UNIVERSIDADE FEDERAL DA PARAÍBA – UFPB
CENTRO DE CIÊNCIAS JURÍDICAS – CCJ
COORDENAÇÃO DO CURSO DE DIREITO – CAMPUS JOÃO PESSOA
COORDENAÇÃO DE MONOGRAFIA

JOÃO PEDRO RIBEIRO BATISTA

O PAPEL E A EFETIVIDADE DO CONSENTIMENTO DA PROTEÇÃO DOS DADOS PESSOAIS

JOÃO PESSOA
2021

JOÃO PEDRO RIBEIRO BATISTA

O PAPEL E A EFETIVIDADE DO CONSENTIMENTO DA PROTEÇÃO DOS DADOS PESSOAIS

Trabalho de Conclusão de Curso apresentado ao Curso de Graduação em Direito de João Pessoa do Centro de Ciências Jurídicas da Universidade Federal da Paraíba como requisito parcial da obtenção do grau de Bacharel em Direito.

Orientador: Dr. Alfredo Rangel Ribeiro.

JOÃO PESSOA
2021

Catalogação na publicação Seção de Catalogação e Classificação

B333p Batista, João Pedro Ribeiro.

O papel e a efetividade do consentimento da proteção dos dados pessoais / João Pedro Ribeiro Batista. - JoãoPessoa, 2021.

51 f.

Orientação: Alfredo Rangel Ribeiro.TCC (Graduação) - UFPB/CCJ.

UFPB/CCJ CDU 34

Elaborado por LUCIMARIO DIAS DOS SANTOS - CRB-645/15

JOÃO PEDRO RIBEIRO BATISTA

O PAPEL E A EFETIVIDADE DO CONSENTIMENTO DA PROTEÇÃO DOS DADOS PESSOAIS

Trabalho de Conclusão de Curso apresentado ao Curso de Graduação em Direito de João Pessoa do Centro de Ciências Jurídicas da Universidade Federal da Paraíba como requisito parcial da obtenção do grau de Bacharel em Direito.

Orientador: Dr. Alfredo Rangel Ribeiro

DATA DA APROVAÇÃO: 15 DE JULHO DE 2021

BANCA EXAMINADORA:

_____

Prof.ª Dr. Alfredo Rangel Ribeiro
(ORIENTADOR)

_____

Prof. André Luiz Cavalcanti Cabral

_____

Prof. Dr. Gustavo Rabay Guerra

RESUMO

O objetivo do presente trabalho é estudar o papel adotado pelo consentimento na proteção de dados pessoais, especialmente, mas não se limitando a legislação brasileira, além disto pretende- se observar sua efetividade como ferramenta de autodeterminação informacional e, por fim, apresenta um caminho a ser seguido para que a norma de proteção atinja de fato seu objetivo .A metodologia utilizada no trabalho é a análise da legislação existente acerca de dados pessoais, buscando identificar conceitos chaves como o de dados pessoais, dados sensíveis bem como compreender onde se insere o consentimento na tutela dos dados pessoais e quais as características deste consentimento e então, olhar para a realidade em busca da identificação entre o objetivo trazido pela norma e as situações fáticas. Para tanto serão utilizados tanto análise doutrinária. A partir da análise da legislação e doutrina adota- se a hipótese de que apesar de ocupar posição central na proteção de dados pessoais, atuando como principal meio de autodeterminação informacional, o consentimento por si só não é suficiente para a efetiva tutela dos dados pessoais em virtude das assimetrias existentes nas relações jurídicas, sendo necessário o desenvolvimento de outras políticas para o empoderamento do titular dos dados.

Palavras-Chave: Autodeterminação informacional. Consentimento. Dados pessoais. Direitos da personalidade.

ABSTRACT

The objective of this work is to study the role adopted by consent in the protection of personal data, especially, but not limited to Brazilian legislation. Furthermore, it is intended to observe its effectiveness as an informational self-determination tool and, finally, presents a way to be followed so that the protection standard actually achieve its objective. The methodology used in the work is the analysis of the existing legislation on personal data, seeking to identify key concepts such as personal data, sensitive data, as well as understanding where consent is inserted in the protection of personal data and his characteristics, then, look at the reality in search of identification between the objective brought by the standard and the factual situations. For this, both doctrinal analysis will be used. From the analysis of legislation and doctrine, the hypothesis is adopted that, despite occupying a central position in the protection of personal data, acting as the main means of informational self-determination, consent, alone, is not sufficient for the effective protection of personal data in due to the asymmetries existing in legal relations, making it necessary to develop other policies for the empowerment of the data subject.

Key-words: Informational self-determination. Consent. Personal data. Personality rights.

SUMÁRIO

1 INTRODUÇÃO

Frente à Revolução 4.0, o panorama jurídico sofreu uma transformação imensurável, na qual houve a necessidade de adequação daquela perante a série de tecnologias cada vez mais inovadoras e disruptivas a uma velocidade nunca vista antes no curso da humanidade. Diante desse quadro, imperioso se faz destacar o papel dos dados pessoais nessa nova sociedade, inclusive na inovadora economia que transformou por completo o mercado mundial. A partir dessa compreensão é necessário entender que qualquer perspectiva de regulação dos dados pessoais deve levar em conta a existência de uma econômica da vigilância. Assim as estratégias regulatórias terminam por empoderar o indivíduo para que este possa exercer um controle acerca de seus dados (BIONI, 2019).

Apesar de os dados pessoais possuírem uma função de destaque nessa nova economia o direito ainda busca as melhores formas de tutelar esse bem jurídico. Atualmente, as normas que pretendem oferecer proteção aos dados pessoais optaram pelo paradigma da autodeterminação informacional adotando o consentimento ferramenta para esse fim.

Isto posto, o objetivo do presente trabalho é localizar o papel do consentimento na tutela dos dados pessoais, avaliar sua efetividade na função que lhe é atribuída pela norma e, se necessário e possível, apresentar um caminho para a efetividade desta proteção tendo em vista relevância dos dados pessoais tanto para o indivíduo quanto para sociedade. Para tanto este trabalho é dividido em 5 capítulos.

O primeiro deles busca traçar um histórico acerca da proteção a privacidade e oferecer um contexto fático do desenvolvimento e atual estágio das inovações tecnológicas, principalmente no tocante a coleta e processamento de dados.

O segundo capítulo tem por objetivo localizar o direito da personalidade no ordenamento jurídico como sendo uma nova espécie de direito da personalidade, são apresentados também conceitos importantes como de dados pessoais e sua importância para o desenvolvimento da pessoa. Ainda neste capítulo é feita a distinção entre a proteção dos dados pessoais e proteção a privacidade tendo em vista a inicial identificação da tutela dos dados pessoais como sendo uma faceta da tutela a privacidade.

O terceiro capítulo busca apresentar um panorama geral das normas brasileiras que tratam, ainda que de forma acidental, dos dados pessoais e de sua proteção.

O quarto busca estudar o consentimento e sua função na proteção aos dados pessoais. A comunidade europeia como pioneira na criação de normas para a tutela dos dados já dava ao usuário um papel ativo na tutela de suas informações pessoais tendo o consentimento estado presente em todas as suas regulações. O Brasil seguindo o modelo europeu adotou a ideia de autodeterminação informacional e em toda a sua legislação sobre o tema trouxe o consentimento como ferramenta para isto. A LGPD deu especial atenção ao tema, tratando amplamente do tema, desde a adjetivação do consentimento, sua dispensa e até casos especiais. Desse modo o capítulo demonstra o protagonismo dado ao consentimento na proteção aos dados pessoas.

O quinto e último capítulo vem trazer os problemas práticos que esse protagonismo do consentimento apresenta. Nesse ponto é apresentado um estudo prático que demonstra o viés dos consumidores no momento em que é dado o consentimento. Outro problema apresentando é a situação de hipervulnerabilidade do titular dos dados em relação aos atores de coleta e processamento de dados, tudo isto cria uma assimetria que impede a efetiva tutela das informações pessoais pautada apenas no consentimento. Por fim o capítulo busca apresentar possíveis soluções para a equalização desta assimetria e, consequentemente, promover a plena tutela dos dados.

A metodologia utilizada no presente trabalho foi a análise da legislação existente acerca de dados pessoais, observando seus conceitos chave as formas de proteção a dados pessoais que apresenta, localizando e entendendo a função posta ao consentimento nestas legislações. Além disto foi feita também a análise de quais seriam os direitos da personalidade buscando entender a natureza jurídica dos dados pessoais e a melhor forma de proteção. Por fim buscou- se na realidade a resposta para a efetividade das normas existentes e se o consentimento é capaz de cumprir o papel que lhe é dado pelo ordenamento jurídico.

2 DA PROTEÇÃO A PRIVACIDADE E DA SOCIEDADE INFORMACIONAL

A proteção do indivíduo e de sua propriedade é um princípio norteador do direito desde que este passou a existir na sociedade, mas de tempos em tempos é necessário que estes conceitos sejam revisitados a luz das alterações ocorridas na sociedade em que estão inseridos para que se defina a abrangência e limites desta proteção (WARREN; BRANDEIS, 1890). As mudanças pelas quais a sociedade passa criam direitos e novas formas de enxergar o indivíduo.

Inicialmente o direito preocupava-se apenas com a proteção física do indivíduo, protegia-se sua integridade física, seus bens materiais tangíveis e a liberdade dizia respeito apenas ao direito de ir e vir. Com o passar o tempo o direito expandiu sua proteção a outras esferas do indivíduo, como a tutela da propriedade intelectual, o reconhecimento de direitos como ao lazer ou a imagem e a honra.

Com o reconhecimento da importância jurídica do bem-estar do indivíduo veio também a proteção barulhos ofensivos e mesmo odores (um exemplo atual é a proibição do tabagismo em lugares fechados) (WARREN; BRANDEIS, 1890). Os ordenamentos passaram para além da esfera individual intervindo nas relações familiares e na proteção a família (outro conceito que também é revisado de tempos em tempos)

Assim sendo a ideia a ideia de propriedade foi expandida para abranger tanto a propriedade tangível como a intangível como a extensão da proteção fornecida ao indivíduo foi expandida para além de sua integridade física.

Ainda nessa atenção dada aos bens intangíveis era necessário que fossem estabelecidos os limites da proteção tendo em vista as diferentes formas que estes poderiam se apresentar, como trabalhos artísticos, segredos de mercado, segredos pessoais, opiniões mais adiante no tempo fotografias, vídeos. Dentre os bens intangíveis foram identificados pertencentes a esfera intima do indivíduo, aqueles de sua esfera privada e que, a priori, não tem valor económico intrínseco, mas que ainda sim passaram a ser protegidos pelo direito. Tais direitos são classificados com o que hoje é chamado direito à privacidade.

O direito à privacidade foi amplamente debatido no século passado, passando esta discussão por situações que para a sociedade atual parecem simples, como a divulgação de fotos pessoais ainda que obtidas de forma legítima ou a divulgação de cartas pessoais sem a devida autorização ainda que não obtida por meios ilícitos.

Inúmeras situações foram levadas aos tribunais para análise e delimitação da extensão da proteção oferecida até que fossem criadas leis que pudessem oferecer de forma satisfatória essa delimitação.

