso à Informação (Lei nº 12.527/11), que garantiu no artigo 4º, inciso IV, também no artigo 6º, inciso III, o acesso à informação pessoal, conforme:

Art. 4º Para os efeitos desta Lei, considera-se:

IV - Informação pessoal: aquela relacionada à pessoa natural identificada ou identificável;

Art. 6º Cabe aos órgãos e entidades do poder público, observadas as normas e procedimentos específicos aplicáveis, assegurar a:

III - proteção da informação sigilosa e da informação pessoal, observada a sua disponibilidade, autenticidade, integridade e eventual restrição de acesso.

Ainda, no primeiro semestre de 2013, sucedeu-se a regulamentação de alguns pontos da lei consumerista, determinando ao fornecedor meios de segurança eficazes para o pagamento e tratamento de dados do consumidor. No mesmo ano, foram divulgadas informações sobre a utilização de um software chamado “PRISM”, esse é utilizado para monitorar e vigiar, de uma forma global, todas as informações que eram transmitidas na rede de computadores.

O programa coletava informações em massa, vigiando não apenas os terroristas, mas qualquer transmissão feita pela web, por qualquer indivíduo, sendo também um modo de espionar países e empresas de alta potência. Podendo ser citada uma das inúmeras vítimas, a então Presidente do Brasil, Dilma Rousseff, que

teve sua conta monitorada. Evoca-se a afirmação de Rodotà, sobre o nó das tutelas individuais:

Às novas formas de coleta e tratamento de informações, possibilitadas sobretudo pelo recurso a computadores, adiciona-se a crescente necessidade de dados por parte das instituições públicas e privadas: como não é imaginável uma ação que vá de encontro a esta tendência, comum a todas as organizações sociais modernas, é necessário considerar de forma realista tal situação, analisando as transformações que causa na distribuição e uso do poder pelas estruturas públicas e privadas. (RODOTÀ, 2008, p. 24)

Após, o Brasil ser alvo da espionagem norte-americana, o governo brasileiro agilizou o trâmite do até então Projeto de Lei nº. 2.126/11, conhecido como Marco Civil da Internet (MCI), que foi promulgado em 2014. Nessa legislação, foi pela primeira vez mencionada a palavra “privacidade”, dando ênfase à necessidade da proteção de dados. Tal dispositivo, assegura vários outros princípios e regramentos que foram implementados à LGPD.

Assim, a recente incorporação do termo “proteção de dados pessoais”, no ordenamento jurídico brasileiro se deve a Lei nº 13.709/2018, conhecida como Lei Geral de Proteção de Dados Pessoais (“LGPD”), foi sancionada pelo ex-presidente Michel Temer em agosto de 2018, e entrou em vigor no dia 18 de setembro de 2020, com exceção das sanções administrativas advindas da ANPD – Autoridade Nacional de Proteção de Dados Pessoais que entraram em vigor, em agosto de 2021. Sem prejuízo, com a vigência dos demais artigos, os titulares de dados, bem como outros órgãos podem fiscalizar e exigir cumprimento da norma.

A LGPD, tem como intuito regulamentar o uso de dados pessoais, 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 bem como os direitos humanos. (PECK, 2020)

Assim, prevê hipóteses legais autorizativas, princípios e outras regras visando legitimar a atividade de tratamento, que será considerada ilegal em caso de descumprimento, sujeitando o infrator a pesadas sanções administrativas, além de indenizações individuais ou coletivas.

Não se trata de uma iniciativa isolada do legislativo nacional, uma vez que com sua aprovação o Brasil entrou no rol de mais de 140 países com legislações específicas e abrangentes sobre proteção de dados pessoais, sendo a norma brasileira claramente inspirada no Regulamento Europeu nº 2016/679, denominado *General Data Protection Regulation* (GDPR). (GREENLEAF, 2020)

Nesse sentido, a proteção de dados pessoais é um aspecto da proteção à própria privacidade. Ressalta-se, todavia, que suas previsões não intencionam impedir negócios, novos ou tradicionais, lastreados no tratamento de dados pessoais, mas sim colocar regras claras, permitindo ao titular maior controle sobre como suas informações são tratadas, gerando, por consequência maior segurança jurídica às empresas que deixam de ficar sujeitas a interpretações dúbias pela ausência de regras específicas em diplomas legais não especializados, como o Código de Defesa do Consumidor.

Considerando sua abrangência e importância, bem como por ser um processo que garante maior segurança jurídica às organizações, a LGPD permite as organizações sustentarem perante terceiros que está em processo de conformidade a legislação, garantindo maior segurança aos envolvidos e fortalecendo a confiança perante seus consumidores e colaboradores.

1.3 – OS PRINCÍPIOS DA LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS

Princípio é o começo, o início, é um fundamento ou essência que permite iniciar algo. A Lei Geral de Proteção de Dados (LGPD), traz um rol de princípios, no artigo 5º, que precisam ser aplicados e seguidos dentro de instituições públicas e privadas para que estejam de acordo com a regulação.

Inspirada na *General Data Protection Regulation* (GDPR), a lei brasileira de proteção de dados traz em seu rol, princípios como publicidade, finalidade, exatidão, livre acesso e segurança física e lógica. Depreende-se, que é uma legislação incontestavelmente principiológica, assim como afirmado pela advogada e estudiosa da LGPD, Patrícia Peck (2020, p.41) “A regulamentação de proteção de dados pessoais é uma legislação principiológica [...]. Sendo assim, tanto na origem europeia como na versão nacional traz um rol de princípios que precisam ser atendidos.”.

O rol de princípios citado acima, deve ser seguido para que haja controle dos dados, logo estará em conformidade com a LGPD, caso não esteja em conformidade, logo também, não atenderá aos princípios redigidos em lei. Vale ressaltar que um dos pontos essenciais para aplicação do tratamento de dados é o consentimento do titular.

A aplicação de princípios visa garantir os direitos fundamentais dos indivíduos, assim como citado no artigo 2º da Lei Geral de Proteção de Dados (LGPD), e ainda tem como objetivo fortalecer a proteção dos dados dos titulares.

Art. 2º A disciplina da proteção de dados pessoais tem como fundamentos:
I - o respeito à privacidade;
II - a autodeterminação informativa;
III - a liberdade de expressão, de informação, de comunicação e de opinião;
IV - a inviolabilidade da intimidade, da honra e da imagem;
V - o desenvolvimento econômico e tecnológico e a inovação;
VI - a livre iniciativa, a livre concorrência e a defesa do consumidor; e
VII - os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.

Os princípios da publicidade, exatidão, finalidade, segurança física e lógica e do livre acesso, estabelecidos na LGPD são comumente vistos em legislações de proteção de dados pessoais, e em ordenamentos jurídicos de vários graus. Esses estão disseminados, mas podem ser encontrados em variadas normativas, também são centro de pautas e questionamentos, no qual os ordenamentos jurídicos buscam para solucionar e garantindo a eficácia da proteção de dados pessoais. (DONEDA, 2019, p. 182)

É válido destacar, que um dos impactos da LGPD está relacionado em garantir os direitos dos titulares de dados, assim como afirma Peck, alguns dos direitos são novos para o ordenamento jurídico, entretanto as instituições devem buscar e se preparem para atender as novas necessidades. (PECK, 2020, p. 44)

1.4 – PROTEÇÃO DE DADOS PESSOAIS: UM DIREITO FUNDAMENTAL

A LGPD, não trata apenas da proteção de dados, mas sim da proteção de pessoas – os titulares. Consequentemente, a LGPD, tem como princípios norteadores, os direitos fundamentais da pessoa humana, tais como direitos de liberdade, de privacidade e o livre desenvolvimento da personalidade.

Vela ressaltar, que muito antes do direito à privacidade ser considerado um direito de caráter fundamental, ele foi distribuído em diversas partes do ordenamento jurídico brasileiro como no direito civil, direito do consumidor, penal, e entre outros, assim como apresentado no tópico anterior, as primeiras aparições da privacidade nas legislações brasileiras. Conclui-se que como forma de garantir o direito à privacidade,

uma grande parte da regulamentação foi desenvolvida em um período, chamado pelo doutrinador Danilo Doneda (2019, p. 261), como “pré-constitucional”, pois foram produzidas normas antes de ser um direito fundamental previsto e tutelado.

