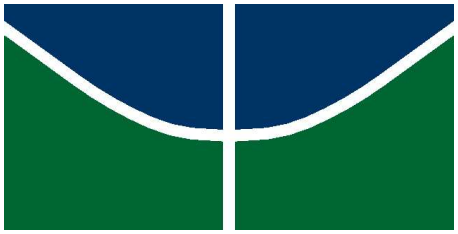


UNIVERSIDADE DE BRASÍLIA (UnB)

FACULDADE DE COMUNICAÇÃO (FAC)

PROGRAMA DE PÓS-GRADUAÇÃO (PPGCOM-FAC)

MARIAH SAMPAIO FERREIRA LUCIANO

COMUNICAÇÃO DIGITAL, PRIVACIDADE E A LEI BRASILEIRA DE PROTEÇÃO DE DADOS PESSOAIS: CARACTERÍSTICAS, CONCEITOS E PROCESSOS

Brasília

2020

MARIAH SAMPAIO FERREIRA LUCIANO

COMUNICAÇÃO DIGITAL, PRIVACIDADE E A LEI BRASILEIRA DE PROTEÇÃO DE DADOS PESSOAIS: CARACTERÍSTICAS, CONCEITOS E PROCESSOS

Dissertação apresentada ao Programa de Pós-Graduação da Faculdade de Comunicação Social da Universidade de Brasília como requisito parcial para a obtenção do grau de mestre em Comunicação e Sociedade.

Linha de pesquisa: Poder e Processos Comunicacionais

Orientador: Sivaldo Pereira da Silva

Brasília

2020

MARIAH SAMPAIO FERREIRA LUCIANO

COMUNICAÇÃO DIGITAL, PRIVACIDADE E A LEI BRASILEIRA DE PROTEÇÃO DE DADOS PESSOAIS: CARACTERÍSTICAS, CONCEITOS E PROCESSOS

Dissertação apresentada ao Programa de Pós-Graduação da Faculdade de Comunicação Social da Universidade de Brasília como requisito parcial para a obtenção do grau de mestre em Comunicação e Sociedade.

Linha de pesquisa: Poder e Processos

Orientador: Sivaldo Pereira da Silva

Aprovada em 13 de março de 2020.

Banca Examinadora:

Prof. Dr. Sivaldo Pereira da Silva (PPGCOM/UnB)
Orientador

Prof. Dr. Fernando Oliveira Paulino (PPGCOM/UNB)

Prof. Dr. Danilo Doneda (IDP)

AGRADECIMENTOS

As linhas que serão lidas por você a seguir foram escritas à base de muita resiliência. Elas foram capazes de questionar escolhas profissionais, acadêmicas e, até mesmo, pessoais. Todas essas palavras são resultado de uma persistência (e insistência) pessoal que, até então, eu desconhecia. Trata-se de uma pesquisa acadêmica intimamente ligada à um amadurecimento profissional e pessoal dessa estudante que vos escreve.

Porém, sabemos que todo trabalho acadêmico é fruto de uma rede de apoio e incentivo que é capaz de acolher tudo que descrevi acima. Eu tenho a minha rede, sempre firme, segura e acolhedora.

Por isso, agradeço, de todo o coração, e dedico não só esse trabalho final, mas todo o processo que o gerou:

Ao Meu Pai do Céu, Deus da minha vida, que me concede a graça de ser e de ter razão para continuar.

À Nossa Senhora, que abençoa cada caminho que eu penso em trilhar.

Aos meus amados Júlio Cesar, Walkiria e Igor, que compartilham comigo o cotidiano e a benção de viver em família.

Ao meu amor e amigo, Matheus, que tem o coração doce e leve, sempre capaz de acalmar a minha ânsia.

Aos amigos e amigas, íntimos ou ausentes, peças essenciais dessa caminhada e de cada bom momento vivido e que ainda há de se viver.

Ao meu querido orientador, Sivaldo Pereira, sempre capaz de compartilhar a sua imensidão de conhecimento.

À Umbelino Lobo e toda sua equipe, que sempre me encorajou e possibilitou meus estudos e hoje faz saudade. Ao deputado Leandro Grass e toda a sua equipe que me inspiram na construção de uma sociedade mais justa.

A todos que cruzaram meu caminho e que, de alguma forma, são partes de quem me tornei: cada linha escrita tem mais de vocês do que de mim.

RESUMO

A Sociedade da Informação é identificada pelo intenso fluxo de dados produzidos e consumidos pela população conectada na rede mundial de computadores, a internet. É neste contexto de ampliação do volume, da coleta e utilização de todos os tipos de dados que o presente trabalho se insere buscando contribuir para a formação do conhecimento acerca da proteção de dados pessoais. A Lei Brasileira de proteção de dados pessoais foi aprovada em 2018 e dentro do cenário da entrada em vigência da Lei Europeia. A escolha da metodologia Hermenêutica da Profundidade, ferramenta proposta por John B. Thompson (1998), considerou a complexidade de um processo legislativo de tramitação. O objetivo foi analisar todo o caminho percorrido pelo projeto de lei que resultou na Lei Brasileira de Proteção de Dados Pessoais considerando como guia principal a construção dos conceitos de dados sensíveis, dados anonimizados e consentimento. Através de um mapeamento dos diversos atores que participaram do processo de construção da lei e seus papeis, o trabalho elaborou um registro histórico e crítico do processo de elaboração da referida regulação, analisando qualitativamente a lei e o contexto político em questão. Com isso, o trabalho expõe a influência internacional na elaboração da lei e como o processo de implementação depende da criação de educação cultural em relação aos direitos à privacidade e à personalidade.

ABSTRACT

Information society is identified by the high flow of data production and consumption by the connected population at the World Wide Web – internet. This analysis inserts itself on the context of increase of volume, data collect and usage of all kinds of data, and it has the purpose to contribute to knowledge formation about personal data. The Brazilian General Law of Personal Data Protection ("Lei Geral de proteção de dados pessoais" – LGPDP) was approved in 2018 and connected with the application of the European law. The comprehension of the legislative process of approval for the legislation, with its focus on the concepts of sensible data, anonymized data and consent goes throughout different analysis based on the interpretation of the process of the original bill. The choice of the Depth Hermeneutic methodology, instrument presented by John B. Thompson (1998), was based on the complexity of the phenomenon to be studied. The research intends to do an analysis of the legislative experience of LGPDP, having the debate about the concepts of sensible data, anonymized data and consent as the main issues. Through the mapping of actors involved in the construction of the proposition and its roles, this work elaborates a historical and critical record of the process of approval for the legislation, examining qualitatively the law and the political context. The work exposes the international influence in this process of elaboration of the law, and the implementation depends on the cultural education to be developed in relation to privacy and personality rights.

LISTA DE ILUSTRAÇÕES

LISTA DE TABELAS

SUMÁRIO

1. INTRODUÇÃO

1.1 CONTEXTO E PROBLEMA DE PESQUISA

A definição dos conceitos de esfera pública e esfera privada e o entendimento das ações realizadas em cada espaço sempre foi objeto de discussão entre filósofos e sociólogos. A dicotomia entre essas esferas sociais é a base teórica para entendermos o impacto da cultura da privacidade e da exposição nas nossas vidas cotidianas. Esse entendimento perpassa pela compreensão não só das principais características das esferas, mas como as funções sociais daqueles que ocupam cada espaço. A narrativa histórica evidencia o protagonismo masculino nos espaços de discurso e de tomada de decisão. Mais do que isso, a vinculação econômica facultava o peso das decisões e da possibilidade de voto nas sociedades gregas. O desenvolvimento e a atualização da sociedade levaram esse debate para novos patamares, principalmente com o surgimento das Tecnologias da Informação e Comunicação e, consequentemente, da Sociedade da Informação. Com a popularização do uso da internet e a ampliação de serviços móveis e tecnológicos, a forma de viver foi influenciada intensamente.

Aplicativos para encontrar a melhor rota para fugir do trânsito, para monitorar a saúde, ou, até mesmo, a quantidade de calorias gastas em um único dia, tornou-se comum para a sociedade nos últimos dez anos. Com o advento da internet, os dados pessoais passam a exercer importâncias distintas das até então conhecidas, visto os diferentes usos de dados pessoais pela indústria da informação. Em uma perspectiva histórica, Doneda (2006), afirma que o Estado foi o primeiro a fazer uso de informações pessoais, justificado pela eficiência da administração pública ao ter conhecimento sobre a população gerida, exemplificado por censos e pesquisas. O autor relata que sem a internet, o uso de dados pessoais apresentava um custo elevado, o que limitava o uso de dados pelo governo. Com as alterações sociais provenientes do desenvolvimento da cibercultura, o mundo passou a discutir a proteção dos dados pessoais, visando o seu correto tratamento e proteção. Silva (2017) afirma que a dinâmica das relações sociais sofreu grande impacto com o "uso generalizado de bases de dados por cidadãos comuns" (SILVA, 2017, p.29)

A quantidade de informações e dados gerados a partir do intenso uso de tecnológicas alterou a forma com que empresa e o estado se relacionavam com toda essa matéria bruta. Vimos a consolidação de tecnologias que envolvem processos de *Big Data,* a datificação e os algoritmos. O armazenamento dessas informações somado ao que conhecemos como algoritmo

tornou possível o tratamento de grandes volumes e variedades de dados em alta velocidade, definindo-se assim *Big Data.* Segundo Mantelero (2016), a possibilidade de armazenamento e análise de grandes quantidades de dados, captados a partir do uso de tecnologias (aplicativos e *sites*, em sua maioria), permitem a identificação de padrões de comportamento em grupos, sejam eles quais for. Porém, as construções lógicas desses padrões perpassam por uma construção humana denominada "algoritmo". Estudiosos da programação, como Manzano e Oliveira (2016, p. 25) definem o termo como "regras formais, sequenciais e bem definidas a partir do entendimento lógico de um problema a ser resolvido por um programador com o objetivo de transformá-lo em um programa que seja possível de ser tratado e executado por um computador".

Todo esse contexto envolve alguns direitos sociais básicos como o Direito à Personalidade e à Privacidade. A tutela desses direitos ganhou desafios ao encarar esse fluxo informacional de dados e informações e a mercantilização desse novo produto. A última década foi marcada por um movimento internacional de busca por legislações coesas, detalhadas e uniformes que garantissem proteção aos usuários da internet e aos consumidores de mídias e que também não fossem capazes de coibir o desenvolvimento tecnológico que gera benefícios sociais, culturais e econômicos já vivenciados pela Sociedade da Informação.

Presenciamos a elaboração de leis que buscavam proteger os dados pessoas dos usuários da internet. Um movimento internacional que começou de maneira lenta, com normas que abordavam apenas alguns aspectos do arcabouço necessário para proteger os titulares dos dados armazenados a partir do uso da tecnologia. No entanto, casos de espionagem, vazamento de dados e pressão internacional, impulsionaram o movimento e elevaram o debate sobre a criação de normais gerais e específicas para a proteção de dados pessoais. A aprovação do Regulamento Geral de proteção de dados pessoais pela União Europeia em 2016 foi a grande impulsionadora das demais leis gerais de proteção de dados pessoais, inclusive da normativa brasileira.

Ainda sem legislação específica sobre o tema, apenas com leis esparsas e pontuais, a elaboração normativa sobre a proteção de dados pessoais era discutida no Congresso Nacional desde 2010. Em 2016, o Poder Executivo encaminhou o Projeto de Lei que posteriormente, em 2018, resultaria na Lei de proteção de dados pessoais.

1.2 OBJETIVO

O processo legislativo de elaboração da Lei Brasileira de proteção de dados pessoais, período que durou cerca de 2 anos, foi o principal objeto de estudo e análise do presente trabalho. A pesquisa analisou toda a tramitação da referida norma. O objetivo principal da pesquisa é a descrição, o mapeamento e a compreensão do processo de elaboração normativa da Lei Brasileira de proteção de dados pessoais, buscando inseri-la no plano mais amplo da política de regulação da comunicação digital no Brasil.

Como objetivos específicos, buscou-se:

a) Produzir um mapeamento dos diversos atores que participaram do processo de construção da lei e seus papeis;
b) Elaborar um registro histórico e crítico do processo de elaboração da referida regulação;
c) Produzir uma análise qualitativa da Lei Brasileira de proteção de dados pessoais em um formato comparativo com o Regulamento Geral de proteção de dados pessoais Europeu, além de elaborar um registro do contexto político no qual a lei foi elaborada, aprovada e regulamentada.

1.3 PARÂMETROS METODOLÓGICOS

A compreensão do processo de elaboração de uma legislação, tendo como eixo principal o debate em torno da definição dos conceitos de dados sensíveis, Dado Anonimizado e consentimento, perpassa por diferentes dimensões de análises baseadas na interpretação da tramitação do projeto de lei originário. A escolha da metodologia Hermenêutica da Profundidade, ferramenta proposta por John B. Thompson (1998), foi baseada na complexidade do fenômeno a ser estudado. Veronese e Guareschi (2006) afirmam que a Hermenêutica da Profundidade é caracterizada pela sua abrangência e completa interpretação dos objetos, por possuir etapas de análise complementares.

A partir dela, o pesquisador analisa os contextos sócio-histórico e espaço-temporal, realiza uma análise discursiva e reinterpreta os fatos com a base elaborada durante o processo. Os autores definem a metodologia elaborada por Thompson (1998) como uma leitura qualificada da realidade. A qualidade tanto elogiada por Veronese e Guareschi (2006) está presente na racionalidade da argumentação que a metodologia exige que o pesquisador aplique.

A interpretação dada ao fenômeno estudado deve ser referendada e, portanto, também deve assumir um caráter propositivo.

Uma vez que o objeto de pesquisa é uma legislação recente, ainda carente de processos normativos de regulamentação, a pesquisa buscou métodos complementares para elaborar uma descrição coerente e crítica da experiência legislativa de elaboração da norma analisada. Entender, não apenas o ambiente formal legislativo, mas os contornos políticos do debate da construção da legislação, tendo sempre como eixo os aspectos técnicos consentimento, dados sensíveis e dados anonimizados. A pesquisa realizou análise documental de todos o processo legislativo que resultou na Lei Brasileira de Proteção de Dados Pessoais. Foram analisadas as atas das Comissões Especiais e de Mérito, atas de Seminários realizados sobre o tema no Congresso Nacional e os discursos durante as votações no plenário da Câmara dos Deputados e do Senado Federal.

1.4 ESTRUTURA DA DISSERTAÇÃO

Com isso, como exposto por Pita (2017), a proteção dos dados pessoais não está somente na garantia da efetivação da legislação aprovada, mas no processo educacional da população brasileira sobre o mercado de dados pessoais e o risco iminente à privacidade. É nesse aspecto que a presente pesquisa buscou contribuir, ao detalhar a experiência normativa e debater a qualidade da Lei Brasileira de proteção de dados pessoais perante outras discussões internacionais. Dessa forma, a pesquisa está organizada em quatro partes. Em um primeiro momento, está apresentado o histórico do debate acadêmico sobre a privacidade e a proteção de dados pessoais como mecanismo para garantia de direitos fundamentais. Em seguida, o cenário internacional de ordenamentos jurídicos no qual a lei brasileira também se insere. Cumprindo-se do seu objetivo, em um terceiro momento da pesquisa, será mapeada a experiência de elaboração normativa da Lei Brasileira de proteção de dados pessoais, tendo como eixos os termos considerados chaves, que são "dados sensíveis, dados anonimizados e consentimento."

Em um momento final, uma breve comparação entre a Lei Geral de dados pessoais da União Europeia e a Lei Brasileira de proteção de dados pessoais. Essa comparação se fez importante e necessária, pois a principal constatação ao longo da análise realizada, foi que a Lei

Brasileira foi completamente influenciada e tendenciada à uma harmonização com a Lei Europeia.

2. PRIVACIDADE, COMUNICAÇÃO DIGITAL E DADOS PESSOAIS

O objetivo principal deste trabalho é evidenciar a relação entre dados pessoais e comunicação digital para compreendermos o processo de elaboração da Lei de proteção de dados pessoais - LGPD. No entanto, antes de adentrarmos nessa esfera, faz-se importante retomarmos a discussão histórica sobre privacidade. Essa discussão inicial se dará como base teórica para os capítulos seguintes. Nesse ponto, será apresentada a dicotomia entre público e privado e os debates em torno das teorias de Jurgen Habermas (2003). O entendimento sobre as esferas públicas e privadas será essencial para compreendermos a argumentação sobre direitos fundamentais que guia a tutela legislativa que se dá na LGPD. Em um segundo momento, a discussão sobre privacidade será vinculada aos eixos estruturantes do debate sobre comunicação digital e dados pessoais. Entenderemos como a garantia do direito à privacidade perpassa ao entendimento sobre algoritmos, Big Data e consentimento.

2.1 PRIVACIDADE EM PERSPECTIVA HISTÓRICA

A história da concepção de privacidade, como hoje a entendemos, está vinculada ao debate sobre o que é público e o que é privado. Em a *Mudança Estrutural da Esfera Pública*, Habermas (2003) apresenta uma análise histórica sobre a concepção das esferas pública e privada. Em um primeiro momento, o autor afirma que os termos "público" e "esfera pública" adquiriram uma pluralidade de significado. Porém, o foco do autor é demonstrar que desde a Grécia antiga, havia uma evidente separação entre as esferas pública e privada.

Habermas (2003) afirma que a esfera privada era edificada no *oikos,* ambiente familiar onde os componentes da família eram submetidos ao patriarca, aquele que mantinha a estrutura financeira e administrativa da esfera. Aqueles que dominavam a *oikos* e possuíam propriedades, poderiam participar da *polis*, espaço para tomada de decisões políticas, de apresentação pública e de discursos para seus pares. Ao falar sobre a sociedade medieval e feudal, Habermas (2003) destaca que as categorias postas na Grécia antiga já não faziam sentido na estrutura dessas sociedades. No período medieval, as relações de dominação não se davam mais pela esfera familiar. Para o autor, a dominação ocorria pelos direitos individuais de *jurisdictio,* sem perpassar pela divisão de *dominium* privado e *imperium* público.

No entanto, em todas as sociedades, o conceito de representatividade pública é fundamental para compreensão da dicotomia principal, do público e privado. Habermas (2003)

entende o conceito como uma "marca de *status* ou uma corporificação de um poder superior". A partir desse entendimento, o autor descreve a esfera pública burguesa, construída nas cidades e impulsionada pelo capitalismo mercantil. Forma-se, então, uma esfera civil oposta ao aparelho burocrático, um setor privado em oposição ao poder público. O primeiro sendo um espaço de troca de mercadorias e familiar e o segundo sendo uma sociedade administrativa e aristocrática.

Hannah Arendt, em *A Condição Humana*, retoma a dicotomia público e privado grega. Para ela, os seres humanos se diferenciam das demais espécies pela sua capacidade de comunicar a si mesmos, mais do que apenas comunicar algo. É, então, através do discurso e da ação que os homens manifestam a si mesmos, não apenas como objetos, mas como humanos. A manifestação do eu é a única coisa que os indivíduos não podem deixar de fazer sem que, se o fizerem, deixem de ser humanos – a vida sem ação e sem discurso não é uma vida humana (ARENDT, 2000, p.189).

Para Arendt, agir é tomar iniciativa, conferir movimento a algo; o próprio nascer do homem é uma tomada de iniciativa. Esta concepção, de início, vincula-se à ideia da criação do novo, um novo imprevisível. Se o homem é capaz de agir, significa dizer que ele é capaz de promover o improvável. Assim, a ação é "a efetivação da condição humana da natalidade". O discurso é, então, a distinção, a "efetivação da condição humana da pluralidade" (ARENDT, 2000, p. 190-191).

Ação e discurso se relacionam na medida em que os atos se revelam através da palavra e, ainda que possam ser percebidos somente através da ação, o que confere sentido a eles são as palavras, as quais, também identificam o ator, o agente do ato. Ação e discurso se necessitam mutuamente, é por meio deles que os humanos exprimem quem são, demarcam suas identidades e apresentam-se ao mundo humano. É na interação, na convivência entre os homens que a ação e o discurso apresentam seu caráter revelador, a capacidade de revelar quem são os indivíduos e onde eles se situam no mundo. Neste sentido, a noção de publicidade envolve a própria construção da noção de realidade.

Ao argumentar sobre a relação entre a ação e a vida comum, Arendt retoma as argumentações apresentadas desde Aristóteles até São Tomás de Aquino para indagar a interpretação dada ao social como político. A autora afirma que somente com a expressão "*a societas generis humani*" que o social foi apresentado como "condição humana fundamental" (ARENDT, 2000, p.33). Além disso, Arendt apresenta a argumentação grega de que a composição política é contrária à associação familiar, o pensamento grego entende que a

cidade-estado representa uma segunda vivência, complementar e diametralmente oposta à vida privada. Para Aristóteles, as atividades consideradas públicas seriam as ações e o discurso, já melhor apresentado acima. É o que se verifica do trecho a seguir em destaque:

> Agora cada cidadão pertence a duas ordens de existência; e há uma grande diferença em sua vida entre aquilo que lhe é próprio (idion) e o que é comum (koinon). Não se tratava de mera opinião ou teoria de Aristóteles, mas de simples fato histórico: precedera a fundação da polis a destruição de todas as unidades organizadas à base do parentesco, tais como a phratria e a phyle. (ARENDT, 2000, p.33)

A autora ainda defende que a formação histórica da esfera pública e política decorre da vida privada e familiar, visto que, para os gregos, os limites das propriedades privadas eram intocáveis, por garantirem ao homem participar dos negócios gerados na esfera pública. Ter uma propriedade familiar tornava possível e justificável a atuação do homem no ambiente público.

Nessa concepção de público e privado, Marilena Chauí (1992) afirma que os gregos e romanos romperam com a ideia de personificação do poder, onde toda a autoridade estava presente no governante. Para ela, eles inventaram a política, com a compreensão de que o poder existe através das leis, que eram postas através de uma vontade coletiva construída na *polis.* A autora destaca que a vontade coletiva possuía espaço de construção nas assembleias, através da discussão, da deliberação e do voto. Em outras palavras, os gregos submeteram o poder a um conjunto de instituições e práticas, criando assim, a esfera pública.

Por outro lado, o rompimento dessa personificação do poder permaneceu na esfera privada. O seu detentor, dentro da *oikos*, possuía toda e qualquer autoridade de acordo com a sua vontade. O chefe de família, o que detém autoridade do espaço privado, é reconhecido como *despostes.*

Ao entendermos a dicotomia entre o que é público e privado, adentramos também na discussão sobre o direito à privacidade dentro do que é privado. Para Doneda (2006), a origem da discussão sobre privacidade está presente no clássico embate entre a esfera pública e privada.

Para os gregos, a publicidade é o espaço da vida pública onde se constrói a realidade e o próprio sentido da *polis* e da noção de igualdade entre pares (entre iguais) e a noção de privado é considera primária (mas não prioritária) pois embora a vida privada (bens, escravos, negócios etc.) permita que o cidadão atuasse na vida pública (na polis) o privado é visto como algo menor

(é como "comer", comer é primário pois sem comida não vivemos mas é menor num contexto de vida pública). Para os gregos, o Estado é algo maior (pois se vincula à noção de público) e o privado está subordinado a este.

Para os liberais, como Alan Westin (1968), há uma mudança importante: privacidade passa a ter uma relevância perante à coisa pública, principalmente em relação ao Estado, não como uma coisa menor, mas como uma algo primordial, cara ao liberalismo político: a liberdade do indivíduo. Na perspectiva liberal, há o medo do Estado totalitário opressor que dita a vida privada e faz com que o privado seja relevante. Assim, passam a considerar o privado como um direito a ser preservado à semelhança à ideia do direito à propriedade. Com isso, o público e o Estado têm restrições para agir na vida privada (não pode entrar na casa de alguém sem um mandado judicial; não pode violar o sigilo bancário senão por autorização judicial; não pode filmar a vida íntima do vizinho, por exemplo).

Diante disso, o que Carole Pateman (1993) contesta em sua obra *O contrato sexual* (e essa é a tônica da crítica feminista) é que essa "preservação" do privado frente ao Estado (público), típica do liberalismo, também gerou um *locu* autoritário patriarcal que é o "privado", onde as leis são suspensas e onde a mulher é a parte mais oprimida. Enquanto o privado é o lar, a família e a mulher, do outro lado, o público é a comunidade política, o patriarcal, o homem.

A argumentação inicial entre o público e privado reforça a esfera pública como arena masculina. É em cima desse ponto que Pateman (1993) apresenta críticas feministas à essa dicotomia, afirmando que a divisão entre o público e o privado exige um entendimento maior do que apenas a distinção entre as atividades de cada esfera, uma vez que a história de construção da sociedade civil e do direito político, por meio do contrato social, é repleta de hipóteses e meias verdades. Segundo Pateman (1993), a teoria do contrato social determina que as relações livres assumem uma forma contratual, ocultando questões acerca do contrato sexual, apresentada pela autora como base argumentativa.

Segundo a autora, o contrato original é composto não somente por aspectos sociais como exposto por autores clássicos do tema. É um contrato sexual-social, afirmando que o foco do contrato sexual é a gênese do direito político. Entretanto, o contexto em torno do contrato social afirma o direito político como direito patriarcal. O contrato social afirma liberdade plena para os indivíduos, porém, segundo a autora, essa ideia é falsa, pois trata de subordinação, e a liberdade civil não pertence a todos, trata-se de um direito masculino concedido por uma sociedade patriarcal composta por contratos que impõem subordinação e dominação, como o

contrato matrimonial e trabalhista. Por exemplo, a mulher possuía papeis sociais definidos dentro das estruturas estabelecidas, como a função materna e cuidadora do lar ao firmar o contrato matrimonial.

Para Pateman (1993), "As mulheres não têm um papel no contrato original, mas elas não são deixadas para trás no estado natural, as mulheres são incorporadas à uma esfera separada da civil" (PATEMAN, 1993, p.27). A oposição entre a esfera pública e privada, para a autora, é mais uma expressão das divisões do contrato sexual, porém a associação não está contida apenas na esfera privada, o patriarcado está presente na sociedade como um todo. "Os homens passam de um lado para o outro, entre a esfera privada e pública, o mandato da lei do direito sexual masculino rege os dois domínios" (PATEMAN, 1993, p.26-35).

A autora realiza críticas à concepção liberal de esfera pública e privada de Benn e Gauss (1983), autores que trabalharam em clássica definição do público e privado. Segundo os autores, essas esferas são opostas e possuem nichos distintos de pautas. Para ela, os autores falham ao colocar o público como oposição ao privado, e não ao político.

> A maneira em que mulheres e homens são situados de forma diferenciada dentro da vida privada e do mundo público é, como indicarei, uma questão complexa, mas, subjacente a uma realidade complicada, há a crença de que as naturezas das mulheres são tais que elas são devidamente submetidas aos homens e seu lugar é na esfera doméstica e privada. Os homens corretamente habitam as duas esferas e tomam as decisões no âmbito delas. O argumento feminista essencial é de que a doutrina "separados, mas iguais" e o individualismo e o igualitarismo ostensivos da teoria liberal obscurecem a realidade patriarcal de uma estrutura social de desigualdade e a dominação das mulheres pelos homens (PATEMAN, 1993, p.57)

A crítica ao liberalismo ocorre principalmente à base teórica proveniente do Segundo Tratado de Locke. Pateman (1993) compreende que a divisão que o filósofo faz entre o familiar e o político também é sexual, já que o Tratado afirma que as diferenças naturais entre os gêneros justificam a submissão das esposas aos maridos e a concentração do poder político para os homens detentores de propriedade privada. A autora afirma que a família é estruturada por vínculos afetivos e "na condição sexualmente definida de esposa e marido (mãe e pai)", e a participação na vida pública estruturada e garantida por parâmetros e critérios liberais empregados somente aos homens (PATEMAN, 1993, p.58). A vida pública tão caracterizada por Pateman (1993) como espaço de poder e domínio masculino é evidenciada pela distinção descrita por Habermas (1997), visto que as mulheres não pertenciam efetivamente à nenhuma das esferas.

A argumentação de Habermas (1997) sobre a definição da esfera pública é estruturada no viés da comunicação que se constitui em um espaço social, de onde surge uma opinião pública. Esta, por sua vez, não é a soma da opinião de diferentes indivíduos: trata-se de um processo de conflitos e discursos que produzem, como resultado, a opinião pública. Esta se traduz em influência, a qual está sempre em disputa na esfera pública.