A medida em que novas tecnologias foram surgindo, com elas também foram surgindo debates acerca de como o direito deveria se portar face as mudanças, até onde caberia a proteção e quais seria a melhor forma de proteger esse novo direito reconhecido. Nesse sentido a tecnologia, fator orientador das alterações da sociedade, trouxe o que hoje é chamado de sociedade da informação (BIONI, 2019).

E partir desta nova configuração da polis veio também a necessidade de se rever conceitos como propriedade e privacidade expandindo e delimitando a abrangência desses conceitos para que se possa promover a proteção adequada a cada bem jurídico de acordo com a sua natureza e peculiaridade não bastando apenas o enquadramento de um novo bem a ser protegido a um modelo já existente apenas por conveniência ou similaridade.

2.1. A SOCIEDADE INFORMACIONAL

Ao longo de sua história a humanidade passou por diversas formas de se organizar em sociedade, sendo cada uma dessas formas detentora de um elemento determinante para seu desenvolvimento e marca na história.

Uma das primeiras formas de sociedade organizada que a humanidade conheceu foi a sociedade agrícola, onde o principal meio de produção vinha da agricultura que, para a época, foi uma descoberta que revolucionou a forma de vida do povo.

Mais para frente a humanidade continuou a se desenvolver até o ponto da criação da máquina a vapor que deu início a primeira revolução industrial e com ela também a sociedade industrial. Ainda na sociedade industrial a humanidade deu outro salto de desenvolvimento com o aproveitamento de outras formas de energia como a eletricidade ou o petróleo entrando assim na segunda revolução industrial, marcada pela produção em massa e especificação do trabalho. Nessa sociedade a indústria era o fato determinante na sociedade.

Com o desenvolvimento para o que seria a base dos computadores na segunda guerra mundial e mais tarde com a criação destes a humanidade se desenvolvia a um

ritmo cada vez maior com mudanças ocorrendo em um período de tempo cada vez menor até o estágio atual.

Na modernidade atual a sociedade tem como elemento principal a informação. Diferente de outras formas de organização a nossa sociedade tem como elemento norteador de decisões a informação.

Para que se possa entender como a informação tomou o papel central na sociedade atual é necessário o entendimento das transformações sofridas pela tecnologia. O principal fator determinante foi a criação do mundo virtual, antes dele as informações eram armazenadas essencialmente por meios físicos, o que, em comparação aos dias atuais, dificultava seu uso. As enciclopédias por exemplo eram coleções de conhecimento humano divididas em grandes volumes e, ainda que bem-organizadas, a procura por algum conhecimento específico nestes tomos exigia certo tempo e dedicação, hoje em dia, com a criação do mundo virtual, o acesso e armazenamento do conhecimento toma menos tempo.

Isso ocorre pela possibilidade de utilização de bits, que conseguem agregar por meio de uma combinação binária (0 e 1) informações em pequenas unidades compreensíveis aos computadores que por sua vez além de armazenar estas informações também é capaz de responder a comandos predeterminados (BIONI, 2019).

Dessa forma a quantidade de informações que era possível de ser armazenada aumento exponencialmente. Mas não houve apenas um aumento quantitativo no armazenamento, mas também uma evolução qualitativa, pois além de guardar os computadores tem condições de executar ordens, ou seja, o acesso aquilo que foi guardado é dado de forma muito mais simples e rápida bastando um comando do usuário para que este tenha acesso direto a informação que deseja.

2.2 DADOS PESSOAIS COMO ATIVOS NA COMUNIDADE

O mundo de hoje é intensamente conectado, em sua grande parte há pessoas conectadas com a internet, seja através de computadores, seja através de smartphones; fato é que a todo momento há muitos indivíduos acessando os mais variados ambientes na internet. Cada uma dessas pessoas ao acessar cada um desses ambientes virtuais gera uma informação, uma busca em um site de compras,

a leitura de uma notícia em um jornal eletrônico ou mesmo as preferências demonstradas nas redes sociais.

Nessa maré de informações gerada por todos reside o valor comercial dos dados pessoais dos cidadãos. Um exemplo cotidiano é uma loja de roupas que apenas pelo número de visitas em seu site tem condições de perceber quais de seus produtos são mais atrativos ao público, e não apenas isso, é ainda possível perceber quais produtos são mais ou menos atrativos a públicos com características específicas e, dessa forma, orientar suas ações para obter mais lucro.

2.2.1 Dados pessoais e as estratégias de Marketing

A publicidade é divulgação de um produto a possíveis consumidores, onde e informa as qualidades do produto com o objetivo que convencer aquele consumidor a de fato comprar o produto ou serviço.

A publicidade feita através de anúncios em revistas jornais e televisão se dirigem a uma coletividade, não há direcionamento nesse tipo de publicidade. Tais anúncios são enquadrados na chamada despersonalização das relações privadas, onde o objetivo é alcançar o maior número de pessoas (BIONI, 2019).

Nesse sentido, a ciência mercadológica percebeu que tais tipos de anúncios não eram efetivos e desperdiçavam esforços em um público que não viria a ser consumidor de tal produto ou serviço.

A partir desta percepção surge a publicidade direcionada. Para as empresas faz muito mais sentido (financeiramente) canalizar seus recursos publicitários em grupos específicos mais propensos a adquirir os bens ou serviços ofertados. Por exemplo a divulgação de um livro de culinária em uma revista de gastronomia por exemplo. Esse tipo de publicidade procura personalizar a propaganda aumentando sua efetividade ao identificar o possível interesse do consumidor através de suas ações (compra da revista por exemplo).

Para Bruno Bioni (2019), dentre as espécies do gênero publicidade direcionada há aquela chamada de publicidade comportamental on-line que permite uma personalização ainda maior da publicidade. No Brasil os números do *e-commerce* vêm crescendo ano a ano, de forma ainda mais intensa com o surgimento da pandemia do COVID-19 tendo apresentado um aumento de 68% de vendas através do meio

eletrônico do ano de 2019 para 2020 (BIONI, 2019). Desse modo cresce cada mais a relevância dos anúncios *on-line*.

Com esse protagonismo do meio eletrônico percebeu- se que a internet possibilitava uma abordagem publicitária mais efetiva mais efetiva através de suas diversas ferramentas de navegação e armazenamento de dados.

Ao navegar pela internet o usuário deixa um rastro de suas predileções o que permite um direcionamento quase pessoal das publicidades uma que vez que os anúncios apresentados a ele estão diretamente relacionados as suas ações (BIONI, 2019). Além do direcionamento a navegação também permite uma avaliação da efetividade de uma determinada propaganda a depender quantos usuários de fato acessam a publicidade que lhes é apresentada.

Não apenas as predileções de navegação dos usuários são utilizadas como forma de direcionar as técnicas de marketing, mas o grande uso de smartphones conectados à internet permitiu o monitoramento também de outros aspectos da vida do cidadão. A localização geográfica é um exemplo de deste monitoramento, ao conhecer a localização daquele indivíduo os anúncios que lhes são apresentados se levam em conta sua posição no globo.

Outro fato que passou a ser levado em conta no direcionamento da publicidade foi o estado emocional das pessoas. A substituição dos meios de comunicação tradicionais pela troca de mensagens e áudios através do uso de smartphones tornou possível a identificação do estado emocional daquele envia as mensagens, de acordo com Bione (2019, p. 45):

> Ao se comunicar com alguém por meio de um ícone de expressão – os chamados *emoticons*; ao responder à sua rede social como está se sentindo ou nela emitir uma opinião sobre um determinado assunto; ao interagir com um aplicativo de música para que ele forneça faixas musicais de acordo com o seu humor, as pessoas fornecem um rico retrato das suas emoções.

Desse modo as empresas buscam entender e utilizar tais informações para melhor direcionar as campanhas publicitárias ao público com maiores chances de interesse.

Percebe- se então uma constante vigilância da vida das pessoas, principalmente naqueles que são considerados potenciais consumidores que tem diversos aspectos de sua vida monitorados, hábitos de navegação, localização geográfica, estado emocional são exemplos de como as informações, muitas vezes

geradas de forma inconsciente, podem ser usadas para a obtenção de retorno financeiro.

2.3 DOS BANCOS DE DADOS

O aprofundamento desta temática não é objeto de estudo do presente trabalho, porém é essencial o conhecimento de alguns conceitos básicos acerca de bancos de dados para que se possa entender a importância dos dados pessoais na sociedade atual.

Incialmente deve- se pontuar que apesar muitas vezes usados como sinônimos dados e informações não tem o mesmo significado, enquanto este diz respeito apenas de fatos aquele diz respeito ao processamento desses fatos em algo inteligível.

Os bancos de dados funcionam da seguinte maneira, eles recebem os dados e entregam informação extraída desses dados, esse processo pode ser feito tanto manualmente como de forma automatizada. Por exemplo, uma loja recebe dados de vendas e saída de seus produtos, mas apenas isso não significa nada, é preciso que estes fatos sejam organizados, afim de identificar quais produtos foram mais vendidos por exemplo, para que se tenha informação.

Os bancos de dados são uma ferramenta que permite a descoberta de informações para a tomada de decisões.

2.3.1 Big Data

Big data é ápice do processamento de dados quando se fala em volume, com a criação desta tecnologia é possível a análise e estruturação de uma quantidade de dados nunca antes vista.

O Big Data é normalmente associado de 3 “Vs”: volume, variedade e velocidade. O volume está ligado ao aumento quantitativo da capacidade de processamento de dados em relação as tecnologias anteriores, a variedade é a característica atribuída pelo fato desta tecnologia conseguir organizar dados em diferentes formatos (fotos, textos e etc.) e a velocidade é devido ao tempo levado para realizar esse processo (BIONI, 2019).

Esse grande salto na mineração dado pelo Big Data veio pelo fato de que não é mais necessária a estruturação destes dados para que possam ser processados, ou

seja, essa tecnologia tem a capacidade processar dados ainda que estes não estejam estruturados.

Com essa evolução no volume de processamento é possível correlacionar uma série de fatos encontrando padrões que antes não eram vistos e inclusive atribuir probabilidades para a ocorrência de eventos futuros.

Um exemplo comumente citado quando se fala da ação do Big Data é a ação da varejista americana Target para identificar mulheres grávidas. A gravidez é um momento da vida onde os indivíduos passam a se interessar por produtos específicos, desse modo a equipe de análise da empresa conseguiu identificar que as consumidoras que estavam grávidas tendiam a comprar determinados produtos em determinadas fases da gravides. A empresa então passou a direcionar seus produtos as consumidoras que se encaixavam em determinado padrão de consumo.

O uso dessa tecnologia permite identificar uma série de padrões comportamentais dos usuários como por exemplo o risco de um tomador ser inadimplente ou das chances de um segurado apresentar maiores riscos de problemas de saúde.

2.4 INTERNET OF THINGS (IOT)

A expressão *Internet of Things* (IoT) ou, em português, Internet das Coisas, é utilizada para designar a conexão entre vários objetos comuns no dia a dia através da internet. Trata- se da detecção de aspectos do mundo real que são convertidos para dados no mundo virtual e que podem servir como ordem para realização de um ato ou tarefa específica. Nas palavras de Magrani (2018, p. 21) “A sigla refere-se a um mundo onde objetos e pessoas, assim acomodados e ambientes virtuais, interagem no espaço e no tempo”.