Entretanto, é perceptível a preocupação da legislação brasileira em garantir os direitos dos titulares, portanto o reconhecimento da proteção de dados como um direito autônomo e fundamental, ocorre de forma implícita, prometendo a proteção da personalidade à luz das garantias constitucionais de igualdade, liberdade e dignidade da pessoa humana, juntamente com a proteção da intimidade e da vida privada.

E é justamente, o alargamento do direito à privacidade como um direito fundamental, que se torna esclarecida a necessidade da oficializar. Como pode-se verificar na Carta de Direitos Fundamentais da União Europeia no art. 8º:

Artigo 8º. Proteção de dados pessoais 1. Todas as pessoas têm direito à proteção dos dados de carácter pessoal que lhes digam respeito. 2. Esses dados devem ser objeto de um tratamento leal, para fins específicos e com o consentimento da pessoa interessada ou com outro fundamento legítimo previsto por lei. Todas as pessoas têm o direito de aceder aos dados coligidos que lhes digam respeito e de obter a respectiva retificação. 3. O cumprimento destas regras fica sujeito a fiscalização por parte de uma autoridade independente.

O Governo Brasileiro, havia firmado a proteção de dados pessoais como direito fundamental a compactuar com a Declaração de Santa Cruz de La Sierra, documento final da XIII Cumbre Ibero-Americana de Chefes de Estado e de Governo, em 2003. No item 45 da referida Declaração lê-se que:

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

Também, a Constituição Federal considera direitos invioláveis a vida privada e a intimidade (art. 5º, X), ainda a interceptação de comunicações telefônicas, telegráficas ou de dados (artigo 5º, XII), bem como instituiu a ação de habeas data (art. 5º, LXXII).

Ademais, refletindo assim, especificamente no Código de Defesa do Consumidor (Lei nº 8.078/90), cujo artigo 43 estabelece uma série de direitos e garantias para o consumidor em relação às suas informações pessoais, ficou estabelecido como marco normativo dos princípios de proteção de dados pessoais do direito brasileiro. (CARVALHO, 2003, p. 77-119)

Dessa maneira, as disposições brasileiras possibilitam, o tratamento de problemas relacionados às informações pessoais em bancos de dados, no qual determina permissões ou proibições para o uso de informações específicas, sem apontar quais seriam os riscos potenciais objetivados pelo tratamento informatizado das informações pessoais. (DONEDA, 2011, p. 104)

Entretanto, ao tratar da privacidade, conforme previsão no artigo. 5º, XII, na qual trata da inviolabilidade da comunicação de dados, em que a privacidade diversas vezes é encarada resumidamente como um direito fundamental que tutelar as informações pessoais, ou seja, os dados pessoais, são somente protegidos em relação à sua “comunicação”.

Dessa maneira, chega ser ilógico tratar a privacidade e proteção de dados, como temas distintos, já que ambos estão correlacionados, portanto a falta de tal menção no ordenamento jurídico brasileiro, ao não considerar a proteção de dados como um direito fundamental, pode acarretar sérios prejuízos futuros com tal permissividade do uso de dados pessoais. Assim, concorda Doneda:

Tal interpretação, além de dissonante com a visão segundo a qual privacidade e informações pessoais são temas sempre mais relacionados e, em muitas ocasiões, quase que indistinguíveis entre si – conforme atesta o mencionado desenvolvimento de leis que tratam da proteção de dados pessoais e também os documentos transnacionais que associam o caráter de direito fundamental à proteção de dados pessoais –, traz consigo o enorme risco de acabar por se tornar uma norma que sugere uma grande permissividade em relação à utilização de informações pessoais. (DONEDA, 2011, p.105)

As garantias constitucionais para os dados somente sob a ótica de sua comunicação e de sua eventual interceptação lastreia-se em uma interpretação restrita a complexidade do sistema de dados e informações. Para tanto, seria facilitador uma norma que se esclarece que a privacidade e os dados pessoais sejam assegurados constitucionalmente, ou seja, reconhecer a proteção de dados como um direito fundamental.

Ressalta-se que hodiernamente as pessoas são facilmente reconhecidas mediante a representação de sua personalidade, que seria a análise dos dados pessoais, permitindo uma íntima relação entre tais dados e a própria identidade e personalidade de cada indivíduo.

Considerando apenas que o direito à privacidade seja aplicado a comunicação, atualmente com a utilização de novas tecnologias, não é possível

proporcionar uma tutela efetiva aos dados pessoais na gama e amplitude no destaque que hoje o tema merece.

O esforço a ser empreendido pela doutrina e pela jurisprudência seria, em nosso ponto de vista, basicamente o favorecimento de uma interpretação dos incisos X e XII do art. 5º mais fiel ao nosso tempo, ou seja, reconhecendo a íntima ligação que passam a ostentar os direitos relacionados à privacidade e à comunicação de dados. Desta forma, seria dado o passo necessário à integração da personalidade em sua acepção mais completa nas vicissitudes da Sociedade da Informação. (DONEDA, 2011, p.106)

Depreende-se, que a proteção de dados pessoais tem ganhado a cada dia mais destaque importância em nossa sociedade, afinal novas tecnologias aparecem a cada dia, e a única forma de proteger e garantir o desenvolvimento da personalidade, a liberdade e igualdade entre todos os indivíduos, é proteger os dados pessoais de forma que sejam tratados e utilizados de forma esclarecida aos seus titulares, e o reconhecimento constitucional de tal peripécia, possibilitaria maior segurança jurídica.

Destaca-se, que até o momento do desenvolvimento do presente trabalho, o Senado Federal havia aprovado no dia 20 de outubro de 2021, a Proposta de Emenda à Constituição (PEC) 17/2019, que reconhece a proteção de dados pessoais, inclusive nos meios digitais, como direito fundamental.

2 – A AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD)

Compreendendo o contexto do desenvolvimento da Lei Geral de Proteção de Dados, permite-se entender a criação da Autoridade Nacional de Proteção de Dados (ANPD), os desafios enfrentados, processo de construção, suas funções e o seu papel, para garantir a proteção dos dados pessoais.

2.1 – A NECESSIDADE DE UMA AUTORIDADE PARA PROTEÇÃO DE DADOS

Rodotà (p. 233, 2008), afirma que o assunto “proteção de dados” discute o presente, mas com implicações no futuro da sociedade. Sobretudo, a sociedade informacional pode se tornar rejeitadora, da mesma forma que acolhedora e igualitária, pois sem a tutela das informações eletrônicas, coloca-se em perigo o direito fundamental à liberdade, pois o livre acesso a determinadas dados, que a Legislação

aponta como dados sensíveis, faz com que os cidadãos sofram exclusão dos processos democráticos.

Os dados pessoais, nas últimas décadas tornaram-se os ativos mais preciosos, e é evidente a importância devido à sociedade informacional. Nesse contexto, foi criada a Lei Geral de Proteção de Dados com intuito de regular o mercado e assegurar uma posição decisiva ao titular de dados.

Com o surgimento de uma nova lei, e analisando a implementação de políticas para assegurar os direitos de proteção de dados e privacidade, desde 1970¹, evidenciou-se a necessidade de regular e fiscalizar a aplicação dos direitos estabelecido pela LGPD.

Gabriel Lochagin e Emanuele Pezati (p. 517, 2019), ao tratarem da preocupação regulatória, sobre o Marco Civil da Internet (Lei nº 12.965/2014 – MCI), justificam que a adoção de medidas para solucionar a violação da privacidade e dos dados pessoais, pelas inúmeras atividades individuais e empresariais que passaram a coletar dados por serviços digitais.

Sendo assim, não basta a existência da Lei como instrumento regulatório, sem que essa seja harmonicamente interpretada e tendo sua aplicação efetivada. Portanto, compreende-se a fundamental existência da Autoridade de proteção de dados, para que seja fomentada a cultura de proteção de dados, pois a Autoridade é um instrumento de garantia da lei.

Há modelos já consolidados no Reino Unido, Alemanha e França. Autoridades assim estabelecidas mostram-se fundamentais para garantir harmonia na interpretação das leis que versam sobre dados pessoais e sua efetiva aplicação, tanto pelo setor público quanto pelo privado. (TEFFÉ, p. 1, 2020)

É nesse mesmo sentido que Doneda (p. 460, 2021) informa, em se tratando da garantia na proteção de dados pessoais, o surgimento de uma autoridade administrativa com intuito de supervisionar o cumprimento da legislação, é uma tendência ao tratar a proteção de dados.