Habermas (1997) explica o conceito de sociedade civil, definindo-a como grupos que 'filtram' questões sociais provenientes da esfera privada, passando-as para a esfera pública. São estes grupos, então, que sustentam as estruturas comunicativas da esfera pública. Ressalta-se que a sociedade civil não é autônoma, mas autolimitada, especialmente pelas razões que se seguem: (1) há formas de vida (racionalidades) concebidas, que devem ser seguidas; (2) não é possível à sociedade civil exercer poder político, apenas influência política; e a sociedade civil pode transformar apenas a própria sociedade civil, quanto ao sistema político, pode apenas influenciar indiretamente.

O conceito de privacidade, segundo Danilo Doneda (2006), evolui em consonância com o desenvolvimento da arquitetura e da estratificação social, fatores que fortaleceram a divisão da sociedade em classes. Com isso, a "proteção" da privacidade do indivíduo em sociedade assume contornos que a levam para a judicialização, processo não identificado em nenhuma doutrina até o século XIX. Passos (2017) afirma que, segundo Paulo José da Costa Júnior, historicamente a França foi o primeiro país a judicializar a privacidade. O caso apresentado pelo autor ocorreu o Tribunal Civil de Sena em 1858, em razão da venda de uma obra de arte sem consentimento da modelo, eis que havia falecido.

Embora os gregos tenham conseguido delimitar as definições de público e privado, ligadas à ideia de propriedade, a doutrina que definiu o conceito contemporâneo de privacidade é relativamente recente. Como contextualiza Silva (2017), isso está diretamente vinculado ao surgimento da comunicação de massa, principalmente a partir do século XIX quando o jornalismo industrial tencionava as fronteiras entre publicidade e privacidade

É neste contexto que a Doutrina Jurídica considera o artigo *The right to privacy*, escrito por Samuel Warren e Louis Brandeis (1984), o marco acadêmico para o conceito contemporâneo de Privacidade. O trabalho dos autores foi relatar a atuação da mídia sensacionalista no rompimento das esferas do sigilo e do segredo de pessoas célebres. A denúncia das práticas invasivas foi fundamental para a consolidação do conceito *inviolate personality.*

> Instantaneous photographs and newspaper enterprise have invaded the sacred precincts of private and domestic life; and numerous mechanical devices threaten to make good the prediction that "what is whispered in the closet shall be proclaimed from the housetops." For years there has been a feeling that the law must afford some remedy for the unauthorized circulation of portraits of private persons; (WARREN; BRANDEIS, 1984 [1890], p. 76).

Os autores argumentaram pela garantia do direito de ser deixado em paz (*right to be alone*) ou "de ser esquecido", vinculados à garantia dos direitos individuais fundamentais, como o direito à vida e à propriedade. A evolução das Tecnologias de Comunicação e Informação proporcionaram, diretamente ou indiretamente, também uma evolução no debate sobre a garantia dos direitos individuais fundamentais em novos contextos sociais até então desconhecidos.

Com o advento da internet, os dados pessoais passam a exercer importâncias distintas das até então conhecidas, visto os diferentes usos de dados pessoais pela indústria da informação. Em uma perspectiva histórica, Doneda (2006), afirma que o Estado foi o primeiro a fazer uso de informações pessoais, justificado pela eficiência da administração pública ao ter conhecimento sobre a população gerida, exemplificado por censos e pesquisas. O autor relata que sem a internet, o uso de dados pessoais apresentava um custo elevado, o que limitava o uso de dados pelo governo. Com as alterações sociais provenientes do desenvolvimento da cibercultura, o mundo passou a discutir a proteção dos dados pessoais, visando o correto tratamento e proteção de dados pessoais.

Doneda (2006) afirma que a necessidade de unificar as regras que regem a proteção de dados pessoais é posta antes da internet ser o que é hoje. Discorre que a discussão Europeia sobre o referido tema teve início em 1995, em razão da diferença na maneira com que os países da União Europeia judicializavam o tema. Porém, o tema emerge na Sociedade da informação quando a tutela da personalidade do indivíduo é necessária para proteção contra tratamentos indevidos dos dados gerados.

Segundo Mendes (2014), a complexidade da vida em comunidade, a burocracia e o uso das Tecnologias da Informação justificam a intensa produção de dados pessoais. A autora exemplifica a informação citando alguns bancos de informações pessoais públicas como Registro de Nascimento, Casamento, Escolares, Formulários hospitalares e outros. Com isso, afirma que "as informações pessoais se constituem em intermediários entre a pessoa e a sociedade, a personalidade de um indivíduo pode ser gravemente violada com a inadequada

divulgação e utilização de informações armazenadas a seu respeito." (MENDES, 2014, p.30) A proteção dos dados pessoais é justificada pela tutela e garantia do direito à personalidade, aqueles considerados essenciais para, além da identificação do indivíduo, possibilitar a individualização dentro do convívio social. Passos (2017) descreve que o Direito à personalidade abrange três categorias dogmáticas do direito: a do Direito Físico, do Direito Psíquico e do Direito Moral.

O intenso fluxo de dados e informações colocou a privacidade e a personalidade do indivíduo em eminente risco visto a monetização dessas informações. A economia dos dados do Século XXI exigiu dos movimentos sociais, dos grupos de interesses e das instituições um movimento de debate sobre a garantia de proteção dos indivíduos sem que haja um retardado na evolução tecnológica.

2.2 INTERNET, ALGORITMOS E BIG DATA: DIMENSÕES POLÍTICAS E A PERSPECTIVA DOS DIREITOS

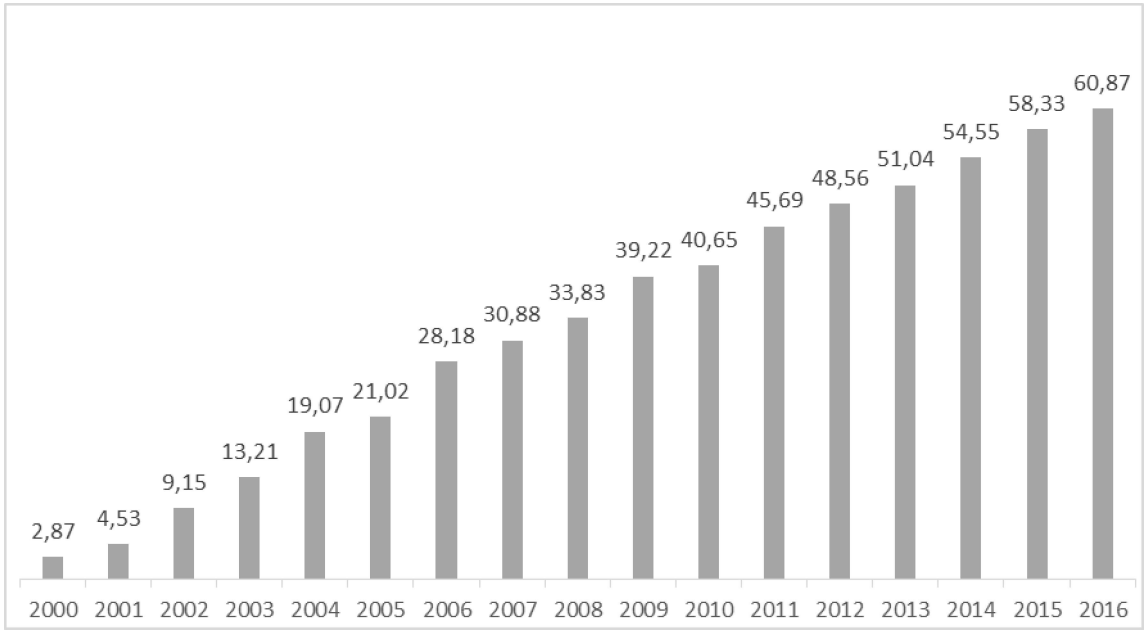
Em 2017, o aplicativo *Whatsapp*, da empresa *Facebook Inc*, divulgou que possui cerca de 1,2 bilhões de usuários ativos, dos quais 120 milhões são brasileiros. Da mesma empresa, o aplicativo *Facebook Messenger* possui o total de 2,047 bilhões de usuários ativos, dos quais 123 milhões são brasileiros (6% dos usuários totais. 3º lugar, atrás dos EUA e Índia). No mesmo ano, o aplicativo *Telegram*, da empresa *Telegram Messenger LLP*, afirma possuir 200 Milhões. Segundo a ONU, em 2017, a população mundial atingiu 7,6 bilhões de habitantes[1].

Embora os números apresentem um uso generalizado de aplicativos digitais, isso não significa que há uma inclusão universalizada. Em países como o Brasil, há importantes assimetrias tanto no acesso quanto no uso de sistemas digitais online. Para Levy (1999), os avanços nos sistemas de comunicação sempre geram alguma exclusão social. Em uma breve ilustração, o autor realiza uma comparação com o advento da televisão quando, em seu início, se estabeleceu como um sistema de comunicação caro e excludente, que se popularizou apenas posteriormente. Nesse sentido, afirma que a análise não deve estar nos números presentes e absolutos, mas na tendência de absorção do novo sistema de comunicação. Conforme a

[1]Disponível em: < https://news.un.org/pt/story/2017/06/1589091-populacao-mundial-atingiu-76-bilhoes-de-habitantes>; Acesso em: 11 de fevereiro de 2020.

Ilustração 1, a tendência de conexão dos Brasileiros corrobora, de certo modo, a compreensão de Levy (1999).

Figura 1: Gráfico sobre evolução do número de Brasileiros usuários da internet
(Fonte: Produzido a partir de dados em IBGE, 2016)



Ainda que a o acesso à rede seja ascendente, a inclusão digital deve ser abordada com cautela, para evitar o senso comum de que estar conectado é ser incluído digital.

De todo modo, o acesso à internet tem se tornado uma realidade e já aparece em diversos documentos como um direito social e à comunicação. Este direito de acesso também coincide com a produtividade em escala crescente de dados, assim como o estabelecimento de novas formas de interação social, advento do desenvolvimento tecnológico. Com isso, o uso de aplicativos de mensagens instantâneas e outros meios que possibilitam o armazenamento de dados já é uma realidade global entre aqueles considerados incluídos digitais, apesar das assimetrias existentes. Os aplicativos de mensagens instantâneas possuem uma política de privacidade que é apresentada aos usuários ao início de sua utilização. Esses termos de privacidade apresentados trazem pedidos de autorização e de uso das informações coletadas. São verdadeiros contratos de troca e venda que não evidenciam o real valor da ação. Quando

socialmente os aplicativos facilitam o cotidiano, o consentimento com os termos da política de privacidade dos aplicativos não é visto com tanto critério.

Aplicativos para encontrar a melhor rota para fugir do trânsito, para monitorar a saúde, ou, até mesmo, a quantidade de calorias gastas em um único dia, tornou-se comum para a sociedade nos últimos dez anos. Silva (2017) afirma que a dinâmica das relações sociais sofreu grande impacto com o "uso generalizado de bases de dados por cidadãos comuns" (SILVA, 2017, pg.29)

A argumentação do autor é sustentada pela afirmação de que a relação da sociedade com os meios de comunicação foi alterada durante o último século. Segundo Silva (2017), essa relação, no século XX, se dava *com* os meios de comunicação, principalmente televisão e rádio. O advento da internet trouxe o vínculo entre pessoas e meios de comunicação para uma perspectiva do *através.* O uso da tecnologia estabeleceu uma dependência na prática de hábitos cotidianos. Como exposto, atividades comuns como dirigir passaram a implicar o uso de aplicativos de instrução de navegação e trânsito, por exemplo.

O uso generalizado dessas ferramentas acarretou numa crescente onda de digitalização da informação e de datificação dos processos de comunicação. Para Silva (2017), "os indivíduos se transformaram, na prática, em produtores diários de *inputs* que alimentam diversos sistemas de captação de informação" (SILVA, 2017, p. 29).

Para Lemos (2003) um dos resultados da associação entre a cibercultura e a tecnologia são as novas formas de sociabilidade e vínculos associativos, causando alteração na percepção temporal e espacial determinada pela velocidade, pela "ubiquidade" e pela conectividade generalizada e quase permanente.

Thompson (2011) também se refere aos meios de comunicação como catalisadores da produção informacional, mais além, que permite o desenvolvimento de novas maneiras de interação, convívio e relacionamento social. Nesse sentido, voltando para a categorização "Interação mediata" apresentada por Thompson (2011), é possível reconhecer na sociedade atual o uso de aplicativos de mensagens instantâneas como um dos principais meios de comunicação. Para Thompson (2011), "Interação mediata" é aquela em que "os indivíduos podem interagir uns com os outros ainda que não partilhem do mesmo ambiente espaço temporal." (THOMPSON, 2011, p. 119).

O armazenamento dessas informações, somado ao que conhecemos como algoritmo, tornou possível o tratamento de grandes volumes e variedades de dados em alta velocidade,

definindo-se assim *Big Data.* Segundo Mantelero (2016), a possibilidade de armazenamento e análise de grandes quantidades de dados, captados a partir do uso de tecnologias (aplicativos e sites, em sua maioria), permitem a identificação de padrões de comportamento em grupos, sejam eles quais for. Porém, as construções lógicas desses padrões perpassam por uma construção humana denominada "algoritmo". Estudiosos da programação, como Manzano e Oliveira (2016, p. 25) definem o termo como "regras formais, sequenciais e bem definidas a partir do entendimento lógico de um problema a ser resolvido por um programador com o objetivo de transformá-lo em um programa que seja possível de ser tratado e executado por um computador". Em sua argumentação, Silva (2017) conceitua "algoritmo" a partir da visão técnica do autor Uricchio (2017), que coloca o termo como sendo um "conjunto de regras geralmente expressas em notação algébrica" (p.33).

A popularização da internet, somado à criação da microinformática (celular, *tablets* ou relógios), colocaram o uso de algoritmo como mecanismo de mediação nos processos de comunicação digital. Mas a sua existência está vinculada a construção de máquinas de calcular e decodificadoras utilizadas na II Guerra Mundial, muito anterior e diferente ao que vivenciamos na internet atualmente, como descrito pelo autor.

Apesar de ser um defensor da potencialidade da tecnologia, Silva (2017) entende que a utilização de *Big Data* e de algoritmos coloca em risco alguns "parâmetros democráticos, como liberdade, autonomia e direitos" (SILVA, 2017, pg.30).

Assim como Mantelero (2016), o autor afirma que os *Big Datas* são capazes de produzir informações valiosas sobre hábitos e padrões sociais. A dataficação possibilita traçar possíveis tendências sociais, com potencial de prever fatos e evitar danos, além de auxiliar nas tomadas de decisões e articulações políticas. Nesse sentido, Galloway (2004) afirma que os processos programados que guiam a coleta de dados e a interação máquina-usuário são capazes de influenciar as relações sociais.

Em reportagem ao jornal Nexo, Dias (2016) afirmou que os aplicativos de monitoramento de ciclos menstruais chegam a capturar dados de 5 milhões de mulheres ao redor do mundo, conseguindo vender esses dados para empresas de planos de saúde ou de *marketing* pessoal, possibilitando ações mais efetivas e estratégicas dessas empresas. A

reportagem afirma que as empresas detentoras dos dados fazem negócio com até 70 outras empresas.[2]

Nesse aspecto, Silva (2017) argumenta que deter esse conjunto de dados e informações sobre as pessoas é uma forma de poder.

> "Quando esse poder passa a servir prioritariamente à lógica de mercado, ou às distorções do papel da autoridade estatal, ou ainda à produção de conhecimento eticamente contestável baseado na coleta de informações pessoais, isso afeta a autonomia dos sujeitos e favorece o acirramento de desigualdades, trazendo à tona diversas implicações políticas" (SILVA, 2017, pg.35).

O tratamento de dados pode incorporar tendências culturais, julgamentos e valores sociais que reproduzem preconceitos e discriminações enraizadas na sociedade, afirma o autor. A fonte que gera todas essas informações é humana e, por isso, dotada de questões sociais e valores culturais que são independentes e indiferentes ao algoritmo aplicado. Considere o mesmo exemplo apresentado anteriormente para entendermos a influência que o tratamento de dados pode ter nas práticas sociais. Ao identificar tendências sexuais das mulheres de uma região, a oferta de medicamentos ou de plano de saúde pode ter sua variação de preço considerando esses fatores. Nas regiões onde há mais incidência de doenças sexualmente transmissíveis ou há registro de um menor uso de preservativos, as empresas podem otimizar a oferta desses serviços e produtos ao analisarem os dados obtidos.

Silva (2017) exemplifica o debate com o processo automatizado que bancos utilizam para fornecer empréstimos e facilitações dos serviços bancários. Afirma que a construção da sociedade brasileira está intimamente relacionada à escravidão dos povos negros e indígenas. O racismo estrutural presente em toda história brasileira coloca a população negra, estatisticamente, nas esferas sociais com menor acesso aos estudos ou em subempregos. A situação oposta se sustenta: pessoas brancas, historicamente privilegiadas, são melhores avaliadas por indicadores financeiros. O que Silva (2017) argumenta é que os cruzamentos estatísticos utilizando *Big Data* podem reforçar essas discriminações sociais enraizadas, já que não consideram outros fatores para além do banco estatístico gerado. Com isso, a possibilidade de bancos disponibilizarem empréstimos considerando fatores sociais que, em sua maioria,

[2] Disponível em: < https://www.nexojornal.com.br/expresso/2016/10/03/Os-aplicativos-sobre-os-ciclos-menstruais-e-a-exposi%C3%A7%C3%A3o-de-dados-pessoais-das-usu%C3%A1rias> Acessado em: 10 de out. de 2019

estão vinculados com fatores raciais históricos e discriminatórios é enorme, resultando na menor oferta de crédito aos negros.

Mantelero (2016) utiliza outro exemplo para discorrer sobre a dimensão política presente no uso indiscriminado de *Big Data.* O autor cita as ações de prevenção policial considerando a antecipação de crimes por software. O aplicativo *PredPol* cruza dados de denúncias policiais para indicar regiões que possuem a maior probabilidade de ocorrer um crime. Com isso, a polícia local é destinada a fazer prevenção dessa região ou bairro indicado, em decorrência de outros. De fato, a tecnologia pode evitar muitos danos sociais e, nesse caso, otimizar o trabalho da polícia. No entanto, Mantelero (2016) argumenta que

> A consequência dessas soluções de software é um potencial discriminação geográfica, que pode não afetar diretamente os indivíduos, mas tem um impacto nas comunidades locais em termos de estigma social ou fornecimento inadequado de serviços policiais. Nesse sentido, existe um interesse coletivo no uso correto e preciso dos dados.[3] (MANTELERO, 2016, p.3)

Além da discriminação, o autor expõe que a indução e a homogeneização podem ser dimensões políticas do *Big Data.* Em 2014, uma pesquisa realizada pela Intel demonstrou que 81% dos brasileiros se dispõe a trocar seus dados por serviços públicos de mais qualidade. "O mesmo estudo aponta que "84% dos participantes estariam dispostos a deixar que um sistema inteligente pudesse escolher as melhores rotas para todos" (CAPELAS, 2014)[4]. Silva (2017) reconhece indução como sendo o direcionamento de escolhas e possibilidades para o cidadão, reduzindo, cada vez mais, as suas possibilidades ou a clareza de informações.

Esse cenário nos leva a outro debate, vinculado às dimensões políticas e perceptivas dos direitos: a vigilância. A capacidade tecnológica que possuímos de controlar, monitorar, vigiar e armazenar é inquestionável e, cada vez mais, rentável e estratégica. Ter controle sobre hábitos, tendências e fenômenos sociais é interessante não só para o mercado, mas para governos. Em 2016, Simões e Correa escreveram uma reportagem sobre um relatório elaborado pela Eletronic Frontie Foundation (EFF).[5] O material analisava as práticas de vigilância em países da América Latina. Os autores do relatório afirmam que o anonimato é importante para garantia de direitos, como a liberdade de expressão e privacidade, de minorias. Nesse sentido, criticam que o estado

[3] Tradução própria do original em inglês.
[4] Disponível em: <https://link.estadao.com.br/noticias/geral,brasileiros-trocariam-privacidade-por-qualidade-de-vida,10000031639.> Acessado em: 06 de dez. de 2019
[5] Disponível em: < https://apublica.org/2016/10/relatorio-brasil-vigia-cidadaos-sem-qualquer-escrutinio-publico/> Acessado em: 17 de ago. de 2019

brasileiro não permite o anonimato na internet e ainda possui práticas de controle de registro telefônicos e de sigilo de informações públicas.

Bruno (2008) define vigilância digital como um "monitoramento sistemático, automatizado e à distância de ações e informações de indivíduos no ciberespaço, com o fim de conhecer e intervir nas suas condutas ou escolhas possíveis" (BRUNO, 2008: p.11). A autora ainda coloca que mecanismos de vigilância digital podem ser reconhecidos a partir de alguns componentes, sendo esses o monitoramento de ações, informações e comunicações dos indivíduos no ciberespaço, a montagem de bancos de dados e a elaboração de perfis computacionais.

O armazenamento de dados, um dos processos do *Big Data,* só ganha relevância e aplicabilidade a partir de cruzamentos, análises e classificações a fim de reconhecer práticas, tendências e comportamentos individuais ou coletivos. São esses dados, gerados por indivíduos a partir da sua relação com a internet e dispositivos, que geram um intenso debate sobre privacidade.

2.3 DEBATES E CONCEITOS-CHAVES SOBRE PROTEÇÃO DE DADOS PESSOAIS NA ERA DA COMUNICAÇÃO DIGITAL

Segundo Doneda (2006), a discussão de proteção de dados pessoais está vinculada à privacidade e à preocupação com a sua tutela, debates que são característicos da atualidade. Não é recente o entendimento da privacidade e de sua aplicação na vida em sociedade. O que fomenta a preocupação com a sua tutela é o reconhecimento da privacidade como delimitador de individualidades nas relações sociais. E, considerando o surgimento das Tecnologias de Informação e Comunicação – TICs e a sociedade cada vez mais *online*, é perceptível o aumento, em volume e intensidade, das relações sociais. Com o advento da internet, os dados pessoais passam a exercer importâncias distintas das até então conhecidas, visto os diferentes usos de dados pessoais pelo Estado ou não.

Doneda (2006) coloca que a "importância da informação aumenta à medida que a tecnologia passa a fornecer meios para transformá-la em uma utilidade" (DONEDA, 2006, p. 448). Em uma perspectiva histórica, o autor afirma que o Estado foi o primeiro a fazer uso de informações pessoais, justificado pela eficiência da administração pública ao ter conhecimento sobre a população gerida, exemplificado por censos e pesquisas. Doneda (2006) relata que sem

a internet, o uso de dados pessoais apresentava um custo elevado, o que, segundo o autor, limitava o uso de dados pelo governo. Com as alterações sociais provenientes do desenvolvimento da cibercultura, o mundo passou a discutir a proteção dos dados pessoais, visando o correto tratamento e proteção de dados pessoais.

Quando Pierre Levy (1999) afirma que o desenvolvimento tecnológico geraria uma exclusão radical daqueles que não participam ativamente, podemos refletir se há espaço para o cidadão não pertencer aos novos meios de comunicação caso não queira consentir com o uso dos seus dados pessoais. Nesse sentido questiona-se se existe a possibilidade de consentir quando a não utilização dos novos meios de comunicação é onerosa e excludente.

A cultura brasileira está vinculada à cultura da exposição. A população possui pouco ou nenhum conhecimento sobre a proteção dos dados pessoais e abrem mão da sua privacidade por barateamento de serviços ou facilitações, dando, por muitas vezes um consentimento tácito. Portanto, se faz necessário um debate sobre a proteção e a tutela dos dados pessoais, como defendido por Pita (2017).

Mendes (2014) inicia a sua descrição do o processo de construção do Direito à Privacidade, citando o emblemático artigo de Warren e Brandeis, "*the right to be alone*" que argumenta sobre o direito de ser esquecido, como marco desse processo. O artigo é considerado um marco pois relaciona o Direito à Privacidade à garantia da personalidade, questionando a relação com a propriedade privada que era até então posta. Mendes (2014) observa que a origem do Direito à Privacidade se dava em uma esfera extremamente individualista, "como a exigência absoluta de abstenção do Estado na esfera privada individual para a sua garantia. (MENDES, 2014, p..29)

A autora afirma que o século XX ficou caracterizado como o tempo de reinvenção da privacidade. Para ela, a revolução tecnológica somada à transformação da função do Estado, alavancou o debate sobre direito à privacidade. Mendes (2014) expõe que houve uma transição em como o Direito à Privacidade era visto na doutrina jurídica e também socialmente. Antes, havia uma conotação negativa e "egoísta" focada na posse de propriedades privadas e no seu domínio estratégico de bens. A transformação a qual a autora se refere corresponde ao controle do indivíduo sobre as suas próprias informações, mudança essencialmente democrática trazida pela ascensão da tecnologia.

Bioni (2019) apresenta o conceito de personalidade para argumentar que nome, honra, integridade física e psicológica compõem a extensão do indivíduo perante à sociedade. E se está atrelado a uma pessoa, deve ser adjetivado como pessoal para garantir a tutela dessa

extensão como é feito com o seu titular. (p.65) “Hoje vivemos em uma sociedade e uma economia que se orientam e movimentam a partir de signos identificadores do cidadão. Trata-se de um novo tipo de identidade” (BIONI, 2019, p.65).

O autor vai além na sua argumentação para firmar a importância da tutela jurídica frente aos novos desafios tecnológicos. Para ele, é direito do cidadão assegurar que a projeção das suas informações pessoais seja fidedigna à sua personalidade, para que não haja distorção de dados no processo de tratamento. Por isso, argumenta que a proteção de dados pessoais está vinculada aos diversos direitos fundamentais, como o da Privacidade e o da Personalidade, a teor do que está disposto no art. 5º da Constituição Federal.

Essa transformação gerou uma movimentação internacional em busca de uma tutela jurídica sobre o que se definia como dados pessoais. A proteção dos dados pessoais se tornou emergencial, pois os dados passaram a ser entendidos como uma extensão da personalidade individual de cada usuário e a privacidade como garantia de outros direitos fundamentais.

Com o avanço tecnológico, informações sobre indivíduos passaram a ser armazenadas em maior quantidade. Fez-se então necessário proteger as informações pessoais e a privacidade frente ao armazenamento em massa que se estabelecia. A Década de 70 foi marcada pelas primeiras legislações, decisões judiciais e acordos internacionais que visavam a proteção aos dados pessoais. Nesse aspecto, Mendes (2014) afirma que “dados pessoais são uma projeção da personalidade do indivíduo e, considerando o Direito à privacidade, precisam de tutela jurídica” (p.29).

Nesse sentido, Doneda (2006) argumenta que o entendimento sobre a tutela do Direito à Privacidade é característica de uma sociedade contemporânea. O autor afirma que a noção de privacidade esteve presente na história da humanidade, porém assumindo diversos sentidos e interpretações. Para os autores, o ordenamento jurídico não cabia na concepção privatista e de viés patrimonialista em sociedades que o Direito à Privacidade era pertencente a “extratos sociais bem determinados” (DONEDA, 2006, p.6)

Porém, com a alteração do conceito de privacidade e com o processamento eletrônico dos dados nas administrações públicas, a década de 70 do século XX vivenciou uma reação jurídica às essas transformações respectivas transformações sociais. Mendes (2014) cita como sendo as primeiras normas de proteção de dados pessoais:

> As leis do Estado alemão de Hesse (1970), a Lei de Dados da Suécia (1973), o Estatuto de proteção de Dados do Estado alemão de

> Rheinland-Pfalz (1974) e a Lei Federal de proteção de Dados da Alemanha (1977). Nos EUA, foram aprovados nesse mesmo período o *Fair Credit Reporting Act* (1970) e o *Privacy Act (1974)* (p.30)

A década de 70, outrora referida, foi emblemática, visto que nesse período passou a ser possível armazenar, processar e utilizar informações pessoais. Cabe analisar que o problema da exposição ou da perda de privacidade saía do nicho das pessoas de grande relevo social e chegava na maior parte da população.

Com a possibilidade de armazenar, processar e utilizar informações pessoais em grande escala, Estados e entes privados passaram a utilizar informações pessoais com a justificativa de controle e eficiências das ações. Doneda (2006) afirma que o Estado foi o primeiro a utilizar as informações pessoais armazenadas devido ao alto custo desses recursos. Para Mendes (2014), o Estado pós-industrial, caracterizado pela burocratização e o desenvolvimento da tecnologia da informação, justificaria o uso das informações. Porém, com o avanço tecnológico e o amadurecimento dos recursos digitais, *Big Data e algoritmos*, a coleta e o processamento dos dados tiveram os seus custos reduzidos. Assim, o mercado privado passa a utilizar essas informações para definir suas ações de marketing e comerciais de maneira mais estratégica.