Na prática os objetos inteligentes além de já estarem efetivamente sendo usados pela população podem também ajudar na solução de problemas reais podendo coletar dados que servem para a economia de recursos naturais e energéticos. Para os consumidores em geral tais objetos possuem funções diversas como eletrodomésticos, brinquedos e até mesmo vestuário, um exemplo comum desse tipo de objeto são a pulseiras com capacidade de monitoramento da frequência cardíaca de seu usuário (MAGRANI, 2018).

A criação de objetos inteligentes sem o devido cuidado pode vir a gerar problemas para a comunidade. A transformação de um objeto comum em um objeto inteligente sem que haja necessidade para tanto pode apenas dificultar seu uso e torná-la mais cara, ou seja, tal adaptação seria um contrassenso onde inexistiu aprimoramento real (MAGRANI, 2018).

Outro problema gerado pela transformação impensada das coisas é a quantidade de lixo produzida por objetos obsoletos. A conectividade dos objetos tende a deixá-lo obsoleto com mais facilidade. Somado ao aumento de produção de lixo é possível ainda que a passagem de um objeto analógico para inteligente venha a causar falhas que não existiriam a *priori*.

Além dos problemas citados há ainda uma questão de privacidade a ser considerada. Tendo em vista que os objetos inteligentes têm a capacidade identificar fatores do mundo real e transformá-los em dados virtuais em conjunto com a capacidade de armazenamento e processamento do Big Data os indivíduos têm seus hábitos, desejos fazendo com que suas escolhas sejam cada vez mais influenciadas pelas publicidades direcionadas.

O desconhecimento geral da forma com que esses dados são coletados, tratados, potencialmente compartilhados e usados por terceiros tem o condão de abalar a confiança dos consumidores nesse tipo de produto. Além disto a conexão com a internet termina por abrir espaço para ataques que tem como objetivo a obtenção de informações geradas por este produto (MAGRANI, 2018).

2.5 A ECONOMIA DA VIGILÂNCIA E A PROTEÇÃO À PRIVACIDADE

Com o avanço da tecnologia de coleta e processamento de dados, os dados pessoais passaram a ser considerados ativos económicos em nossa sociedade (BIONI, 2019).

Isso ocorreu pela mudança organizacional das empresas que passaram a ter a capacidade de adaptar seus produtos e serviços as reações dos consumidores de forma quase instantâneas.

Além da rápida resposta as reações dos consumidores os dados pessoais permitiram uma melhor alocação das campanhas publicitárias que passaram a ser cada vez mais personalizadas ao levar em conta fatores como localização geográfica

ou hábitos de navegação do indivíduo, tornando assim as campanhas publicitárias mais economicamente eficientes.

Percebe- se que todas essas mudanças decorrem da vigilância constante a qual o cidadão é submetido, onde seu comportamento, movimentação passaram a ser explorados para a geração de riqueza (BIONI, 2019).

Diante deste cenário, onde os indivíduos têm diversos aspectos de sua vida monitorados, é preciso estabelecer com clareza os limites de até onde as empresas e tecnologias podem ir na coleta e tratamento dos dados pessoais de seus usuários.

Tendo em vista as complexidades apresentadas ao direito em decorrência das novas tecnologias é necessário, assim como em outras épocas, a revisão do conceito de privacidade estudando a possibilidade de dispor da proteção dos dados pessoais da mesma forma como é tutelada a privada ou admitindo a necessidade de uma proteção jurídica própria a esse bem para que, desse modo, o direito possa se posicionar afim de oferecer as melhores respostas aos problemas que lhes são apresentados.

Com essa preocupação diversos países do mundo passaram a atualizar sua legislação com intuito de abarca estas mudanças. A General Data Protection Regulation (GDPR) elaborada pela União Europeia serviu de marco regulatório que inspirando a criação de diversas legislações acerca de proteção de dados ao redor do mundo.

O legislador brasileiro seguiu a tendência mundial ao perceber a importância do tema, criando assim a Lei Geral de Proteção de Dados (LGPD) com inspiração na GDPR com o intuito de regular a forma de coleta e tratamento dos dados pessoais dos brasileiros.

3 DADOS PESSOAIS E O DIREITO A PERSONALIDADE

Personalidade pode ser descrita como o conjunto de características que distingue uma pessoa das outras. Partindo dessa ideia os direitos da personalidade podem ser corpóreos ou incorpóreos, como por exemplo nome, honra integridade física. Dada a essa característica distintiva dos direitos da personalidade a ciência jurídica proteger os protegem de agressões (BIONI, 2019).

Nesse sentido, um dado, ligado a uma pessoa, pode se inserir dentre os direitos da personalidade, sendo assim considerado um dado pessoal. Essa ideia ganha força com o fato de que, cada vez mais, as atividades de processamento de dados têm ingerência na vida das pessoas onde tanto a sociedade como a economia são orientadas a partir desses signos identificadores do cidadão (BIONI, 2019).

Nas palavras de Bioni (2019, p. 100), “trata-se de um novo tipo de identidade e, por isso mesmo, tais dossiês digitais devem externar informações corretas para que seja fidedignamente *projetada* a identidade do titular daquelas informações”.

Desse modo a inserção dos dados pessoais como direitos da personalidade é justificável, permitindo assim que, por exemplo, um indivíduo peça a retificação de seus dados pessoais que estejam incorretos.

Apesar de relacionados com a privacidade os dados pessoais transitam em mais de uma espécie de direito da personalidade sendo tal ideia necessária para a efetiva tutela desses dados.

A limitação da proteção dos dados pessoais da mesma forma a privacidade não é suficiente pois está ligado a informações que seja intimo ou privado do sujeito enquanto a proteção de dados pessoais vai além da esfera intima pois, por exemplo, existe a possibilidade de os dados estarem sob a esfera pública e a discussão recair apenas sob sua exatidão por exemplo.

3.1 ADOÇÃO DO CONCEITO EXPANSIONISTA DE DADOS PESSOAIS PELA LEI GERAL DE PROTEÇÃO DE DADOS

A definição de o que são os dados pessoais é essencial para o estudo de sua natureza e da definição da forma e limites de sua proteção. Desse modo é necessário que se trace critérios para a definição do que seria um dado pessoal, tendo assim a

tutela destinada a este objeto, e o que seria apenas um dado, sem que este represente extensão do indivíduo.

A Lei Geral de Proteção de Dados (LGPD) traz sem seu art. 5 a seguinte definição: “Art. 5º Para os fins desta Lei, considera-se: I - dado pessoal: informação relacionada a pessoa natural identificada ou identificável” (BRASIL, 2018).

Apesar de simples a redação usada pelo legislador brasileiro adota um conceito expansionista de dado pessoal ao trazer o termo “identificável” ao invés de apenas termo “identificada”.

A classificação do que é um dado pessoal vem do contexto em que ele está inserido, dependendo do tipo de informação que pode ser extraída do banco de informações onde o dado está inserido, desse modo a adoção de um conceito expansionista de dados pessoais faz com que esse enquadramento seja mais flexível, abrangendo assim um número maior de situações.

3.2 DADOS PESSOAIS E DADOS ANÔNIMOS

Enquanto dado pessoais são aqueles que podem identificar uma pessoa o dado anônimo, ao contrário, é aquele que não é capaz de fazê-lo. A incapacidade de identificação pode ser fruto de um processo intencional a qual é submetido um dado pessoal. Para tanto este processo pode se valer de diferentes técnicas que tem como objetivo a eliminação de fatores identificadores como a supressão, onde algum dado é suprimido, como o CPF por exemplo; generalização, do nome completo ou da localidade por exemplo; randomização e pseudoanonimização (BIONI, 2019).

Todas essas técnicas têm como objetivo retirar a identificabilidade de um dado por isso sua aplicação depende do contexto a qual o dado está inserido. Ocorre que, esse processo de anonimização dos dados é algo falível, sendo a ideia de que a eliminação completa dos vínculos de identificação de uma base de dados apenas um mito.

Sempre é possível que uma base de dados que passou a ser anônima possa, ao ser agregada a outra, ser mais uma vez ter seus dados como identificadores. Partindo dessa possibilidade de identificação a partir dos dados anônimos resta a questão de como lidar com eles, tendo em vista a adoção do conceito expansionista dos dados pessoais adotados pelo legislador brasileiro.

Tendo em vista que o conceito expansionista de dados pessoais inclui em si não apenas dos dados de pessoas identificadas, mas também aqueles dados que tornam o indivíduo identificável, em última análise os dados anônimos também seriam considerados dados pessoais, tendo em vista a possibilidade de reversão do processo que tornou o dado anônimo e, portanto, também seria um dado identificável, ainda que anônimo (BIONI, 2019).

Tendo em vista essa questão em relação aos dados anônimos a solução foi a adoção de uma espécie de filtro que serviria como limitador do conceito expansionista para impedir que todo dado anônimo fosse também considerado dado pessoal. Nesse sentido a LGPD se valeu do critério da razoabilidade para delimitar o conceito expansionista dos dados pessoais (BIONI, 2019). Como diz o autor (BIONI, 2019, p. 111):

> Não basta a mera possibilidade de que um dado seja atrelado a uma pessoa para atrair o termo identificável. Essa vinculação deve ser objeto de um "esforço razoável", sendo esse o perímetro de elasticidade do conceito de dado pessoal como aquele relacionado a uma pessoa identificável.

A própria LGPD estabelece critérios para avaliar essa razoabilidade quando traz em seu art. 12:

> 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.
> **§ 1º A determinação do que seja razoável deve levar em consideração fatores objetivos, tais como custo e tempo necessários para reverter o processo de anonimização, de acordo com as tecnologias disponíveis, e a utilização exclusiva de meios próprios** (BRASIL, 2018, *grifos do autor*).

Trata-se aqui do reconhecimento de que os dados anônimos são sempre reversíveis e da adoção da razoabilidade para definir qual seria um "risco aceitável" para que um dado anônimo fosse considerado um dado pessoal.

3.3 A RELEVÂNCIA DA CLASSIFICAÇÃO DOS DADOS PESSOAIS COMO DIREITO DA PERSONALIDADE

Há alguns anos um engenheiro do google afirmou que eles não coletavam informações utilizando os nomes das pessoas pois isto geraria ruído e ainda que não era necessário de fato encontrar o nome das pessoas para que estas fossem alvos das publicidades (HARDY, 2012).

Pelas características da internet não é necessário o conhecimento do nome da pessoa em específico, bastando que lhe seja atribuída um fato identificador para que seja possível o direcionamento de conteúdo, por exemplo a criação de perfis comportamentais de navegação.

Partindo da ideia de que a proteção dos dados pessoais é a tutela do cidadão, cada vez mais exposto a práticas como a definição de seu perfil comportamental com base em seus hábitos de navegação, uma separação dura entre dados pessoais e dados anonimizados não faz sentido (BIONI, 2019). Tal ideia é reforçada quando essa criação de perfis comportamentais tem como objetivo influenciar a vida de uma pessoa, pouco importando se ela é identificável ou não.

Nesse sentido a normatização não é feita apenas pelos conceitos excludentes de dados pessoais e dados anônimos, mas também pelas consequências que e o tratamento desses dados podem trazer (BIONI, 2019).

Dados minerados, ainda que sejam anônimos, podem trazer práticas discriminatórias em prejuízo de uma coletividade ou de um indivíduo.