Ressalta-se, a Diretiva 95/46/CE em que estipulou aos países membros da União Europeia a obrigação à cada Estado de instituir uma “autoridade de controle”, assim tornando a *Data Protection Authority* (DPA) elemento fundamental para cumprimento da GDPR.

¹ A Lei de Proteção de Dados *Land* alemão de Hesse foi promulgada em 1970. *Hessisches Datenschutzgesetz* (The Hesse Data Protection Act), Gesetz und Verordnungsblatt I (1970).

Essas autoridades foram plenamente recepcionadas pelo Regulamento Geral de Proteção de Dados (GDPR), que, tendo entrado em vigor em 2018, teve como uma das de suas principais inovações justamente a sistematização de mecanismos de colaboração e de ação integrada dessas autoridades dentro do espaço jurídico europeu. (DONEDA, p. 461, 2021)

Entretanto, apesar da forte presença do modelo Europeu para o desenvolvimento de leis de proteção de dados em todo o mundo, afinal a GDPR foi a precursora, ainda há casos de não instituição de uma autoridade de proteção de dados em muitos países.

Dessa maneira, compreende-se que a falta da nomeação de uma Autoridade torna a lei inoperante, e em alguns casos as leis de proteção de dados pretendem a criação da DPA, mas mesmo após anos da promulgação da lei não ocorre a nomeação, dessa forma as leis não operam de maneira eficaz.

Apenas 10% das leis nacionais não criam DPAs especializados e apenas muito raramente são explicitamente sujeitos ao controle governamental. Outros 10% não nomearam um DPA dentro de um prazo razoável vez (ou em três casos pôs a sua lei em vigor). O resultado é que 80% dos 132 países com leis de privacidade de dados os têm administrados por nomeados e em funcionamento, DPAs especializados (quase sempre independentes). (GREENLEAF, p. 2, 2019, tradução livre)²

Tratando-se da LGPD, a ausência de uma Autoridade estruturada, acarretaria a ineficácia da Lei, além da não haver especificamente um órgão para fiscalizar e aplicar as sanções estabelecidas. Além do mais, restaria insegurança jurídica, por várias questões da legislação que ainda precisam ser interpretadas, e o Brasil perderia credibilidade perante o mercado digital global. (TEFFÉ, p. 5, 2020)

2.2 – CRIAÇÃO DA AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS

A LGPD, começou a ser desenvolvida em meados de 2010, em que abrangeu debates públicos, no qual foram estabelecidas duas fases, tendo como referência ao Anteprojeto, de Lei Geral de Proteção de Dados.

O mencionado Anteprojeto, encaminhado pelo Ministério da Justiça à Câmara dos Deputados, deu início formal ao procedimento legislativo como Projeto de Lei

² “Only 10% of national laws do not create specialised DPAs, and only very rarely are explicitly subject to government control. Another 10% have not appointed a DPA within a reasonable time (or in three cases brought their law into force). The result is that 80% of the 132 countries with data privacy laws have them administered by appointed and functioning, specialised DPAs (almost always independent).” (inglês no original)

5.276/2016³. Ressalta-se, que o texto desenvolvido e enviado pelo Poder Executivo ao parlamento brasileiro, não abrangeu a criação da autoridade proteção de dados, no entanto nas ocasiões em que foram debatidas a matéria foram apresentadas a instituição, atualmente chamada de ANPD.

Doneda (p. 267, 2021), afirma que embora reconhecida a essencialidade da autoridade, na época não foi compreendido um texto com a criação do órgão, pois não possuíam um entendimento uniforme sobre o assunto.

Apesar disso, é perceptível que a redação elaborada presumia a criação da Autoridade Nacional de Proteção de Dados, pois diversas vezes ao longo da redação referem-se a um determinado ao “órgão competente” para exercer a proteção de dados pessoais e de maneira que haveria a aplicação eficaz da legislação elaborada.

Aprovado o projeto, foi criada a Comissão especial na Câmara de Deputados, para análise da PL 5.276/2016, que teve relatório aprovado por unanimidade em 2018.

Entretanto, o Brasil fez parte temporariamente do cenário apontado anteriormente por Greenleaf, em que 10% dos países não criam uma autoridade. Esteve prevista a criação da Autoridade Nacional de Proteção de Dados (ANPD), na Lei nº 13.853/2018 (LGPD), salienta-se que foi incluída na redação a criação da autoridade como uma autarquia federal em regime especial, e justo, por esse motivo os dispositivos que previam sua criação da Autoridade foram vetados no ato da sanção da Lei.

Tal peripécia restou clara a insegurança jurídica, pois ao não ser criada, no mesmo tempo que a aprovação da Lei, permitiu uma lacuna na aplicação da LGPD, na qual não permitiria a aplicabilidade de algumas normas que requisitam interpretações. (MENDES, p. 23, 2018)

Sendo reconhecida a imprescindibilidade da atuação da Autoridade para efetividade da LGPD, logo, foi apresentada modificações pela Lei nº 13.853/2019 à LGPD (Lei nº 13.853/2018), que restou na criação da ANPD.

Depreende-se, que a criação da ANPD foi fundamental para se estabelecer vinculação entre o titular de dados ao setor privado e público. Ainda, a ANPD, tem como papel de alinhar com demais autoridades de fiscalização e regulação, e com os

³ Processo legislativo do Projeto de Lei 5.276/2016, disponível em:
<https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2084378>

poderes do país, dentre outras funções que foram determinadas na LGPD. (MENDES, p. 24, 2018)

Sendo assim, a Autoridade Nacional de Proteção de Dados não é mais um órgão sancionatório, assim como já apresentado o posicionamento por essa, inicialmente desenvolverá papel orientativo, para que seja estabelecida a cultura e sistema de proteção de dados nas esferas público e privado, e logo mais desempenhará o papel sancionatório como medida de impor o comportamento e demonstrar a necessidade da privacidade.

Conclui-se, que a Autoridade foi criada com o objetivo de trazer estabilidade e segurança jurídica para a execução da LGPD. No caso da legislação brasileira, é prevista uma vastidão de artigos que dependem da regulação e interpretação da Autoridade, adequando-se a realidade social e econômica do país, ao estabelecer políticas para adequação da cultura de privacidade e proteção de dados no Brasil. (PECK, p. 49, 2020)

2.3 – ESTRUTURA, NATUREZA E FUNCIONAMENTO DA ANPD

Apresentadas as modificações pela Lei nº 13.853/2019 à LGPD (Lei nº 13.853/2018), ficou-se estabelecida que a Autoridade Nacional de Proteção de Dados como órgão da administração pública federal vinculada diretamente a Presidência da República, ou seja, tem cunho político.

Para melhor compreender, a regulamentação da ANPD, ficou reservado o Capítulo IX, nos artigos 55-A a 55-K, para discorrer sobre a matéria, e o presente trabalho discorrerá minuciosamente, de maneira a explicar o papel do órgão competente para a proteção dos dados pessoais.