Diante do exposto, o Direito à Privacidade ganha relevância e o debate sobre a proteção de dados pessoais assume o protagonismo frente aos novos desafios tecnológicos. Mendes (2014) afirma que ao assumirmos os riscos eminentes do tratamento em massa de dados pessoais, a tutela dessas informações assume não só a proteção dos dados, mas, principalmente, do seu titular. Para Doneda (2006), não podemos afirmar que a informação é algo tão característico da sociedade atual. Para ele, o que ganha relevância é a forma como lidamos com o armazenamento em massa dessa matéria-prima. Para exemplificar a questão, o autor argumenta que "dado" e "informação" possuem o mesmo sentido. Porém, possuem pesos completamente diferentes ao longo da história. "Dado" sendo algo mais primitivo e cru e "informação" possuindo maior abrangência e conteúdo. A forma como a sociedade aplica os conceitos e elabora a jurisprudência do Direito à Privacidade, para Doneda (2006), possui um influenciador, que é "o vetor que faz diferença é exatamente o tecnológico" (p.153)

No entanto, os primeiros esboços jurídicos estavam focados apenas no processo de utilizar, receber e enviar informação, não considerando o meio no qual isso ocorria. Essa visão fenomenológica é característica da classificação feita por Pierre Catala (1983).

> O autor classificou-a em quatro modalidades: (i) as informações relativas às pessoas e seus patrimônios. (ii) as opiniões subjetivas das pessoas. (iii) as obras do espírito. (iv) as informações que, fora as modalidades anteriores, referem-se a 'descrições de fenômenos, coisas e eventos. (CATALA, p.22, 1983/ DONEDA 2006)

Mesmo não possuindo nenhum viés funcional, a primeira classificação, demonstra que já havia um entendimento de que algumas informações são vinculadas aos indivíduos e são capazes de o identificar, reforçando toda a compreensão de que a informação é uma extensão da personalidade da pessoa e, portanto, carece de tutela jurídica frente ao Direito à Personalidade e ao Direito à Privacidade. No mesmo período, a Convenção de Strassbourg do Conselho Europeu, emitiu uma definição de informação pessoal. O documenta conceitua o termo da seguinte maneira: "qualquer informação relativa a um indivíduo identificado ou identificável" (DONEDA, p. 157, 2006)

Considerando a distinção dos termos 'dado' e 'informação', sendo o primeiro um material ainda sem tratamento, Doneda (2006) argumenta que um dado pode estar vinculado à uma pessoa indeterminada ou não identificada. Dessa forma, surge o que entendemos como Dados Anônimos. Podemos definir o termo como sendo aqueles dados que após processados são desconectados do seu tutor e podem ser utilizados para identificar fluxos, características e informações de um coletivo sem que haja identificação das partes componentes.

O entendimento de "dado anônimo" se faz importante visto que a sua identificação pode violar a autonomia do sujeito e a sua liberdade. Alguns anos após esse reconhecimento internacional, o *Manifesto Cypherpunk,* publicado em 1993 por Eric Hughes, defende a ideia de que privacidade não é o mesmo que segredo, trata-se de outro nível da esfera privada. O texto afirma que "um assunto privado é uma coisa que alguém não quer que o mundo inteiro saiba; um assunto secreto é uma coisa que alguém não quer que ninguém saiba. A privacidade é o poder de revelar-se seletivamente para o mundo". (HUGHES, 1993, p.9)[6]

Dado esse entendimento, o Manifesto defende que para garantir a proteção da individualidade, e com isso as transições anônimas, a única forma encontrada é o uso de criptografia. Para eles, somente a criptografia é capaz de balizar as zonas particulares e reservadas. Nesse sentido, a anonimização de dados pessoais se torna um recurso muito

[6] Disponível em: < https://www.tecmundo.com.br/criptografia/41665-cypherpunk-o-ativismo-do-futuro.htm> Acessado em 06 de dez. 2019

utilizado por legislações para garantir o uso dos dados coletados e garantir a privacidade individual.

A definição de dados anonimizados na legislação brasileira é apresentada como sendo o dado relativo ao titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento. De maneira similar ao que é colocado à categorização de dados sensíveis, a crítica realizada por Mendes (2014) é que, apesar de existir a possibilidade de tratamento dos dados para que, no processo de coleta haja a anonimização, a mesma tecnologia que anonimiza os dados é capaz de tornar o indivíduo identificável, características da sua personalidade ou distorções sociais, podendo gerar práticas discriminatórias ou, até mesmo, excludentes. Mendes (2014) defende que para garantir o Direito à Personalidade, sabendo da possibilidade de reindentificação dos dados, faz-se justificável a aplicação da proteção de dados pessoais em qualquer circunstância.

Segundo Pita (2017), há uma necessidade latente de conscientizar a população através do rompimento do discurso de que "a coleta de informações ocorre para entregar o melhor produto dentro dos seus interesses, de maneira personalizada" A coleta, o armazenamento, o processamento de dados e a venda de dados são etapas de um mercado de informação, de "exploração econômica dos indivíduos" (PITA, 2017, p.187)

A Lei Europeia apresenta um incentivo para utilização de técnicas de anonimização e, caso a anonimização seja considerada efetiva e irreversível, é prevista a utilização daquelas informações. "O uso de anonimização para dados pessoais pode reduzir os riscos para os titulares de dados, além de permitir que controladores e processadores atendam às exigências de proteção de dados" (Regulamento Geral de proteção de Dados, 2016)

Ainda nesse nicho, a informação pessoal pode possuir categorizações considerando fatores pessoais e sociais. Nas palavras de Doneda (2006), "a informação pessoal pode ser agrupada em subcategorias ligadas a determinado aspecto da vida de uma pessoa" (p.160). Como exemplo, podemos pensar em informações vinculadas aos dados bancários pessoais ou aos dados de compras. Dessa forma, entendemos o conceito de dados sensíveis, sendo aqueles que exigem um cuidado maior em sua tutela, pois, caso processados e levados à identificação, o potencial discriminatório ou invasivo para o indivíduo é enorme. Para o autor, "a categoria dados sensíveis é fruto de uma observação pragmática da diferença que apresentam o efeito do tratamento destes dados em relação aos demais" (DONEDA, 2006, p.161).

A Lei Brasileira, lei nº 13.709 no art. 5º, conceitua dados sensíveis como 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. Segundo Doneda (2010), a estratificação dos dados coletados se fez necessária para melhor aplicação das normas, considerando que o fluxo de determinadas informações é mais danoso aos seus titulares. O debate em torno da categorização dos dados sensíveis ocorre em relação aos dados que, inicialmente não são categorizados assim, mas ao passarem por tratamento se tornam dados sensíveis. Existem quatro processos que buscam retirar elementos identificadores dos dados pessoais para que se tornem dados sensíveis. As técnicas buscam reduzir o grau de identificabilidade e são a de supressão, a de generalização, e de randomização e a de pseudoanonimização.

Para Borgesius (2016), nenhuma dessas técnicas é capaz de tornar o dado anônimo de fato, visto que a associação com outras informações é facilmente realizada, e consequentemente, revela características do indivíduo ou possibilitando práticas discriminatórias.[7]

> In conclusion, singling out a person implies identifying this person, even if the data controller cannot tie a name to the data it processes about an individual. Therefore, behavioural targeting generally entails personal data processing. More-over, regardless of whether singling out an individual implies identifying this individual, it is often fairly easy to tie a name to behavioural targeting data, as discussed in the next section. (BORGESIUS, 2016, p.7)

Nessa mesma linha, Bioni (2019) afirma que sempre haverá uma base de dados para ser agregada a outra e gerar um processo de reidentificação. (BIONI, 2019, p.74)

Doneda (2010) defende que a tendência das legislações é utilizar-se da noção de tratamento sensíveis de dados pessoais e não ao conceito puro de dados sensíveis. Afirma que essa posição considera a impossibilidade de "predizer os efeitos que um tratamento de dados pessoais possa causar ao seu titular apenas a partir da consideração da natureza dos dados que são tratados." (DONEDA, 2010, p.27)

O Regulamento Geral sobre a proteção de Dados Europeu – GDPR traz em seu texto o entendimento de que existem dados, considerados sensíveis, os quais o processamento coloca

[7] Disponível em: <http://revista.ibict.br/fiinf/article/view/1768> Acessado em: 04 de set. de 2019.

em risco à privacidade do indivíduo. O artigo 9º da normativa europeia entende que dados sensíveis são aqueles de origem racial ou étnica; sobre opiniões políticas, crenças religiosas ou filosóficas; relacionada à associação a sindicatos; dados genéticos e dados biométricos para fins de identificação pessoal, assim como os dados relativos ao estado de saúde ou à vida sexual e/ou orientação sexual de uma pessoa. Contudo, é prevista a possibilidade de tratamento desses dados seguindo algumas exigências descritas na lei, como o expresso consentimento ou em caso de proteção vital do indivíduo ou razões substanciais de interesse público.

O Direito à proteção de dados pessoais tem ainda como um de seus pilares o consentimento. De forma breve, o consentimento é a permissão ou autorização apresentada pelo usuário para que o aplicativo em questão colete, trate, transfira, armazene ou comercialize os seus dados pessoais. No entanto, a conceituação do 'consentimento' é um debate oneroso à proteção de dados pessoais, visto que o seu entendimento pode variar desde o uso reiterado do aplicativo em questão ou a um clique de aceitação até as formas mais claras e acessíveis de consentimento.

A discussão sobre o seu conceito busca dar ao usuário o controle sob as suas informações, tendo a sua decisão os elementos essenciais para anuência, que são a liberdade de escolha, a especificidade do consentimento, se ele é expresso e informado. O consentimento deve ser estabelecido quando o usuário está repleto de informações a respeito da gestão dos seus dados pessoais tendo, portanto, a capacidade de tomar decisão.

O Regulamento Geral de proteção de Dados Europeu inova em seu artigo 7º ao tratar sobre consentimento 'livre' e ao colocar fim na ideia de consentimento forçado. A inovação apresentada na lei é o mecanismo para evitar que o acesso ao serviço seja condicionado ao consentimento do usuário na cessão dos seus dados pessoais para além do que é necessário para execução do serviço, evitando a prática da ampla coleta para destinação posterior.

> Condiciones para el consentimiento: 1. Cuando el tratamiento se base en el consentimiento del interesado, el responsable deberá ser capaz de demostrar que aquel consintió el tratamiento de sus datos personales; 2. Si el consentimiento del interesado se da en el contexto de una declaración escrita que también se refiera a otros asuntos, la solicitud de consentimiento se presentará de tal forma que se distinga claramente de los demás asuntos, de forma inteligible y de fácil acceso y utilizando un lenguaje claro y sencillo. No será vinculante ninguna parte de la declaración que constituya infracción del presente Reglamento. 3. El interesado tendrá derecho a retirar su consentimiento en cualquier momento. La retirada del consentimiento no afectará a la licitud del tratamiento basada en el consentimiento previo a su retirada. Antes de dar su consentimiento, el interesado será informado de ello. Será tan fácil retirar el consentimiento como darlo. 4. Al evaluar si el consentimiento se ha dado libremente, se tendrá en cuenta en la mayor medida posible el hecho de si, entre otras cosas, la ejecución

> de un contrato, incluida la prestación de un servicio, se supedita al consentimiento al tratamiento de datos personales que no son necesarios para la ejecución de dicho contrato. (REGULAMENTO GERAL DE PROTEÇÃO DE DADOS)

Segundo Mendes (2014), a base para debater e definir consentimento deve ser sempre a possibilidade do indivíduo controlar a utilização dos seus dados pessoais de modo que o Direito à Personalidade também seja garantido. A autora destaca a importância do consentimento para a discussão de proteção de dados pessoais, afirmando que somente o próprio indivíduo pode determinar em que dimensão a sua privacidade está garantida ao permitir a coleta, o processamento e a transferência dos seus dados pessoais. E é exatamente nesse âmbito que surgem pontos críticos na aplicação jurídica do conceito consentimento. Com isso, a autora destaca três aspectos que exigem certa cautela:

> i) o problema da eficácia do consentimento de dados pessoais, em face da possibilidade do não consentimento de o indivíduo acarretar a sua exclusão do mercado de consumo e da sociedade; ii) o problema da violação da proteção de dados pessoais, após o tratamento ter sido consentido pelo titular dos dados; iii) a questão do consentimento aplicado aos dados sensíveis. (MENDES, 2014, p.67)

Mendes (2014) utiliza-se da explanação de Mayer-Schönberger (2001) para apresentar o argumento sobre custo social, que indaga o preço pago pelo indivíduo para garantir o seu direito à privacidade e à proteção de dados pessoais. A busca pelas legislações deve ser a minimização desse custo social. Assim como Mendes, Doneda (2016) também indaga sobre o que nomeia como "Paradoxo da Privacidade", os autores se preocupam que a tutela jurídica dos dados ocorre somente após a coleta das informações. Primeiro o indivíduo autoriza e consente com a coleta e com o tratamento dos seus dados, e somente depois pode utilizar-se do ordenamento jurídico.

A autora conclui que, principalmente, nas relações assimétricas de poder, é necessário que a tutela jurídica garanta que o consentimento tenha sido dado de "forma livre e informada, resguardando não apenas a liberdade de escolha meramente formal do indivíduo, mas efetivamente a sua liberdade material" (MENDES, 2014, p.70).

A Lei Brasileira de proteção de dados pessoais define consentimento como a "manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada". Assim como a legislação europeia, a

Lei Brasileira expressa que o consentimento deve referir-se somente às finalidades determinadas para a prestação do serviço, sendo as autorizações genéricas para o tratamento de dados pessoais nulas de pleno direito.

Outro ponto de destaque na normativa brasileira, também em sintonia com o GDPR, é que o consentimento pode ser revogado a qualquer momento mediante manifestação expressa do titular, por procedimento gratuito e facilitado.

2.4 CONTEXTUALIZANDO A LEI EUROPEIA E OUTRAS LEGISLAÇÕES

Na seção anterior, a lei europeia de proteção de dados pessoais foi citada na discussão sobre temas-chave acerca da concepção sobre privacidade e direito. Nesta seção, convém contextualizar melhor como a GDPR foi editada.

A década de 70 do século XX foi marcada pela edição das primeiras leis de proteção de dados pessoais, que surgiram em contraponto ao desenvolvimento tecnológico que possibilitou o armazenamento, tratamento e processamento de dados em massa. Mayer-Schönberger (2001) considera que as transformações sociais, econômicas e tecnológicas sempre foram capazes de alterar as legislações de proteção de dados pessoais ao redor do mundo. Por isso, criou uma análise de desenvolvimento geracional dessas normativas desde a década de 70. Considerando o cenário da União Europeia, Mayer-Schönberger (2001) identifica quatro gerações de lei.

A primeira geração de lei é marcada pelo cenário do Estado Social. O autor afirma que na década de 70, houve um processo generalizado de expansão do Estado Social, que passou a tutelar os cidadãos para implementar uma burocracia institucional. Mendes (2014) exemplifica esse processo citando a ação, em 1960, do governo alemão, de criar um Comitê para unir a base de dados de bancos municipais, estaduais e federais. Nos Estados Unidos, houve processo similar, o *National Data Center*, apesar de nunca ter sido posto em prática, buscou criar uma central com todas as informações coletadas da população americana.

Situações como as citadas por Mendes (2014), referenciando Mayer-Schönberger, geraram uma reação de medo nos cidadãos. Na época, a ameaça se dava ao controle que um Estado possuiria com uma burocracia dotada de informação e, consequentemente, de poder. A

crítica ao controle não estava relacionada à individualidade do cidadão, mas ao coletivo dentro da relação com o Estado.

Com isso, a primeira geração de normas de proteção de dados pessoais possuía características funcionais, visando apenas o processo de armazenagem e tratamento de dados. Como resultado do processamento em massa de dados por entes públicos, a década de 70 viu leis como a do Estado Alemão de Hesse (1970), a Lei de Dados da Suécia (1973), o Estatuto de proteção de Dados de Estado alemão de Rheinland-Pfalz (1974) e a Lei Federal de proteção de Dados da Alemanha (1977) surgirem.

No entanto, as leis não foram capazes de acompanhar a transformação tecnológica que pulverizou a criação de bancos de dados. A primeira geração de leis se demonstrou frágil para contornar os desafios postos nessa expansão, principalmente por estarem focadas em processos e não nos direitos fundamentais, como o Direito à Privacidade e à Personalidade. Os titulares dos dados se viram incapazes de garantir a sua privacidade e personalidade frente ao controle informacional que os Estados passaram a possuir com a criação dos bancos de dados.

Segundo Mayer-Schönberger (2001), o debate em torno dessa incapacidade de proteção das normativas vigentes gerou um processo de atualização e edição de novas leis. A segunda geração de leis foi uma reação à ausência de tutela jurídica aos direitos fundamentais dentro do contexto tecnológico de expansão dos bancos de dados. Entende-se, portanto, que a segunda geração de leis teve por foco as liberdades individuais e o debate do direito ao esquecimento.

Estão dentro desse bloco, as leis da Áustria, da França, da Dinamarca e na Noruega[8]. Essas normativas fortalecem a construção do debate sobre consentimento e exclusão social.

Mayer-Schönberger (2001), ao desenhar o desenvolvimento geracional das leis de proteção de dados pessoais, afirma que a segunda geração de leis evidenciou que existe um custo social, exclusão, para aqueles indivíduos que optam pelo seu direito à privacidade e à proteção de dados pessoais.

Em 1983, o Tribunal Constitucional Alemão proferiu histórica decisão que determinou parte da Lei do Censo inconstitucional, considerando que os cidadãos possuem direito à autodeterminação informativa, ou seja, possuem controle no processamento dos seus dados. A Lei do Censo alemã determinava que os cidadãos eram obrigados a participar do processo.

[8] Mayer-Schönberger. **Generational development of data protection in Europe**. In: Technology and Privacy: The New Landscape. 2001

Mayer-Schönberger (2001) identifica como sendo característica principal da terceira geração de normas a inserção do cidadão como controlador e parte de todo o processo de tratamento de dados. A ideia de que o cidadão só pode concordar ou discordar, permitir ou não, tudo ou nada, perde espaço nesse terceiro bloco normativo.

Ao analisar a teoria de Mayer-Schönberger (2001), Mendes (2016) afirma que "o ideal participativo dos cidadãos no controle de informações pessoais, consubstanciado na ideia de autodeterminação informativa, provou-se não ser factível no mundo real" (p.42).

Para Mendes (2016), o custo social e econômico não incentivava os cidadãos à exerceram os seus direitos fundamentais. Não era atrativo proteger os seus dados, mas abrir mão de acesso a bens e serviços popularizados.

A quarta geração identificada por Mayer-Schönberger (2001) buscou trabalhar a garantia da integridade pessoal nos casos de violação dos direitos à privacidade e à personalidade. Em 1995, com a Diretiva Europeia, a quarta geração se inicia e ganha espaço com a construção de regulamentações gerais de proteção de dados pessoais.

As leis mais atuais, pertencentes à última geração, estão vigentes e fazem parte de uma onda mundial de atualização e aperfeiçoamento. Para Mendes (2016), a aprovação dos *Standards Internacionais sobre proteção de dados pessoais*, em 2019, na 31ª Conferência Internacional de Autoridades de proteção de dados pessoais, evidenciou o consenso mundial sobre a necessidade de uma legislação geral, mesmo que mínima, que garanta os direitos à personalidade e à privacidade.

Apesar desse entendimento sobre a necessidade de uma regulamentação mínima, as leis internacionais vigentes evidenciam algumas diferenças de tratamento e processo tutelar dos direitos em questão. Nesse cenário de equilíbrio entre a garantia dos direitos fundamentais dos indivíduos usuários da rede mundial de computadores e a evolução tecnológica, a regulação do tratamento de dados pessoais vive uma variação mundial dos níveis de discussões e normas vigentes.

Na contramão do movimento europeu, os Estados Unidos, tradicionalmente reconhecidos pela garantia das liberdades individuais, possuem uma forte e independente agência, a *Federal Trade Comission.* O órgão é ativo na proteção dos consumidores e coíbe práticas anticompetitivas, como a criação de monopólios na coleta e tratamento de dados pessoais. O país norte-americano utiliza-se da Diretriz *Safe Harbor,* fundamentada nos princípios de Aviso, Escolha, Acesso, Transferência Progressiva, Segurança, Integridade de Dados e Execução. Além dessa base, os Estados Unidos possuem legislações avulsas que

abordam o tema, como a *Children's Online Privacy Protection Act,* que tutela os dados dos cidadãos americanos menores de 13 anos e o *Health Insecurance Portability and Accoutability Act* que legisla sobre dados relacionados à saúde de pacientes. Apesar de terem a reconhecida normativa *Privacy Act*, ela possui foco apenas na ação do governo e apresenta aplicação limitada.

A legislação americana é abrangente para a esfera pública. Em termos do âmbito público, ela é segmentada, com designação setorial e esparsa.

Como mencionado acima, de forma distinta da orientação americana, a Diretiva Europeia 95/46/CE firmou o acordo, entre os países membros, que determinava a elaboração de leis abrangentes, que legislassem sobre o público e o privado através da proteção constitucional e também do regime legal. O objetivo era garantir a tutela do Estado sobre a sociedade e, também, sobre os seus próprios órgãos.

A União Europeia possui hoje a mais completa regulamentação para proteção de dados pessoais. Em 2011, o órgão Supervisor de proteção de Dados Europeu emitiu um comunicado reiterando a necessidade de rever a legislação sobre a proteção de dados pessoais. Até então, a União Europeia fazia uso da Diretiva nº 95/45/EC que, de forma geral, garantia uma uniformização do tratamento dos dados. No entanto, a Diretiva indicava que o processamento de dados pessoais deveria ser realizado seguindo a legislação do Estado-membro em questão, o que gerava distorções nos níveis de debate e exigências entre dos Estados-membros. A proposta de criação da GDPR foi realizada em 2012 pela Comissão Europeia, com o principal objetivo de garantir a privacidade dos cidadãos europeus e um tratamento harmônico do tema. Após o período de deliberação legislativa objetivando um padrão comum aos países europeus sobre privacidade, tratamento e coleta de dados pessoais, o Regulamento Geral de proteção de dados pessoais – GDPR foi aprovado em 2016 entrando em vigência em maio de 2018.

A normativa possui 99 capítulos e é considerada, por especialistas, o regramento mais moderno e detalhado sobre o tema. O GDPR concede maior poder aos consumidores, principalmente no que diz respeito ao consentimento e ao tratamento dos dados. É exigida das empresas uma explicação clara e concisa sobre o porquê da coleta dos dados, esclarecendo a finalidade para aquela coleta ser realizada. Com isso, também há o impedimento da coleta de dados não justificados pelo serviço prestado pela empresa. A legislação também prevê o acesso do usuário ao seu respectivo banco de informações. Para a empresa, fica exigida a comunicação às autoridades e aos usuários em caso de vazamento de dados. Assim como multas de 10 milhões de euros ou 2% do faturamento anual (prevalecendo o que for maior) até 20 milhões

de euros ou 4% do faturamento anual em caso de violação aos direitos regulamentados no GDPR.

Após 4 anos de debates com países do bloco, a lei foi aprovada em abril de 2016, entrando em vigência em 2018. A entrada em vigor da lei ocorreu, embora por acaso, junto com o caso de vazamento de dados pessoais envolvendo o Facebook, e a empresa britânica *Cambridge Analytica.*

Em março de 2018, os jornais *The New York Times e The Guardian* denunciaram o uso político de dados pessoais de usuários da rede social, *Facebook*. Segundo os jornais, dados de mais de 50 milhões de pessoas foram utilizadas sem o consentimento pela empresa *Cambridge Analytica* para fazer propaganda partidária. A denúncia afirmou que a *Cambridge Analytica* teve acesso às informações dos usuários e da sua rede de amigos através da realização de um teste psicológico, realizado por aplicativo, no *Facebook.*

A entrada em vigor da GDPR gerou um movimento internacional para atualizações das legislações e também para adequação das empresas às novas regras. Empresas atualizaram ou refizeram os seus termos e condições de uso, além de revisitar as suas cadeias de negócios e parceiros. A distinção de exigências judiciais entre países pode gerar efeitos negativos para empresas que possuem sede em países que possuem leis de níveis distintos ou realizam transferência, processamento e tratamento de dados em diferentes nacionalidades. Antes da aprovação da Lei Brasileira de proteção de dados pessoais, Doneda[9] (2018) afirmou que

> Isso vai fazer com que o país perca acesso ao mercado, porque para muitas transações é necessário ter padronização em termos de proteção de dados. Nenhum país europeu vai poder passar dados para o Brasil sem uma legislação minimamente adequada. Isso inviabiliza inclusive o pleito do Brasil a fazer parte da OCDE, porque ela faz uma série de exigências, incluindo padrões normativos sobre proteção de dados. Como está hoje, o Brasil não se adequa aos padrões da OCDE. É uma questão bastante séria. (DONEDA, 2018)

A aprovação de GDPR, juntamente com os escândalos internacionais e os casos de espionagem denunciados em 2014, impulsionaram o debate sobre a elaboração da Lei Brasileira de proteção de dados pessoais e também em outros países latinos. No entanto, alguns países, como Chile e Argentina, já possuíam legislações sobre o tema e são percussores no debate sobre a proteção de dados.

[9] Disponível em: https://www.nexojornal.com.br/expresso/2018/05/25/O-que-diz-a-nova-lei-de-prote%C3%A7%C3%A3o-de-dados-da-Europa.-E-o-efeito-no-Brasil Acessado em: 17. Set. 2019.

O Chile foi o primeiro país da América Latina a ter uma legislação específica para a proteção de dados pessoais. Em 1999, entrou em vigor a lei geral sobe proteção da informação pessoal[10] que, para a época, possuía uma normativa moderna e que buscava garantir os direitos fundamentais. Com a evolução do debate sobre a proteção de dados pessoais, o congresso chileno iniciou um processo de atualização em 2011. Após longo processo de desgaste, em 2013, através de um acordo parlamentar um novo projeto de lei foi apresentado. Em 2017, durante o 15º Encontro Ibero-Americano de proteção de Dados, organizado pela Rede Ibero-Americana de Autoridades de proteção de Dados e pelo Conselho de Transparência do Chile, foram aprovadas as Normas de proteção de Dados para os Estados Ibero-Americanos. O encontro fortaleceu a onda de atualização das normativas dos países membros.

Na ocasião, o Chile anunciou que aceleraria a atualização da lei de proteção de dados pessoais, criada em 1999, e criação da Agência de proteção de dados pessoais do Chile. Somente em 2018, o Senado chileno aprovou uma normativa que agora colocava o país em sintonia com a legislação europeia.

Na linha de frente do debate na América Latina, a Argentina possui algumas normativas de proteção de dados pessoais desde 1994. Porém, em 2000, o país aprovou a sua Lei de proteção de dados pessoais. O texto argentino regula bases de dados públicas e privadas, limitando o uso dos dados de acordo com a finalidade com a qual foram obtidos. A lei também é clara no que diz respeito ao consentimento do titular, definindo que o mesmo deve ser livre, expresso e informado. Uma das especificidades da normativa é que o consentimento não é exigido nos casos de bases públicas, "no cumprimento de uma obrigação legal, no exercício de funções próprias do Estado e quando as informações se limitam a nome, identidade, profissão, data de nascimento e endereço"[11].

Com legislação bem próxima ao texto argentino, o Uruguai definiu, em 2000, a sua legislação geral de proteção de dados pessoais. No país, o direito à proteção de dados está previsto na lei n° 18.331, de 11 de agosto de 2000, e é reconhecido como direito pessoal. Este marco normativo contém diversas disposições que se referem à forma que se pode recolher informação, armazenar e tratar dados pessoais. O texto permite a utilização de dados pessoais que possibilitem a definição de determinados perfis com fins promocionais, comerciais ou publicitários, ou o estabelecimento de hábitos de consumo, quando eles figurem em documentos acessíveis ao público, ou tenham sido fornecidos pelos próprios titulares, ou

[10] Disponível em: < https://www.leychile.cl/Navegar?idNorma=141599 > Acessado em: 18 de set.2019.

[11] Disponível em: https://cio.com.br/protecao-de-dados-na-america-latina/ Acessado em: 06 de dez. 2019

obtidos com seu consentimento. A segurança da informação no Uruguai é gerida pela Agência para o Desenvolvimento do Governo de Gestão Eletrônica da Sociedade da Informação e do Conhecimento, o país mantém um ranking de empresas que seguem o código de conduta de proteção de dados pessoais posto pelo país.