Por exemplo uma empresa que pretende realizar um processo seletivo de candidatos de forma anônima (RINNE, 2018). Em processos seletivos anônimos as empresas buscam normalmente diminuir discriminações que possam vir a ocorrer no procedimento comum. Em situações como esta é necessário observar com atenção qual o critério de seleção adotado, caso o critério de seleção fosse as características preponderantes daqueles que já trabalham na empresa, estas obtidas pela mineração dos dados pessoais dos trabalhadores provavelmente o algoritmo de seleção replicaria vieses já enraizados naquela empresa como questões de gênero e etnia, perpetuando assim discriminações já existentes.

Na pratica a discussão orbita em como arquitetar processos de governança ao introduzir esse tipo de tecnologia nas práticas decisórias do nosso cotidiano.

Nessa ceara a LGPD vem trazer algumas dessas práticas de governança ao dispor sobre qualquer tratamento de dados que sujeite um indivíduo ou coletividade a uma decisão automatizada, sejam estes dados individuais ou coletivos, pessoais ou anônimos, bastando apenas que tenha impacto na vida e desenvolvimento pessoal do indivíduo. Assim sendo a LGPD traz em seu art. 12:

> 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.

> § 2º **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** (BRASIL, 2018, *grifos do autor*).

A importância de entender a proteção de dados pessoais como um direito da personalidade, e, portanto, um direito fundamental, vem exatamente desse alcance normativo que tem a capacidade de tutelar qualquer processamento de dados que possam impactar na vida de uma pessoa. É possível perceber então que o foco da LGPD recai sob as consequências que a atividade de tratamento de dados pode ter sob o sujeito, estando o foco no uso desses dados e não apenas nos dados em si.

Tal entendimento é corroborado pelo artigo 20 da LGPD que traz:

> 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).

A permissão conferida ao titular dos dados de solicitar revisão de decisões automatizadas alcança quaisquer tipos de tratamento automatizado de “seus interesses”, ou seja, há um alargamento no espectro da LGPD que não condiciona o exercício desse direito a um perfil relacionado a uma pessoa identificada ou identificável, mas sim a todos os aspectos da personalidade e que afetem seus interesses (BIONI, 2019).

Esse entendimento, de que a o escopo da LGPD abrange o tratamento de dados, sejam eles pessoais ou anônimos, que submete um indivíduo ou uma coletividade a um processo de decisões automatizadas; é essencial para que o direito possa dar uma adequada resposta aos problemas apresentados por uma sociedade e economia cada vez mais movida por dados.

3.4 O DESENVOLVIMENTO DA PERSONALIDADE EM MEIO A SOCIEDADE INFORMACIONAL

Tomando emprestado o conceito de Gagliano e Pamplona Filho (2021, p. 69) temos “os direitos da personalidade *como* aqueles que têm por objeto os atributos físicos, psíquicos e morais da pessoa em si e em suas projeções sociais”. A partir desta definição é possível inferir a necessária relação da pessoa como indivíduo e suas relações sociais, ou seja, a tutela jurídica dos direitos da personalidade passa a

proteção para que a pessoa possa se realizar e se relacionar junto a sociedade (BIONI, 2019).

Nesse sentido, os dados pessoais não podem ser considerados apenas como prolongamentos da pessoa, mas também como fator influenciador de sua relação com os demais cidadãos. Isso significa dizer que a proteção dos dados pessoais é necessária para que o livre desenvolvimento do indivíduo.

3.4.1 Dados sensíveis

A LGPD em seu artigo 5 traz a definição de dados sensíveis*:*

> Art. 5º Para os fins desta Lei, considera-se: [...]
> **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, *grifos do autor)*.

Ou seja, dados pessoais sensíveis são espécie de dados pessoais que em razão de seu conteúdo apresentam especial vulnerabilidade. Quando os dados pessoais dizem respeito aos assuntos elencados no inciso segundo do artigo quinto da Lei Geral de Proteção de Dados Pessoais há uma preocupação em haver uma discriminação a esta pessoa por conta de tais aspectos de sua personalidade.

Assim como dados anônimos podem vir a se tornarem dados pessoais, existe a possibilidade que dados a princípio triviais possam vir a ser considerados como dados sensíveis quando postos em conjunto com outros que permitem, através da correlação entre eles, a identificação de traços sensíveis da personalidade daquele indivíduo (BIONI, 2019).

Para Michal Kosinski, David Stillwell e Thore Graepel (2013) um exemplo disto é mostrado por um estudo na Inglaterra mostrou que as redes sociais podem criar um perfil das preferências de seus usuários que permite uma série de inferências acerca de sua personalidade. A pesquisa identificou corretamente a orientação sexual de homens heteros e homossexuais com 88% de eficácia, 95% de eficácia para brancos e negros e 85% para democratas e republicanos com base nas curtidas na rede social Facebook.

Assim como foi demonstrado no estudo é possível ainda que outros registros inicialmente triviais como histórico de navegação, lista de compras tem o potencial de revelar vários traços da personalidade do usuário.

Nesse sentido que várias legislações acerca da proteção de dados, incluindo a brasileira, dispende proteção especial a dados sensíveis, para evitar possíveis práticas discriminatórias.

Tal tutela liga- se ao princípio da isonomia, onde a proteção dos dados pessoais exerce um papel fundamental na promoção da dignidade humana e na construção de uma sociedade livre e justa garantindo o desenvolvimento do indivíduo em seu relacionamento com a sociedade.

3.4.2 A vida em dados

Para além dos celulares smartphones atualmente diversos outros objetos estão conectados à internet, tal tecnologia é a chamada *Internet of Things* (IoT). Através dela é possível que uma geladeira identifique quais alimentos então faltando ou uma bandeja de ovos saiba quantos ovos ela possui. Com o aumento da coleta de dados dos usuários aumentou exponencialmente.

A partir desse fenômeno de captação de dados criam- se verdadeiros estereótipos que marcam o sujeito e servem de fator determinante para a tomada de decisões automatizadas como a concessão de crédito, estipulação de prêmio nos contratos securitários e até mesmo risco de não embarca em avião em decorrência de seus hábitos alimentares serem semelhantes ao perfil de um terrorista[1].

De certa forma cria- se uma espécie de bolha onde a interação do indivíduo com o resto da sociedade seria direcionada em torno dos interesses deduzidos a partir de seus dados, dificultando ou impossibilitando o contato com informações diferentes que escapariam dessa catalogação.

Desse modo, para Bioni (2019) a proteção de dados influi no próprio rumo da vida das pessoas trazendo um novo desafio a tutela da personalidade humana, não podendo ser considerada apenas como evolução da privacidade tendo em vista seu impacto em direitos como liberdade de expressão, autodeterminação, não discriminação; tão caros ao nosso ordenamento jurídico. Assim é necessária uma normatização própria para a proteção deste bem jurídico.

[1] Referência à troca de dados pessoais de passageiros aéreos entre União Europeia e Estados Unidos sob o fundamento de que se combateria o terrorismo. Disponível em: https://www.bbc.com/news/world-europe-17764365. Acesso em 26 de maio de 2021

3.5 A PROTEÇÃO DOS DADOS, O DIREITO A PRIVACIDADE E OS DIREITOS DA PERSONALIDADE

O direito à privacidade pressupõe uma dicotomia básico entre as esferas pública e privada sendo a sua tutela construída em torno destas duas esferas. O indivíduo tem sua esfera privada protegida em face do público.

Assim a privacidade além de permitir o desenvolvimento pessoal do ser humano é também essencial a democracia pois é em seu íntimo que o sujeito desenvolve sua particularidade, sua subjetividade e seus anseios sociais para que no futuro possa apresentar aquilo que foi desenvolvido em sua vida privada a sociedade, contribuindo assim para o processo democrático.

Nas palavras de Uadi (2018, p. 572), “a vida privada e intimidade são apenas outros nomes do direito de estar só, porque salvaguardam a esfera de reserva do ser humano, insuscetível de intromissões externas”.

O fato de a vida privada ser insuscetível a intromissões externas (em regra ao menos) traz a dualidade entre público e privado e esse conteúdo que traz a normatização do direito à privacidade, com sua proteção focada na liberdade negativa, ou seja, a proteção é dada com o impedimento da interferência.

Historicamente a proteção à privacidade se deu de forma negativa, o bem jurídico tutelado já existia a espera de sua delimitação do que seria público ou privado por parte de seu titular. Por outro lado, a proteção dos dados pessoais engloba uma proteção positiva.

Os bens tutelados pela LGPD não estão prontos a espera de uma violação, mas são uma construção feita através do controle das informações pessoais (BIONI, 2019). Desse modo a proteção dos dados pessoais não pode ser feita da mesma forma com que se tutela o direito à privacidade.

A tutela dos dados pessoais necessita de uma forma de proteção própria não podendo ser considerada mera evolução do direito à privacidade exigindo assim a criação de uma normatização própria para que haja efetiva proteção a este bem.

No caso em questão a definição do objeto jurídico tutelado não se relaciona necessariamente com a diferença entre público e privado, mas sim pelo conceito do que é um dado pessoal, por exemplo, dados públicos em regra não geram preocupação a vida privada, porém ao se relacionarem com outros dados é possível parte da personalidade do indivíduo seja revelada. Desse modo o objeto que se

pretende proteger através da LGPD não pode ser definido apenas através da dicotomia entre público e privado, mas sim através da análise contextual do dado e de como este se relaciona com o indivíduo.

Por exemplo, os direitos de acesso e retificação se encontram na esfera pública, porquanto se busca apenas garantir que o dado pessoal represente de forma correta seu titular. Assim os dados pessoais devem ser considerados uma espécie diferente de direitos da personalidade do que a privacidade sob pena de, ao ser limitado por este, não conseguir regular de forma satisfatória a coleta e tratamento de dados como fator de promoção ao desenvolvimento humano.

3.5.1 A função da Lei Geral de Proteção de Dados

Muito se fala em “morte da privacidade” na economia informacional, onde os dados pessoais servem como base para diversas estratégias e são considerados verdadeiros ativos nos dias de hoje.

Assim, historicamente, os regulamentos de proteção de dados trazem não apenas a proteção à privacidade, mas também se preocupam com o desenvolvimento econômico (BIONI, 2019). Na década de 1980, quando a Organização para o Desenvolvimento e Cooperação Econômica (OCDE) emitiu as primeiras regulações acerca do tema, já havia a preocupação com o desenvolvimento socioeconômico, ao conferir segurança jurídica tanto ao cidadão como ao setor privado e estatal garantia também a continuidade e uma certa estabilidade das relações económicas (OECD, 2013).

No Brasil, até a elaboração da LGPD o país contava apenas com legislações esparsas e setoriais não havendo um dispositivo legal único que regulasse de forma clara a forma de tratamento de dados e que permitia a permuta de dados entre entes, tanto públicos como privados.

A LGPD em seu artigo primeiro traz:

> 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, *grifos do autor)*.

Nesse sentido o legislador deixa claro que a LGPD veio para proteger a dignidade da pessoa humana e o desenvolvimento do indivíduo, atendendo assim os princípios constitucionais. Porém não apenas essa proteção, em seu artigo segundo temos os fundamentos da proteção de dados pessoais[2].

Ou seja, a legislação traz também uma preocupação de ordem econômica, conciliando assim suas duas funções, a proteção do indivíduo e a promoção do desenvolvimento econômico.