A LGPD com as mudanças inseridas, estabeleceu em seu artigo 55-A, uma característica transitória para a ANPD, nos parágrafos 1º e 2º, no qual em até dois anos da entrada em vigor a estrutura regimental, será procedida uma avaliação em que poderá ser convertida em “entidade da administração pública federal indireta, submetida a regime autárquico especial e vinculada à Presidência da República.”. Ainda, no parágrafo 3º deixa claro, que em virtude da crise fiscal que o Brasil vive, foi criada sem aumento de despesa. (BRASIL, 2019)

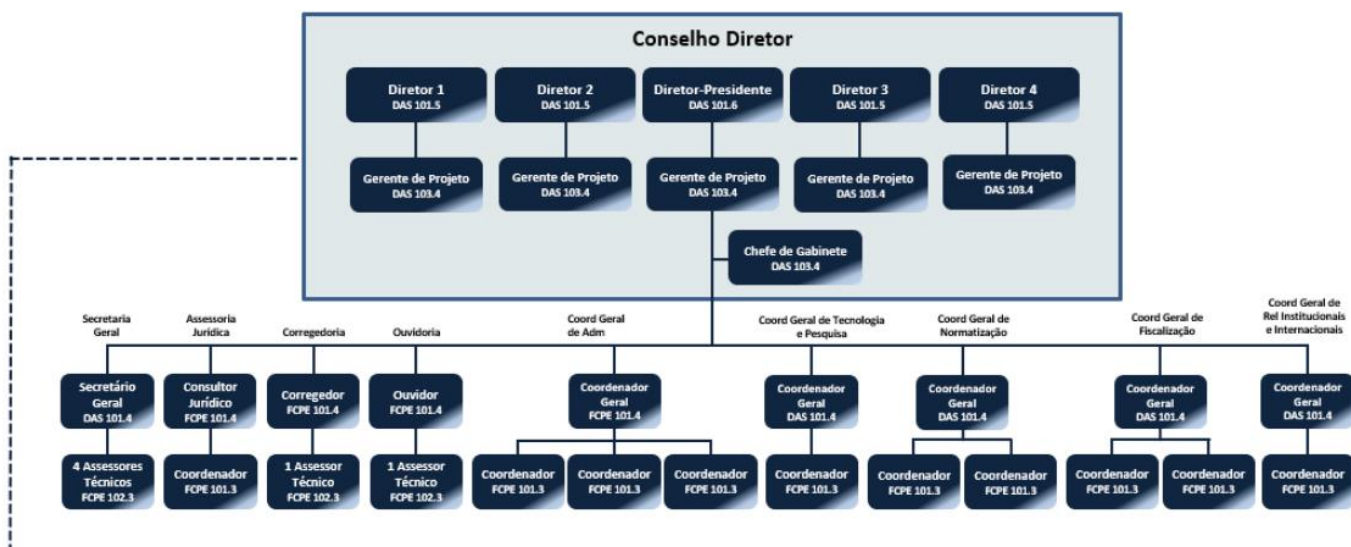
Ao tratar-se do artigo 55-B, estabeleceu a autonomia técnica e decisória da ANPD, vale mencionar o comparativo descrito por Patrícia Peck (2020), sobre outras autoridades de proteção de dados, tratando da possibilidade de garantir maior autonomia a ANPD.

De maneira comparada, observa-se que a Autoridade de Proteção de Dados da Inglaterra segue uma natureza jurídica possivelmente similar, tendo em vista que o ICO é um órgão público que reporta diretamente ao Parlamento inglês e não possui um departamento especial. Outros países, como França, Portugal e Irlanda, optaram por modelos independentes, do tipo agência reguladora.

A previsão de alteração do status da ANPD é positiva, tendo em vista que isso poderá garantir mais autonomia ao órgão, embora também seja possível observar em outros países exemplos positivos que adotam esses modelos de dependência do Poder Público central. (PECK, 2020, p. 53)

A composição da ANPD, é abordada no artigo 55-C, da MP nº 869, no qual estabeleceu que a Autoridade Nacional será composta de 6 elementos seguintes: I) Conselho Diretor; II) Conselho Nacional de Proteção de Dados; III) Corregedoria; IV) Ouvidoria; V) Órgão de assessoramento Jurídico Próprio; VI) unidades administrativas e unidade especializadas necessárias à aplicação do disposto nesta Lei (BRASIL, 2019). Para melhor compreensão dessa estrutura, veja-se:

Figura 1 – Estrutura da ANPD



Fonte: www.gov.br/anpd/pt-br/aceso-a-informacao/institucional/estrutura-organizacional-1

O Conselho Diretor da ANPD, é a direção máxima, assim como determinado no artigo 55-D, §1º, 2º e 3º, será composto de cinco diretores que serão escolhidos pelo Presidente da República, para compor o Conselho devem ser brasileiros de

reputação ilibada, com nível superior de educação e elevado conceito no campo em que atuarão, onde será cumprido o mandato de quatro anos.

Figura 2 – Estrutura do CNPD



Fonte: www.gov.br/anpd/pt-br/acesso-a-informacao/institucional/estrutura-organizacional-1

Os membros do Conselho, apenas perderão o cargo, em casos de renúncia, condenação judicial transitada em julgado, e por último, em caso de demissão decorrente de processo administrativo disciplinar, cuja competência para instaurar caberá ao Ministro de Estado Chefe da Casa Civil e o julgamento, será de competência do Presidente da República, que inclusive poderá determinar o afastamento preventivo. Após o exercício do cargo, ficou determinado pelo artigo 55-F sobre a disciplina de conflito de interesses, previsto no artigo 6º da Lei nº 12.813, de 2013.⁴

Sobre as competências da ANPD, estão previstas no art. 55-J, que traz um rol taxativo extenso, que resumidamente caberá a Autoridade deliberar, normatizar, fiscalizar e sancionar. Destacando-se que a principal competência é “zelar pela proteção dos dados pessoais” (art. 55-J, inc. I)

Além das atribuições previstas em lei, considera-se que a ANPD tem o dever de promover aos indivíduos e organizações o conhecimento das normas e políticas

⁴ BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Disponível em: . Acesso em: 07 de setembro de 2021. Art. 6º Configura conflito de interesses após o exercício de cargo ou emprego no âmbito do Poder Executivo federal: I - a qualquer tempo, divulgar ou fazer uso de informação privilegiada obtida em razão das atividades exercidas; e II - no período de 6 (seis) meses, contado da data da dispensa, exoneração, destituição, demissão ou aposentadoria, salvo quando expressamente autorizado, conforme o caso, pela Comissão de Ética Pública ou pela Controladoria-Geral da União: a) prestar, direta ou indiretamente, qualquer tipo de serviço a pessoa física ou jurídica com quem tenha estabelecido relacionamento relevante em razão do exercício do cargo ou emprego; b) aceitar cargo de administrador ou conselheiro ou estabelecer vínculo profissional com pessoa física ou jurídica que desempenhe atividade relacionada à área de competência do cargo ou emprego ocupado; c) celebrar com órgãos ou entidades do Poder Executivo federal contratos de serviço, consultoria, assessoramento ou atividades similares, vinculados, ainda que indiretamente, ao órgão ou entidade em que tenha ocupado o cargo ou emprego; ou d) intervir, direta ou indiretamente, em favor de interesse privado perante órgão ou entidade em que haja ocupado cargo ou emprego ou com o qual tenha estabelecido relacionamento relevante em razão do exercício do cargo ou emprego.

públicas relacionadas a proteção de dados pessoais e medidas de segurança, vigentes na legislação, portanto, a ANPD deve promover e guiar a mudança cultural de toda a sociedade diante do tratamento de dados pessoais, conforme apresentado por Reis (n.p., 2021) “Diante disso, cabe à ANPD estimular e promover as boas práticas para que todos estejam adequados a LGPD, pois atuará como elo entre os titulares dos dados pessoais e os controladores e operadores.”.

As sanções estabelecidas na LGPD, competem a aplicação exclusivamente à ANPD. As competências da ANPD, previstas no artigo 55-K, prevalecerão sobre as de outras entidades, assim como de outros órgãos da administração pública, quando se tratar a matéria de proteção de dados pessoais.

Dessa maneira, Autoridade de proteção de dados ao ser criada da convergência do legislador brasileiro ao modelo teórico da regulação de risco. A regulação de risco foi criada como um modelo de direito regulatório, em busca de desenvolver mecanismo para conter abusividade, bem como técnicas de prevenção e mitigação a riscos a direitos coletivos.

Rafael Zanatta (2017, p.7) destaca que o modelo de regulação de risco na LGPD permite explorar informações sobre os riscos regulados, a criação de padrões de conduta e, principalmente, o *enforcement* e o monitoramento das mudanças de comportamento social. Buscando que a LGPD seja efetiva, é depositada sobre ela, o *enforcement* do seu modelo regulatório a uma agência reguladora.

3 - AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS E A DEFESA DO CONSUMIDOR

Neste capítulo, será discutida a estreita relação entre a LGPD e o CDC, e reconhecer o consumidor, que também é titular de dados pessoais como vulnerável, e como é possível realizar a defesa desse através do Acordo de Cooperação entre a ANPD e a Secretaria Nacional do Consumidor (Senacon).