Na Colômbia, a lei de nº 1.266/2008 regula o tratamento da informação contida em bases de dados pessoais, especialmente a informação financeira, creditícia, comercial, de serviços e proveniente de terceiros países. Em 2012, a lei nº 1.581 complementou o texto vigente regulamentando a proteção das informações pessoais registradas em bases de dados que permitam a coleta, o armazenamento e o tratamento por entes privados ou públicos. Assim como o Uruguai, a Colômbia também possui uma Divisão para a proteção de dados pessoais pertencente à Superintendência da Indústria e Comércio.

Em 2010, o México implementava a sua Lei Federal de proteção de dados pessoais em Poder de Particulares, responsável pela regulamentação da proteção de dados pessoais em geral. Porém, até essa data, assim como no Brasil, outras normativas abordavam a temática. Destaque para o artigo 6º da Constituição mexicana, que dispõe o direito de acesso às tecnologias da informação e da comunicação. A Lei Federal de Telecomunicações e Radiodifusão e a Lei Federal de Transparência e Acesso à Informação Pública Governamental também perpassam a proteção de dados pessoais. Uma particularidade da normativa mexicana é a criação do Instituto Federal de Acesso à Informação e proteção de Dados (IFAI).

Em 2011, o Peru aprovou a sua normativa de proteção de dados que define autoridade e acesso transparente às informações públicas. O texto objetiva proteger os direitos dos indivíduos e garantir que as empresas privadas e públicas cumpram as obrigações previstas em lei no processamento e tratamento de dados. No mesmo ano, a Costa Rica aprovou a Lei Geral de proteção de dados pessoais, com foco absoluto na garantia dos direitos fundamentais presentes na sua Constituição.

Como visto, os países da América Latina possuíam normativas que regulavam, de certa forma, a proteção de dados pessoais e buscavam garantir o Direito à Privacidade e à Personalidade. No entanto, os casos de espionagem americana, somados à atualização da normativa europeia geraram uma onda de atualização das normas latinas. Os dados se estabeleceram como um dos ativos mais valiosos do mundo e a cibersegurança é uma necessidade para todos os países e, com isso, a proteção de dados pessoais uma necessidade. Os fatos tensionadores acima mencionados colocaram os países latinos em uma situação de

emergência. Ou havia uma legislação ou haveria uma retaliação econômica visto a impossibilidade de empresas europeias trabalharem em solo latino sem a harmonização das leis.

Essa influência também chegou no Brasil que discutia a regulamentação da proteção de dados pessoais desde 2010. Com toda essa movimentação internacional, em agosto de 2018, após anos de discussão, o Brasil aprovou a Lei Brasileira de proteção de dados pessoais, a Lei nº 13.709/2018. Com isso, o Brasil passou a possuir uma legislação harmônica com a GDPR.

3. O PROCESSO DE CONSTRUÇÃO DA LEI BRASILEIRA DE PROTEÇÃO DE DADOS PESSOAIS: CARACTERÍSTICAS, APLICABILIDADE E ATORES

Compreendermos como outros países e, principalmente, a América Latina legislou e legisla sobre o direito à privacidade é fundamental para entender os nuances do debate histórico feito pelo Brasil. A construção da normativa brasileira foi fundamentalmente influenciada pela construção internacional. O presente capítulo descreve os anos de maturação do tema no governo brasileiro e como foi a construção da Lei Geral de proteção de dados pessoais (LGPD). Apesar do Brasil só ter finalizado a LGPD, lei nº 13.709, em 2018, algumas normativas, apesar de avulsas e sem conexão umas com as outras, tratavam de alguns aspectos do Direito à Personalidade e à Privacidade e tutelavam sobre os temas. O debate inicial mapeia todas essas legislações e explica como o Brasil acompanhou os diversos entendimentos sobre a tutela desses direitos fundamentais.

3.1 PARÂMETROS METODOLÓGICOS

A pesquisa analisou três anos de tramitação legislativa que resultou na Lei de Proteção de Dados Pessoais. O processo legislativo analisado contou com dezenas de audiências públicas, seminários, discursos e votações. Toda a movimentação política entorno da tramitação da LGPD está registada no *site* da Câmara dos Deputados e do Senado Federal. São diversas atas e vídeos que foram objeto de análise documental da pesquisa. O objetivo em questão é compreender todo o debate tendo como norteador a definição dos conceitos de dados sensíveis, dados anonimizados e Consentimento,

Considerando a complexidade e a ausência de linearidade de construções políticas e legislativas, a pesquisa utilizou a metodologia Hermenêutica da Profundidade, ferramenta proposta por John B. Thompson (1998).

De acordo com Veronese e Guareschi (2006), a Hermenêutica da Profundidade tem como principal característica a sua amplitude e interpretação dos objetos, visto as etapas de análise crítica complementares. A partir dela, o pesquisador analisa o contexto sócio-histórico e espaço-temporal, realiza uma análise discursiva e reinterpreta os fatos com a base elaborada durante o processo.

A metodologia proposta para o estudo possui quatro etapas de análise que não são cronológicas, mas complementares e com funções distintas. Objetiva-se realizar uma leitura qualificada dos fatos.

Em um primeiro momento, foi realizada uma análise história das normas que antecederam a Lei Brasileira de Proteção de Dados Pessoais. Definida metodologicamente como uma "análise etnográfica", é nela onde identifica-se a realidade em que o objeto de estudo se insere. A pesquisa utilizou análise documental e levantamento bibliográfico para compreender o contexto no qual o processo de elaboração normativa da legislação brasileira de proteção de dados pessoais foi criado.

A etapa seguinte consistiu em uma análise sócio-histórica, responsável por reconstruir e identificar as condições sociais relativas ao objeto de análise. Veronese e Guareschi (2006) afirmam que o "interesse da HP irá centrar-se naquelas relações em que o sentido opera ideologia. É no nível das interações e da semantização do mundo que se produzem as estratégias e as constelações relacionais de poder" (p.89). Após essa etapa, há a realização de uma análise formal, onde há a possibilidade de o pesquisador utilizar o padrão mais adequado ao material de pesquisa. Visto que a pesquisa em questão analisou a experiência legislativa de elaboração da Lei Brasileira de Proteção de Dados Pessoais, o material disponibilizado para estudo são as notas taquigráficas e vídeos das reuniões que deliberaram a proposição. Com isso, utilizou-se a análise de conteúdo para buscar o contorno dado nos termos-chaves identificados acima.

Por fim, a Hermenêutica de Profundidade propõe a etapa da reinterpretação, uma explicação interpretativa que une todo o arcabouço construído nas outras etapas. Com isso, constrói-se referencias, categorizações e interpretações. Nessa etapa, a pesquisa buscou identificar e classificar os atores presentes no processo descrito a fim de descrever e monitorar o comportamento, influência e atuação dos mesmos nas discussões que cercearam os termos-chaves da lei, sendo esses: "dados sensíveis", "dados anonimizados" e "consentimento". Os relatórios de audiência e de eventos foram analisados e os atores presentes categorizados.

Os atores foram classificados em Atores Políticos, aqueles que ocupam algum cargo público nos Poderes Executivo ou Legislativo; Atores Acadêmicos, sendo aqueles que representam instituições acadêmicas e técnicas; Atores do Setor Regulado, aqueles que fazem parte de instituições do mercado que serão submetidas à legislação aprovada; E, por fim, Atores da Sociedade Civil, aqueles representantes da sociedade, agrupados em associações, coalizões ou ONGs.

O mapeamento de atores demonstrou que durante todo o processo legislativo há recorrência na partição dos atores, principalmente no que se refere aos atores políticos. Esses, burocraticamente, estão em maior quantidade devido à composição das comissões, porém a atuação dos relatores e presidentes se mostra mais presente e efetiva.

Como se trata de uma legislação aprovada recentemente e que teve o seu processo legislativo nos últimos dois anos, os materiais de relato, como vídeos, áudios e atas das reuniões estão disponíveis para consulta (http://www.camara.gov.br/ e https://www12.senado.leg.br/hpsenado) e já coletadas pela pesquisadora. Segundo Veronese e Guareschi (2006), a Hermenêutica da Profundidade permite que:

> O pesquisador pode analisar o contexto sócio-histórico e espaço-temporal que cerca o fenômeno pesquisado, pode empreender análises discursivas, de conteúdo, semióticas ou de qualquer padrão formal que venha a ser necessário; pode analisar a ideologia como vertente social importante, conferindo um caráter potencialmente crítico à pesquisa, o que vem a ser destacado por Thompson (1998) em sua obra Ideologia e cultura moderna. O referencial metodológico da HP inclui formas de análise complementares entre si, partes de um processo interpretativo complexo acompanhamento presencial do processo. (VERONESE E GUARESCHI, 2006, p.87)

Visto que o objeto de pesquisa é uma legislação recente, ainda carente de processos normativos de regulamentação, a pesquisa irá buscar métodos complementares para conseguir elaborar uma descrição coerente e crítica da experiência legislativa de elaboração da normativa analisada, como análise de reportagens publicadas durante o período. Entender, não apenas o ambiente formal legislativo, mas os contornos políticos do debate da construção da legislação, tendo sempre como eixo os aspectos técnicos “consentimento, dados sensíveis e dados anonimizados.”

3.2 REGULAÇÕES DO DIREITO À PRIVACIDADE NO BRASIL ANTES DA NOVA LEI

Até o ano de 2018, o Brasil não possuía uma legislação geral que tutelasse a privacidade e a proteção de dados pessoais. Não havia um único texto que abarcasse o arcabouço administrativo, civil e penal. Até a sanção da Lei Geral de proteção de dados pessoais, a legislação brasileira possuía normas avulsas que consideravam alguns pontos do debate, como o Código de Defesa do Consumidor, a Lei do Cadastro Positivo, a Lei sobre a tipificação

criminal de delitos informáticos, popularizada como a Lei Carolina Dieckmann, o Marco Civil da internet e a própria Constituição Federal.

A harmonização dessas normativas e a garantia de seus cumprimentos frente aos nossos desafios postos pela evolução tecnológica, foram as principais incitações para que o Brasil trabalhasse em uma legislação que estivesse em sintonia com a Lei Europeia de proteção de dados pessoais e garantisse a manutenção de acordo e negócios internacionais que envolvessem o país.

Antes de debruçarmos sob a nova Lei de proteção de dados pessoais, se faz necessário entendermos a base normativo que nos trouxe até essa elaboração que coloca o Brasil no grupo de países com modernas legislações sobre o tema.

3.2.1 Constituição Federal de 1988 – Art. 5º.

O emblemático art. 5º da Constituição da República Federativa do Brasil, em 1988, trazia a intimidade como um direito fundamental. O seu inciso X dispõe 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 da sua violação." A Constituição define, de forma clara e expressa que a violação à privacidade deve ser reparada.

3.2.2. Código de Defesa do Consumidor – Lei Federal nº 8.078/1990

Dois anos depois da promulgação da Constituição de 88, o Código de Defesa do Consumidor é sancionado. A Lei nº 8.078/1990 é vista por pesquisadores do tema (Bioni, 2018; Doneda, 2006; e Mendes, 2014) como uma normativa moderna e impulsionadora do debate sobre consentimento dentro da proteção de dados pessoais.

O art. 43, que disciplina os bancos de dados e o cadastro de consumidores, é taxativo no cumprimento dos padrões de amplitude, direito ao acesso, princípio da qualidade dos dados, direito de retificação e cancelamento, garantia da personalidade, controle do titular sobre os seus dados, princípio do esquecimento e transparência. Mendes (2014) afirma que o Código de Defesa do Consumidor foi inspirado nas normas americanas *National Consumer Act e Fair Credit Reporting Act.*

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

Bioni (2018) destaca que a peça legislativa, de maneira vanguardista, garante ao consumidor o controle sobre os seus dados aliado à possibilidade de mapear todo o percurso dado a eles desde a sua coleta. O texto também opta por uma amplitude que abarque quaisquer bancos de dados que possam afetar a livre personalidade do consumidor. Para o autor, a normativa capacita o cidadão, visto nesse caso como consumidor, para uma autodeterminação informacional. Por outro lado, Mendes (2014) destaca que a normativa coloca o qualquer armazenamento de dados pessoais sob o crivo da legalidade. "Qualquer armazenamento de dados pessoais, por se referir à personalidade do consumidor, não diz respeito à esfera empresarial apenas, mas sim ao público e, portanto, a ele se aplica o regime constitucional e legal" (MENDES, 2014, p.143). Considerando os pontos destacados, a Lei nº 8.078/1990 é vista como uma normatiza destaque e base legal para a elaboração da Lei Geral de proteção de dados pessoais.

3.2.3 Lei do Cadastro Positivo – Lei Federal nº 12.414/2011

Também com foco na autodeterminação informacional, a Lei Federal nº 12.414/2011, conhecida como a Lei do Cadastro Positivo, dispõe sobre a criação de bancos de dados com informações de adimplemento para formação de cadastro de crédito. A normativa é de alta

complexidade, uma vez que amplia a viabilidade de formação de bancos de dados e, consequentemente, do seu fluxo de informações no mercado. O texto é considerado complexo, também porque, além dessa ampliação, ele define, em certa dimensão, regras de proteção à privacidade e formas de controle e fiscalização do uso de dados coletados.

A complexidade da Lei não fica apenas na sua redação. A sua edição inovou ao considerar no histórico de crédito também os dados relativos a capacidade financeira e bons pagamentos, não apenas as situações de inadimplência. Apelidada como Lei do Cadastro Positivo, a Lei nº 12.414 concedeu ao titular das informações a possibilidade de gerencia-las e não apenas dar o consentimento ao processo informado (arts. 4º ao 9º).

Outro ponto de destaque da normativa é que o gestor (definido na lei como "pessoa jurídica responsável pela administração de banco de dados, bem como pela coleta, pelo armazenamento, pela análise e elo acesso de terceiros aos dados armazenados") é proibido de coletar informações que não sejam consideradas úteis para análise de crédito. Doneda (2002) afirmou que a Lei do Cadastro Positivo conseguiu estabelecer na legislação brasileira alguns dos conceitos básicos da proteção de dados pessoais. Para o autor, mesmo que restrita ao processo de formação de histórico de crédito, foi capaz de estabelecer esses princípios norteadores para o debate. Recentemente, em abril de 2019, foi publicada a Lei Complementar nº 166 que alterou o texto vigente da lei do cadastro positivo de crédito e estabeleceu novas regras para a responsabilidade civil dos operadores.

Entre outros pontos, destaque para a modificação do art.9º, que definia que o compartilhamento de informação de adimplemento só seria permitido se autorizado expressamente pelo cadastrado, por meio de assinatura em instrumento específico ou em cláusula apartada. A nova redação permite que o gestor inclua, de forma automática, dados e informações do cadastrado em autorização. Ou seja, a lei perde o princípio do consentimento, porém mantém o direito de retificação e cancelamento. O Governo Federal justificou a alteração afirmando que democratizará o acesso às informações para o mercado.

3.2.4 Lei de Acesso à Informação – Lei Federal nº 12.527/2011

A Lei nº 12.527/2011 foi sancionada em meio ao debate sobre a necessidade de mais transparência nas ações da Administração Pública. Faz-se necessária uma breve consideração sobre a discussão acadêmica sobre *accountability* e participação política para entendermos

como a Lei de Acesso à Informação - LAI é estratégica para o debate da Lei de proteção de dados pessoais, principalmente por entendermos o Estado como um dos maiores detentores de dados pessoais dos cidadãos brasileiros.

Gomes (2011) afirma que a participação política é o aspecto mais delicado da democracia atual. Para ele, é inquestionável a ideia de que a soberania popular é indispensável para a democracia constitucional (GOMES, 2011, p.216), consequentemente, a opinião popular deve ser considerada nas decisões do Estado. Contudo, a opinião popular deve ser qualificada com o compartilhamento de informações por parte do Estado.

O distanciamento entre sociedade e a esfera governamental (ou de decisão política) por definição, deslegitima as tomadas de decisão da Administração Públicas (Representantes) enfraquecendo a democracia. De acordo com Sampaio (2011) é unanimidade entre diferentes teóricos que as democracias representativas "não são responsivas o suficiente e que as eleições, como forma única de controle dos cidadãos sobre seus representantes, não são suficientes para legitimar as decisões políticas" (SAMPAIO, 2011, p.13).

A participação civil nas tomadas de decisão é vital para a democracia. Sampaio (2011) ainda defende que a sociedade deve ter papel efetivo na administração pública assim como ter um canal direto e de fácil contato com seus representantes.

Com o problema posto e a urgência de encontrar soluções que cessem o afastamento da sociedade da esfera de decisão política, a discussão reflete sobre formas, meios e legislações. Assim a LAI, em seu Art. 3º, buscou conceder ao cidadão um direito geral de acesso às informações públicas.

> Art. 3º Os procedimentos previstos nesta Lei destinam-se a assegurar o direito fundamental de acesso à informação e devem ser executados em conformidade com os princípios básicos da administração pública e com as seguintes diretrizes:
> I - observância da publicidade como preceito geral e do sigilo como exceção;
> II - divulgação de informações de interesse público, independentemente de solicitações;
> III - utilização de meios de comunicação viabilizados pela tecnologia da informação;
> IV - fomento ao desenvolvimento da cultura de transparência na administração pública;
> V - desenvolvimento do controle social da administração pública.

No entanto, cabe destacar como o vínculo entre o direito de acesso à informação pública e a proteção de dados pessoais. Segundo Mendes (2014), a relação entre esses direitos é vista como complementar, já que o acesso à informação pública possibilita que o cidadão tenha conhecimento de como o Estado utiliza os seus dados pessoais. Em uma seção destinada às

informações pessoais, a normativa determina que o tratamento deve ser feito de forma transparente, em consonância com os direitos previstos no art. 5º da Constituição Federal, além de definir orientações quanto ao direito ao esquecimento, privacidade e consentimento. Cabe destacar também que o art. 34 que responsabiliza a Administração Pública por danos causados em decorrência da divulgação não autorizada ou utilização indevida de informações sigilosas ou informações pessoais.

Mendes (2014) afirma que a LAI consegue definir o limiar entre o direito à privacidade e o direito à informação. Apesar de vigente um texto normativo bem conceituado e moderno, o Brasil ainda enfrenta desafios referentes à vigilância. Em 2016, a Organização Não Governamental *Eletronic Frontier Foundation* publicou um relatório técnico sobre vigilância e legislações dos países da América Latina. O documento expõe que os cidadãos brasileiros são ameaçados por um Estado vigilante que não permite o anonimato; que possui ausência de transparência com os dados dos usuários da Agência Nacional de Telecomunicações; que não tem normas reguladoras do segredo. A EFF afirma que o Estado brasileiro controla dados pessoais dos cidadãos que frequentam prédios públicos ou comerciais sem justificativa. O estudo também critica a exigência, por lei, que os provedores possuem de armazenar os "metadados", que são dados como ligações, mensagens, localização, tempo de uso na internet, contatos e outros. Essa exigência está presente no Marco Civil da internet, um importante normativo que possui origem no mesmo debate da Lei Geral de proteção de dados pessoais.

No ano seguinte, em 2012, foi aprovada a Lei Federal nº 12.737 sobre crimes cibernéticos, mas também conhecida como Lei Carolina Dieckmann. A normativa foi uma resposta ao vazamento criminoso de fotos intimas da atriz, que posteriormente protagonizou o debate sobre a invasão de privacidade na internet. Porém, somente o Marco Civil da internet, Lei nº 12.965/2014, foi capaz de impulsionar um acordo legislativo para construção de uma normativa específica para os direitos e garantias do usuário da internet e também de proteção de dados pessoais.

3.2.5 Marco Civil da internet – Lei Federal nº 12.965/2014

A Lei de Crimes Cibernéticos gerou um movimento social contra uma proposta legislativa de regulação da internet através de leis penais. A construção desse marco normativo capaz de definir direitos e garantias do cidadão no uso da internet foi acelerado pelo episódio de espionagem revelado por Edward Snowden. O histórico de debate sobre crimes cibernéticos,

somado ao caso de espionagem americana, não foi só capaz de acelerar a sua aprovação, mas também de enrijecer alguns princípios originais, aprovados em Consulta Pública, do Marco Civil da internet. Sancionada em 2014, a lei possui quatro pilares que a permite ser reconhecida como inovadora e eficaz. O seu texto prevê, como direitos, a proteção da privacidade, dos dados pessoais, da neutralidade de rede e da liberdade de expressão.

O Marco Civil da internet define, pela primeira vez, o consentimento como sendo livre, expresso e informado, adjetivos estratégicos para o posterior debate sobre a proteção de dados pessoais. O texto estabelece o direito ao esquecimento e ao controle sobre os dados. Porém, é internacionalmente criticado pela previsão de armazenagem, por parte dos provedores de internet, de "metadados". O art. 15º prevê que o provedor de aplicações de internet deve manter os registros de acesso a aplicações de internet, sob sigilo, em ambiente controlado e de segurança, pelo prazo de 6 meses.

Bioni (2018) afirma que o Marco Civil da internet é taxativo no processo de controle do titular sobre os seus dados. Independente da etapa do fluxo, a lei define que o consentimento prevalece, desde a coleta, ao compartilhamento ou exclusão. Nas palavras de Bioni (2018), "verifica-se ser a autodeterminação informacional o parâmetro normativo eleito pelo Marco Civil para a proteção de dados pessoais" (BIONI, 2018, p.132)

Com a movimentação que antecedeu a aprovação do Marco Civil da internet, Lei n° 12.965/14[12], que "dispõe sobre o uso da internet no Brasil por meio da previsão de princípios, garantias, direitos e deveres para quem usa a rede, bem como da determinação de diretrizes para a atuação do Estado", houve um direcionamento mais efetivo de diversos atores em direção para a criação de uma lei mais completa e atual sobre proteção de dados.

Entender todas as normativas explanadas acima se faz necessário na construção do entendimento do processo normativo da Lei Geral de proteção de dados pessoais, visto que a articulação sobre a construção de uma normativa única que tutelasse a privacidade e a proteção de dados pessoais teve início ainda em 2010. O debate, realizado no blog Culturadigital.br[13] foi idealizado através de uma parceria entre a Secretaria de Assuntos Legislativos - SAL[14] e o Departamento de proteção e Defesa do Consumidor – DPDC do Ministério da Justiça – MJ[15].

[12] Disponível em: < http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm> Acessado em 06 de dez. 2019
[13] Disponível em: http://culturadigital.br/atividades/, acessado em 05/09/2017
[14]Disponível em: http://www.justica.gov.br/Acesso/institucional/sumario/quemequem/secretaria-de-assuntos-legislativos, acessado em 05/09/2017.
[15]Disponível em: http://www.justica.gov.br/Acesso/institucional/sumario/quemequem/departamento-de-protecao-e-defesa-do-consumidor-2013-dpdc, acessado em 05/09/2017.

A discussão esteve aberta à sociedade entre os meses de novembro de 2010 a abril de 2011. Em janeiro de 2015, a Secretaria Nacional do Consumidor do MJ informou[16] que o texto resultante do debate deveria ser revisto, em virtude de mudanças na conjuntura nacional trazidas pela aprovação das leis relatadas acima, que são normativos importantes e que possuíam correlação ao tema, como a Lei do Cadastro Positivo (Lei 12.414/2011)[17] a Lei de Acesso à Informação (Lei 12.527/2011)[18] e o Marco Civil da internet[19].

3.3 PROCESSOS REGULATÓRIO, PARTICIPAÇÃO E ATORES

Na seção anterior, apresentamos o conjunto de normas que precedeu à edição da Lei Geral de proteção de dados pessoais. Entendemos como o Brasil tutelava até então o Direito à Privacidade. Diante desse cenário, iniciamos aqui a descrever a construção legislativa da Lei Geral de proteção de dados pessoais. Com foco nos atores e no processo legislativo, percorremos os 13 anos de debate sobre o processo legislativo brasileiro sobre a proteção de dados pessoais.

Em 2005, no âmbito do Mercosul, a Argentina pautou a proposta de harmonização de legislações que tutelassem a proteção de dados pessoais. Porém, somente em 2010, após debates internos no Governo Federal, o Brasil iniciou uma consulta pública para elaboração de um Marco Regulatório de proteção de dados pessoais. O debate, realizado no blog *Culturadigital.br,* foi idealizado através de uma parceria entre a Secretaria de Assuntos Legislativos - SAL e o Departamento de proteção e Defesa do Consumidor – DPDC do Ministério da Justiça – MJ, em parceria com o Comitê Gestor da internet e a FGV-RIO. A discussão esteve aberta à sociedade entre os meses de novembro de 2010 a abril de 2011. Ao longo dos cinco meses de debate, o texto proposto recebeu cerca de 800 comentários e sugestões e tinha uma proposta final em fase de consolidação.

Em outubro de 2014, a Secretaria Nacional do Consumidor do MJ informou que o texto deveria ser revisto, em virtude de mudanças na conjuntura nacional trazidas pela

[16]Disponível em: http://www.justica.gov.br/noticias/governo-lanca-debate-publico-sobre-regulamentacao-de-lei-e-anteprojeto, acessado em 22/08/2017.
[17] Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/L12414.htm, acessado em 05/09/2017
[18] Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm, acessado em 05/09/2017.
[19] Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm, acessado em 05/09/17.

aprovação de diversos marcos normativos importantes, como a Lei do Cadastro Positivo (Lei 12.414/2011), a Lei de Acesso à Informação (Lei 12.527/2011), a Lei dos Crimes Cibernéticos (Lei 12.737/2012) e o Marco Civil da internet. Assim, no início do ano de 2015, o Poder Executivo retoma o tema e busca novamente atrair a participação popular.

O objetivo passa a ser a construção de um projeto de lei a ser encaminhado pelo Poder Executivo ao Congresso Nacional, o Anteprojeto de Lei – APL - de proteção de dados pessoais. O debate público iniciado em 2015, esteve constantemente relacionado pelo Ministério da Justiça à Discussão Pública realizada em 2010. Denominada como 2ª fase, o APL foi apresentado em formato de Consulta Pública para incentivar a participação popular na elaboração da minuta da Lei Brasileira de proteção de dados pessoais que seria encaminhada como Projeto de Lei para a Câmara dos Deputados.

A proposta visava assegurar ao cidadão uma série de direitos básicos sobre seus dados pessoais, armazenados em território nacional, bem como em centrais fora do país. A minuta objeto da Consulta Pública abordou também questões relativas ao vazamento e uso compartilhado de dados, além da responsabilidade daqueles que lidam com essas informações, e clareza sobre os procedimentos adotados para garantir a segurança desses dados. O Projeto de Lei foi encaminhado ao Poder Legislativo em 2016, nº 5.276, sendo objeto de debate e intensa participação dos setores interessados no tema.

Durante o processo de elaboração normativa, principalmente no período de Consulta Pública, alguns temas foram alvo de maior debate. A distribuição das participações por eixos temáticos evidenciou a concentração do debate em alguns temas. Os destaques que podem ser feitos, considerando essa categorização, são nos eixos (i) dados pessoais, Dados Anônimos e dados sensíveis – arts. 5º, 12º e 13º e (ii) consentimento – arts. 7º ao 11º, que tiveram, respectivamente 164 (17,5%) e 177 (19%) participações.

Tabela 1 – Participações por Eixos Temáticos

Eixos Temáticos	Nº	%
Escopo e Aplicação – Arts. 1º ao 4º	210	22
dados pessoais, Dados Anônimos e dados sensíveis – Arts. 5º, 12º e 13º	164	17,5
Princípios – Art. 6º	51	5,46

Fonte: Elaboração Própria - Debate Público sobre proteção de dados pessoais do Ministério da Justiça.

consentimento – Arts. 7º ao 11º	177	18,97
Término do Tratamento – Arts. 14º e 15º	26	2,8
Direitos do Titular – Arts. 16º ao 21º	62	6,6
Comunicação, Interconexão e Uso Compartilhado De Dados – Arts. 22º ao 27º	26	2,8
Transferência Internacional de Dados – Arts. 28º ao 33º	50	5,3
Responsabilidade dos Agentes – Arts. 34º ao 41º	51	5,4
Segurança e Sigilo de dados pessoais – Arts. 42º ao 47º	38	4,07
Capítulo VII Seção IV	38	4,07
Boas Práticas – Arts. 48º e 49º	21	2,25
Como assegurar estes Direitos, Garantias e Deveres – Art. 50	38	4,07
Disposições Transitórias – Arts. 51º e 52º	19	2,03
Total	933	100

O Debate Público ou Consulta Pública do Anteprojeto de Lei de proteção de dados pessoais ocorreu na Plataforma do Projeto *Pensando Direito* da Secretaria de Assuntos Legislativos do Ministério da Justiça, porém está ligada ao *Participa.br*, plataforma digital do governo federal de consultas e debates públicos. Com início no dia 28 de janeiro de 2015, a minuta do APL de dados pessoais foi disponibilizada para debate público, tendo sido elaborada com as informações coletadas na 1ª fase do Debate Público (2010). A proposta visava assegurar ao cidadão uma série de direitos básicos sobre seus dados pessoais, armazenados em território nacional, bem como em centrais fora do país. A minuta objeto da Consulta Pública abordou também questões relativas ao vazamento e uso compartilhado de dados, além da responsabilidade daqueles que lidam com essas informações, e clareza sobre os procedimentos adotados para garantir a segurança desses dados.