[2] Art. 2º A disciplina da proteção de dados pessoais tem como fundamentos [...] VI - a livre iniciativa, a livre concorrência e a defesa do consumidor" (BRASIL, 2018).

4 A REGULAMENTAÇÃO DE DADOS NA SOCIEDADE INFORMACIONAL

A sociedade informacional trouxe consigo uma gama de desafios regulatórios. Diante do armazenamento, tratamento, compartilhamento e monetização dos dados que trafegam online é necessário estabelecer um norte para orientar a normatização do tema tendo em vista o tipo de sociedade que se busca alcançar e como é visto esse mundo pautado por dados.

A Constituição Federal de 1988 (CF/88) protege de maneira esparsa o direito à privacidade ao trazer em seu artigo 5, X traz que “são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação” (BRASIL, 1988). Apesar da proteção dos dados pessoais não se confundir com a proteção à privacidade, é possível entender que tal proteção está inserida no dispositivo constitucional.

Na legislação infraconstitucional o Código de Defesa do Consumidor e o Marco Civil da Internet trouxeram de forma mais detalhada a proteção aos dados pessoais.

Por conta da complexidade da questão, diversos autores, artefatos, temas envolvidos, em conjunto com a necessidade das empresas de assegurar um custo competitivo para alcançar um mercado em massa se faz necessária a atenção especial a dois pontos privacidade e segurança quando se fala em regulamentação dos dados pessoais (MAGRANI, 2018).

Além disto, é preciso também atentar aos princípios da livre iniciativa observando os impactos que a legislação pode ter no fomento de inovações tecnológicas tendo em vista que não benéfico a sociedade a criação de leis com rigidez excessiva que impedissem o desenvolvimento da tecnologia. Assim, é preciso as leis acerca do tema busquem um equilíbrio entre a proteção dos usuários e liberdade para as inovações tecnológicas.

4.1 O CÓDIGO DE DEFESA DO CONSUMIDOR E O TRATAMENTO DE DADOS

O CDC em seu art. 4, II traz como princípio a ação governamental no sentido de proteger o consumidor, seja por iniciativa direta ou por outros meios. Tal princípio é benéfico ao consumidor, mas deve ser visto com cautela afim de evitar a criação de dispositivos excessivamente repressivos ao ponto de prejudicar a liberdade econômica.

A seção VI do Código que trata dos Bancos de Dados e Cadastros de Consumidores permite ao consumidor o acesso a informações existentes em cadastros, fichas e registros de dados pessoais arquivados sobre ele bem como sua alteração em caso de incorreção. Em cima disto quando a prática de publicidade direcionada leva ao envio abusivo de mensagens o CDC responde através do art. 6, IV: “IV - a proteção contra a publicidade enganosa e abusiva, métodos comerciais coercitivos ou desleais, bem como contra práticas e cláusulas abusivas ou impostas no fornecimento de produtos e serviços” (BRASIL, 1990). Como diz Magrani (2018, p. 48):

> A publicidade comportamental é capaz de aumentar a assimetria de informação na relação de consumo, potencializar a discriminação entre os consumidores, minimizar a capacidade de escolha livre e autônoma do consumidor, dentre outras consequências.

Assim, com o aumento da conectividade e, por conseguinte, da geração de dados pode gerar um desequilíbrio de poder entre os consumidores e as empresas, o que torna o consumidor ainda mais vulnerável. Assim a privacidade e a segurança dos usuários devem ser tuteladas ao mesmo tempo em que deixa espaço para o surgimento inovações tecnológicas. O CDC parece compactuar com tal ideia ao quando prevê em seu art. 4, III: “harmonização dos interesses dos participantes das relações de consumo e compatibilização da proteção do consumidor com a necessidade de desenvolvimento econômico e tecnológico [...]” (BRASIL, 1990).

4.2 MARCO CIVIL DA INTERNET (MCI)

O Marco Civil da Internet aprovado em 2014 estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil determinando as diretrizes para atuação da União, dos Estados, do Distrito Federal e dos Municípios em relação à matéria. Antes de sua sanção era difícil e gerava diversas decisões judiciais conflitantes em virtude da ausência de disposições acerca de direitos fundamentais como a liberdade e expressão ou acesso ao conhecimento envolvendo o uso da internet (MAGRANI, 2018).

O MCI trouxe explicita diversos princípios e direitos fundamentais quanto ao uso da internet como a proteção aos dados pessoais e a garantia a liberdade de

expressão tendo se tornado diploma essencial na criação de um ambiente virtual saudável e seguro para os cidadãos.

Em seu art. 7º o MCI traz o acesso à internet como sendo essencial ao exercício da cidadania assegurando ainda uma série de direitos ao usuário:

> Art. 7º O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos:
> I - inviolabilidade da intimidade e da vida privada, sua proteção e indenização pelo dano material ou moral decorrente de sua violação;
> II - inviolabilidade e sigilo do fluxo de suas comunicações pela internet, salvo por ordem judicial, na forma da lei;
> III - inviolabilidade e sigilo de suas comunicações privadas armazenadas, salvo por ordem judicial;
> IV - não suspensão da conexão à internet, salvo por débito diretamente decorrente de sua utilização;
> V - manutenção da qualidade contratada da conexão à internet;
> VI - informações claras e completas constantes dos contratos de prestação de serviços, com detalhamento sobre o regime de proteção aos registros de conexão e aos registros de acesso a aplicações de internet, bem como sobre práticas de gerenciamento da rede que possam afetar sua qualidade;
> **VII - não fornecimento a terceiros de seus dados pessoais, inclusive registros de conexão, e de acesso a aplicações de internet, salvo mediante consentimento livre, expresso e informado ou nas hipóteses previstas em lei;**
> **VIII - informações claras e completas sobre coleta, uso, armazenamento, tratamento e proteção de seus dados pessoais, que somente poderão ser utilizados para finalidades que:**
> **a) justifiquem sua coleta;**
> **b) não sejam vedadas pela legislação; e**
> **c) estejam especificadas nos contratos de prestação de serviços ou em termos de uso de aplicações de internet;**
> **IX - consentimento expresso sobre coleta, uso, armazenamento e tratamento de dados pessoais, que deverá ocorrer de forma destacada das demais cláusulas contratuais;**
> **X - exclusão definitiva dos dados pessoais que tiver fornecido a determinada aplicação de internet, a seu requerimento, ao término da relação entre as partes, ressalvadas as hipóteses de guarda obrigatória de registros previstas nesta Lei;**
> XI - publicidade e clareza de eventuais políticas de uso dos provedores de conexão à internet e de aplicações de internet;
> XII - acessibilidade, consideradas as características físico-motoras, perceptivas, sensoriais, intelectuais e mentais do usuário, nos termos da lei; e
> XIII - aplicação das normas de proteção e defesa do consumidor nas relações de consumo realizadas na internet (BRASIL, 2014, grifos do autor).

Alguns direitos merecem destaque como o inciso VII a X que tratam especificamente da proteção de dados pessoas. No artigo seguinte (art. 8) a legislação traz o direito à privacidade e à liberdade de expressão nas comunicações como condição para o pleno exercício do direito de acesso à internet (BRASIL, 2014).

A proteção aos dados pessoais vem de forma específica na seção II sendo relevante atentar para o disposto no art. 10 que dispõe sobre a guarda e disponibilização dos registros de conexão e de acesso a aplicações de internet

Apesar do disposto ainda não é possível garantir a total proteção dos dados por conta da não proteção da conexão entre servidor e usuário (MAGRANI, 2018).

Apesar da sua importância o MCI não esgota a tutela do cidadão pois é aplicável somente ao espaço virtual deixando de lado os abusos que possam ocorrer no mundo físico. Além disso a norma peca ao deixar de trazer definições importantes como o conceito de dado pessoal, e, por isso, dificulta a determinação efetiva de seus limites e atribuir responsabilidade no caso de ilegalidades.

Nesse sentido a tutela oferecida aos usuários pelo CDC e pelo MCI vem ser complementadas pela entrada em vigor da Lei geral de Proteção de Dados.

4.3 LEI GERAL DE PROTEÇÃO DE DADOS (LGPD)

Tendo em vista que tanto o Código de Defesa do Consumidor quanto o Marco Civil da internet são insuficientes para proteger efetivamente os dados pessoais a Lei Geral de Proteção de Dados veio para preencher essa lacuna legislativa.

Partindo da ideia de que a proteção de dados passa pelo controle das próprias informações tem-se que esta tutela possui não apenas o caráter negativo, a liberdade de não ser obrigado a fazer algo, mas também perpassa pela liberdade positiva, a possibilidade de controlar suas próprias ações e vontades (MAGRANI, 2018).

A LGPD, aplicada a entidades públicas e privadas que fazem o tratamento de dados pessoais, enumera uma série de princípios que devem orientar a forma com que os dados são tratados[3].

O princípio da finalidade (art. 6, I) exige que os dados colhidos devem ser informados previamente ao usuário bem como só podem ser utilizados para fins legítimos, específicos e explícitos.

O princípio da adequação (art. 6, II) dispões que os dados colhidos devem ser e usados apenas na medida em que seja necessário para atingir os objetivos anteriormente informados.

[3] A partir desse ponto, nos parágrafos seguintes serão tratados os princípios com base no texto legislativo disposto no Art. 6º da LGPD – Lei 13.709 de 14 de agosto de 2014. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em 25 maio 2021.

Em conjunto com a adequação, o princípio da necessidade (art. 6, III) diz que os dados colhidos devem ser apenas aqueles indispensáveis para atingir a finalidade.

O princípio do livre acesso (art. 6, IV) garante aos usuários que eles tenham acesso a seus dados quando desejarem, tal princípio se coaduna no direito à livre consulta de seus dados, que deve ainda ser de fácil entendimento e gratuita.

O princípio da qualidade dos dados (art. 6, V) diz que os dados colhidos devem ser verídicos, atualizados e correspondam com a forma com que a pessoa utilizou a tecnologia (MAGRANI, 2018). Deste princípio advém o direito de retificação dos dados por parte de seus titulares.

Pelo princípio da transparência (art. 6, VI) as informações acerca do tratamento dos dados, do seu uso e dos agentes do tratamento devem ser disponíveis de forma clara aos titulares dos dados.

O princípio da segurança (art. 6, VII) propugna que os mecanismos de segurança devem ser atualizados e hábeis a proteger os dados de quaisquer perigos como acessos não autorizados ou situações de perda.

Apesar do princípio da prevenção (art. 6, VIII) ter a mesma finalidade que o da segurança este trata da adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais.

O princípio da não discriminação (art. 6, IX) traz que os dados colhidos não podem ser tratados de forma discriminatória nem usados para fins de discriminação.

O último princípio, da responsabilização (art. 6, X) requer a 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.

Além de apresentar os princípios que norteiam a proteção de dados a LGPD também trata de dar conceitos necessários ao entendimento tema bem como facilitam a responsabilização em caso de falta.

Com as definições trazidas pela lei é possível estabelecer os limites da norma assim como atribuir as devidas responsabilidades, sendo este artigo essencial para a efetiva tutela dos dados pessoais.

A LGPD veio em boa hora ao sanar a necessidade de tutela específica dos dados pessoais que surgiu em decorrência das novas tecnologias. Apesar de merecedoras de algumas críticas, como o veto a criação da Autoridade Nacional de Proteção de Dados (vetada do texto original), a LGPD não tem como objetivo frear as

inovações tecnológicas estando em harmonia com as normas de proteção de dados no cenário internacional.