3.1 – O CONSUMIDOR QUE A PROTEÇÃO DE DADOS TUTELA

No Código de Defesa do Consumidor (Lei nº 8.078/1990 - CDC), no artigo 2º, caput, estabelece-se que o conceito de consumidor é: “Art. 2º - Consumidor é toda

pessoa física ou jurídica que adquire ou utiliza produto ou serviço como **destinatário final.**” (sem grifo no original)

A respeito do “destinatário final”, foi expressamente adotada pelo CDC a teoria finalista. Essa teoria no Brasil, é considerada majoritária, e estabelece a ideia do consumidor como *destinatário final e econômico*, de acordo com os ensinamentos de Claudia Lima Marques:

Destinatário final seria aquele destinatário fático e econômico do bem ou serviço, seja ele pessoa jurídica ou física. Logo, segundo essa interpretação teleológica, não basta ser destinatário fático do produto, retirá-lo da cadeia de produção, levá-lo para o escritório ou residência – é necessário ser destinatário econômico do bem, não adquiri-lo para revenda, não adquiri-lo para uso profissional, pois o bem seria novamente um instrumento de produção, cujo preço será incluído no preço final do profissional para adquiri-lo. Nesse caso, não haveria exigida ‘destinação final’ do produto ou do serviço, ou, como afirma o STJ, haveria consumo intermediário, ainda dentro das cadeias de produção e de distribuição. Essa interpretação restringe a figura do consumidor àquele que adquire (utiliza) um produto para uso próprio e de sua família, consumidor seria o não profissional, pois o fim do CDC é tutelar de maneira especial um grupo da sociedade que é mais vulnerável. (MARQUES, p. 85, 2010)

Assim, o CDC, estabelece como pessoa natural aquela que consome para necessidade pessoal. Sabe-se que a LGPD, objetiva proteger os direitos fundamentais da pessoa natural, no qual seria o titular de dados pessoais. Conforme previsões sobre a proteção de dados pessoais, tanto no CDC, quanto na LGPD, o titular de dados seria a parte vulnerável na relação consumerista, sendo esse o consumidor tutelado para que ocorra a proteção dos dados pessoais.

3.1.1 – VULNERABILIDADE DO CONSUMIDOR E A HIPERVULNERABILIDADE NO AMBIENTE DIGITAL

Quando se trata dos direitos do consumidor, depara-se com diversos princípios em busca de proteger os interesses econômicos do consumidor. A legislação nacional, foi estabelecida com cunho de evitar que o consumidor seja lesado, pressupondo a vulnerabilidade dele, conforme estabelecido no artigo 4º, inciso I, do Código do Consumidor. (Lei nº 8.078/1990):

Art. 4º A Política Nacional das Relações de Consumo tem por objetivo o atendimento das necessidades dos consumidores, o respeito à sua dignidade, saúde e segurança, a proteção de seus interesses econômicos, a melhoria da sua qualidade de vida, bem como a transparência e harmonia das relações de consumo, atendidos os seguintes princípios:

I - reconhecimento da vulnerabilidade do consumidor no mercado de consumo;

Flávio Tartuce e Daniel Amorim (p. 49, 2021) apontam que o surgimento do Código de Defesa do Consumidor ocorreu diante da vulnerabilidade do consumidor. Dessa forma, a vulnerabilidade é um princípio do CDC, como dito por João Batista de Almeida (p. 15, 2003) a “vulnerabilidade do consumidor: é a espinha dorsal da proteção do consumidor”, resume-se na fragilidade do consumidor diante das práticas lesivas do mercado.

Depreende-se que o consumidor é um sujeito vulnerável ao se expor as práticas do mercado, ou até mesmo, ao adquirir produtos e serviços, sendo imprescindível a intervenção de instrumentos e órgãos para a proteção do consumidor. (BESSA e MOURA, 2014)

Conforme a doutrina clássica, é possível dividir a vulnerabilidade em três âmbitos: a técnica, jurídica e fática. Devida as alterações propostas por Cláudia Lima Marques também se inclui o conceito de vulnerabilidade informacional.

Segundo as lições de Bruno Miragem (p. 123 e 124, 2012), a vulnerabilidade técnica ocorre quando o consumidor não tem conhecimentos técnicos e específicos a respeito de um produto ou serviço adquirido. De outro lado, a vulnerabilidade jurídica é aquela em que o consumidor não conhece, e nem entende as consequências de firmar um contrato, ou seja os direitos e deveres de uma relação de consumo. Já a vulnerabilidade fática, ocorre quando é reconhecida no caso concreto, é relevante, pois essa se estabelece ao evidenciar a debilidade do consumidor idoso e criança.

Ainda, Bessa e Moura (p. 81, 2014) citam o conceito estabelecido por Marques, sobre a vulnerabilidade informacional, que hoje representa a melhor compreensão sobre a sociedade em que vivemos, onde o ambiente digital é complexo e o consumidor está exposto a inúmeros riscos, a vulnerabilidade informacional se caracteriza conforme o acesso à informação e sua rapidez.

Considera-se a vulnerabilidade do consumidor no ambiente digital, pois as informações extraídas do consumidor estabelecem uma representação virtual da pessoa na sociedade, dessa maneira observa-se que ocorre de forma generalizada e em toda a sociedade uma coação para utilizar-se dos meios digitais. Assim, muitos utilizam os meios digitais, entretanto poucos entendem de conceitos informáticos, e se tornarão codependentes dos meios digitais, o fato de a sociedade estar a cada dia mais interconectada torna o ciberespaço inseguro.

É bem verdade que o termo vulnerabilidade não pode ser banalizado e tampouco superestimado. A pergunta que deve ser feita – e o argumento que é defendido – é se a vulnerabilidade dos consumidores na Internet, em função do grande déficit de informação, da falta de conhecimentos técnicos e diante com a insegurança inerente deste ambiente, em algumas situações, seria um caso de vulnerabilidade agravada ou hipervulnerabilidade digital. (COLOMBO e GOULART, 2019, n.p.)

É necessário esclarecer que a vulnerabilidade do consumidor não se resume aos vazamentos de dados pessoais, mas também é a simples manifestação de vontade viciada, na qual não ocorre o oferecimento correto de informações ao consumidor, conforme o art. 31 do CDC.

Art. 31. A **oferta e apresentação de produtos ou serviços devem assegurar informações corretas**, claras, precisas, ostensivas e em língua portuguesa sobre suas características, qualidades, quantidade, composição, preço, garantia, prazos de validade e origem, entre outros dados, bem como sobre os riscos que apresentam à saúde e segurança dos consumidores. (sem grifo no original)

Sendo assim, se reconhece o enfraquecimento do consumidor em situações de mineração de dados, cujo dados são coletados com a finalidade de estabelecer um padrão consistentes, para prever resultados, muitas vezes a coleta ocorre sem autorização do usuário ou até mesmo com obscura finalidade do serviço a ser prestado. Para Rita Peixoto Ferreira Blum (p. 61, 2018), o consumidor que tiver os dados coletados, sem atentar-se ao fato, ou ainda sem manifestar-se a respeito da conduta, estará em perceptível situação de hipervulnerabilidade.

3.2 – O PROTAGONISMO DA BASE LEGAL DO CONSENTIMENTO

Ao navegar pela Internet, é comum deparar-se com as hipóteses legais que permitem o tratamento dos dados pessoais pelos agentes de tratamentos, essas são conhecidas como bases legais e estão previstas no artigo 7º, da Lei 13.709/18.

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, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária;

IX - quando necessário para atender aos interesses legítimos do controlador ou de 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.

Qualquer tratamento de dados pessoais necessita de um fundamento legal, ou seja, de uma base legal que esclareça e explique a necessidade do tratamento do dado pessoal. No entanto, salienta-se que ao apontar um base legal para o tratamento de dados pessoais, não justifica sua adequação, que será analisada e considerada pela Autoridade Nacional de Proteção de Dados.

Ainda, Matheus Noronha Sturari (p. 78, 2019) esclarece que mesmo havendo o apontamento de uma base legal pelo agente e estando a base legal em conformidade ao tratamento, será objeto de avaliação. Também caberá, ao agente de tratamento observar e cumprir com todas as demais legislações que tratem do tema, bem como, todas as disposições previstas na legislação tratada até então.