O texto de apresentação afirmava que o objetivo do espaço não seria a formação de um fórum de conversação entre os colaboradores. A ideia de constituir um "plebiscito" de concordância ou discordância com outro participante por meio dos comentários não foi estabelecida como objetivo do projeto e nem da estrutura da plataforma. O texto de apresentação afirmava que se buscava apenas colher as opiniões e contribuições, ainda que se tratasse de um debate público. A apresentação do projeto solicitou aos cidadãos a coerência

temática e a qualificação em suas manifestações. Todas as exigências foram justificadas como forma de melhor aproveitamento das discussões no espaço para constituição textual.

O debate público possuía moderação, conforme anunciado no texto introdutório. Comentários realizados em locais indevidos ou desrespeitosos seriam excluídos. Apesar das exigências, a participação popular foi colocada como eixo fundamentador do debate público: "Contamos novamente com sua contribuição para fortalecer a democracia na internet".

O debate ocorreu em torno do corpo do texto, sendo permitida a participação de 3 (três) formas. O participante poderia (i) realizar comentários em cada parte do texto, artigos, parágrafos e/ou incisos; (ii) enviar comentários por eixos temáticos; e (iii) enviar contribuições documentais por arquivos em formato *.pdf.*

O primeiro modo permitia a interação direta entre os participantes em cada um dos dispositivos da lei. Esse formato fomentava o diálogo e o embate direto de ideias, devido a exposição constante e ampla dos comentários realizados. A participação por meio dos eixos temáticos fornecia um acesso mais fácil e simples aos temas de interesse, visto a complexidade de um texto jurídico. No entanto, esse modelo não dava acessibilidade aos comentários já realizados. Por fim, o envio de contribuições em arquivos permitia participações mais complexas e consolidadas sem limite de espaço ou adequação a algum dispositivo textual, porém sem interação entre os participantes.

Em outubro de 2015, o Ministério da Justiça realizou o Seminário 'Anteprojeto Brasileiro de proteção de dados pessoais em Perspectiva Comparada' para apresentar a versão consolidada do Anteprojeto de Lei – APL elaborado pela Secretaria Nacional do Consumidos – SENACON, em conjunto com a Secretaria de Assuntos Legislativos – SAL, após a realização de dois debates públicos. Durante a abertura do evento, a então Secretária Nacional do Consumidor, Juliana Pereira, afirmou que o APL representava um marco no tema de proteção de dados pessoais, pois é a primeira vez que o Brasil discute uma lei geral sobre o assunto. O evento contou com a participação do Secretário de Assuntos Legislativos, Gabriel Sampaio, do Senador Aloysio Nunes (PSDB/SP), e de especialistas da Rede Ibero-americana de proteção de Dados – RIPD.

Segundo Juliana Pereira, considerando todas as formas de participação, o Debate Público recebeu 1127 contribuições oriundas de diversas frentes. Segundo a Secretária, os temas mais debatidos foram sobre o entendimento do consentimento, o Legítimo Interesse,

a Utilização de Dados Anônimos, o Tratamento de Dados pelo Setor Público e o Órgão Competente.

Em relação aos temas citados, as contribuições convergiram para o mesmo fim. Como o debate sobre o consentimento, que esteve voltado para a mudança do foco, e para a definição do mesmo como inequívoco. Foi demanda a inclusão da possibilidade de tratamento de dados pessoais por Legítimo Interesse e, também, o estabelecimento de critérios objetivos para a sua caracterização. Sugeriu-se que os dados anônimos poderiam ser utilizados desde que não identifiquem o titular nem o afetem diretamente. As análises do debate público foram realizadas em parceria com o Comitê Gestor da internet do Brasil – CGI e com a Universidade Federal de Minas Gerais – UFMG.

Na ocasião, o Consultor da Secretaria Nacional do Consumidor, Danilo Doneda, realizou a apresentação do texto final do APL de dados pessoais. Segundo Doneda, o texto apresenta alguns destaques em comparação com o texto disponibilizado durante a consulta pública:

- Art.2º - Trata-se de uma listagem de fundamentos com o objetivo de ser um guia interpretativo da legislação. Assim, coloca-se a autodeterminação informativa; a liberdade de expressão, comunicação e opinião; a inviolabilidade da intimidade, vida privada, honra e imagem; o desenvolvimento econômico e tecnológico; e a livre iniciativa, a livre concorrência e a defesa do consumidor como bases legais;
- Precisão da definição de dados pessoais, incluindo no escopo identificadores eletrônicos, quando referidos a uma pessoa identificada;
- Inclusão do Termo 'dados anonimizados', fazendo-se referência a técnica de anonimização e não propriamente aos dados anônimos. Essa técnica consiste na retirada de identificação dos dados pessoais;
- Definição de consentimento, colocado como manifestação livre e inequívoca.
- O Capítulo 2º não faz mais referência ao consentimento, o novo texto apresenta Requisitos do Tratamento de dados pessoais. O consentimento tornou-se uma das 9 (nove) hipóteses apresentadas no texto para o tratamento de dados. (art. 7º);
- O 'Interesse Legítimo' tornou-se uma das hipóteses para tratamento de dados pessoais, e não mais, uma exceção. Mantendo a ressalva na aplicação de ser necessário o rigor conceitual, para que o 'Interesse Legítimo' não tornasse uma válvula de escape da norma. Dessa maneira, foram introduzidos no Art. 10º, os requisitos de configuração do 'Interesse Legítimo' para o tratamento de dados pessoais;
- Art. 13º – Inclusão do marco normativo em relação aos dados anonimizados, enquanto tais não estão dentro do escopo da lei. Porém quando revertidos, obviamente cabe a aplicação da lei. Também quando utilizados para perfilhamento;
- Inclusão do Direito de Portabilidade;

- Definição clara sobre as situações de transferência internacional de dados pessoais;
- Inclusão de um Capítulo sobre o tratamento de dados pessoais pelo Poder Público; e
- Criação de um órgão Competente e Independente, sendo este o Conselho Nacional de proteção de Dados e da Privacidade.

Após o encerramento do Debate Público, o Anteprojeto de Lei foi encaminhado ao Congresso Nacional por meio da Mensagem nº 255, de 11 de maio de 2016. O texto foi recebido no dia 13 de maio de 2016, como Projeto de Lei – 5276/2016, que dispõe sobre o tratamento de dados pessoais para a garantia do livre desenvolvimento da personalidade e da dignidade da pessoa natural.

No entanto, tanto a Câmara quanto o Senado, já possuíam Projetos de Leis que tratavam sobre a temática. Considerando o processo legislativo, vamos abordar primeiramente como ocorreu o debate na Câmara dos Deputados, com os projetos 4060/2012 e 5276/2016. Em seguida, retomamos a construção feita no Senado Federal com o projeto 330/2013 e com o debate final da aprovação.

Na Câmara dos Deputados, o PL 4060 foi apresentado em 2012 pelo Deputado Milton Monti (PR/SP) e designado como relator, o Deputado Orlando Silva (PCdoB/SP). Na época, as Comissões de ciência e tecnologia, comunicação e informática, trabalho, de administração e serviço público e constituição e justiça e de cidadania foram instadas a dar parecer.

Em agosto de 2016, o projeto também foi encaminhado à Comissão de desenvolvimento econômico, indústria, comércio e serviços para manifestação. Em razão da distribuição a mais de três comissões de mérito, foi determinado a criação de comissão especial para analisar a matéria, por expressa ordem regimental.

Até então, o PL 4060 seguia em uma tramitação lenta. A Comissão então foi criada em agosto de 2016 e instalada em outubro do mesmo ano. A chegada da matéria oriunda do Poder Executivo mudou o cenário e acelerou o debate. Porém, não foi o único fator responsável por essa mudança de perspectiva. Cabe destacar que em 2013, o bloco europeu iniciou a revisão da normativa após o caso de denúncia revelado por Edward Snowden. Foi no mesmo ano de 2016, que a lei europeia foi aprovada com um prazo de 2 anos para entrada em vigor.

O movimento brasileiro de aceleração do debate foi uma evidente reação à aprovação internacional de um marco legal de proteção de dados pessoais. A norma europeia forçou não

só comunidade internacional a rever as suas normativas, mas também às inúmeras empresas a atualizarem as suas políticas de privacidade. A lei europeia apresenta pontos de forte reação à espionagem feita pelos Estados Unidos e influenciou debates para a elaboração de regulamentações de outros países, como a Lei Brasileira de proteção de dados pessoais.

Considerando a influência internacional, compreendemos a chegada do PL 5217/2016 e a Criação da Comissão Especial de proteção de dados pessoais ao Poder Legislativo. O PL, oriundo do Poder Executivo, foi recebido pela Comissão de Trabalho, de Administração e Serviço Público – CTASP e pela Comissão de Constituição, Cidadania e Justiça – CCJC, designando como relatores os Deputados Orlando Silva (PCdoB/SP) e Alessandro Molon (REDE/RJ), respectivamente. No dia 10 de junho, a Comissão de Ciência e Tecnologia, Comunicação e Informática – CCTCI foi incluída no despacho da matéria, tendo sido designado o Deputado Sandro Alex (PSD/PR) como relator. Em seguida, o texto foi apensado ao Projeto de Lei 4060/2012, de autoria do Deputado Milton Monti (PR/SP) e que possuía como relator, o Deputado Orlando Silva (PCdoB/SP) e passou a tramitar pela Comissão Especial.

Seguindo os passos regimentais, a Comissão foi criada em agosto, constituída em outubro e instalada em novembro, do mesmo ano de 2016. Durante a reunião de instalação e eleição, a composição da Comissão foi feita. Como presidente, a Deputada Bruna Furlan (PSDB/SP). Na 1º Vice-Presidente, Deputado André Figueiredo (PDT/CE). Como 2º Vice-Presidente, Alessandro Molon (REDE/RJ). O 3º Vice-Presidente ficou sendo o autor do PL 4060/2012, Milton Monti (PR/SP). E foi designado como relator, o deputado. Orlando Silva (PCdoB/SP). O grupo também era composto por mais 23 parlamentares de diversos partidos.[20]

Em novembro de 2016, o Deputado Orlando Silva apresentou o Plano de Trabalho para a Comissão Especial então criada. O texto, padrão para as Comissões Especiais, prevê a aprovação de requerimentos diversos; realização de audiências públicas com convite a autoridades públicas; especialistas e membros da sociedade civil; realização de missões externas, no país e no exterior; e, consultas públicas utilizando as ferramentas à disposição da Casa.

O parlamentar também relata os objetivos, métodos e atividades previstas para o grupo. Independente do fluxo de atividades estabelecidos pelo relator, cabe destacar que é posto com

[20] Disponível em: < https://www2.camara.leg.br/atividade-legislativa/comissoes/comissoes-temporarias/especiais/55a-legislatura/pl-4060-12-tratamento-e-protecao-de-dados-pessoais/conheca-a-comissao/membros-da-comissao> Acesso em: 11 de fevereiro de 2020

objetivo final da Comissão Especial o oferecimento e votação do parecer sobre o PL 4060/12, do Deputado Milton Monti, que "dispõe sobre o tratamento de dados pessoais, e dá outras providências", e dos seus apensos, PL 5276/16, do Poder Executivo, que "dispõe sobre o tratamento de dados pessoais para a garantia do livre desenvolvimento da personalidade e da dignidade da pessoa natural"; assim como de outros que porventura vierem a ser apensados ao longo dos trabalhos da Comissão.

Em seguida, no dia 06 de dezembro de 2016, a Comissão realizou a sua primeira Audiência Pública sobre o tema[21]. O encontro foi presidido pela deputada Bruna Furlan e deu início a um processo de protagonismo de alguns atores e temas que serão estratégicos para entendermos o contorno dado para a normativa aprovada.

A análise da experiência legislativa de elaboração da Lei Brasileira de proteção de dados pessoais que será feita a seguir, terá como eixo principal a formação dos conceitos, presentes na lei, de dados sensíveis, dados anonimizados e consentimento, não se aprofundando em outras questões também abordadas no processo, visto que todo o debate foi protagonizado pelo definição desses conceitos. Ao final da análise, será apresentado um mapeamento dos diversos atores que foram citados durante a descrição do processo de construção da lei e seus papeis.

3.3.1 Comissão Especial de proteção de dados pessoais - CESP

A CESP foi responsável pela discussão norteadora do processo legislativo. Presidida pela deputada Bruna Furlan, o grupo realizou diversos encontros temáticos, denominados Audiência Pública. Em tais audiências, uma mesa de convidados temática era montada em uma Sala de Comissões na Câmara dos Deputados, onde cada convidado teria um tempo para explanar sobre o assunto e apresentar seu posicionamento. Sempre presidida pela deputada Bruna Furlan, a plateia contava com outros deputados membros ou não da comissão e visitantes da Câmara. Como exposto, no dia 06 de dezembro de 2016, a CESP realizou a sua primeira Audiência Pública. Participaram do debate, a Coordenadora do Grupo de Trabalho de proteção de Dados da Associação Brasileira de Empresas de Tecnologia da Informação e Comunicação - BRASSCOM, Ana Paula Bialer. A Coordenadora de Análise e Orientação Técnica em Defesa

[21] Disponível em:< https://www.camara.leg.br/evento-legislativo/46016. Acesso em: 11 de fevereiro de 2020

do Consumidor - SENACON, Michelle Ferreira Rodrigues e o Professor da UERJ e Especialista em proteção de dados pessoais, Danilo Doneda.

Na ocasião, a BRASSCOM discursou levantando a bandeira dos dados anonimizados e de uma melhor definição de dados pessoais e dados sensíveis. Em sua fala, externou a preocupação de uma influência da lei nos serviços ofertados pelo mercado, afirmando a necessidade de garantia dos negócios, da inovação e do crescimento econômico.

> Eu gostaria que a gente parasse um pouquinho para desmistificar algumas questões entorno dos dados coletados. É verdade que muitos dos dados coletados são dados pessoais, são informações pessoais. No entanto, a maioria dos dados que nós trabalhamos, não são dados pessoais. São dados que são criados, como monitoramento climático, turbina de aviões, transações financeiras. Que, muito embora, possam ser gerados com relação a uma pessoa, eles não são trabalhados de maneira a identificar uma ou outra pessoa. São trabalhados de maneira não identificada e agregada, gerando uma série de benefícios a sociedade. O dado só tem valor a partir do momento que ele pode ser compreendido. Ou seja, um monte de dado amontoado não passa de algumas observações aleatórias. A compreensão desses dados só é possível a partir do momento que a gente, de fato, agregue." (BIALER, Ana Paula. Durante Reunião Ordinária da Comissão Especial de proteção de dados pessoais no dia 06/12/2016)

Ao final de sua exposição, a representante da BRASSCOM cita a elaboração de Manifesto[22] assinado por diversas empresas do terceiro setor que traz indicação para definição de alguns conceitos-chaves, sendo esses Dado Pessoal, Dado Sensível, dados anonimizados, consentimento, Interesse Legítimo, Responsabilidade Civil, Transferência Internacional de Dados, Órgão Regulador Independente e Sanções.

Como dados sensíveis, o grupo recomenda a classificação como "dados pessoais sobre a origem racial ou étnica, as convicções religiosas, as opiniões políticas, a filiação a sindicatos ou organizações de caráter religioso, filosófico ou político, dados relacionados a condição médica do titular, genéticos e referentes à orientação afetiva e de gênero."

Sobre a anonimização, o documento afirma que não devem estar sujeitas à aplicação da Lei dados pessoais os dados que tenham sido anonimizados e, sobre consentimento, indicam a utilização de uma classificação livre e inequívoca.

[22] Disponível em: < https://brasscom.org.br/manifesto-sobre-a-futura-lei-de-protecao-de-dados-pessoais/> Acesso em: 11 de fevereiro de 2020

Ainda na referida audiência, o professor Danilo Doneda, especialista em proteção de dados pessoais e consultor do Ministério da Justiça no processo de elaboração do Anteprojeto de Lei de proteção de Dados, expôs o seu entendimento. Íntimo do texto em debate, o professor realiza uma defesa do texto do PL 5276/16 e critica a posição da BRASSCOM, afirmando que todos os dados são pessoais, e defendeu o conceito de dados anonimizados, argumentando uma harmonização com a legislação internacional e garantia de um livre fluxo internacional de dados. Em sintonia com o discurso de Danilo Doneda, a representante do Governo Federal faz nova defesa do texto.

A segunda reunião da Comissão, realizada no dia 14 de dezembro de 2016, foi uma nova Audiência Pública com representantes de outros segmentos. Estiveram presentes a representante do Intervozes - Coletivo Brasil de Comunicação Social, Beatriz Barbosa; o pesquisador do GPoPAI/USP - Grupo de Pesquisa em Políticas Públicas de Acesso à Informação, Bruno Bioni; e o pesquisador do Instituto Brasileiro de Defesa do Consumidor – IDEC, Rafael Zanatta.

Diferentemente da primeira Audiência Pública, a mesa foi composta por atores com discursos mais protecionistas. Nessa oportunidade, os deputados membros da comissão se posicionaram de forma mais clara, principalmente o relator Orlando Silva, a presidente Bruna Furlan e o deputado André Figueiredo. Bruno Bioni foi o primeiro a apresentar as suas contribuições no encontro. O pesquisador chamou atenção para a construção dos conceitos de Dado Pessoal, Dado Anônimo e consentimento, pois considera estes o tripé da regulamentação da proteção de dados pessoais, e na sistematização dos três projetos de leis que existiam no parlamento sobre o tema. Além disso, argumentou pela construção de uma lei expansionista que considera dados pessoais aquelas informações com potencialidade de identificação, para garantia da privacidade dos cidadãos brasileiros. Para Bioni, uma lei reducionista pouco seria efetiva na proteção de dados pessoais. Na prática, para ele, relacionar dados os torna identificável.

A participação do Intervozes seguiu harmônica com a fala do Bioni. Beatriz defendeu uma proteção efetiva dos dados pessoais para garantia da liberdade de expressão e do Direito à Comunicação. Beatriz defendeu a possibilidade de revogação do consentimento e do Direito ao Esquecimento.

O representante do IDEC, Rafael Zanatta, fez uma intensa defesa do texto do PL 5276/2016, afirmando ser ele um resultado de intendo debate com a sociedade. Em sua fala,

demonstrou preocupação com o Manifesto apresentado pela BRASSCOM, assinado também por diversas empresas do setor de comunicação, publicidade e tecnologia, destacando que que o texto apresenta graves distorções. Rafael afirmou que o IDEC se manifestou a favor da versão final do PL 5276/16, pelo seu conteúdo e método democrático de construção legal. Em sua manifestação, demonstrou preocupação com o atraso regulatório e as tentativas de desmonte ao texto, em apoio a projetos paralelos. Apresentou, também, uma carta aberta da Coalização Direitos na Rede, onde 35 Organizações Não-Governamentais apoiam a versão do PL, que foi construída em 6 anos.

O relator, deputado Orlando Silva, defendeu uma harmonização do conceito de consentimento com o texto do Marco Civil da internet.

O terceiro encontro da Comissão Especial ocorreu em março de 2017[23]. O grupo realizou uma Audiência Pública para debater a definição de dados pessoais, Sensíveis e Anonimizados. Estiveram presentes na ocasião, a Diretora da Área Legal da Associação Nacional de Birôs de Crédito – ANBC, Vanessa Butalla; O Conselheiro do Comitê Gestor da internet no Brasil - CGI.br, Luiz Fernando; o Representante do Instituto Beta para internet e Democracia – IBIDEM, Paulo Rená; e a Representante do Centro de Direito, internet e Sociedade do Instituto Brasiliense de Direito Público - Cedis/IDP-DF, Laura Schertel. O debate contou, pela primeira vez, com a participação do Deputado Celso Russomanno e da Deputada Margarida Salomão.

Vanessa Butalla, representante da ANBC, apresentou algumas sugestões da Associação que representa a totalidade do mercado brasileiro de birôs de crédito. Para ela, o texto da lei deve conter uma identificação de que dados pessoais são aqueles referentes a uma pessoa natural identificada ou razoavelmente identificável pelo responsável pelo tratamento de dados pessoais. argumentaram-na mesma linha, defendeu que a biometria não pode ser considerada como dado sensível, visto que é utilizada para fins de identificação ou confirmação de identidade de pessoas naturais.

A principal argumentação da ANBC é em relação à finalidade do dado pessoal coletado. eis que os dados pessoais abrangem um espectro de espécies, e a associação se preocupa com o tratamento que a lei dá para os dados cadastrais. Segundo a ANBC, é evidente que os dados cadastrais são dados pessoais por essência, pois identificam o indivíduo. No entanto, merecem

[23] Disponível em: <https://www.camara.leg.br/evento-legislativo/46522> Acesso em: 11 de fevereiro de 2020

um tratamento diferenciado quando usado para uma finalidade específica. Nome, filiação, data de nascimento, e outros, quando usados para identificar uma pessoa não deve requerer consentimento visto que há o interesse legítimo, por prevalecer o interesse público perante o particular. A mesma argumentação foi usada para a biometria.

Para a ANBC, tratamento atual de dados anonimizados é importante e é base de serviços e produtos do setor. Ainda que sejam colhidos de forma identificada, são armazenados e tratados de forma anônima. Se a lei não admitir o uso de dados anonimizados, o setor afirma que não conseguirá trabalhar com o *score* de análise de histórico de crédito. A associação também se mostrou contrária à proibição de transferência de dados mantidos por órgãos públicos para empresa privada.

Paulo Rená, representante do IBIDEM, enalteceu as qualidades técnicas do projeto de lei 5276/2016. O Instituto Beta radicaliza na definição de dado pessoal, que é qualquer dado que possa identificar um indivíduo. Paulo cita a definição de dados pessoais utilizada pelo Conselho da Europa, que afirma que dados sobre uma pessoa cuja identificação é evidente ou que pode, pelo menos ser determinada através da obtenção de informações adicionais. Para ele, se for possível identificar uma pessoa agregando outro dado, a lei deve tutelar essa informação como sendo dado pessoal.

A Audiência seguiu com a participação do Comitê Gestor da internet no Brasil, representada pelo Luiz Fernando, e pela Laura Schertel, representante do Centro de Direito, internet e Sociedade. Ambas as participações reiteraram o texto do projeto de lei em discussão. Laura Schertel demonstrou preocupação com os conceitos em debate, afirmando que a definição de dados pessoais, sensíveis e anonimizados são a essência de uma lei geral de proteção a esses dados,. Para ela, o objetivo do debate é a regulamentação e não uma proibição do tratamento de dados, por isso a importância de garantir uma definição clara de conceitos. Luiz Fernando afirmou que o Brasil estava atrasado e demonstrou preocupação com a morosidade do debate. Para ele, a coleta de dados tem que ser transparente e possuir uma finalidade. O Conselheiro classificou o entendimento de interesse legítimo como uma alternativa de burlar as proibições previstas em lei. Reconheceu que evitar o fluxo de dados não é possível nem devido, mas a lei deve garantir quais dados devem ser coletados e tratados de forma a garantir os direitos fundamentais do cidadão.

Uma figura emblemática no debate sobre o direito do consumidor, o deputado Celso Russomano, participou pela primeira vez da discussão. O parlamentar relatou algumas experiências particulares para demonstrar apoio ao texto do poder executivo.

O quarto encontro da Comissão ocorreu no dia 29 de março de 2017[24] sendo mais um debate público com presença de atores representantes de diversos setores. Na ocasião, estiveram presentes Carlos Affonso Souza, Diretor do Instituto de Tecnologia & Sociedade do Rio - Its; Efraim Kapulski, Presidente da Associação Brasileira de Marketing Direto - ABEMD; e Henrique Lian, Coordenador Institucional da Proteste.

A ABEMD defendeu que o consumidor deve ser responsável por escolher o que deve ser feito com os seus dados, não devendo a legislação criar barreiras que dificultem ou proíbam o tratamento de dados.

Henrique Lian, representante da Proteste, anunciou a criação da Frente Parlamentar única de defesa do consumidor para ampla defesa da proteção dos dados pessoais e defendeu o texto em debate. Assim como o representante do ITS, Carlos Affonso, que destacou uma preocupação para que não haja distorção do conceito de consentimento no texto normativo.

Os encontros seguintes tiveram como objeto o debate sobre legítimo interesse e responsabilidade objetiva e solidária. [25] Por não ser um dos eixos de análise do trabalho em questão, as Audiências Públicas não foram analisadas.

Nos dias 10 e 11 de maio de 2017, a Comissão Especial realizou o Seminário Internacional de proteção de dados pessoais. [26] Foram dois dias de intensa discussão sobre as experiências internacionais de regulamentação. Em suma, o evento evidenciou o atraso normativo que o Brasil se encontrava e o risco de interferência no livre fluxo de dados, caso não fosse aprovada uma Lei Geral de proteção de dados pessoais antes da entrada em vigor da Lei Europeia.

Após o Seminário, a Comissão continuou realizando uma série de encontros considerando partes específicas do texto e setores que seriam impactos pela legislação em construção. No dia 31 de maio de 2017, foi realizada uma Audiência Pública sobre o tema

[24] Disponível em: https://www.camara.leg.br/evento-legislativo/46615. Acesso em
[25] Disponível em: https://www.camara.leg.br/evento-legislativo/46723. Acesso em
[26] Disponível em: https://www2.camara.leg.br/atividade-legislativa/comissoes/comissoes-temporarias/especiais/55a-legislatura/pl-4060-12-tratamento-e-protecao-de-dados-pessoais/documentos/outros-documentos/programacao-seminario-internacional-sobre-privacidade-e-protecao-de-dados-pessoais.Acesso em

"Modelo Regulatório órgão, agência e autorregulamentação". O quinto encontro recebeu a Coordenadora da Área de Conjuntura do internetLab, Beatriz Kira; a professora da Faculdade de Direito da USP, Cintia Rosa; o Diretor-Substituto de proteção de Defesa do Consumidor do MJ, Gabriel Carvalho; o Secretário de Política de Informática, Maximiliano Martinhão; o Coordenador Estratégico de Segurança da Informação do Serviço Federal de Processamento de Dados, Ulysses Machado; e o Diretor Regulatório do Sindicato Nacional das Empresas de Telefonia e de Serviço Móvel Celular e Pessoal do SindiTelebrasil, Alexandre Castro.

Beatriz Kira, representante do internetLab, apresentou pesquisas realizadas pelo grupo, mas manteve as contribuições focadas no tema da Audiência Pública. Cintia Rosa elogiou o trabalho da Comissão Especial e enalteceu a atuação da Deputada Bruna Furlan e do Relator Orlando Silva. A professora relatou sua experiência na Itália e a sua avaliação no modelo regulatório aplicado no país.

O representante do SindiTelebrasil, Alexandre Castro, manifestou-se com foco no processo de revolução tecnológica. Na ocasião, afirmou que o Marco Legal em debate tem que estabelecer práticas de privacidade e segurança adequadas ao risco de danos ao titular. Também deve minimizar custos operacionais viabilizando a criação de milhares de pequenas e médias empresas. O sindicato defende que a normativa crie um ambiente de estímulo e fomento a inovação e ao investimento estável, duradouro e transparente em TICs, além de minimizar as restrições sobre fluxos de dados transfronteiriços.

Os representantes do governo, Ulysses Machado, Gabriel Carvalho e Maximiliano Martinhão, não entraram em nenhum momento no debate conceitual de interesse da análise feita na pesquisa. Sobre o tema objetivo da Audiência Pública, todos fizeram uma defesa da criação de uma agência independente para regulação da proteção de dados pessoais.

O relator Orlando Silva reconheceu ser consenso entre todas as partes a constituição de uma agencia reguladora de proteção de dados pessoais.

Seguindo a construção de debates temáticos, a sexta reunião, realizada no dia 07 de junho de 2017, tratou de Transferência Internacional de Dados. O encontro não adentrou nos aspectos que nos interessa, porém reforçou o protagonismo de alguns atores, como Bruno Magrani, representante do Facebook, e o Danilo Doneda, representando o *Open Knowlegde Foundation*. Além desses atores, participaram do encontro Joana Varon, Diretora da *Coding Rights* e Thiago Sombra, Docente da Universidade de Brasília.