5 O PAPEL DO CONSENTIMENTO NA PROTEÇÃO DE DADOS PESSOAIS

A necessidade da regulação acerca de dados surge logo após a segunda guerra mundial. A tecnologia, especialmente com a ciência computacional, foi fator determinante dessa necessidade em decorrência da capacidade de armazenamento e processamento de grande quantidade de dados. Nesse contexto, alguns países passaram a refletir acerca da criação de um grande banco de dados unificado.

Inicialmente deu- se prioridade não ao tratamento dos dados, mas sim a regulamentação da tecnologia através da concessão de autorização para seu financiamento, ocorre que, com os avanços tecnológicos tal modo de regulação se mostrou insuficiente (BIONI, 2019). Posteriormente a regulação passou a dar ao cidadão a responsabilidade de proteção pelos seus dados que agora estabelece os limites da coleta, uso e compartilhamento dos dados, daí surge a ideia de autodeterminação informacional, onde o sujeito tem um papel ativo nos processos envolvendo seus dados.

Nessa forma de regulação é conferido ao consentimento um papel fundamental devendo este, para ser valido, ser livre, informado, inequívoco, explícito e/ou específico. Com isso o titular dos dados é o ponto central das regulações atuais acerca dos dados.

5.1 O CONSENTIMENTO E SEU PAPEL NA NORMATIZAÇÃO DOS DADOS PESSOAIS

A OCDE, cujo objetivo é estabelecer uma relação de cooperação entre seus países membros, na década de 1980 emitiu dois documentos, *privacy guidelines* em 1980 e *declaration on transborder data flows* em 1985 afim de orientar a normatização dos dados criando padrões básicos para esta regulamentação.

O primeiro (*privacy guidelines)* veio para a servir como norte para os ordenamentos jurídicos nacionais no tocante a proteção de dados pessoais, fornecendo não apenas conceitos importantes, mas também a adoção de princípios a serem adotados pelos países com o intuito de trazer uma certa harmonia em relação ao tratamento de dados em diferentes países.

Dentre os princípios elencados a maioria deles tem como foco o titular dos dados, sendo relevante citar alguns deles como: “Individual Participation Principle” em

tradução livre “princípio da participação individual”, reforçando a relevância da participação do indivíduo na proteção de seus dados (OECD, 2013). Outros princípios importantes são o da limitação da coleta ou da especificação dos propósitos, que estabelece a necessidade de informa ao titular dos dados a finalidade de seu processamento para que então este possa fornecer autorização.

Diante destes princípios eleva- se o titular dos dados não apenas a sujeito passivo que fornece os dados de maneira cega, mas confere a ele um papel ativo e central na proteção de seus dados pessoais ao vincular o tratamento de seus dados a seu consentimento.

O segundo documento (*declaration on transborder data flows*) veio tratar acerca do fluxo de informações transfronteiriço e surgiu pela necessidade da harmonização dos ambientes regulatórios ao redor do mundo, sob o risco de, em decorrência de uma possível disparidade regulatória, o fluxo informacional entre países fosse prejudicado.

Em 2013 ambos os documentos passaram por uma revisão, sem, entretanto, que houvesse mudanças em sua base.

O primeiro deles manteve sua diretriz com foco na autodeterminação dos dados, mas com a ressalva de que, diante das novas tecnologias que surgiram a coleta e uso de dados estava cada vez mais complexa e opaca[4], sendo necessária a busca por meios que aumentassem a transparência e conferissem ao titular controles sobre suas informações.

O segundo ainda busca uma harmonização normativa, porém traz também a necessidade de ações coordenadas para fiscalização e aplicação das leis de proteção de dados (BIONI, 2019).

5.2 O CONSENTIMENTO NO DIREITO COMUNITÁRIO EUROPEU

A comunidade europeia teve sua primeira norma acerca de dados com a convenção 108 na década de 1980 como resultado das *guidelines* elaboradas pela OCDE para facilitar a legislação sobre dados pessoais (BIONI, 2019). O próprio

[4] No capítulo 4 é disposto o seguinte “It is increasingly difficult for individuals to understand and make choices related to the uses of their personal data” (OECD, 2013, p. 67). Esse capítulo fala acerca da dificuldade de entender os riscos acerca de suas informações pessoais frente a complexidade de seus possíveis usos.

preâmbulo faz a correlação entre proteção de dados pessoais e o livre fluxo de informações[5].

Duas décadas após a Diretiva Europeia de Proteção de Dados Pessoais (95/46/EC) trouxe normas mais específicas a ideia apresentada na convenção acerca da garantia dos indivíduos ao controle sobre suas informações pessoais.

A diretiva traz a adjetivação do consentimento ao tomá-lo como livre e informado. Além de conferir direitos ao titular dos dados, a diretiva traz também obrigações ao *data controller*, aquele que processa os dados, como a não coleta excessiva de dados para além da necessidade especificada (BIONI, 2019). A inovação trazida pela diretiva está nessa atribuição da limitação pois, diferente das *guidelines* onde a atribuição era apenas do titular dos dados agora o próprio agente que processa os dados tem o dever legal de cooperar com o titular nessa atividade.

Em seguida a Diretiva Europeia (2002/58) trata sobre a proteção das comunicações eletrônicas. Além das disposições gerais que reafirmam a necessidade do consentimento ser livre, específico e informado[6], essa diretiva traz ainda normas específicas onde são apresentados os meios pelos quais o controle será realizado. A referida norma propões a utilização de meios eu permitam ao usuário exercer o controle sob seus dados pessoais, a norma ainda traz exemplos de ferramentas de coleta de dados pessoais como *cookies* ou *spywares*[7].

A GDPR – *General Data Protection Regulation* trouxe a mesma matriz já existente nas outras regulações da comunidade europeia no tocante ao consentimento[8]. A GDPR elenca novamente uma série de qualificadoras para o consentimento desta vez adicionando a partícula aditiva “e” garantindo assim que tais requisitos são cumulativos e ainda traz o resultado esperado, o consentimento deve corresponder a vontade do titular dos dados seja por meio de uma declaração ou por meio de uma ação afirmativa representativa (BIONI, 2019).

Diante do exposto é possível perceber que o consentimento ocupa um papel fundamental nas normas da comunidade europeia desde seus primórdios, servindo

[5] Na parte final do preâmbulo onde é disposto “Recognising that it is necessary to reconcile the fundamental values of the respect for privacy and the free flow of information between peoples” (OECD, 2013, p. 1)
[6] Consideração 17 da Diretiva Europeia (2002/58).
[7] Considerações 24 e 25 da Diretiva Europeia (2002/58).
[8] *General Data Protection Regulation,* art.7: “Conditions for consents...” onde são dispostas as condições para o consentimento (OECD, 2011).

como ferramenta para autodeterminação informacional ao conferir ao titular dos dados a decisão acerca do tratamento destes.

5.3 O CONSENTIMENTO NA LEGISLAÇÃO SETORIAIS BRASILEIRAS

Como tratado anteriormente o legislador brasileiro ao reconhecer a necessidade de regulamentar a forma de tratamento dos dados pessoais optou por trazer esta tutela atrelada ao paradigma de autodeterminação informacional, oferecendo ao titular dos dados poderes sob eles.

Assim como a legislação europeia a brasileira decide pela utilização do consentimento como principal ferramenta de empoderamento do titular dos dados como é possível perceber em toda legislação acerca do tema.

5.3.1 Código de Defesa do Consumidor

O Código de Defesa do Consumidor (CDC) traz em seu artigo 43 a regulamentação dos bancos de dados e cadastros dos consumidores. A norma consumerista além de ter um caráter amplo ao incluir em seu escopo qualquer banco de dados que diga respeito ao consumidor, indo além de apenas bancos de dados com informações negativas; confere a esse especial importância no tratamento destes dados.

Inicialmente a norma traz a necessidade de clareza e objetiva quanto aos cadastros e dados dos consumidores, é exido ainda a comunicação ao titular dos dados a abertura de cadastro quando este não a solicitar, tal comunicação deve ser anterior a criação do cadastro permitindo assim o acompanhamento do consumidor o tratamento de seus dados.

Além da comunicação o CDC dispõe ainda da possibilidade de imediata correção sempre que o consumidor encontrar inexatidão em relação a seus dados.

Diante dos direitos conferidos ao consumidor pelo CDC acerca de cadastro e banco de dados, acesso, retificação e cancelamento; além de buscar a transparência é perceptível a busca do legislador pela autodeterminação informacional (BIONI, 2019).

5.3.2 Lei do Cadastro Positivo

A Lei 12.414/2011 (lei do cadastro positivo) trata da formação e consulta a bancos de dados com informações de adimplementos[9] para fins de concessão de crédito (BIONI, 2019). A referida legislação traz um fato adicional a análise para concessão de crédito além do registro de dívidas não pagas ao permitir também a análise da situação financeiro do cidadão através do seu histórico de adimplemento das dívidas.

No texto original o artigo 4 da lei trazia o seguinte texto: “Art. 4 - abertura de cadastro requer autorização prévia do potencial cadastrado mediante consentimento informado por meio de assinatura em instrumento específico ou em cláusula apartada” (BRASIL, 2011).

Porém a lei complementar nº 166 de 2019 veio a alterar esta redação retirando a necessidade da autorização prévia para a abertura do cadastro exigindo- se apenas a comunicação ao cadastrado em até 30 dias da abertura do cadastro[10]. Nesse sentido o legislador brasileiro retirou parte do poder conferido ao titular pela redação original ao igualar a criação do banco de dados a legislação consumerista onde é exigida apenas a comunicação e não sua expressa autorização.

Além da comunicação a lei traz algumas características para os bancos de dados como a clareza, objetividade e veracidade das informações neles contidas bem como também a proibição de informações excessivas e aquelas sensíveis, que dizem respeito à origem social e étnica, à saúde, à informação genética, à orientação sexual e às convicções políticas, religiosas e filosóficas[11].

5.3.3 Marco Civil da Internet

A Lei 12.965/2014, também conhecida como marco civil da internet (MCI) veio estabelecer os princípios, garantias, direitos e deveres para o uso da internet no Brasil e determina as diretrizes para atuação da União, dos Estados, do Distrito Federal e

[9] Lei 12.414/2011, art. 1 “Esta Lei 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, sem prejuízo do disposto [...]” (BRASIL, 2011).
[10] Lei 12.414/2011, art. 4 dispõe apenas da necessidade da comunicação ao titular dos dados (BRASIL, 2011).
[11] Lei nº 12.414/2011, art. 3 dispõe acerca das condições da criação do banco de dados (BRASIL, 2011).

dos Municípios em relação à matéria inaugurando uma normativa específica para os direitos do cidadão em relação ao uso da internet (BIONI, 2019).

O MCI busca assegurar os direitos dos cidadãos no ambiente virtual sem, no entanto, inibir as inovações trazidas pela internet. Tal ideia fica consagrada quando em seu artigo 2, V a lei consagrada a livre iniciativa e a livre concorrência como parte de seus princípios norteadores.