Neste tópico, tratará apenas da base legal do consentimento, considerada a mais conhecida das bases legais, que estende inúmeras discussões sobre a sua eficácia e a legitimidade em determinadas situações, em que ocorre a coleta de maneira inadequada.

O consentimento, é sobre o direito de o indivíduo de poder controlar seus dados pessoais, considerando o titular de dados como consumidor de determinado produto, é a manifestação de vontade desse titular de dados. Sendo assim, é a forma como os consumidores poderão autodeterminar suas informações pessoais. (BIONI, 2021)

As previsões estabelecidas no MCI, determinam que o consentimento deve ser informado, inequívoco, expresso, livre e específico. Assim, como Claudia Lima

Marques (p. 82, 2016), enfatiza que a declaração de vontade nos contratos deverá possibilitar o acesso à informação através da leitura e compreensão por qualquer indivíduo, salientando a transparência nas relações de consumo.

Nessa perspectiva, levando em consideração que o consentimento deve ser informado, Bruno Bioni aponta que:

O dever-direito de informação é o primeiro instrumento para desencadear a referida perspectiva solidária das relações obrigacionais. Isso porque apenas com uma informação adequada o cidadão estará capacitado para controlar seus dados. O fluxo dos seus dados precisa tomar forma (ser informado), sendo *pressuposto* para que haja qualquer tipo de processo de tomada de decisão por parte do titular de dados. (BIONI, p. 184, 2021)

Depreende-se, que o consentimento é eficaz quando o consumidor ao manifestar sua vontade, teve informações claras e suficientes para compreender o conteúdo para tomar tal decisão. Bruno Miragem (p. 18, 2019), enfatiza que se torna ilícito o tratamento de dados que venha a se basear na manifestação de vontade com informações incorretas ou até mesmo incompletas.

Ainda, adjetivando o consentimento, ao se dizer livre o consentimento deve ser a livre manifestação espontânea de vontade, ou seja, sem pressões que influenciem na decisão do consumidor. Ademais, inequívoca, é a clara intenção do indivíduo, não restando dúvidas para a sua manifestação de vontade. (BIONI, p. 189 e 190, 2021)

Já, em relação aos adjetivos especificidade e de maneira expressa, Bioni explica que:

Como já defendemos anteriormente, essa adjetivação mais extensa – expresso e específico – desemboca para o mesmo lugar: a carga máxima de participação do cidadão dentro da dinâmica da proteção dos dados pessoais baseada, a partir da aceitação de que ele deveria seguir seus dados em todos os seus movimentos. (BIONI, p. 194, 2021)

Entretanto, Laura Schertel (n.p., 2017), evidencia as dificuldades da proteção de dados pessoais em relação ao consentimento:

Sabe-se, contudo, que o consentimento, aplicado ao tema da proteção de dados pessoais, apresenta diversas dificuldades, devendo ser tratado com cautela em razão dos seguintes aspectos: i) o problema da eficácia do consentimento no tratamento de dados pessoais, em face da possibilidade do não consentimento de o indivíduo acarretar a sua exclusão do mercado de consumo e da sociedade; ii) o problema da violação da proteção de dados pessoais, após o tratamento ter sido consentido pelo titular dos dados; iii) a questão do consentimento aplicado ao tratamento de dados sensíveis.

Conclui-se, que a base legal do consentimento, na Lei Geral de Proteção de Dados não esclarece o suficiente as adjetivações do consentimento para aplicação, destacando-se a importância da requisição da Autoridade Nacional de Proteção de Dados para interpretar e esclarecer a aplicação do consentimento, para o tratamento de dados e subsidiariamente a aplicação do MCI.

3.3 – ACORDO DA AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD) E A SECRETARIA NACIONAL DO CONSUMIDOR (SENACON)

Como já abordado anteriormente no presente trabalho, a ANPD é o órgão estatal responsável por zelar pelo cumprimento da LGPD, ficando a cargo da entidade fiscalizar e orientar o tratamento de dados pessoais no Brasil, previsto na Lei 13.709/18.

A Senacon é o órgão estatal vinculado ao Ministério da Justiça e da Segurança Pública, no qual planeja, elabora, coordena e executa a Política Nacional das Relações de Consumo. Também fica a cargo da Senacon, conforme o Decreto Presidencial nº 2.181/1997, em seu art. 3º, X, fiscalizar e aplicar as sanções administrativas da Lei 8.078/1990.

No dia 22 de março de 2021, que ambas as entidades firmaram um acordo de cooperação técnica, com os objetivos de alinhar os entendimentos e coordenar ações conjuntas para a atuação em casos de incidentes envolvendo dados pessoais inseridos em uma relação de consumo.

Evidencia-se que ambos os órgãos possuem funções semelhantes, e juntas poderão criar normas conjuntas, a fim de serem complementares. Conforme, disciplinado pelo artigo 2º, VI, LGPD, em que prevê a defesa do consumidor, sustentando tal acordo de cooperação técnica.

Ao tratar das normas serão desenvolvidas pela ANPD e Senacon, deve ser observado o ponto já mencionado neste capítulo, sobre a relação do conceito de Titular de dados, descrito no art. 5, V, LGPD e o contido no conceito de Consumidor descrito no art. 2º do CDC.

É nessa perspectiva, que a análise que antes do surgimento da LGPD, a Senacon já realizava a fiscalização e sancionamento de empresas envolvidas em

vazamentos de dados que prejudicavam os consumidores. São exemplos de tal atuação no ano de 2019 e o vazamento de dados do Facebook, vazamento de dados da operadora de telefonia Tim. Nas situações apontadas, houve plena atuação estatal com o objetivo de investigar e eventualmente sancionar as companhias tendo-se como um dos fundamentos basilares a violação da privacidade dos consumidores, por estes terem seus dados vazados. A Senacon, por já ter anos de experiência e ter aperfeiçoado em tais práticas de fiscalização e sancionamento tem muito a contribuir para o corpo técnico da ANPD, que está começando a ganhar forma em 2020 e tem dado os primeiros passos de sua atuação em todo território nacional e internacional, como ser aceita como membro da *Global Privacy Enforcement Network* (GPEN).

Ademais, a LGPD possui imensas semelhanças com o CDC, vale destacar as posições de Controlador (art. 5, VI, LGPD) e Fornecedor (art. 3º, CDC), em que ambos possuem mais poderio econômico e informacional diante do Titular e/ou Consumidor, deixando estes em situação de vulnerabilidade, assim como já apresentado nesse capítulo.

Entre outras semelhanças, ressalta-se o direito do Titular acessar seus dados pessoais de posse do Controlador (art. 18, II, LGPD) e o direito ao acesso aos bancos de dados do Fornecedor (art. 43, CDC), em casos em que a pessoa solicitante terá direito a receber uma informação clara, completa, verdadeira e em linguagem de fácil compreensão.

A ANPD e Senacon foram instigados a investigarem possíveis violações das leis e suas consequências sociais, bem como já firmado neste trabalho falar da proteção de dados, é falar sobre o futuro, e os recentes grandes vazamentos de dados de brasileiros, provocaram os órgãos a agirem.

A relação em comum com as entidades públicas tende a ser mais próxima com o Acordo, em que ambas buscam cumprir com finalidades e responsabilidades comuns, observando sempre o interesse social através da orientação e regulamentação de normas e também na aplicação de sanções.

O Acordo de Cooperação Técnica entre a ANPD e Senacon, estabeleceu funções específicas, a princípio atuaram em conjunto para identificar os problemas para que, ato contínuo, a ANPD faça as orientações à Senacon, bem como a Senacon atuará na recepção das principais reclamações e buscará uniformização das medidas a partir de normativas da ANPD, dessa maneira haverá a aplicação do artigo 45, da

LGPD, sem nenhuma intercorrência e inviabilidades de competência entre os órgãos, uniformizando assim o entendimento.

A criação desse documento, permitiu como meio regulador do vazamento de dados pessoais de consumidores, um meio para evitar-se as ambiguidades e interpretações sobre a atuação das entidades públicas no caso concreto, que servirão, principalmente, para os infratores protelarem a atuação sancionatória através de discussões jurídicas intermináveis.