A e sétima última audiência pública temática foi realizada no dia 05 de julho de 2017 e tratou sobre "Liberdade de Expressão e proteção de dados pessoais". Na ocasião, os expositores foram a Associação Brasileira de Rádio e Televisão – ABRATEL; a Beatriz Barbosa, representante do Fórum Nacional pela Democratização da Comunicação[27]; o Marcelo Berchara, consultor da Associação Brasileira de Emissoras de Rádio e Televisão; Pedro Mizukami, do Centro de Tecnologia e Sociedade da Fundação Getúlio Vargas; e Maria Inês, Presidente do Instituto Nacional de Estudos e Pesquisas Educacionais Anísio Teixeira.

As reuniões seguintes foram realizadas para debate sobre dois setores: "Inovação e Indústria 4.0" e sobre "Agricultura de Precisão". Os encontros realizados nos dias 11 e 12 de julho de 2017 foram os únicos que debateram setores específicos. Quando falamos de articulação política e defesa de interesses, esses dois encontros devem ser vistos como um espaço de protagonismo dos dois setores dentro da discussão de lei brasileira de proteção de dados pessoais.

O tema *Agricultura de Precisão* foi debatido pela Escola de Direito da Fundação Getúlio Vargas - SP; pela Comissão Brasileira de Agricultura de Precisão; pela Associação Brasileira de Sementes e Mudas - ABRASEM; pela Empresa Brasileira de Pesquisa Agropecuária - EMBRAPA; e pela Confederação da Agricultura e Pecuária do Brasil - CNA.

O debate buscou promover o entendimento de que a Agricultura de Precisão tem por objeto melhorar a produção agrícola, causando menos impacto ambiental. Para tanto, o uso de dados gerados na produção agrícola deve ser de uso livre para fomentar a tecnologia. A CNA defendeu uma estrutura normativa eficiente, simplificada e moderna, para que o setor avance e aproveite suas potencialidades, respeitando os direitos dos produtores rurais. Assim como o setor agropecuário, o grupo que debateu a "Inovação e Indústria 4.0", manteve o discurso de garantia do desenvolvimento tecnológico.

---

[27] "Grupo que congrega mais de 500 filiadas, entre associações, sindicatos, movimentos sociais, organizações não-governamentais e coletivos que se articulam para denunciar e combater a grave concentração econômica na mídia, a ausência de pluralidade política e de diversidade social e cultural nas fontes de informação, os obstáculos à consolidação da comunicação pública e cidadã e as inúmeras violações à liberdade de expressão. Organizado em quase todo o Território Nacional, em 20 Comitês Estaduais ou Regionais pela Democratização da Comunicação, o FNDC nasceu nos anos 80 como movimento social pela democratização da comunicação. Nessa época, teve papel essencial no embate político, institucional e teórico sobre o setor. Foi atuante na finalização dos trabalhos da Assembleia Nacional Constituinte que preparava a nova Constituição Federal. Ao final, foi instituído o capítulo V da Carta Magna, com artigos que tratam especificamente da Comunicação." (Fórum Nacional pela Democratização da Educação, disponível em: < http://fndc.org.br/forum/quem-somos/>. Acesso em....

Foram convidados para o encontro do dia 12 de julho de 2017, a Associação Brasileira das Empresas de Software - ABES; a Confederação Nacional da Indústria - CNI; a Associação Brasileira da Indústria Elétrica e Eletrônica - ABINEE; e a Câmara Americana de Comércio - AMCHAM.

Na ocasião, a AMCHAM defendeu que o escopo de aplicação da lei deve considerar os dados pessoais coletados em território brasileiro ou gerados por cidadãos brasileiros residentes no Brasil ou por empresas brasileiras ou sujeitas à legislação nacional.

As atividades da Comissão Especial foram encerradas em um Seminário conjunto com a Comissão de Ciência e Tecnologia, Comunicação e Informática da Câmara do Deputados, tratou de tema sensíveis ao debate sobre a proteção de dados pessoais, mas que não estiveram presentes nos momentos temáticos. Foram esses: "Abordagem regulatória para o tratamento de dados pessoais"; o "O uso de dados pessoais como instrumento de campanha eleitoral e a persuasão da opinião pública"; e "Tratamento a notícias falsas - *fake news*".

Além dos representantes do governo e do judiciário, o terceiro setor foi representado pelo Empresa de pesquisa A Ponte Estratégia; pelo Facebook no Brasil; Empresa de marketing digital Yey Inteligência; Google no Brasil e ABRATEL.

3.3.2 Contribuições ao texto

Além das contribuições durante as 13 audiências, a Comissão Especial recebeu contribuições diretas ao texto. Foram 21[28] enviadas por representantes da academia, da sociedade e civil e do setor regulado (terceiro setor).

Das 21 contribuições, 11 fizeram sugestões para a construção do conceito de dados sensíveis. (Apêndice B) Para a Brasscom, a LGPD deveria categorizar dados sensíveis como dados pessoais sobre a origem racial ou étnica, as convicções religiosas, as opiniões políticas, a filiação a sindicatos ou organizações de caráter religioso, filosófico ou político, dados relacionados à condição médica do titular, referentes à saúde ou a vida sexual, e dados genéticos e referentes à orientação afetiva e de gênero e biométricos;

[28] Disponível: < https://www2.camara.leg.br/atividade-legislativa/comissoes/comissoes-temporarias/especiais/55a-legislatura/pl-4060-12-tratamento-e-protecao-de-dados-pessoais/documentos/outros-documentos/copy_of_contribuicoes-ao-texto>. Acesso em: 11 de fevereiro de 2020

Para a Associação Brasileira das Empresas de Software, assim como a Brasscom, o conceito de dados sensíveis não deveria considerar a biometria. Para o Facebook, deveriam estar previstas exceções claras às formalidades para o tratamento de dados sensíveis, em especial quando o seu tratamento for voltado a trazer benefícios aos titulares ou quando os titulares houverem voluntariamente disponibilizado os dados. A Febraban defendeu a inclusão da possibilidade de tratamento dos dados sensíveis se justificado por cumprimento de legislação específica, no exercício regular de direito do responsável ou quando for necessário como meio de prova.

A Comissão recebeu 9 contribuições sobre o conceito de dados anonimizados. Para a ANBC, dados anonimizados são os dados relativos a um titular que não seja identificado pelo responsável para a finalidade a que se destina o tratamento. O Facebook defendeu que dados anonimizados devem ser claramente excluídos do escopo da lei. Já a Câmara de Comércio dos Estados Unidos defendeu em seu texto que os dados genéticos ou biométricos devem estar expressamente ligados a um registo individual ou médico, a fim de incentivar a inovação e a investigação médica contínua. Grandes avanços médicos estão ocorrendo atualmente com o uso dos dados genéticos que são anonimizados frequentemente ou completamente randomizados, e agregados de modo a fazer com que os indivíduos fiquem virtualmente não identificáveis.

Para a ABRANET, Dados anonimizados devem ser considerados aqueles dados relativos a um titular que não possa ser identificado no nível individual pelo responsável pelo tratamento, tendo em conta o conjunto de meios suscetíveis de serem razoavelmente utilizados para identificar o referido titular, ou desde que os responsáveis pelo tratamento estejam sob obrigação contratual, administrativa ou legal de manter os dados anonimizados.

Sobre consentimento, a ABRASEM apresentou argumentação para que sejam nulas as autorizações excessivamente genéricas para o tratamento de dados pessoais em descumprimento da lei. A ABRANET defende o consentimento como manifestação inequívoca realizada pelo titular de dados de maneira livre e informada para autorização do tratamento de seus dados pessoais. Para o Facebook, a regra do consentimento livre, informado e inequívoco deve prevalecer sobre regras de consentimento expresso

3.3.3 Aprovação no Plenário da Câmara dos Deputados

O PL 4020/2012 e seus apensados foram pautados em sessão plenária na Câmara dos Deputados no dia 29 de maio de 2018 após aprovação de um requerimento de urgência. A deputada Bruna Furlan defendeu a aprovação do PL de proteção de dados pessoais.

O Deputado Orlando Silva emitiu parecer em plenário ao PL 4060/2012. Em sua fala como relator, elogiou o trabalho do deputado Milton Monti e da deputada Bruna Furlan. Destacou também os parlamentares Sandro Alex, Gourlart, Margarida Salomão, Celso Pancera e Celso Russomano. Orlando afirmou que durante 2 anos, o grupo que compunha a CESP realizou 13 audiências temáticas e um seminário internacional. Informou que há uma necessidade de aprovação da normativa para o Brasil ter uma legislação compatível com a União Europeia e não prejudicar os negócios e o fluxo de dados entre as partes.

Ainda em seu parecer, Orlando Silva destacou que buscou ouvir todos as partes interessadas e teve cuidado e rigor com a definição de dado pessoal e sensível. Segundo ele, buscou um conceito preciso, mas que não inibisse a inovação tecnológica. O relator também discorreu sobre o tratamento próprio de dados presentes no arcabouço da segurança púbica. E fixou o consentimento como expresso e inequívoco. Durante a tramitação, o texto recebeu 11 emendas, sendo que 6 foram acatadas pelo relator. No Dia 29 de maio de 2018, a matéria foi aprovada na forma do substitutivo apresentado pelo deputado Orlando Silva. A matéria seguiu para o Senado Federal como PLC 53/2018.

3.3.4 Debate e aprovação no Senado Federal

O PL 4060/2016 chegou ao Senado Federal como PLC 53/2018 no dia 01 de junho de 2018. O texto passou a tramitar em conjunto do PLS 330/2013, que já tramitava em conjunto com os PLS 131/2014 e PLS 181/2014, devendo ser analisado pela Comissão de Assuntos Econômicos, pela Comissão de Ciência e Tecnologia e pela Comissão de Constituição e Justiça.

Cabem algumas observações sobre os projetos que já estavam em debate na Casa, antes da chegada do Projeto aprovado na Câmara dos Deputados. Durante a discussão feita pelos Deputados, o Projeto de Lei do Senado n° 330, de 2013, de autoria do Senador Antônio Carlos

Valadares (PSB/SE), já estava sendo debatido simultaneamente à tramitação do PL 4060/2016. Durante esse tempo, diversos setores movimentaram-se para que o PLS 330/2013 fosse aprovado antes no Senado, visto que o texto era considerado mais ameno. Por exemplo, o texto originário da Câmara dos Deputados previa multa de até 4% do faturamento da companhia, limitada, no total, a R$ 50 milhões. Já o texto do Senado, previa multa de até 2% sobre o faturamento da empresa.

Na época, os relatores, deputado Orlando Silva e o senador Ricardo Ferraço negaram que existia uma disputa na autoria do texto base para a futura Lei Geral de proteção de dados pessoais. Porém, nos bastidores das casas legislativas havia evidente mobilização para angariar apoio dos setores interessados em cada texto.

Por fim, o PL 4060/2016 foi aprovado na forma do substitutivo proferido pelo deputado Orlando Silva e seguiu para revisão do Senado Federal. A primeira comissão a analisar o texto, PLC 53/2018 apensado ao PLS 330/2013, foi a Comissão de Assuntos Econômicos. Em junho, o senador Ricardo Ferrado foi designado relator e, após intensa articulação com setores interessados, o seu relatório foi aprovado no dia 3 de julho de 2018, tendo recebido 9 emendas.

A Comissão de Assuntos Econômicos, através do senador Ricardo Ferraço, emitiu parecer favorável ao PLC 53/2018, que dispõe sobre a proteção de dados pessoais. O documento apresentado por Ferraço realizou alterações no texto originário da Câmara dos Deputados e rejeitou as proposições com origem no Senado que tramitavam em conjunto: PLS 131/2014, PLS 181/2014 e PLS 330/2013. Durante as discussões, Ferraço afirmou que as emendas aprovadas foram para aprimorar a técnica legislativa e garantir o equilíbrio entre a proteção à privacidade e a inovação tecnológica. Na mesma reunião em que houve a aprovação do parecer do relator, houve a aprovação de um requerimento de urgência. Dessa forma, a matéria seguiu direto para o Plenário.

No dia 10 de julho de 2018, a matéria foi pautada em plenário e aprovada por unanimidade.[29] Devido ao regime de urgência, o Senador Eduardo Braga proferiu parecer pela CCT e CCJ no plenário. Com parecer favorável, Eduardo Braga defendeu a necessidade de aprovação do texto para estabelecimento de uma segurança jurídica na proteção de dados

[29] Disponível em:< https://www12.senado.leg.br/tv/plenario-e-comissoes/ordem-do-dia/2018/07/protecao-de-dados-pessoais-tem-regras-aprovadas-e-segue-para-sancao-presidencial> Acesso em: 11 de fevereiro de 2020

pessoais no Brasil. O texto foi discutido pelo senador Lindberg Faria, pela senadora Vanessa Grazziotin, pelo senador Jorge Viana, pela senadora Lídice da Mata

O relator da matéria Ricardo Ferraço afirmou, em seu parecer, o tempo que a matéria esteve em debate nas casas legislativas. Afirmou que 60 entidades atuaram na construção coletiva do texto aprovado. Com isso, o texto foi aprovado por unanimidade no Senado Federal.

Após elaboração legislativa, a Lei de proteção de dados pessoais foi sancionada e publicada no dia 14 de agosto de 2018, como Lei nº 13.709/2018, "que dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da internet)". Porém, a normativa só entrará em vigor em 2020.

Para Pita (2017), o cenário brasileiro exige que as organizações pró-privacidade trabalhem formas de diálogo próximo com a população, para colaborar com a criação de uma consciência social do valor dos seus dados pessoais e da compreensão dos conceitos de privacidade, sigilo e vigilância no seu cotidiano.

3.3.5 Medida Provisória e alterações legislativas

No dia 28 de dezembro de 2018, foi publicada no Diário Oficial da União, a Medida Provisória nº 869/2018, que alterava a Lei nº 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de proteção de Dados.[30] Em fevereiro de 2019, o Senado Federal criou a Comissão Mista para analisar e debater o texto em questão. O grupo recebeu 176 emendas dentro do prazo regimental.[31] A Comissão foi instalada em março de 2019, sendo eleito Presidente o Senador Eduardo Gomes e designado Relator o Deputado Orlando Silva.

A comissão realizou diversos debates e audiência pública para debater as principais alterações na lei de proteção de dados pessoais proposta pela Medida Provisória. No dia 8 de julho de 2019, a Medida Provisória nº 869/2018 foi convertida na Lei nº 13.853/2019, alterando

[30] Disponível em: http://pesquisa.in.gov.br/imprensa/jsp/visualiza/index.jsp?jornal=515&pagina=8&data=28/12/2018 Acesso em: 11 de fevereiro de 2020

[31] Disponível em: < https://legis.senado.leg.br/sdleg-getter/documento?dm=7915984&ts=1571777425585&disposition=inline>. Acesso em: 11 de fevereiro de 2020

a Lei de proteção de dados pessoais. A principal alteração foi sobre a criação da Autoridade Nacional de proteção aos Dados – ANPD e a definição do conceito de Encarregado. A ANPD foi instituída com natureza "transitória", ou seja, pode ser absorvida pelo Executivo como entidade da administração pública federal indireta, como autarquia e com vínculo direto com a Presidência da República. O texto aprovado prevê a criação em até dois anos.

Apesar de ser de grande importância estrutural, o texto que será utilizado para análise e comparação que serão feitas a seguir será o texto aprovado e sancionado em agosto de 2018. O objetivo da pesquisa é realizar um recorte histórico e conceitual da normativa brasileira, descrevendo o processo de criação da lei, reconhecendo os atores-chaves e suas influencias e interferências. A aprovação da Lei Brasileira de proteção de dados pessoais ocorreu no mesmo período da entrada em vigor do Regulamento Geral de proteção de Dados (a Lei Europeia de proteção de dados pessoais), por isso, o texto aprovado na época se faz útil para a finalidade.

3.4 LEI BRASILEIRA DE PROTEÇÃO DE DADOS PESSOAIS: CARACTERÍSTICAS E ASPECTOS-CHAVES

Após anos de debate, em agosto de 2018, a Lei de proteção de dados pessoais foi sancionada e entrará em vigor após 24 meses da sua publicação. A Lei foi sancionada com alguns vetos, em destaque nos artigos que criavam a agência reguladora de dados pessoais (arts. 55 a 59), que estabeleciam as regras de compartilhamento de dados entre administração pública e empresas privadas (art. 23, inc. II, art. 26, inc. II, §1º e art. 28).

O texto que entrará em vigor no ano de 2020 é considerado uma normativa harmônica com a legislação internacional e satisfatória para a sua finalidade. A LGDP reconhece dado pessoal como aquela informação relacionada a pessoa natural identificada ou identificável. O texto sancionado em agosto[32] prevê 9 hipóteses para que o tratamento dos dados pessoais seja realizado. Quando o fornecimento é dado pelo titular é a primeira delas. As demais hipóteses consistem na autorização da administração pública na execução de políticas públicas; para a realização de estudos por órgão de pesquisa; para garantir a execução de contratos; para a proteção da vida e para a proteção do crédito.

[32] Em 2019, foi realizada uma alteração incluindo mais uma hipótese para o tratamento de dados. Sendo assim: VIII - para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; (Redação dada pela Lei nº 13.853, de 2019). Disponível em http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2019/Lei/L13853.htm#art2

A seguir analisaremos como a lei definiu os aspectos-chaves analisados ao decorrer da pesquisa.

3.4.1 Dados sensíveis

O artigo 5º da lei definiu dado pessoal sensível aquele "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;"[33]

Cabe destacar que, durante o debate de construção da lei, alguns setores trabalharam para a retirada dos dados genéticos ou biométricos do conceito. Porém o texto original do PL 5276/2016 não faz essa vinculação a uma pessoa natural. A Associação Brasileira de Marketing Pessoal[34] foi um dos grupos que articulou por uma definição que vinculasse expressamente os dados sensíveis à identificação de uma pessoa natural. Em sua contribuição ao texto, a Associação indicou a seguinte definição para dados sensíveis:

> III – dados sensíveis: dados pessoais sobre a origem racial ou étnica, as convicções religiosas, as opiniões políticas, a filiação a sindicatos ou a organizações de caráter religioso, filosófico ou político, dados referentes à saúde ou à vida sexual e dados genéticos ou biométricos, salvo quando a utilização destes últimos for exclusivamente para identificação de pessoas naturais, hipótese em que o dado será considerado pessoal, nos termos do inciso I.

O grupo argumenta que o texto original considerava indistintamente informações biométricas sem correlação ao uso destas informações. Para eles, poderia causar restrição na utilização de dados. Assim como a ABEMD, o Facebook, a ABES e a AMCHAM foram grupos que articularam por essa definição correlacionada.

Dado o exposto, a Lei 13.709 regula como sendo dados sensíveis aqueles os dados pessoais que dizem sobre 7 categorias, sendo essas: 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

[33] Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709compilado.htm

[34] Disponível em: https://www2.camara.leg.br/atividade-legislativa/comissoes/comissoes-temporarias/especiais/55a-legislatura/pl-4060-12-tratamento-e-protecao-de-dados-pessoais/documentos/outros-documentos/ABEMDAssociaoBrasileiradeMarketingDireto.pdf Acesso em: 11 de fevereiro de 2020

vinculado a uma pessoa natural. Essas informações são consideradas "sensíveis" e tuteladas pela lei de maneira especial pela garantia do Princípio da Não-Discriminação.

No entanto, mesmo que o dado pessoal seja considerado sensível, a normativa brasileira de proteção de dados pessoais permite o tratamento desse tipo de dado em algumas hipóteses. Essas hipóteses são descritas no art. 11, sendo a primeira estabelecida pelo consentimento do titular.[35] Porém, o texto prevê uma série de possibilidades para o tratamento desses dados sem o fornecimento de consentimento do titular. São 7 situações[36] que se concentram na execução de políticas públicas, realização de pesquisas e estudos, proteção da vida e tutela da saúde e garantia da prevenção à fraude.

3.4.2 Dados anonimizados

Um dos conceitos mais debatidos no processo de formulação da lei foi o de dados anonimizados. O texto final consentiu com a possibilidade de anonimização e de existência de dados anonimizados, definindo como sendo aquele dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento. Em seu artigo 12, a normativa dispõe que os dados anonimizados não serão considerados dados pessoais. Ou seja, caso os dados sejam anonimizados em sua totalidade, eles deixam de ser tutelados pela LGPD. No entanto, deve-se garantir que os dados não sejam passíveis de reversão.

> 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

[35] Art. 11. O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses: I - quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas;

[36] II - sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para: a) cumprimento de obrigação legal ou regulatória pelo controlador; b) tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos; c) realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis; d) exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral. e) proteção da vida ou da incolumidade física do titular ou de terceiro; f) tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; g) garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no art. 9º desta Lei e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais.

> anonimização, de acordo com as tecnologias disponíveis, e a utilização exclusiva de meios próprios.
> § 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.
> § 3º A autoridade nacional poderá dispor sobre padrões e técnicas utilizados em processos de anonimização e realizar verificações acerca de sua segurança, ouvido o Conselho Nacional de proteção de dados pessoais.

Durante a construção da lei, o debate sobre a possibilidade real de anonimização de dados foi intenso. Diversas contribuições acadêmicas, como a do professor Bruno Bioni, do Intervozes e da Coalização pelos Direitos em Rede, buscaram apresentar uma visão de que o processo de anonimização é falho e o dado pode ser identificável quando associado com outras informações. Por outro lado, o Facebook e outros grupos articularam por uma normativa que não abarcasse os dados anonimizados, ou seja, se um dado for anonimizado, a LGPD não se aplicará a ele.

3.4.3 Consentimento

O consentimento aparece diversas vezes no texto da lei, como condição, hipótese ou sua simples definição. O art. 5º da LGPD define consentimento como a "manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada".

Ao analisar a construção do debate sobre normativas de proteção de dados pessoais, Mendes (2014) discorre sobre alguns princípios fundamentais. Sendo eles, o *princípio da finalidade; da transparência; da qualidade dos dados; da responsabilidade e do consentimento.* A autora defende que o consentimento é um dos eixos estratégicos de uma normativa que tutela os dados pessoais. Para ela, o consentimento é algo tão sensível que pode ser questionado em sua eficácia, haja vista a possibilidade de exclusão do indivíduo que não fornecer o seu consentimento para o tratamento de seus dados. Mendes (2014) também chama atenção para a violação da proteção de dados após o consentimento ser fornecido e o consentimento para aqueles dados considerados sensíveis.

Todas essas questões estão previstas nas 35 vezes que o termo aparece no texto da LGPD. No entanto, ao analisar a legislação, Bioni (2018) destaca uma alteração importante entre o Anteprojeto de Lei de proteção - APL de dados pessoais, que se transformou no PL

5276/2018, e o texto sancionado. Bioni (2018) afirma que a lei considera o consentimento como uma hipótese legal, o APL trazia o consentimento como base legal para o tratamento de dados.

No entanto, o autor reconhece que a LGPD aplica o consentimento em todo o seu texto, evidenciando-o como valor fundamental da normativa. Para Bioni (2018), a Lei Brasileira de proteção de dados pessoais possui uma carga principiológia "que procura conformar, justamente, a ideia de que o titular dos dados pessoais deve ser empoderado com o controle de suas informações pessoais e, sobretudo, na sua autonomia da vontade". (BIONI, 2018, p.135) Além disso, o texto buscar determinar que o controle dos dados se dará através do consentimento.

A LGPD prevê que o consentimento pode ser revogado a qualquer momento mediante manifestação expressa do titular, por procedimento gratuito e facilitado. consentimento este que, segundo o art. 8º, deverá ser fornecido por escrito ou por outro meio que demonstre a manifestação de vontade do titular.

O art. 18º define todos os direitos do titular dos dados pessoais. A qualquer momento, o cidadão pode requerer a confirmação da existência de tratamento dos seus dados; ter acesso aos dados; corrigir dados incompletos, inexatos ou desatualizados.

A Lei Brasileira de proteção de dados pessoais entra em vigor em 2020. No entanto, será ineficiente até o momento em que a população tenha acesso e conhecimento sobre o tratamento dos dados pessoais e seus direitos. A questão posta é que a normativa brasileira segue o entendimento internacional de que o titular dos dados pessoais deve autodeterminar as suas informações pessoais. As normativas mais atuais reconhecem o direito do indivíduo de controlar os seus dados e, com isso, o consentimento é visto como eixo estratégico dessas construções legislativas. Doneda (2006) e Bioni (2018) criticam sobre a real capacidade de racionalidade, conhecimento e de poder de negociação que esses titulares possuem frente a todo processo de tratamento das informações pessoais. De toda forma, as legislações mais atuais de proteção de dados pessoais, a brasileira e a europeia, identificam o titular dos dados como controlador das suas informações.

3.5 A LEI BRASILEIRA VERSUS A LEI EUROPEIA EM PERSPECTIVA COMPARADA

A proposta de criação da *General Data Protection Regulation* - GDPR foi apresentada apenas em 2012 pela Comissão Europeia. A lei foi aprovada em abril de 2016, entrando em

vigência em 2018. A entrada em vigor da lei ocorreu, embora por acaso, junto com o caso de vazamento de dados pessoais envolvendo o Facebook, e a empresa britânica *Cambridge Analytica.*

A aprovação de GDPR, juntamente com os escândalos internacionais e os casos de espionagem denunciados em 2014, impulsionaram o debate sobre a elaboração da Lei Brasileira de proteção de dados pessoais.

A Lei Brasileira de proteção de dados pessoais, nº 13.709, sancionada no dia 14 de agosto de 2018, foi o resultado do processo de discussão da regulamentação brasileira da internet.

A normativa europeia gerou uma onda de atualização das leis de outros países e das políticas de privacidade de empresas ao redor do mundo. Por exemplo, a lei geral de proteção de dados pessoais do Brasil foi aprovada meses depois da entrada em vigor da lei europeia. A normativa europeia possui 99 capítulos e é considerada, por especialistas, o regramento mais moderno e detalhado sobre o tema. O GDPR concede maior poder aos consumidores, principalmente no que diz respeito ao consentimento e ao tratamento dos dados. É exigido das empresas uma explicação clara e concisa sobre o porquê da coleta dos dados, esclarecendo a finalidade para aquela coleta ser realizada. Com isso, também há o impedimento da coleta de dados não justificados pelo serviço prestado pela empresa. A legislação também prevê o acesso do usuário ao seu respectivo banco de informações. Para a empresa, fica exigido a comunicação às autoridades e aos usuários em caso de vazamento de dados. Assim como multas de 10 milhões de euros ou 2% do faturamento anual (prevalecendo o que for maior) até 20 milhões de euros ou 4% do faturamento anual.

É posto que a *General Data Protection Regulation - GDPR*[37] influenciou não só a atualização mas o conteúdo dessas leis. O caso brasileiro evidenciou essa busca por uma harmonização com a GDPR para garantir o livre fluxo internacional de dados.

Nesse sentido, o maior impacto no cenário regulatório da privacidade de dados causado pela GDPR foi a aplicabilidade extraterritorial. A normativa possui uma jurisdição estendida e abarca empresas que coletam e processam dados pessoais de pessoas residentes na União Europeia, não sendo relevante a localização da empresa, mas do titular dos dados. Sobre dados

[37] Disponível em: https://eugdpr.org/ Acesso em: 11 de fevereiro de 2020

pessoais, a definição apresentada no art. 4º da lei é que dados pessoais são entendidos como "qualquer informação relativa a uma pessoa singular identificada ou identificável".

O GDPR define que existem dados, considerados sensíveis, os quais o processamento coloca em risco à privacidade do indivíduo. O art. 9 da normativa europeia entende que dados sensíveis são aqueles de origem racial ou étnica; sobre opiniões políticas, crenças religiosas ou filosóficas; relacionada à associação a sindicatos; dados genéticos e dados biométricos para fins de identificação pessoal, assim como os dados relativos ao estado de saúde ou à vida sexual e/ou orientação sexual de uma pessoa. Porém, é prevista a possibilidade de tratamento desses dados seguindo algumas exigências descritas na lei, como o expresso consentimento ou em caso de proteção vital do indivíduo ou razões substanciais de interesse público.

Outro ponto de destaque da lei é o estabelecimento do controle do titular sobre os seus dados em todo o processo de tratamento de dados. O consentimento é posto como eixo principal de toda normativa. A GDPR define que o consentimento dado deve ser claro e acessível, além de ser reforçado em cada etapa.

O consentimento é definido como "qualquer indicação dada livremente, específica, informada e inequívoca dos desejos do titular dos dados pelos quais ele ou ela, por uma declaração ou por uma ação afirmativa clara, significam concordância com o tratamento de dados pessoais relacionados"

Diferente da Lei Brasileira de proteção de dados pessoais, a GDPR não considera a anonimização dos dados, e essa é a primeira grande diferença entre as normativas. No Brasil, por ser considerado a anonimização dos dados, a criptografia não é posta. No entanto, a GDPR exige a criptografia dos dados em todo o processo de tratamento.