Dentre os direitos previsto nesta lei são previstas as proteções a privacidade e aos dados pessoais que servem como pilares da norma sendo o usuário posto em uma posição fundamental em relação a proteção de seus dados (BRASIL, 2014). O artigo sétimo desta lei, responsável por apresentar alguns dos direitos dos usuários, dispões de diversos dispositivos que fazem menção expressa a necessidade do consentimento do usuário para coleta, uso, armazenamento e tratamento de seus dados pessoais (BRASIL, 2014).

Além da necessidade do consentimento o Marco Civil da Internet qualifica este consentimento como sendo livre, expresso e informado. A norma se aprofundou ainda mais de como é dado este consentimento ao, em seu inciso IX e XI do art. 7, trazer orientações acerca do que seria este consentimento expresso e informado.

Ainda no sentido de chamar o usuário ao papel ativo na proteção de seus dados o MCI traz a possibilidade deste requerer a exclusão definitiva de seus dados pessoais que tiver fornecido a determinada aplicação da internet ao término da relação entre as partes (BRASIL, 2014).

Assim percebe- se legislação pátria decidiu, assim como a comunidade europeia, pela adoção da ideia de autodeterminação informacional como orientação normativa para a proteção dos dados pessoais. Tal parâmetro coloca o cidadão para que, tendo o conhecimento acerca de seus fluxos de dados pessoais, possa controlá-lo através do consentimento, seja este controle incidente sob a coleta, compartilhamento e até mesmo de exclusão destes dados.

5.4 O CONSENTIMENTO NA LEI GERAL DE PROTEÇÃO DE DADOS

Após uma década de debates em 2018 foi sancionada a lei Nº 13.709 (Lei geral de Proteção de Dados, LGPD) que trata, como seu nome sugere, do tratamento de dados pessoais, atuando desde então como principal norma a respeito do tema.

A LGPD trouxe o consentimento em seu artigo 7 como requisito para o tratamento de dados pessoais ao lado de diversas outras hipóteses. Conforme Bioni (2019) apesar de, topograficamente, vir de forma horizontal a outros requisitos ao realizar a análise dos princípios trazidos pela norma e de seu corpo normativo total é possível dizer que o consentimento se encontra como vetor principal da proteção aos dados pessoais por diversos motivos.

Primeiro porque, seguindo suas antecessoras e o direito comunitário europeu a LGPD também traz adjetivos ao consentimento, exigindo que este seja livre, informado, específico, com alguma finalidade determinada e em alguns casos específico[12].

Segundo pois, grande parte dos princípios trazidos pela lei dirá em torno do indivíduo. O artigo sexto da lei traz além dos princípios clássicos como a transparência, especificação do proposito, livre acesso ao titular dos dados sobre a forma e tratamento destes; também princípios mais "modernos" como a adequação, que é a compatibilidade do tratamento com as finalidades informadas ao titular e a necessidade que limita o tratamento ao mínimo necessário a realização de suas finalidades (BIONI, 2019). A partir da análise dos princípios dispostos na norma obtém-se a ideia de que o titular dos dados deve sempre ter controle sob estes.

Em terceiro lugar porque existe uma série de dispositivos que, na prática, dão o controle dos dados pessoais ao seu titular através do consentimento. Por exemplo:

> Art. 8º O consentimento previsto no inciso I do art. 7º desta Lei deverá ser fornecido por escrito ou por outro meio que demonstre a manifestação de vontade do titular.
> § 1º Caso o consentimento seja fornecido por escrito, esse deverá constar de cláusula destacada das demais cláusulas contratuais.
> ...
> § 3º É vedado o tratamento de dados pessoais mediante vício de consentimento.
> § 4º O consentimento deverá referir-se a finalidades determinadas, e as autorizações genéricas para o tratamento de dados pessoais serão nulas.
> § 5º O consentimento pode ser revogado a qualquer momento mediante manifestação expressa do titular, por procedimento gratuito e facilitado, ratificados os tratamentos realizados sob amparo do consentimento anteriormente manifestado enquanto não houver requerimento de eliminação, nos termos do inciso VI do caput do art. 18 desta Lei.
> § 6º Em caso de alteração de informação referida nos incisos I, II, III ou V do art. 9º desta Lei, o controlador deverá informar ao titular, com destaque de forma específica do teor das alterações, podendo o titular, nos casos em que

[12] Lei nº 12.965, **art.14,** § 1º "O tratamento de dados pessoais de crianças deverá ser realizado com o consentimento específico e em destaque dado por pelo menos um dos pais ou pelo responsável legal" (BRASIL, 2014).

> o seu consentimento é exigido, revogá-lo caso discorde da alteração (BRASIL, 2018).

O artigo oitavo é apenas um dos dispositivos que a relevância do consentimento que ainda aparece diversas outras vezes no corpo da legislação. A análise da legislação deixa claro que o consentimento é a feramente fundamental pela qual o titular dos dados exerce seu controle acerca de suas informações.

Além do consentimento a lei traz ainda em seu artigo sétimas cerca de 9 hipóteses em que há legitimação para o tratamento de dados sem a necessidade do consentimento prévio de seu titular. Nestes casos é necessário debater qual seria a forma de assegurar a transparência desse tratamento[13] para que o cidadão possa realizar seu controle acerca do tratamento de seus dados ainda que a posteriori.

5.5 O PROTAGONISMO DO CONSENTIMENTO NA REGULAMENTAÇÃO DE DADOS

O titular dos dados passou a ter um papel de protagonista da proteção de suas informações com a adoção de uma estratégia normativa que conferia a ele a responsabilidade de autoproteger suas informações pessoais (BIONI, 2019). Esse caminho tomado pela veio através da adoção da ferramenta do consentimento, que passou a ser exigido, em regra, para coleta, tratamento e compartilhamento desses dados.

Essa estratégia normativa, criado nos anos 80, conduz ao protagonismo do consentimento. O resultado disto é a aposta na racionalidade do indivíduo e em sua capacidade para controlar de forma satisfatória seus dados pessoais.

Nesse sentido é necessário a reavaliação de tal estratégia e do que é autodeterminação informacional para assim encontrar soluções que, por um lado mantenham o poder que o titular dos dados tem sobre estes, mas também não deixe apenas sob seus ombros a proteção de suas informações pessoais.

[13] Da leitura da Lei nº 12.965**, art. 7,** §6 infere-se a necessidade de transparência quanto ao tratamento de dados.

6 REAVALIAÇÃO DO CONSENTIMENTO NA PROTEÇÃO DE DADOS PESSOAIS

Apesar da adoção do paradigma da autodeterminação informacional ter sido adotado pela maioria dos ordenamentos jurídicos ele não é perfeito e isento de falhas. Ao tornar o titular protagonista na tutela de seus dados é também imposto a este uma grande responsabilidade, muitas vezes além de sua capacidade.

Nesse sentido é necessário revisar o papel adotado pelo consentimento na proteção de dados, fazendo um olhar crítico acerca de sua eficácia como meio de tutela dos dados.

6.1 QUESTÕES ACERCA DA POSIÇÃO DO CONSENTIMENTO NA TUTELA DE DADOS

Para que seja possível entender a real eficácia do consentimento é preciso observar se aquele que tem o poder de dar seu consentimento é plenamente capaz de fazê-lo na prática, não basta apenas sua adjetivação pela norma é preciso que se olhe para as situações do mundo real para auferir sua efetividade.

6.1.1 O ecossistema informacional e a limitação da livre decisão

Partindo do seguinte exemplo prático, um negócio baseado em publicidade direcionada com diversos parceiros comerciais e, portanto, diversos atores pelos quais passam os dados pessoais. A estruturação dessa indústria resulta na agregação de dados, a própria ideia de rede implica o compartilhamento de informações para que seja alcançado um objetivo em comum (BIONI, 2019). Assim, pequenos pedaços de informações são combinados para a criação mais precisa de um perfil preciso dos hábitos do consumidor tornando o fluxo informacional complexo e de difícil determinação.

Tendo em vista essa multiplicidade de atores e complexidade do fluxo informacional o titular dos dados pessoais, que deveria conhecimento de todos os atores e processos pelos quais passam seus dados para que pudesse exercer de forma efetiva seu controle, termina por não ter capacidade de fazê-lo.

Adotando a ideia de que o ser imano tende a ser imediatista é provável que o consumidor foque apenas nos benefícios imediatos em detrimento de possíveis prejuízos futuros, o que no tema abordado se configura como o acesso ao produto ou

serviço oferecido em detrimento a possibilidade de perda do controle sob suas informações pessoais no futuro.

A ideia de que o cidadão é um sujeito totalmente racional o tempo todo não encontra respaldo na realidade, e frente a arquitetura de escolha de decisões entre o benefício imediato com prejuízo futuro este se encontra em uma situação de hipervulnerabilidade (BIONI, 2019). Nas palavras de Bioni (2019, p. 213) “Ele está em uma situação de vulnerabilidade específica em meio a uma relação assimétrica que salta aos olhos [...]”.

Tal vulnerabilidade pode ser confirmada por diversos estudos como por exemplo Mental Models (Universidades *de Stanford e Carnegie Mellon)*. Esse estudo foi realizado através de entrevistas focando na visão dos participantes acerca da publicidade online e na habilidade deles de tomar decisões acerca do custo/benefício relacionados a privacidade. Em suma, buscou- se verificar o quanto os usuários compreendiam de fato o fluxo de suas informações.

Para Cranor e McDonald (2012), a primeira constatação é o fato dos usuários não têm conhecimento técnico suficiente para controlar seus dados quando da coleta, apenas 23% dos participantes usam o modo de navegação privada, aquele que impede a coleta de dados, enquanto o resto ou não utiliza essa ferramenta ou não sabe. Além dos poucos usuários que fazem a limpeza de *cookies* disso apenas 30% destes o fazem por razões de segurança e privacidade enquanto os demais o fazem apenas por indicação de algum conhecido.

A pesquisa segue revelando que 70% dos entrevistados levam em consideração o fato do website compartilhas suas informações com parceiro, cujas atividades se relacionam com a vida publicitária. Em conjunto a isto 64% dos participantes considera invasiva a vigilância sob suas atividades online, o que demonstra um descolamento do modelo de negócios atual com a perspectiva dos usuários (CRANOR; MCDONALD, 2012).

Porém, ao serem divididos em dois grupos onde um grupo é perguntado se pagariam o valor de um dólar para evitar que os provedores de internet deixassem de coletar seus dados enquanto no outro é questionado se aceitariam um desconto de 1 dólar para que os provedores pudessem realizar a coleta de seus dados. No primeiro grupo, 11% estavam dispostos a pagar o valor em troca da não coleta de seus dados, enquanto no segundo 69% aceitaram o desconto oferecido em troca da coleta (CRANOR; MCDONALD, 2012).

A pesquisa conclui que a publicidade comportamental viola as expectativas do consumidor e é entendida como prejudicial (CRANOR; MCDONALD, 2012). Além disso percebe- se que os usuários não estão capacitados para tomar decisões acerca de seus dados pessoais, por falta de conhecimento acerca de como funciona a coleta de dados, pela predisposição no *tradeoff* que ocorre na economia informacional onde a proteção de dados é um benefício mediato e por fim, pela discordância dos usuários da lógica de que deveriam pagar pela garantia de seu direito à privacidade.