Portanto, espera-se da parceria entre a ANPD e a Senacon seja eficiente e pautada na responsabilidade para com os brasileiros, que já reconhecem os usos abusivos dos dados pessoais por parte dos Fornecedores e Controladores que têm, sabendo que os titulares e consumidores são a parte mais vulnerável da relação consumerista, e ainda estabelecem ideia de absoluto controle advindo da assimetria informacional e técnica dos titulares de dados pessoais.

CONCLUSÃO

O trabalho apresentado acima busca informar de maneira didática como a implementação da Lei Geral de Proteção de Dados (LGPD) e a criação da Autoridade Nacional de Proteção de Dados (ANPD) visa proteger a vulnerabilidade do consumidor.

A princípio buscou-se estabelecer o direito à proteção de dados pessoais no âmbito constitucional, reconhecendo a necessidade de ser um direito fundamental, percorreu o caminho histórico da privacidade até as criações das Leis de proteção de dados pessoais, em tempos hodiernos. Longe de estabelecer uma linha de conteúdo, foi apresentada a ANPD, sua importância, funções, competências, atuação e o grande desafio de sua criação.

Ainda, com o intuito de identificar soluções no ordenamento jurídico brasileiro a proteção da privacidade do titular de dados, que também é consumidor, apresentou-se uma interpretação dialógica sobre as semelhanças entre a legislação do Código de Defesa do Consumidor (CDC) e a LGPD.

Como foi demonstrado, a inviolabilidade da vida privada, sob as atuais maneiras de processar os dados pessoais, estabelece a pressuposição da proteção do indivíduo contra a coleta, o armazenamento, o uso e a transmissão irrestrita dos dados pessoais. Dessa forma, o reconhecimento da proteção de dados como um direito fundamental, permitiria ao cidadão controlar livremente a divulgação, transmissão e uso de seus dados pessoais, daria poder ao indivíduo de se autodeterminar informativamente, que é um dos princípios da LGPD.

Além disso, seria um grande passo constitucional para o reconhecimento internacional, demonstrando para as relações exteriores a preocupação da nação com a proteção de dados, ao consolidar com direito fundamental.

Como já demonstrado, sabe-se que a importância da privacidade não se iniciou nos últimos anos, mas é um processo já de séculos, assunto que ganhou destaque para a sociedade que começou a preocupar-se como suas vidas eram divulgadas, como descreveram Warren e Brandeis.

Depreende-se que hoje vai muito além, o avanço tecnológico possibilitou um maior processamento de informações, permitindo a incorporação de dados para o desenvolvimento da atividade empresarial, estabelecendo assim, os dados pessoais como maiores ativos econômicos.

Os dados pessoais de consumidores tornaram-se relevante para promover-se os bens de consumo. Para aumentar a eficiência do processo produtivo, reconheceu a necessidade de inovar as publicidades através da utilização de dados, possibilitando que as publicidades sejam direcionadas para o consumidor específico permitiu o monitoramento do comportamento do consumidor, ainda a criação de perfis mais direcionados e a troca de um produto barato pelas informações do consumidor.

Em resumo, essa é “a vida na sociedade da vigilância”, como afirmado por Rodotà. Assim, a vigilância não está diante daquilo que se pode ver, e sim próximo daquilo que se pode clicar, conclui-se que o consumidor e titular de dados pessoais, é hipervulnerável no ambiente virtual, a falta de conhecimento técnico e informacional, como a clareza de consentir ao fornecer os dados pessoais, tornou o consumidor vulnerável.

Discutiu-se que os pontos fundamentais que devem ser seguidos pelas entes públicos e privados, para que seja lícito o consentimento para adquirir os dados dos indivíduos, entretanto, pressupõe-se que muitos consumidores ainda não sabem de tal informação, que muitas das vezes os dados são coletados de maneira inadequada e assim tratados, correndo o risco extremo de serem expostos. Pode-se afirmar, que a proteção de dados e a proteção do consumidor são processos codependentes, ou seja, um depende que o outro seja efetivo.

Ainda, a complexidade da legislação e sua recente implementação ainda gera grandes dúvidas sobre sua interpretação, portanto a grande relevância da ANPD. A inexistência de uma Autoridade, resultaria na ineficácia da Lei Geral de Proteção de Dados Pessoais

Sendo assim, a ANPD foi criada para facilitar a interpretação legislativa e efetivar a aplicação da LGPD, reconhece-se que não seria possível colher frutos da proteção de dados caso a Autoridade Nacional não fosse estabelecida, bem como apresentado no trabalho a ineficácia de legislações que foram criadas e permanecem sem agentes regulatórios de risco.

Ademais, a criação de um órgão regulador da LGPD, permitiu reconhecimento internacional do ente público, e ainda o reconhecimento para com as relações econômicas internacionais, vendo a necessidade do mercado no exterior que reconhece a imprescindibilidade da proteção de dados pessoais para o desenvolvimento humano.

É necessário o reconhecimento da existência de uma economia que está sob a vigilância, para que sejam estabelecidos meios e parâmetros regulatórios para eficácia legislativa, no caso a criação da ANPD, e ainda o estabelecimento de um acordo cooperativo com a Senacon.

A ANPD, ao escolher estabelecer seu primeiro acordo cooperativo com a Senacon, tem como objetivo alinhar e determinar metas e meios para que ocorra a fiscalização e sancionamento sem que haja conflito de competência entre os órgãos, ainda permite que a ANPD, aprenda com a Senacon, que já está a anos realizando a fiscalização e sancionando todos aqueles que violavam os direitos de consumidores através de vazamentos de dados.

Entende-se, como eficiente e importante tal cooperação para a aplicação da LGPD, que ainda tem muitas lacunas interpretativas e tem iniciado sua aplicação, como movimentado o sistema judiciário, ainda a há muito a que ser discutido, e o tema por ser amplo e abarcar diversas áreas do ordenamento jurídico brasileiro, promete render intensas discussões.

Sabe-se que a Lei Geral de Proteção de Dados, tem dado pequenos passos para alteração socio-cultural e a mudança de como tratar os dados pessoais, não é só sobre informações, mas sim sobre pessoas.

REFERÊNCIAS

540 MILHÕES de dados de usuários do Facebook ficam expostos em servidores da Amazon. G1, RIO DE Janeiro, 04 abr. de 2019. Seção de Economia e Tecnologia. Disponível em: <<https://g1.globo.com/economia/tecnologia/noticia/2019/04/04/dados-de-540-milhoes-de-usuarios-do-facebook-ficam-expostos-em-servidor.ghml>> Acesso em: 17 de nov. de 2021.

ABILIO, Vivianne da Silveira. *Compliance* de dados pessoais. In: FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato (coord). A Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro. 1. ed. São Paulo: Thomson Reuters Brasil, 2019.

ALMEIDA, João Batista de. Manual de direito do consumidor. São Paulo: Saraiva, 2003, p. 15.

BARROSO, Luís Roberto. A viagem redonda: *habeas data*, direitos constitucionais e prova ilícitas. In: WAMBIR, Teresa Arruda Alvim (coord.). Habeas data. São Paulo: RT, 1998. p. 212.

BESSA, Leonardo Roscoe; MOURA, Walter José Faiad de. Manual de direito do consumidor. 4. ed. Brasília: SENACON, 2014.

BIONI, Bruno Ricardo. Proteção de dados pessoais: a função e os limites do consentimento. 3. ed. Rio de Janeiro: Forense, 2021.

BRASIL. Lei nº 8.078, de 11 de setembro de 1990. Dispõe sobre a proteção do consumidor e dá outras providências. Brasília, DF: Presidência da República, [1990]. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm> Acesso em: 13 de nov. de 2021.

BRASIL. Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília, DF: Presidência da República, [2014]. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm> Acesso em: 16 de nov. 2021.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, [2018]. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm> Acesso em: 09 de nov. de 2021.

BRASIL. Lei nº 13.709, de 08 de julho de 2019. Altera a Lei nº 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados; e dá outras providências. Brasília, DF: Presidência da República, [2019]. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2019/Lei/L13853.htm#art2> Acesso em: 09 de nov. de 2021.

BRASIL. PL 5276/2016. Dispõe sobre o tratamento de dados pessoais para a garantia do livre desenvolvimento da personalidade e da dignidade da pessoa

natural. Brasília, DF: Senado Federal, 2016. Disponível em:
<<https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2084378>> Acesso em: 09 de nov. 2021.