A LGDP é mais amena em relação às sanções. A normativa brasileira prevê desde advertência, passando por eliminação de dados e multas que chegam a 2% do faturamento total. Existem algumas diferenças pontuais entre as normas, como o tratamento de dados de menores. A lei brasileira determina o consentimento dos responsáveis legais para o tratamento de dados pessoais para menores de 18 anos. Já a lei europeia aceita o consentimento dos indivíduos acima de 16 anos.

Sobre a transferência internacional de dados, a LGPD autoriza a transferência de dados pessoais para países que proporcionem grau de proteção de dados pessoais em harmonia com a lei nacional. Enquanto a GDPR, a transferência pode ser realizada se houver reconhecimento

pela comissão europeia do país terceiro como um detentor de um nível de proteção adequado. Caso não, a transferência internacional estará condicionada a garantias asseguradas pelo Agente.

Por fim, regulamentação europeia estabeleceu a criação do Comitê Europeu para proteção de Dados, responsável por assegurar a aplicação coerente da GDPR. O Brasil inicialmente teve a criação da Autoridade Nacional de proteção de Dados vetada. Em acordo legislativo, o Poder Executivo encaminhou a criação do órgão de fiscalização através de Medida Provisória no ano seguinte. A seguir, apresentamos um quadro comparativo com algumas definições importantes para entendimento da relação entre as normativas.

Quadro 1 – Comparativo GDPR e LGPD

CONCEITOS	GDPR	LGPD
Tratamento de dados sensíveis	Tratamento é proibido. Porém, o texto apresenta algumas exceções, como os dados tornados públicos pelo titular e dados referentes a atuais ou ex-membros de entidades sem fins lucrativos para fins de segurança.	Tratamento é proibido. Sendo permitido, independente de consentimento, para execução de políticas públicas pela administração pública e para garantia de segurança.
Tratamento de dados de menores de idade	Aceita o consentimento para maiores de 16 anos.	Aceita o consentimento para maiores de 18 anos.
Políticas de proteção de dados	Dispõe sobre aplicação de medidas técnicas	Dispõe sobre aplicação de medidas técnicas
Representantes	A GDPR exige que o controlador ou processador dos dados tenha um representante em cada Estado-Membro	Não possui definição expressa. Prevê notificação da empresa estrangeira
Responsabilização dos agentes	Prevê responsabilização quando houver danos ao titular.	Replica a orientação da GPRD
Transferência Internacional de Dados	Autoriza se a Comissão Europeia assegurar que o terceiro país tenha um nível de segurança equivalente	Autoriza, porém, não determina procedimentos nem referência de segurança.
Autoridade Nacional		Determinava a criação da Autoridade Nacional de

	Determina a criação do Comitê Europeu para a proteção de Dados	proteção de dados pessoais, porém foi vetada no ato de sanção

Fonte: Elaboração Própria

3.6 APLICABILIDADE E PERSPECTIVAS

A divisão entre o público e o privado e o entendimento das ações realizadas em cada esfera sempre foi objeto de discussão entre filósofos e sociólogos. O desenvolvimento e a atualização da sociedade levaram esse debate para novos patamares, principalmente com o surgimento das Tecnologias da Informação e Comunicação e, consequentemente, da Sociedade da Informação.

A tutela pelo Direito à Personalidade, à Privacidade e ao Direito de "Ser esquecido" ganhou desafios ao encarar um fluxo informacional de dados e informações e a mercantilização desse novo produto. As gerações de normatização da proteção de dados pessoais e do direito à personalidade elaborada por Mayer-Schönberg (2011) exemplifica o acompanhamento da doutrina jurídica com o desenvolvimento tecnológica para garantir os direitos fundamentais à população. A última década foi marcada por um movimento internacional de busca por legislações coesas, detalhadas e uniformes que garantissem essa proteção ao usuário da internet e os consumidores de mídias, mas que não fosse capaz de coibir o desenvolvimento tecnológico que é capaz de trazer benefícios sociais, culturais e econômicos.

Com a aprovação do Regulamento Geral de proteção de dados pessoais pela União Europeia, houve um impulso no debate brasileiro de elaboração da Lei de proteção de dados pessoais. Ainda sem legislação específica sobre o tema, apenas com leis esparsas e pontuais, a elaboração normativa sobre a proteção de dados pessoais ocorria no Congresso Nacional desde 2010. Em 2016, o Poder Executivo encaminhou o Projeto de Lei que posteriormente, em 2018, resultaria na Lei de proteção de dados pessoais.

Em agosto de 2020, o Brasil verá o a sua Lei Geral de proteção de Dados entrar em vigor. Alguns meses separam a elaboração desse trabalho do prazo previsto em lei. Nesse espaço temporal e no procedimento de elaboração normativa, houve mudanças importantes no cenário político que influenciaram as discussões, como escândalos de vazamento de dados, o processo de impeachment e a eleição de um governo de liberal-conservador representado pela

figura de Jair Bolsonaro. Após meses desse governo, o Brasil se depara com diretrizes políticas que denotam que a proteção de dados pessoais não é a sua preocupação e que o controle dos dados pessoais dos cidadãos brasileiros é estratégico. Nesse sentido, no dia 10 de outubro de 2019, o presidente Jair Bolsonaro instituiu o Cadastro Base do Cidadão[38]. A iniciativa irá integrar em uma plataforma única os dados pessoais de brasileiros e permitirá o compartilhamento de dados entre órgãos de toda administração pública federal direta. O decreto que instituiu a base de dados única concentrará dados biográficos em geral, como CPF, nome, data de nascimento, sexo, filiação, endereço, vínculos empregatícios. Também será composta por dados biométricos, características biológicas e comportamentais da pessoa natural, como a palma da mão, as digitais dos dedos, a íris dos olhos, o formato da face ou a voz.

Com o objetivo de simplificar a oferta de serviços públicos e a elaboração de políticas públicas, o texto prevê o cumprimento dos requisitos de segurança da informação presentes na Lei Geral de proteção de dados pessoais.

Em entrevista[39], especialistas demonstraram preocupação com o decreto e com a necessidade de segurança desse banco de dados, afirmando que um possível vazamento seria catastrófico para a segurança internacional no país.

Além das dúvidas geradas pelo perfil de gestão do Governo Bolsonaro, a rápida evolução das tecnologias de tratamento de dados também coloca em xeque a efetividade das legislações ao decorrer dos anos. A Lei Geral de proteção de dados pessoais possui definições e conceitos claros em relação aos direitos dos titulares dos dados e deveres das empresas, organizações e do estado. A normativa brasileira é moderna em conceitos como a autodeterminação informativa, segurança e no estabelecimento de bases legais para o tratamento, revogação do consentimento e tantos outros.

No entanto, o mercado é dinâmico na ampliação das formas de tratamento, o que gera novos desafios na tutela dos dados pessoais. Nesse sentido, a autodeterminação informativa e

---

[38] Disponível em: https://static.poder360.com.br/2019/10/Decreto-cadastro-base.pdf Di Acesso em 11 de fevereiro de 2020

[39] Disponível em: https://www.terra.com.br/noticias/brasil/cidades/bolsonaro-cria-cadastro-que-interliga-dados-de-brasileiros-e-inclui-informacoes-biometricas,16cc475212dc49f80c7daf7a73af77e0bayolyzr.html Acesso em 11 de fevereiro de 2020

o controle total do usuário passas a serem questionados. Até que ponto será possível o usuário consentir, com entendimento e consciência, perante um mercado em constante atualização?

Pita (2017) indaga que a proteção dos dados pessoais não está somente na garantia da efetivação da legislação aprovada, mas no processo educacional da população brasileira sobre o mercado de dados pessoais e o risco eminente à privacidade. A autora demonstra preocupação sobre a falta de conhecimento dos titulares dos dados sobre o valor das suas informações no mercado, afirma que é essencial evidenciar a quão lucrativa é a economia dos dados.

> A partir de uma narrativa da proteção dos dados pessoais, podemos descontruir o discurso de quem afirma que leis, ferramentas e estratégias e comportamento são úteis apenas para proteger informações comprometedoras com potencial de constrangimento. A cultura da privacidade pode prosperar entre as pessoas que não querem ser alvo da indústria do consumo e do marketing tão capazes de nos manipular. (PITA, 2017, p.186)

A aplicabilidade da Lei Geral de proteção de dados pessoais e as perspectivas de proteção de dados no Brasil não dependem somente da garantia de sua entrada em vigor ou da criação, de fato, da Autoridade Nacional de proteção de dados pessoais. Um dos maiores problemas da execução da lei é a definição do responsável pela tutela e garantia da lei. Sem a criação da Autoridade Nacional de proteção de dados pessoais, o risco de a LGPD entrar na lista de leis inócuas é elevado. A efetiva tutela do Direito à Privacidade, à Personalidade e tantos outros direitos fundamentais vinculados à proteção de dados pessoais perpassa por uma questão cultural e educacional. A tão exaltada e elogiada autodeterminação informacional presente na LGPD não terá sentido e aplicabilidade enquanto a população acreditar ser vantajoso trocar a privacidade por benefícios ou gratuidades em serviços como evidenciado na pesquisa realizada pela Symantec, por exemplo.[40] Ou enquanto o conhecimento sobre tratamento de dados pessoais ou sobre os direitos do titular estiverem concentrados em determinados grupos sociais.

Reiterando o exposto por Pita (2017), “a privacidade só existe como cultura compartilhada – especialmente em estruturas baseadas em redes, em que pesa o efeito manada. A segurança de uma ponta só existe quando as outras também se responsabilizam pela proteção.” (PITA, 2017, p.190) É emergencial rompermos o ciclo de convencimento dos que já

[40] Disponível em: < https://www.symantec.com/pt/br/security-center/threat-report> Acesso em 11 de fevereiro de 2020

estão convencidos da importância da proteção dos dados pessoais em uma sociedade cada vez mais conectada.

4. CONCLUSÃO

A pesquisa se propôs a analisar o processo legislativo, político e internacional que circundou a elaboração da Lei Brasileira de proteção de dados pessoais. Teve como base teórica o debate histórico sobre privacidade e, em um segundo momento, a relação entre comunicação digital e dados pessoais. Em um terceiro momento, o debate acadêmico sobre inovação tecnológica trouxe novos conceitos e desafios para o que entendemos até então como direitos fundamentais e se somou à toda narrativa apresentada.

O texto abordou, inicialmente, o histórico debate sobre dicotomia entre público e privado, o entendimento sobre as relações dessas esferas e o protagonismo masculino no que era entendido como espaços de poder. Posteriormente, entendendo as características dessas esferas, somamos o debate sobre a relação público e privado à inovação tecnológica vivenciada nas últimas décadas, além da evolução digital dos algoritmos e do *Big Data* para relatar sobre a influência da tecnologia no cotidiano do cidadão comum. Discorremos sobre a facilidade que o uso de diversos aplicativos pode proporcionar aos usuários, porém, chamamos atenção para a coleta e tratamento de dados. Alguns dados apresentados, como a ausência de compreensão sobre o que é privacidade, sobre a coleta de dados ou sobre segurança digital, foram essenciais para basear o entendimento da pesquisa sobre o predomínio da cultura da exposição na sociedade brasileira, conforme apresentado por Pita (2017).

Nesse ponto, adentramos ao nicho do debate sobre consentimento e a proteção de dados pessoais. Ao evidenciar que o debate sobre privacidade e proteção de dados pessoais é histórico e norteador da sociedade brasileira, a pesquisa demonstrou como o direito à privacidade e à personalidade carece de tutela jurídica. Assim, entender a construção da tão aclamada normativa de proteção de dados pessoais nos mostra como o Brasil ainda carece de políticas públicas educacionais sobre o uso da internet.

A pesquisa mapeou e relatou todo o processo de construção da Lei Brasileira de proteção de dados pessoais. Compreendemos como ocorreu a tomada de iniciativa do Poder Executivo para pautar o assunto na esfera legislativa. Evidenciamos os diversos formatos de debates, reuniões e discursos feitos para consolidação de uma lei harmônica com a Lei Europeia de proteção de dados pessoais. Além de compreender que os eixos sobre dados sensíveis, dados anonimizados e consentimento foram fundamentais para garantir a almejada harmonização com

a lei internacional. Porém, a construção do que seria a Autoridade Nacional de proteção de dados pessoais assumiu o protagonismo no desafio de implementação da normativa.

A análise dos dois anos de construção ativa da Lei Brasileira de proteção de dados pessoais nos mostrou que, por mais que houvesse um debate acadêmico e técnico, o objetivo maior era entregar uma normativa harmônica com a legislação europeia e que fosse acatada pelo Setor Privado. De fato, a normativa sancionada é moderna e possui poucos gargalos. No entanto, a crítica feita pela pesquisa é que pouco foi debatido sobre a aplicação da legislação. O Brasil é reconhecido por elaborar legislações que, apesar de sancionadas, não são postas em prática, por falta de fiscalização, regulamentação ou por não serem harmônicas com a cultura social.

Segundos dados do IBGE (2006), 60,9% da população brasileira está conectada. Dado que deve ser analisado com cautela, visto que estar conectado não é estar incluído digitalmente. Segundo pesquisa da *GlobalWebIndex*[41], o brasileiro usa a internet majoritariamente para o uso das redes sociais. Atualmente, é o 2º no ranking que analise o tempo gasto nessas plataformas. Resultado esperado para um país que vive intensamente a cultura da exposição. Segundo Pita (2014) a cultura da exposição pessoal no Brasil é o maior contraponto e impedimento do fortalecimento da cultura da privacidade. A autora afirma que o tema tem pouca aderência na população devido ao processo de construção da cultura e da identidade nacional. Ainda mais preocupante, é somar todas essas informações ao fato de que o Brasil ainda possui péssimas taxas educacionais.[42] No Brasil, 11,1% da população é analfabeta ou possui menos de 1 ano de de estudo. 9,5% da população estudou somente 1 a 3 anos. 21,7% possui de 4 a 7 anos de estudo.

Dessa forma, entendemos que a grande parte da população que está online possui pouca instrução ou conhecimento. Está vulnerável na internet e não entende o que isso significa. A pesquisa reforça a falta de conhecimento sobre o debate da proteção de dados pessoais. Entre outras questões, os dados também demonstram a disponibilidade dos cidadãos brasileiros em ceder os seus dados em troca de benefícios pessoais, como o uso de aplicativos. [43]

A questão a ser debatida é se somente a Lei de proteção de dados pessoais será capaz de garantir os direitos fundamentais dos usuários, que muitas vezes desconhecem o seu direito.

---

[41] Disponível em: < https://epocanegocios.globo.com/Tecnologia/noticia/2019/09/brasil-e-2-em-ranking-de-paises-que-passam-mais-tempo-em-redes-sociais.html> Acessado em: 07 de dez. 2019

[42] IBGE, Diretoria de Pesquisas, Coordenação de Trabalho e Rendimento, Pesquisa Nacional por Amostra de Domicílios 2007/2015. Disponível em: https://biblioteca.ibge.gov.br/visualizacao/livros/liv98887.pdf

[43] Disponível em: https://www.symantec.com/pt/br/security-center/threat-report. Acesso em 11 de fevereiro de 2020

O debate sobre a proteção de dados pessoais não esbarra somente na questão cultural brasileira, mas, na questão política. O governo Bolsonaro já demonstrou, através de discursos e normativas, que não fará esforços para regulamentação e aplicação da normativa, visto que a coleta de informações pessoais significa poder e controle sobre a população.

Para Pita (2017), o cenário brasileiro exige que as organizações pró-privacidade trabalhem formas de diálogo próximo com a população, para colaborar com a criação de uma consciência social do valor dos seus dados pessoais e da compreensão dos conceitos de privacidade, sigilo e vigilância no seu cotidiano.

A fim de colaborar para a construção do debate, a presente pesquisa buscou mapear e descrever o processo de elaboração legislativa da Lei de proteção de dados pessoais para demonstrar, com esse recorte histórico e conceitual, que somente o debate legislativo não será suficiente para proteger os usuários brasileiros. Quem, de fato, está exposto, também é privado de informações básicas sobre garantias de direitos. A discussão sobre a proteção de dados pessoais esbarra na nossa capacidade de conexão real com a população. De chegarmos ao patamar de discutir formas de conscientização e empoderamento social na internet. Talvez, quando alcançarmos a verdadeira democratização do conhecimento, cidadãos brasileiros passarão a ter maior consciência política, social e cidadã. Poderemos vivenciar participações políticas online, eleições sem *fakenews* e ativismos políticos sem cooptação. A internet não é a solução nem a causa dos nossos gargalos sociais, mas pode ser uma ferramenta de amadurecimento e revolução cívica.[44]

Com isso, é emergencial que continuemos uma provocação sobre o entendimento social sobre a proteção de dados pessoais. Os usuários da internet possuem conhecimento sobre os seus direitos ou sobre os possíveis riscos que assumem ao se conectar? Os titulares dos dados possuem conhecimento sobre o valor do que está fornecendo em troca de alguns serviços digitais? Conversamos com os brasileiros, pelos menos os 60,9% que está conectado, sobre as possibilidades que a internet pode oferecer frente à sua realidade? Ou, nos orgulhamos desse dado, mas não assumimos que estar conectado não é estar inserido digitalmente e relativizamos o potencial da internet para os mais pobres e vulneráveis?

Chamamos aqui atenção para a real necessidade de tentarmos responder às essas perguntas. A pesquisa alarma para a superficialidade com que tratamos o uso da internet e seus

[44] GOMES, Wilson. *A democracia digital e o problema da participação civil na decisão política.* Vol. VII Nº 3 – Setembro/Dezembro, 2005 – Revista Fronteiras – estudos midiáticos, p. 221

efeitos em um país que ainda não garante os direitos fundamentais para toda a sua população. Não é o objetivo aqui criticar a internet e à torna-la vilã, mas almejo alarmar para a fragilidade da nossa base educacional que reforça e projeta a vulnerabilidade social para uma nova esfera, agora digital.

Vibro a existência de uma Lei Geral de proteção de dados pessoais e como o processo legislativo foi maduro e respeitado. Porém, lamento que a ausência do debate com a população, maior impactado, reforce a entrega de mais uma lei apenas para o mercado, maiores interessados no tratamento de dados pessoais. Tutelamos os dados, mas não tutelamos os usuários e nem realizamos um processo educativo para que todos conheçam os seus direitos. Assim, continuamos replicando falhas sociais e reforçando a cultura do predomínio econômico frente aos direitos sociais fundamentais.

REFERÊNCIAS

AIETA, Vania Siciliano. *Marco Civil da internet: marco civil da internet e o direito à intimidade.* Organizadores: George Salomão e Ronaldo Lemos. São Paulo: Atlas, 2014.

AMARAL, Fernando. *Introdução à Ciência de Dados: mineração de dados e big data.* Rio de Janeiro: Alta Books, 2016.

ARAÚJO, Tarso. *Como surgiu o computador?* Disponível em: <https://mundoestranho.abril.com.br/tecnologia/como-surgiu-o-computador/>.

ARENDT, Hannah. *A Condição Humana*; tradução de Roberto Raposo; posfácio de Celso Lafer. Forense Universitário, Rio de Janeiro, 1995.

ARTIGO 19. *proteção de dados pessoais no Brasil: Análise dos Projetos de Lei em Tramitação no Congresso Nacional.* 2017. Disponível em: <http://artigo19.org/wp-content/blogs.dir/24/files/2017/01/proteção-de-Dados-Pessoais-no- Brasil-ARTIGO-19.pdf>.

ASSOCIAÇÃO INTERNETLAB DE PESQUISA EM DIREITO E TECNOLOGIA. *O que está em jogo no debate sobre dados pessoais no brasil?* Relatório final sobre o debate público promovido pelo ministério da justiça sobre o anteprojeto de lei de proteção de dados pessoais, 2016.

BANISAR, Dave; GUILLEMIN, Gabrielle; BLANCO, Marcelo. *proteção de dados pessoais no Brasil - Análise dos projetos de lei em tramitação no Congresso Nacional.* 2017. Disponível em: <http://artigo19.org/wp-content/blogs.dir/24/files/2017/01/proteção-de-Dados-Pessoais-no-Brasil-ARTIGO-19.pdf>.

BBC BRASIL. *5 coisas que você talvez não saiba sobre o Facebook reveladas por Zuckerberg em depoimento*. 2018. Disponível em: <https://www.bbc.com/portuguese/geral-43727418>.

BBC BRASIL. *Conheça as principais revelações feitas pelo site Wikileaks.* 2010. Disponível em: <https://www.bbc.com/portuguese/noticias/2010/11/101129_wiki_ponto_ji>.

BENN, Stanley I.; GAUS, Gerald. *The liberal conception of the public and the private.* In: BENN, Stanley I.; GAUS, Gerald (Org). Public and Private in Social life. Nova York: St Martin´s Press, 1983, p. 31-65.

BEZERRA, Arthur Coelho. *Privacidade em perspectivas: Os Reflexos do Grande Irmão no Admirável Espelho Novo de Black Mirror.* Organizadores: Sérgio Branco e Chiara de Teffé. Rio de Janeiro: Lumen Juris, 2018.

BIONI, BRUNO RICARDO. *proteção de dados pessoais - A Função e os Limites do consentimento.* Forense, 201

BONIFÁCIO, R. *A Participação Política no Brasil.* Em Debate. Belo Horizonte, v.4, n.6, set 2012, p. 34-45

BORGESIUS, FREDERIK ZUIDERVEEN. *consentimento Informado. Podemos Fazer Melhor Em Defesa Da Privacidade,* 2016

espaçamentoBRUNO, FERNANDA. *Monitoramento, classificação e controle nos dispositivos de vigilância digital.* Revista FAMECOS. Porto Alegre. Nº 36. Agosto de 2008

BUCHSTEIN, H. *Bytes that bite: the internet and deliberative democracy*. Constellations, v. 4, n. 2, p. 248-263, 1997.

BURCH, Sean. *Facebook Is Rotten, Privacy Is Its „Kryptonite, Says Ex-FTC Advisor: Social network‘s business model is at odds with protecting its users, according to one expert.* 2018. Disponível em: <https://www.thewrap.com/facebook-privacy-kryptoniteftc/>.

CABELLO, Marcos Antonio Assumpção. *Marco Civil da internet: Da guarda de registros de acesso a aplicações de internet.* Organizadores: George Salomão e Ronaldo Lemos. São Paulo: Atlas, 2014.

CABRAL, Rafael. *A questão dos metadados tem sérias implicações para a privacidade.* Disponível em: <http://revistagalileu.globo.com/Revista/Common/0,,EMI340880-17770,00-A+QUESTAO+DOS+METADADOS+TEM+SERIAS+IMPLICACOES+PARA+A+PRIVACIDADE.html>.

CASTELLS, Manuel. *A Galáxia internet: reflexões sobre a internet, negócios e a sociedade.* Rio de Janeiro: Jorge Zahar Ed., 2003. Tradução: Maria Luiza X. de A. Borges.

_____. A sociedade em rede. São Paulo: Paz e Terra, 2016.

CASTRO, Catarina Sarmento e. *Direito da Informática, Privacidade e dados pessoais*. Coimbra: Almedina, 2005.

CELLA, José Renato Gaziero; COPETTI, Rafael. *Compartilhamento de dados pessoais e Administração Pública Brasileira.* Disponível em: <http://indexlaw.org/index.php/revistadgnt/article/view/2471/pdf>.

COLNAGO, Cláudio Oliveira Santos. *Marco Civil da internet: Provedores de conexão e guarda de registros de acesso a aplicações de internet: o art. 14 do Marco Civil no contexto do dever fundamental de preservação do meio ambiente digital.* São Paulo: Atlas, 2014.

DANCE, Gabriel J.x.; CONFESSORE, Nicholas; LAFORGIA, Michael. *Facebook Gave Device Makers Deep Access to Data on Users and Friends: The company formed datasharing partnerships with Apple, Samsung and dozens of other device makers, raising new concerns about its privacy protections*. 2018. Disponível em:

DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*. Rio de Janeiro: Renovar, 2006. v. 1

DOTTI, Renè Ariel. *proteção Da Vida Privada e Liberdade de Informação*. São Paulo: RT, 1980.

DUPAS, G. Atores e poderes na nova ordem global: assimetrias, instabilidades e imperativos de legitimação. São Paulo: Editora da Unesp, 2005.

ELIAS, Paulo Sá. *algoritmos, Inteligência Artificial e o Direito*. Disponível em: <https://www.conjur.com.br/dl/algoritmos-inteligencia-artificial.pdf>.
(ver espaçamento)

ELOLA, Joseba. *O reconhecimento facial abre caminho para o pesadelo de George Orwell:* Tecnologia ameaça a privacidade das pessoas e abre as portas à distopia descrita no livro '1984'. Por outro lado, permite identificar em tempo recorde terroristas logo após cometerem atentados. 2018. Disponível em: <https://brasil.elpais.com/brasil/2018/01/05/tecnologia/1515156123_044505.html>.

FARIAS, Edilsom Pereira de. *Colisão de direitos: a honra, a intimidade, a vida privada e a imagem versus a liberdade de expressão e informação.* Porto Alegre: Sérgio Antônio FOXX, Chris. Google e Facebook são acusados de violar nova lei de proteção de dados da Europa. 2018. Disponível em: <https://www.bbc.com/portuguese/internacional-44259419https://www.bbc.com/portuguese/internacional-44259419>.

FREDOOM HOUSE. *Manipulating Social Media to Undermine Democracy*. Disponível em: <https://freedomhouse.org/report/freedom-net/freedom-net-2017>.

FREITAS, Christiana Soares. *Mecanismos de Domicação Simbólica nas Redes de Participação – Política Digital*. In: Democracia Digital, Comunicação Política e Redes – Teoria e Prática. Folio Digital, 2017

FURLANETO NETO, Mario; GARCIA, Bruna Pinotti. *Marco Civil da internet: Da guarda de registros de acesso a aplicações de internet na provisão de aplicações*. São Paulo: Atlas, 2014.

GADELHA, Julia. *A evolução dos computadores.* Disponível em: <http://www2.ic.uff.br/~aconci/evolucao.html>.

GALLOWAY, Alexander. *Protocol: how control exists after decentralization*. Cambridge: MIT Press, 2004.

GIACCHETTA, André Zonaro; MENEGUETTI, Pamela Gabrielle. *Marco Civil da internet: A garantia constitucional à inviolabilidade da intimidade e da vida privada como direito dos usuários no marco civil da internet*. Organizadores: George Salomão e Ronaldo Lemos. São Paulo: Atlas, 2014.

GIMMLER, Antje. *Deliberative democracy, the public sphere and the internet*. Philosophy and Social Criticism, v. 27, n. 4, 2001.

GODINHO, Adriano Marteleto; ROBERTO, Wilson Furtado. *Marco Civil da internet: A guarda de registros de conexão: o marco civil da internet entre a segurança na rede e os riscos à privacidade.* Organizadores: George Salomão e Ronaldo Lemos. São Paulo: Atlas, 2014.

GOMES, Rodrigo Dias de Pinho. *Privacidade em perspectivas: Desafios à privacidade: Big Data, consentimento, Legítimos Interesses e Novas Formas de Legitimar o Tratamento de dados pessoais.* Organizadores: Sérgio Branco e Chiara de Teffé. Rio de Janeiro: Lumen Juris, 2018.

GOMES, Wilson. *Transformações da Política na era da comunicação de massa.* São Paulo: Paulus, 2004.

GOMES, Wilson. *A Democracia Digital e o Problema da participação civil na decisão política.* Revista Fronteiras, São Leopoldo, v. VIII, n.3, p.214-222, 2005.

GONÇALVES, Victor Hugo Pereira. *Marco civil da internet comentado*. São Paulo: Atlas, 2017.

GUERRA, Gustavo Rabay. *Marco Civil da internet: Direito à inviolabilidade e ao sigilo de comunicações privadas armazenadas: um grande salto rumo à proteção judicial da privacidade na rede.* Organizadores: George Salomão e Ronaldo Lemos. São Paulo: Atlas, 2014.

GUGIK, Gabriel. *A história dos computadores e da computação*. Disponível em: <https://www.tecmundo.com.br/tecnologia-da-informacao/1697-a-historia-dos-computadorese-da-computacao.htm>.

GUIDI, Guilherme Berti de Campos. *Privacidade em perspectivas: Modelos Regulatórios para proteção de dados pessoais.* Organizadores: Sérgio Branco e Chiara de Teffé. Rio de Janeiro: Lumen Juris, 2018.

HABERMAS, Jürgen. *Mudança Estrutural da Esfera Pública – Investigações Quanto A Uma Categoria Da Sociedade Burguesa.* Tradução, Flávio R. Kothe. Rio De Janeiro: Tempo Brasileiro, 1984.