6.1.2 A hipervulnerabilidade na proteção dos dados pessoais

O cidadão na sociedade informacional deve ser visto como vulnerável nas relações jurídicas com aqueles responsáveis pela coleta e tratamento de seus dados, tendo em vista que ele traz para si várias das fraquezas próprias desse contexto. Nas relações de consumo a situação de vulnerabilidade do consumidor é fato conhecido, porém, apesar destas relações envolver mais de um ator na cadeia produtiva esse número não se iguala a diversidade de agentes presentes na estrutura da economia informacional suscitando assim um desequilíbrio ainda maior entre as partes da relação jurídica (BIONI, 2019).

Somado a isto tem o fato de que em uma sociedade em que informação passou a ser moeda de troca o consumidor não sabe exatamente o valor que seus dados têm já que é incerto o alcance do fluxo de seus dados pessoais e, por conseguinte, o que deles se pode extrair (BIONI, 2019). Por fim existe a idiossincrasia no *tradeoff* da economia informacional demonstrada pelos estudos empíricos.

Todos esses fatores resultam em uma vulnerabilidade de diversas facetas, informacional, técnica e económica. Desse modo, o consumidor no mercado informacional quanto a seus dados assume a condição hipervulneravel. Desse modo, é vista uma contradição, pois a estratégia regulatória aponta como principal responsável pela proteção de seus dados o sujeito mais vulnerável da relação.

Desse modo deve buscar não apenas a estratégia regulatória puramente liberal acreditando na capacidade do indivíduo por si só atingir a plena proteção de seus dados sendo necessário o desenvolvimento de políticas públicas para o empoderamento desse sujeito hipossuficiente.

6.2 EQUALIZAÇÃO DAS ASSIMETRIAS NAS RELAÇÕES JURÍDICAS

A ideia de que a concepção de um produto ou serviço deve ser orientada para proteção de dados pessoais é conhecida como *Privacy by Desing* onde este produto ou serviço são pensados com base em tecnologias que facilitam o controle e a proteção das informações pessoais (BIONI, 2019).

Como exemplos clássicos tem- se a criptografia, que garante a confidencialidade das informações; anonimização, que dificulta a identificação entre o titular e a informação ou a navegação anônima que impedem a colheita de informações.

Nesse sentido é possível a criação de ferramentas que possam servir de solução para a assimetria entre titular de dados e controlador. Essas ferramentas (como as citadas acima) podem oferecer novas formas de operacionalização do consentimento dando a este a força necessária para a efetiva tutela dos dados.

Outro exemplo deste tipo de iniciativa é o chamado *Do Not Track* (DNT). Houve uma divergência acerca do momento em que o titular dos dados deveria dar seu consentimento para a coleta de seus dados de navegação, podendo este ser prévio ou a posteriori, que poderia ser extraída implicitamente por meio das configurações dos navegadores.

A primeira opção obteve um efeito adverso inesperado pois, na medida em que se exigia o consentimento prévio e expresso dos usuários, estes foram bombardeados com uma série de avisos que terminaram por prejudicar a sua navegação (BIONI, 2019).

A segunda opção trouxe questões como a forma com que as configurações dos navegadores seriam disponibilizadas aos usuários, se essas deveriam ser as configurações padrão ou se deveria haver uma padronização dessa ferramenta entre os navegadores.

Nesse sentido o DNT surge para facilitar o controle de dados. Ao invés de aceitar ou bloquear as diversas notificações o consumidor acionaria o DNT para externar sua escolha de barrar ou não a coleta de dados, tal funcionalidade seria ativada no navegador sendo a forma pela qual o usuário daria, ou não, seu consentimento acerca da coleta de seus dados.

O DNT é apenas uma dentre tantas ferramentas que buscam acabar com assimetria existente na sociedade informacional, sendo necessária a adoção de uma

verdadeira arquitetura de rede que tenha por objetivo facilitar o entendimento e controle do titular sob seus dados para que haja a verdadeira proteção delas. Trata-se do encontro entre o paradigma adotado pela norma de proteção de dados, que põe o sujeito como protagonista da proteção de seus dados, através do consentimento, e da realidade, onde o sujeito é exposto a diversas vulnerabilidades.

7 CONSIDERAÇÕES FINAIS

Na sociedade moderna o avanço da tecnologia permitiu um salto tanto qualitativo quanto quantitativo em relação a coleta e armazenamento de informações, nesse cenário vive- se uma sociedade informacional, onde dados pessoais passaram a ser moeda de troca em vista de seu potencial para gerar retorno pecuniário.

Essa nova sociedade trouxe consigo questões relativas a vida intima de cada um, se o motor da economia é agora os dados do cidadão surge a necessidade de se revisitar o conceito de privacidade e do conteúdo dos direitos da personalidade para que se possa estabelecer limites quanto a coleta e tratamento desses dados para evitar lesões ao livre desenvolvimento do indivíduo e a sua dignidade.

Assim o direito em sua necessidade de acompanhar as mudanças da sociedade para que possa promover a harmonia social passa então a se preocupar com essa delimitação e proteção do indivíduo frente a novas tecnologias. Com isto surgiram regulações que buscaram promover a tutela dos dados pessoais.

Inicialmente é possível confundir a proteção dos dados pessoais como sendo apenas uma faceta do direito a privacidade, tendo em vista que dados pessoais são informações acerca do indivíduo. Porém percebeu-se que apesar da semelhança entre dados pessoais e privacidade o primeiro não poderia ser efetivamente protegido da mesma forma que o segundo, enquanto a tutela a privacidade pode ser considerada um direito de estar só se apresentando essencialmente na forma de liberdade negativa, a proteção a privacidade não pode se limitar a isto, a sua efetiva proteção perpassa pela liberdade positiva, sendo necessária a ação tanto do estado como do titular dos dados para que se possa efetivamente realizar a tutela dos dados pessoais.

Diante na necessidade de atuação do indivíduo inicialmente a comunidade europeia e seguindo seu exemplo o Brasil, as normas relacionadas a proteção de dados pessoais buscaram dar poder ao titular dos dados, para que ele tivesse condições de dispor de seus dados da forma com que lhe fosse conveniente. Partindo dessa ideia adotou- se então um paradigma de autodeterminação informacional, ou seja, a norma busca que o sujeito é aquele quem determina a forma e extensão de coleta, tratamento e compartilhamento de seus dados.

Para atingir essa autodeterminação informacional a ferramenta adotada pela legislação foi o consentimento. A norma adota o consentimento como principal meio

pelo qual o titular dos dados exerça seu controle acerca de suas informações, exigindo ainda alguns requisitos para a validade desta ferramenta. A norma brasileira, mais especificamente a Lei Geral de Proteção de Dados, adota como requisitos de validade do consentimento a necessidade deste ser livre, informado, específico e com finalidade determinada, ou seja, é preciso que este seja espontâneo, que o titular dos dados esteja devidamente informado acerca de seu ato, que o consentimento seja dado a uma finalidade conhecida e por fim que seja expresso.

Desse modo a legislação elevou o consentimento ao papel central na tutela dos dados pessoais, sendo usada tanto de forma preventiva (o titular dá o consentimento antes da coleta, tratamento ou compartilhamento) como de forma repressiva (com a retirada do consentimento para determinado ato).

Ocorre que, apesar do paradigma adotado pela norma, a autodeterminação informacional na prática não pode ser atingida apenas pela adjetivação do consentimento, pois a realidade apresenta situações em que o titular dos dados é na verdade um agente hipervulnerável em face dos outros atores da relação jurídica informacional, essa vulnerabilidade informacional, técnica e económica inviabiliza que o usuário tenha pleno controle sob suas informações.

Em face dessa assimetria se faz necessário a adoção de políticas e medidas que busquem equalizar o titular dos dados com as outras partes, empoderando assim o consumidor para que a autodeterminação informacional não seja exista apenas na norma, mas também na realidade.

Por fim, conclui- se que, apesar do consentimento ocupar um papel importante na proteção dos dados pessoais, ele, por si só, não tem capacidade permitir a autodeterminação informacional ao titular dos dados sendo necessário também a adoção de outras medidas para que o indivíduo tenha controle sob suas informações e possa efetivamente atuar na proteção deste bem jurídico permitindo assim seu livre desenvolvimento pessoal e protegendo sua dignidade.

REFERÊNCIAS

BIONI, Bruno. **Ricardo Proteção de dados pessoais: a função e os limites do consentimento**. – Rio de Janeiro: Forense, 2019.

BRASIL. **LEI Nº 12.414, DE 9 DE JUNHO DE 2011.** Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12414.htm. Acesso em 25 de maio de 2021.

BRASIL. **LEI Nº 12.965, DE 23 DE ABRIL DE 2014.** Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em 25 de maio de 2021.

BRASIL. **LEI Nº 8.078, DE 11 DE SETEMBRO DE 1990.** Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm. Acesso em 25 de maio de 2021.

BRASIL. **Constituição Federal de 1988.** Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 25 de maio de 2021.

BRASIL. **LEI Nº 13.709, DE 14 DE AGOSTO DE 2018.** Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em 25 de maio de 2021.

Bulos, Uadi Lammêngo; **Curso de Direito Constitucional** – 11. Ed.- São Paulo: Saraiva Educação, 2018.

CRANOR, Lorrie Faith; MCDONALD, Aleecia M.. **Beliefs and Behaviors**: internet users' understanding of behavioral advertising. Internet Users' Understanding of Behavioral Advertising. 2012. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1989092. Acesso em: 07 jun. 2021.

DIRECTIVA 2002/58/CE. 12 de julho de 2002. **Diretiva relativa à privacidade e às comunicações eletrônicas.** Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32002L0058. Acesso em: 20 jun. 2021.

HARDY, Quentin. **Rethinking Privacy in an Era of Big Data.** 2012. Disponível em: https://bits.blogs.nytimes.com/2012/06/04/rethinking-privacy-in-an-era-of-big-data/?_r=0. Acesso em 24 Maio 2021.

GAGLIANO, Pablo Stolze; PAMPLONA FILHO, Rodolfo. **Novo curso de direito civil - Parte geral - vol. 1** – 23. ed. – São Paulo: Saraiva Educação, 2021.

KOSINSKI, Michal; STILLWELL, David; GRAEPEL. **Thore. Private traits and attributes are predictable from digital records of human behavior**. 2013. Disponível em: https://www.pnas.org/content/110/15/5802. Acesso em 26 de mai. 2021

MAGRANI, Eduardo. **Entre dados e robôs: ética e privacidade na era da hiperconectividade**. —— Rio de Janeiro: Konrad Adenauer Stiftung, 2018.

OECD. **Guidelines on the Protection of Privacy and Transborder Flows of Personal** OECD Publications Service, 2011.*The OECD Privacy Framework. 2013*. Disponível em: https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf. Acesso em 20 de jun. 2021.

OECD. **THE OECD PRIVACY FRAMEWORK**. 2013. Disponível em: https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf. Acesso em: 25 maio 2021.

RINNE, Ulf, **Anonymous job applications and hiring discrimination**. IZA WORLD OF LABOR. 2018. Disponível em: https://wol.iza.org/articles/anonymous-job-applications-and-hiring-discrimination/long. Acesso em 25 de maio de 2021

WARREN, Samuel D.; BRANDEIS, Louis D. “The Right to Privacy”. *Harvard Law Review*, vol. 4, no. 5, 1890, p. 193–220. JSTOR. Disponível em: www.jstor.org/stable/1321160. Acesso em: 20 maio. 2021.