BRASIL. Autoridade Nacional de Proteção de Dados (ANPD); Secretaria Nacional do Consumidor (Senacon).

CARVALHO, Ana Paula Gambogi. O consumidor e o direito à autodeterminação informacional: considerações sobre bancos de dados eletrônicos. *Revista de Direito do Consumidor*, São Paulo, v. 46, 2003.

CASO, Cambridge Analytica. El País. Madrid: Prisa, 19 mar. 2018 Disponível em:
<https://brasil.elpais.com/brasil/2018/03/20/tecnologia/1521582374_496225.html> Acesso em: 05 abril 2021.

COMISSÃO EUROPEIA, Carta dos Direitos Fundamentais da União Europeia. 2000. Disponível em: < https://www.europarl.europa.eu/charter/pdf/text_pt.pdf > Acesso em: 29 de out. 2021.

COLOMBO, Cristiano; GOULART, Guilherme Damásio, Hipervulnerabilidade do consumidor no ciberespaço e o tratamento dos dados pessoais à luz da Lei Geral de Proteção de Dados Pessoais Brasileira (LGPD). *In: IX Congresso Iberoamericano de investigadores y docentes de derecho e informática*. 2019. Disponível em:
<<https://www.academia.edu/39347952>> Acesso: 12 de out de 2021

DONEDA, Danilo. A proteção dos dados pessoais como um direito fundamental. *Espaço Jurídico*, Joaçaba, v. 12, n. 2, p. 91-108, jul/dez. 2011.

DONEDA, Danilo. Da privacidade à proteção de dados pessoais. 2. ed. São Paulo: Thomson Reuters Brasil, 2019.

DONEDA, Danilo. A Autoridade Nacional de Proteção de Dados e o Conselho Nacional de Proteção de Dados. *In: DONEDA, Danilo; SARLET, Ingo Wolfgang; MEENDAES, Laura Schertel; RODRIGUES JUNIOR, Otavio Luiz (coord). Tratado de Proteção de Dados Pessoais*. 1. ed. Rio de Janeiro: Editora Forense. 2020. p.459-469

EUROPA. Directiva 95/46/CE do parlamento europeu e do conselho. Luxemburgo: 1995. Disponível em: <<https://www.conjur.com.br/dl/diretiva-europeia.pdf>> Acesso: 06 de set. de 2021

GREENLEAF, Graham. Global Data Privacy 2019: DPAs, PEAs and their Networks. *Privacy Laws & Business International Report*, p. 1-2, 2019. Disponível em:
<https://papers.ssrn.com/SOL3/PAPERS.CFM?ABSTRACT_ID=3434407> Acesso: 07 de set. de 2021

GREENLEAF, Graham. 2020 ends a decade of 62 new data privacy laws. 2020. Disponível em: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3572611> Acesso em: 28 de out. 2021

INSTITUTO, notific Dataprev e aponta vazamento de dados do INSS. UOL. São Paulo: UOL, 03 set. 2019. Seção Economia. Disponível em: <<https://www.google.com.br/amp/s/economia.uol.com.br/noticias/redacao/2019/09/03/idec-notifica-dataprev-licitacao-reconhecimento-facial-beneficiarios-inss.amp.htm>> Acesso em: 05 abril 2021

KOTLER, P. *Administração de Marketing*. 14. ed. São Paulo: Pearson Brazil, 2012
 ONU, Assembleia Geral. *Declaração Universal dos Direitos Humanos*. Paris: ONU, 1948. Disponível em: <<https://www.un.org/en/about-us/universal-declaration-of-human-rights/>> Acesso em: 05 abril 2021

LOCHAGIN, Gabriel. Pezati, Emanuele. A economia da privacidade: Fundamentos econômicos e aspectos regulatórios da proteção de dados. *In*: NEWTON, Lucca de; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira; MACIEL, Renata Mota (coord). *Direito & Internet IV*. 1. ed. São Paulo: Quartier Latin, 2019. p. 513-532.

MARQUES, Claudia Lima; BENJAMIN, Antonio Herman V.; BESSA, Leonardo Roscoe. *Manual de Direito do Consumidor*. 3. ed. São Paulo: Revista dos Tribunais, 2010. p. 85

MARQUES, Claudia Lima. *Contratos no Código de Defesa do Consumidor: o novo regime das relações contratuais*. 8. ed. São Paulo: Editora Revista dos Tribunais, 2016. p.82.

MENDES, Laura Schertel. *Privacidade, proteção de dados e defesa do consumidor: Linhas gerais de um novo direito fundamental*. 1. ed. São Paulo: Saraiva, 2014.

MENDES, Laura Schertel. *Comentário à nova Lei de Proteção de Dados (lei 13.709/2018): o novo paradigma da proteção de dados no Brasil*, p. 23, 2018. Disponível em: <<https://www.academia.edu/42740879>> Acesso: 06 de set. de 2021

MIRAGEM, Bruno. *A Lei Geral de Proteção de Dados (Lei 13.709/2018) e o direito do consumidor*. 2019. Disponível em: <<https://www.brunomiragem.com.br/wp-content/uploads/2020/06/002-LGPD-e-o-direito-do-consumidor.pdf>> Acesso: 15 de set. de 2021

MIRAGEM, Bruno. *Curso de direito do consumidor*. São Paulo: Revista dos Tribunais, 2012.

ONU, Assembleia Geral. *Declaração Universal dos Direitos Humanos*. Paris: ONU, 1948. Disponível em: < <https://www.un.org/en/about-us/universal-declaration-of-human-rights>> Acesso em: 30 de jun. de 2021.

PINHEIRO, Patrícia Peck. *Proteção de dados pessoais: comentários à Lei n. 13.709/2018 (LGPD)*. 2. ed. São Paulo: Atlas, 2020

REIS, Natanrry; CHEDE, Gabriel. A Autoridade Nacional de Proteção de Dados: função sancionadora ou de aculturação. *In*: PIRONTI, Rodrigo (coord). *Lei Geral*

de Proteção de Dados no Setor Público. 1. ed. São Paulo: Quartier Latin, 2021. p. 367-376.

ROCHA, Henrique. Desafios, funções e referências internacionais para a Autoridade Nacional de Proteção de Dados, p. 41, 2019. Disponível em: <<http://www.direitorp.usp.br/pesquisa/publicacoes/anais/>> Acesso: 04 de set. 2021

RODOTÀ, Stefano. A vida na sociedade da vigilância. Rio de Janeiro: Renovar, 2008.

SILVA, Roberto pessoa Madruga. *Implementação de CRM para viabilização de marketing de relacionamento: um estudo de caso*. 2002. Dissertação (mestrado em Gestão Empresarial) – Escola Brasileira de Administração Pública e de Empresas da Fundação Getúlio Vargas. Rio de Janeiro, 2002 Disponível em: <<http://bibliotecadigital.fgv.br/dspace/bitstream/handle/10438/8645/000320652.pdf;jsessionid=>> Acesso em: 05 abril 2021

STURARI, Matheus Noronha. Proteção de dados pessoais e privacidade nos contratos de consumo. Monografia (Especialização em Direito dos Contratos) – Escola Paulista de Direito. São Paulo. 2019.

TARTUCE, Flávio; NEVES, Daniel Amorim Assumpção. Manual de Direito do Consumidor: direito matéria e processual, volume único. 10. ed. Rio de Janeiro: Forense; Método, 2021.

TEFFÉ, Chiara Spadaccini de. Por que precisamos de uma Autoridade Nacional de Proteção de Dados?, 2020. Disponível em: <https://www.academia.edu/41562812/Por_que_precisamos_de_uma_Autoridade_Nacional_de_Prote%C3%A7%C3%A3o_de_Dados> Acesso: 06 de set. de 2021

ZANATTA, Rafael A. F. Proteção de dados pessoais como regulação de risco: uma nova moldura teórica?. I Encontro da Rede de Pesquisa em Governança da Internet. Rio de Janeiro, 2017. p. 181-188.

WARREN, Samuel; BRANDEIS, Louis. The right to privacy. Harvard Law review, v. 4, p. 193-220, 1890. Disponível em: <https://www.jstor.org/stable/1321160?seq=1#metadata_info_tab_contents> Acesso em: 28 de out. d 2021