_____. *Sociedade Civil e a Esfera Pública Política. In: Direito E Democracia, Entre Facticidade E Validade.* Tempo Brasileiro, volume 1, tradução: Flávio Beno Siebeneichler. -. Rio de Janeiro: Tempo Brasileiro, 1997. pp. 91–121.

_____. *Três Modelos Normativos de Democracia,* Ed. Lua Nova nº36,1993, p.39-53.

HORWITZ, Morton. *The history of the public/private distinction*. University of Pennsylvania Law Review, vol. 130, p. 1423-1428, 1982.

IGLESIAS, Daphne. *Privacidade em perspectivas: Nudging Privacy: Benefits and Limits of Persuading Human Behaviour Online.* Organizadores: Sérgio Branco e Chiara de Teffé. Rio de Janeiro: Lumen Juris, 2018.

ITSRIO. *Anteprojeto de lei de proteção de dados pessoais: Contribuição do ITS para o debate público.* 2015. Disponível em: <https://itsrio.org/wpcontent/uploads/2015/07/Consulta-APL-de-Dados.pdf>.

KENNEDY, Ducan. *The stages of the decline of the public/private distinction.* University of Pennsylvania Law Review, 120, p. 1359-1357, 1982.

KILTIDOU, Despina. *Privacy as a Right: History and lnternational Recognition. In: IRMA, Information Science Reference*. Social Media and Networking: Concepts, Methodologies, Tools, and Applications, Hershey: IGI Global, 2016, p. 1-10

KUJAWSKI, Fábio Ferreira; THOMAZ, Campos Elias. *Marco Civil da internet: Da proteção aos registros, dados pessoais e comunicações privadas – um enfoque sobre o marco civil da internet.* Organizadores: George Salomão e Ronaldo Lemos. São Paulo: Atlas, 2014.

LÉVY, P. *Cibercultura.* São Paulo: Editora 34, 1999.

LIMA, Caio César Carvalho. *Marco Civil da internet: Garantia da privacidade e dados pessoais à luz do marco civil da internet*. Organizadores: George Salomão e Ronaldo Lemos. São Paulo: Atlas, 2014.

LUCA, Cristina de. *Manifestos pedem aprovação do PL de proteção de dados, sem mudanças*. 2018. Disponível em: <https://porta23.blogosfera.uol.com.br/2018/06/26/manifestos-pedem-aprovacao-do-pl-deprotecao-de-dados-sem-mudancas/?cmpid=copiaecola>.

LYCARIÃO, Diógenes. SAMPAIO, Rafael Cardoso. *Sociedade Civil online: diferentes usos da internet para fomentar a participação política.* Rev. Estud. Comum, Curitiba, v. 11, n.25, p.97-106, maio/ago. 2010.

LYON, David. Surveillance Culture: Engagement, Exposure, and Ethics in Digital Modernity. International Journal of Communication, 11, p. 824-842, 2017.

MAFFESOLI, Michel. *A comunicação sem fim* (teoria pós-moderna da comunicação). Revista FAMECOS, Porto Alegre, nº 20, abril 2003, quadrimestral.

MAILJET. *GDPR and Profiling.* 2018. Disponível em:<https://www.mailjet.com/gdpr/profiling/>.

MANTELERO, ALESSANDRO. *Personal data for decisional purposes in the age of analytics: From an individual to a collective dimension of data protection*. Comuter Law & Security Review: The International Journal of Technology Law and Practice, 2016.

MANZANO, José Augusto N. G.; OLIVEIRA, Jayr Figueiredo de. *algoritmos: Lógica para Desenvolvimento de Programação de Computadores.* 28. ed. São Paulo: Érica, 2016.

MARCUSE, Herbert; *A ideologia da sociedade industrial,* Editora ZAHAR, 1973, Introdução e capítulo 1.

MATTIUZZO, Marcela. *Privacidade em perspectivas: Business Models and Big Data: How Google uses your Personal Information*. Organizadores: Sérgio Branco e Chiara de Teffé. Rio de Janeiro: Lumen Juris, 2018.

MAYER-SCHONBERGER, Viktor; CUKIER, Kenneth. *Big Data: A Revolution That Will Transform How We Live, Work, and Think.* New York. Houghton Mifflin Harcourt, 2013, p. 190 apud GOMES, Rodrigo Dias de Pinho. Desafios à Privacidade: Big Data, consentimento, Legítimos Interesses e Novas Formas de Legitimar o Tratamento de dados pessoais, 2018, p. 236.

MAYER-SCHÖNBERGER. *Generational development of data protection in Europe.* In: Technology and Privacy: The New Landscape. 2001

MEHL, JOÃO PAULO. DA SILVA, SIVALDO PEREIRA. *Cultura Digital, internet e apropriações políticas. Experiências, desafios e horizontes.* Rio de Janeiro: Folio Digital: Letra e Imagem, 2017

MENDONÇA, Renata. *Como os testes de Facebook usam seus dados pessoais* - e como empresas ganham dinheiro com isso. 2018. Disponível em: <http://www.bbc.com/portuguese/salasocial-43106323>.

MONDAINI, Marco. *Jürgen Habermas E A Teoria Crítica*, artigo disponível no endereço http://www.historia.uff.br/nec/textos/text25.PDF, acessível a 5.07.2019

MONTEIRO, Renato Leite. *A nova Regulação de proteção de dados pessoais aprovada na União Europeia e sua influência no Brasil.* Disponível em: <https://renatoleitemonteiro.jusbrasil.com.br/artigos/273633610/a-nova-regulacao-deprotecao- de-dados-pessoais-aprovada-na-uniao-europeia-e-sua-influencia-no-brasil>.

MORAIS, José Luiz Bolzan de; MENEZES NETO, Elias Jacob de. Marco Civil da internet: *A insuficiência do marco civil da internet na proteção das comunicações privadas armazenadas e do fluxo de dados a partir do paradigma da surveillance.* Organizadores: George Salomão e Ronaldo Lemos. São Paulo: Atlas, 2014.

MORSE, Jack. *Facebook bug affected 14 million people's privacy settings*. 2018. Disponível em: <https://mashable.com/2018/06/07/facebook-public-settings-14-millionbug/#Wnk.aQAXliqn>. Acesso em: 15 jun. 2018.

O'BRIEN, Danny. *Why Am I Getting All These Terms of Service Update Emails?* 2018. Disponível em: <https://www.eff.org/deeplinks/2018/05/why-am-i-getting-all-these-termsservice-update-emails>. Acesso em: 15 jun. 2018.

PERES-NETO, Luiz. *Privacidade em perspectivas: Ética e Privacidade: Múltiplos Olhares e Partir do Campo da Comunicação*. Organizadores: Sérgio Branco e Chiara de Teffé. Rio de Janeiro: Lumen Juris, 2018.

PHILLIPS, David J. *Privacy policy and PETs: The influence of policy regimes on the development and social implications of privacy enhancing technologies.* New Media & Society, 6(6), p. 691–706, 2004

POLÍTICAS PÚBLICAS. *Governança eletrônica.* Disponível em: <https://politicaspublicas.almg.gov.br/temas/governanca_eletronica/entenda/informacoes_gerais.html?tagNivel1=176&tagAtual=10260>.

RODOTÀ, Stefano. *A vida na sociedade da vigilância - a privacidade hoje.* Rio de Janeiro: Renovar, 2008. Tradução de: Danilo Doneda, Luciana Cabral Doneda.

SAFERNET. *O que são os Metadados?* Disponível em: <http://new.safernet.org.br/node/199.>.

SANTOS, Andréia. *Privacidade em perspectivas: O Impacto do Big Data e dos algoritmos nas Campanhas Eleitorais.* Organizadores: Sérgio Branco e Chiara de Teffé. Rio de Janeiro: Lumen Juris, 2018.

SAXONHOUSE, Arlene. *Classical greek conceptions of public and private.* In: BENN, S.I; GAUS, G.F. (Org). Public and Private in Social Life. Nova York: St. Martins Press, 1983, p. 363-384.

SCHERTEL MENDES, LAURA. *Privacidade, proteção de Dados e Defesa do Consumidor* - Série Idp. 2014

SCHINCARIOL, Fernando. *Privacidade em perspectivas: Filtros Bolha, as Escolhas que Fizemos e as que Faremos: Considerações sobre como (Não) Regular a internet.* Rio de Janeiro: Lumen Juris, 2018.

SCHUMPETER, Joseph. *Capitalismo, socialismo e democracia*. Rio de Janeiro: Fundo de Cultura, 1961. Capitulos XX (item 4), XXI e XXII, pp. 297-344.

SEVIGNANI, Sebastian. *The commodification of privacy on the internet.* Science and Public Policy, 40, p. 733–739, 2013.

SILVA, Sivaldo Pereira da. Estado, *Democracia e internet: requisitos democráticos e dimensões analíticas para a interface digital do Estado*. 2009. 424 f. Tese.

_____ *algoritmos, comunicação digital e democracia: Dimensões culturais e implicações políticas nos processos de Big Data*. In: Cultura digital, internet e apropriações políticas : experiências, desafios e horizontes / organização João Paulo Mehl e Sivaldo Pereira da Silva – Rio de Janeiro: Folio Digital: Letra e Imagem, 2017.

SILVEIRA, A. Sérgio. *A noção de exclusão digital diante das exigências de uma Cibercidadania.* Políticas Públicas e Inclusão Digital. Org. Tânia Maria Hetkowski. UDUFBA. Salvador, 2008.

SOLOVE, Daniel J. *Understanding Privacy*. Cambridge: Harvard University Press, 2008.

TAVANI, Herman T. *Philosophical theories of privacy: implications for an adequate online privacy policy*. Metaphilosophy, vol. 38 (1), 2007.

THOMPSON, J. B. *A mídia e a modernidade: uma teoria social da mídia*. 8.ed. Petrópolis, RJ: Vozes, 2011

TRIVINHO, E. A*; Dromocracia cibercultural: lógica da vida humana na civilização mediática avançada.* São Paulo: Paulus, 2007. (Comunicação)

VERONESE, Marília. GUARESCHI, Pedrinho. *Hermenêutica da Profundidade na Pesquisa Social.* Ciência Sociais Unisinos, 42(2) maio/ago, 2006, 85-93.

WARREN, Samuel D.; BRANDEIS, Louis D. *The right to privacy.* In: SCHOEMAN, Ferdinand David (Org.). Philosophical Dimensions of Privacy: an Anthology. Londres e Nova York: Cambridge University Press, 1984, p. 75-9

MANGETH, Ana Lara; NUNES, Beatriz Marinho. *A proteção de seus dados pessoais está em jogo no Senad*o. 2018. Disponível em: <https://feed.itsrio.org/senado-vs-câmara-seusdados-pessoais-em-jogo-97d7b0cefc54>. Fora de ordem – 4 últimos

_____. *Seis pontos para entender o Regulamento Geral de proteção de Dados da UE*. 2018. Disponível em: <https://feed.itsrio.org/seis-pontos-para-entender-alei-europeia-de-proteção-de-dados-pessoais-gdpr-d377f6b691dc>.

LEMOS, André. *Cibercultura - Tecnologia e vida social na cultura contemporânea*. Porto Alegre: Sulina, 2013.

_____ C*omunicação e práticas sociais no espaço urbano: as características dos Dispositivos Híbridos Móveis de Conexão Multirredes (DHMCM).* Comunicação Mídia e Consumo, São Paulo, Vol. 4, nº10, p.23-40, ju. 2007.

PITA, Marina. *Quando o lucro está nos dados, a privacidade se torna contracultura.* In: Cultura digital, internet e apropriações políticas: experiências, desafios e horizontes / organização João Paulo Mehl e Sivaldo Pereira da Silva – Rio de Janeiro: Folio Digital: Letra e Imagem, 2017

WESTIN, Alan. *Privacy and freedom (Fifth ed.).* New York, U.S.A.: Atheneum. 1968

APÊNDICES

Apêndice A - Mapeamento dos Atores

Durante todo o processo de tramitação da Lei de proteção de dados pessoais, alguns atores estiveram presentes nas principais discussões realizadas, sejam elas nas comissões permanentes, nas audiências públicas ou no plenário da Câmara dos Deputados e do Senado Federal.

Em 24/08/2016, a presidência da Câmara dos Deputados criou a Comissão Especial (CESP) referente ao PL 4060/2012, onde o Deputado Orlado Silva (PCdoB/SP) foi designado relator. Em 24/05/2018, o relator apresentou parecer pela aprovação do projeto principal e dos apensados, com acolhimento de algumas emendas, na forma do Substitutivo. Em 29/05/2018, em Plenário, foi aprovado o parecer da Comissão Especial e a matéria seguiu para o Senado Federal. Quando recebido pela Casa, o projeto passou a tramitar em conjunto com o PLS 181/2014, 131/2014 e 330/2013. Cabe destacar que o bloco de projetos já havia recebido parecer da Comissão de Ciência e Tecnologia (CCT) e da Comissão de Meio Ambiente (CMA), pela aprovação do PL 330/2013 nos termos de Substitutivo e pela prejudicialidade dos PLS 131/2014 e 181/2014, conforme relatório do senador Aloysio Nunes Ferreira (PSDB/SP) nas duas comissões.

Assim, quando o PLC 53/2018 se acoplou ao bloco de apensados, foram recebidos pela Comissão de Assuntos Econômicos (CAE) onde o senador Ricardo Ferraço (PSDB/ES) foi designado relator. Em 14/06/2018, Ferraço apresentou relatório favorável ao PLC 53/2018 com emendas e pela prejudicialidade dos demais. O parecer foi aprovado pela comissão em 03/07/2018. No mesmo dia, foi aprovado requerimento de urgência para apreciação da matéria e, em 05/07, o projeto foi encaminhado ao Plenário. Em razão de seu regime de urgência, o projeto foi aprovado diretamente pelo Plenário da Casa. Como as emendas aprovadas alteraram apenas a redação do texto, não alterando substancialmente seu conteúdo, a matéria não precisou ser analisada novamente pela Câmara dos Deputados (casa de origem).

A pesquisa buscou identificar e classificar os atores presentes no processo descrito a fim de descrever e monitorar o comportamento, influência e atuação dos mesmos nas discussões que cercearam os termos-chaves da lei, sendo esses: “Dados sensíveis”, “Dados anonimizados” e “consentimento”. Os relatórios de audiência e de eventos foram analisados e os atores presentes categorizados.

Os atores foram classificados em Atores Políticos, aqueles que ocupam algum cargo público nos Poderes Executivo ou Legislativo; Atores Acadêmicos, sendo aqueles que representam instituições acadêmicas e técnicas; Atores do Setor Regulado, aqueles que fazem parte de instituições do mercado que serão submetidas à legislação aprovada; E, por fim, Atores da Sociedade Civil, aqueles representantes da sociedade, agrupados em associações, coalizões ou ONGs.

O mapeamento de atores demonstra que durante todo o processo legislativo há recorrência na partição dos atores, principalmente no que se refere aos atores políticos. Esses,

burocraticamente, estão em maior quantidade devido à composição das comissões, porém a atuação dos relatores e presidentes se mostra mais presente e efetiva. A pesquisa irá evidenciar como cada ator se comportou no debate dos principais termos da legislação aprovada.

A legislação brasileira define dado pessoal sensível como "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." Outro termo identificado como chave para mapeamento do debate de construção da lei brasileira de proteção de dados pessoais é o conceito de dado anonimizado, definido como "dado relativo a titular que não possa ser identificado, considerando a utilização de meio técnicos razoáveis e disponíveis na ocasião do eu tratamento". E, consentimento, sendo "manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada."

Observa-se que os atores do Setor Regulado estão presentes em maioria e possuem, por vezes, mais de um espaço de fala em seminários, audiências públicas, reuniões e contribuições formais ao texto.

NOME	INSTITUÇÃO	AÇÃO	CLASSIFICAÇÃO
Deputada Bruna Furlan (PSDB/SP)	Câmara dos Deputados	Presidente da Comissão Especial do PL 4020/2012	Ator político
Deputado Orlando Silva (PCdoB/SP)	Câmara dos Deputados	Relator na Comissão Especial do Projeto de Lei 4020/2012	Ator político
Deputado Milton Monti (PR/SP)	Câmara dos Deputados	Autor do Projeto de Lei 4020/2012	Ator político
Deputado André Figueiredo (PDT/CE)	Câmara dos Deputados	Coordenador do Seminário Internacional sobre Privacidade e proteção de dados pessoais realizado em maio de 2017	Ator político

		na Câmara dos Deputados.	
Miriam Winner	Diretora de Políticas para Transformação Digital do Ministério da Ciência, Tecnologia, Inovações e Comunicações.	Mediadora no Seminário Internacional sobre Privacidade e proteção de dados pessoais	Ator político
Bruno Ricardo Bioni	Comitê Gestor da internet - CGI.br e Núcleo de Informação e Coordenação do Ponto BR - NIC.br	Mediador no Seminário Internacional sobre Privacidade e proteção de dados pessoais, Palestrante no Seminário em conjunto da CCTCI com a Comissão Especial realizado em maio de 2018, Participante da Audiência Pública na Comissão Especial no dia 14/12/2016	Ator político
Secretaria Nacional de Defesa do Consumidor do Ministério da Justiça	Poder Executivo	Contribuições ao texto e Palestrante na Audiência Pública de 06.12.16 e Palestrante no Seminário em conjunto da CCTCI com a Comissão Especial	Ator político

		realizado em maio de 2018	
Fabrício Vieira Juntolli	Coordenador da Comissão Brasileira de Agricultura de Precisão - CBAP / MAPA;	Palestrante na Audiência Pública - 11.07.17	Ator político
Ricardo Yassushi Inamas	Pesquisador da Empresa Brasileira de Pesquisa Agropecuária - EMBRAPA;	Palestrante na Audiência Pública - 11.07.17	Ator político
Sérgio Alves	Instituto Brasiliense de Direito Público	Mediador no Seminário Internacional sobre Privacidade e proteção de dados pessoais	Ator político
Danilo Doneda	Centro de Direito, internet e Sociedade - IDP e Representante da Open Knowledge Foundation e Professor da UERJ e Especialista em proteção de dados pessoais	Mediador no Seminário Internacional sobre Privacidade e proteção de dados pessoais e Palestrante na Audiência Pública - 07.06.17 e na 06.12.16	Ator Acadêmico e Ator Sociedade Civil
Dra. Cíntia Rosa Pereira de Lima	Universidade de São Paulo	Contribuições ao texto	Ator Acadêmico
IRIS e GNET	Universidade Federal de Minas Gerais	Contribuições ao texto	Ator Acadêmico

Alexandre Pacheco Silva	Professor e Pesquisador da Escola de Direito da Fundação Getúlio Vargas - SP;	Palestrante na Audiência Pública - 11.07.17	Ator Acadêmico
Pedro N. Mizukami	Centro de Tecnologia e Sociedade | FGV DIREITO RIO	Palestrante na Audiência Pública - 05.07.17	Ator Acadêmico
Professora Maria Inês Fini	Instituto Nacional de Estudos e Pesquisas Educacionais Anísio Teixeira – INEP	Palestrante na Audiência Pública - 05.07.17 e na 14.12.16	Ator Acadêmico
Rafael Zanatta	Instituto Brasileiro de Defesa do Consumidor – IDEC	Palestrante na Audiência Pública 03.05.17 e Palestrante no Seminário em conjunto da CCTCI com a Comissão Especial realizado em maio de 2018	Ator Sociedade Civil
Instituto Alana - Programa Prioridade Absoluta	Instituto Alana - Programa Prioridade Absoluta	Contribuições ao texto	Ator Sociedade Civil
Beatriz Barbosa	Fórum Nacional Pela Democratizaçã o da Comunicação – FNDC	Palestrante na Audiência Pública - 05.07.17	Ator Sociedade Civil
Francisco Camargo	Associação Brasileira das Empresas de Software	Contribuições ao texto	Ator Setor Regulado

Associação Nacional de Birôs de Crédito	Associação Nacional de Birôs de Crédito	Contribuições ao texto e palestrante da Audiência Pública de 22.03.17	Ator Setor Regulado
BRASSCOM - Associação Brasileira das Empresas de Tecnologia da Informação e Comunicações	BRASSCOM - Associação Brasileira das Empresas de Tecnologia da Informação e Comunicações	Contribuições ao texto e palestrante na Audiência Pública - 06.12.16	Ator Setor Regulado
ABEMD - Associação Brasileira de Marketing Direto	ABEMD - Associação Brasileira de Marketing Direto	Contribuições ao texto e palestrante na Audiência Pública 29.03.17	Ator Setor Regulado
SindiTelebrasil - Sindicato Nacional das Empresas de Telefonia e Serviço Móvel Celular e Pessoal	SindiTelebrasil - Sindicato Nacional das Empresas de Telefonia e Serviço Móvel Celular e Pessoal	Contribuições ao texto	Ator Setor Regulado
FEBRABAN – Federação Brasileira de Bancos	FEBRABAN – Federação Brasileira de Bancos	Contribuições ao texto e palestrante na Audiência Pública 05.04.17	Ator Setor Regulado
Bruno Magrani	FACEBOOK	Contribuições ao texto e palestrante da Audiência Pública de 07.06.17 e Palestrante no Seminário em conjunto da CCTCI com a Comissão Especial realizado em maio de 2018	Ator Setor Regulado

ABRANET – Associação Brasileira de internet	ABRANET – Associação Brasileira de internet	Contribuições ao texto	Ator Setor Regulado
Tiago Machado	Associação Brasileira da Indústria Elétrica e Eletrônica – ABINEE	Contribuições ao texto e palestrante na Audiência Pública - 12.07.17	Ator Setor Regulado
Wanderley Mariz	Câmara Americana de Comércio – AMCHAM BRASIL	Contribuições ao texto e palestrante na Audiência Pública - 12.07.17	Ator Setor Regulado
Pedro Palatnik	Associação Brasileira de Sementes e Mudas – ABRASEM	Contribuições ao texto e palestrante na Audiência Pública - 11.07.17	Ator Setor Regulado
Rogério Avellar	Confederação da Agricultura e Pecuária do Brasil - CNA.	Palestrante na Audiência Pública - 11.07.17	Ator Setor Regulado
Aline Sordili	Associação Brasileira de Rádio e Televisão - ABRATEL	Palestrante na Audiência Pública - 05.07.17 e Palestrante no Seminário em conjunto da CCTCI com a Comissão Especial realizado em maio de 2018	Ator Setor Regulado
CIPL - Centre for Information Policy Leadership	CIPL - Centre for Information Policy Leadership	Contribuições ao texto	Ator Internacional
Seção Americana do Conselho	Seção Americana do Conselho	Contribuições ao texto	Ator Internacional

Empresarial Brasil-EUA	Empresarial Brasil-EUA		
Câmara de Comércio dos Estados Unidos	Câmara de Comércio dos Estados Unidos	Contribuições ao texto	Ator Internacional
ITI- Information Technology Industry Council	ITI- Information Technology Industry Council	Contribuições ao texto	Ator Internacional
BSA - The Software Alliance	BSA - The Software Alliance	Contribuições ao texto	Ator Internacional
Joana Varon	Diretora Fundadora da Coding Rights	Palestrante na Audiência Pública 07.06.17	Ator Sociedade Civil
Thiago Luís Santos Sombra	Professor de Direito Privado na Faculdade de Direito da UnB	Palestrante na Audiência Pública 07.06.17	Ator Acadêmico
Beatriz Kira	internetLab	Palestrante na Audiência Pública 31.05.17	Ator Sociedade Civil
Cintia Rosa Pereira Lima	Professora da Faculdade de Direito da USP	Palestrante na Audiência Pública 31.05.17	Ator Acadêmico
Maximiliano Salvadori Martinhão	Secretário de Política de Informática - SEPIN/MCTIC	Palestrante na Audiência Pública 31.05.17	Ator político
Ulysses Alves de Levy Machado	Coordenador Estratégico de Segurança da Informação do Serviço Federal de Processamento de Dados – SERPRO	Palestrante na Audiência Pública 31.05.17	Ator político

Alexander Castro	Diretor Regulatório do Sindicato Nacional das Empresas de Telefonia e de Serviço Móvel Celular e Pessoal do SindiTelebrasil	Palestrante na Audiência Pública 31.05.17	Ator Setor Regulado
Rafael Zanatta	Pesquisador do Instituto Brasileiro de Defesa do Consumidor – IDEC	Palestrante na Audiência Pública - 03.05.17	Ator Sociedade Civil
Laura Tresca	Organização Não-Governamental "Artigo 19"	Palestrante na Audiência Pública - 05.04.17	Ator Sociedade Civil
Renato Leite Monteiro	Especialista em Privacidade e proteção de Dados e Professor de Direito Digital e Internacional da Universidade Presbiteriana Mackenzie	Palestrante na Audiência Pública - 05.04.17	Ator Sociedade Civil
Carlos Affonso Souza	Diretor do Instituto de Tecnologia & Sociedade do Rio – ITS	Palestrante na Audiência Pública - 05.04.17	Ator Sociedade Civil
Paulo Rená	Representante do Instituto Beta para a internet e Democracia – IBIDEM	Palestrante na Audiência Pública - 22.03.17	Ator Sociedade Civil
Bruno Bioni	Pesquisador do GPoPAI/USP - Grupo de Pesquisa em Políticas	Palestrante na Audiência Pública - 14.12.16	Ator Acadêmico

	Públicas de Acesso à Informação		
Thiago Camargo Lopes	Secretário de Políticas Digitais do Ministério da Ciência, Tecnologia, Inovações e Comunicações (Mctic)	Palestrante no Seminário em conjunto da CCTCI com a Comissão Especial realizado em maio de 2018	Ator político
Gilson Libório de Oliveira Mendes	Secretário-executivo do Ministério da Justiça	Palestrante no Seminário em conjunto da CCTCI com a Comissão Especial realizado em maio de 2018	Ator político
Luis Felipe Salim Monteiro	Secretário de Tecnologia da Informação e Comunicação do Ministério do Planejamento, Desenvolvimento e Gestão	Palestrante no Seminário em conjunto da CCTCI com a Comissão Especial realizado em maio de 2018	Ator político
Frederico Ceroy	Promotor de Justiça e coordenador da Comissão de proteção dos dados pessoais do Ministério Público do Distrito Federal e Territórios (MPDFT)	Palestrante no Seminário em conjunto da CCTCI com a Comissão Especial realizado em maio de 2018	Ator político
Bruno Gencarelli	Diretor da Unidade Internacional de proteção de Fluxos de Dados da Comissão	Palestrante no Seminário em conjunto da CCTCI com a Comissão Especial	Ator Internacional

	Europeia (DG Justiça e Consumidores)	realizado em maio de 2018	
André Torreta	Sócio-fundador da empresa de pesquisa A Ponte Estratégia	Palestrante no Seminário em conjunto da CCTCI com a Comissão Especial realizado em maio de 2018	Ator Sociedade Civil
Carlos Amaral	Membro do Conselho Consultivo sobre internet e Eleições do Tribunal Superior Eleitoral	Palestrante no Seminário em conjunto da CCTCI com a Comissão Especial realizado em maio de 2018	Ator político
Paulo Brancher	Advogado e professor livre docente pela Pontifícia Universidade Católica de São Paulo (PUC/SP)	Palestrante no Seminário em conjunto da CCTCI com a Comissão Especial realizado em maio de 2018	Ator Acadêmico
Gustavo Artese	Mestre em Direito pela Universidade de Chicago e membro da Associação Internacional de Profissionais de Privacidade (IAPP)	Palestrante no Seminário em conjunto da CCTCI com a Comissão Especial realizado em maio de 2018	Ator Acadêmico
Deputado Sandro Alex (PSD/PR)	Câmara dos Deputados	Membro da Comissão Especial	Ator político
Natália Viana	Agência Pública	Palestrante no Seminário em conjunto da CCTCI com a Comissão	Ator Sociedade Civil

		Especial realizado em maio de 2018	
Carlos Afonso	Consultor de TI e sócio da empresa de marketing digital Yey Inteligência	Palestrante no Seminário em conjunto da CCTCI com a Comissão Especial realizado em maio de 2018	Ator Setor Regulado
Marcelo Lacerda	Diretor de Relações Governamentais e Políticas Públicas do Google no Brasil	Palestrante no Seminário em conjunto da CCTCI com a Comissão Especial realizado em maio de 2018	Ator Setor Regulado
Fábio Gouveia	Coordenador do Laboratório de Estudos sobre Imagem e Cibercultura (Labic) da Universidade Federal do Espírito Santo (Ufes)	Palestrante no Seminário em conjunto da CCTCI com a Comissão Especial realizado em maio de 2018	Ator Setor Regulado
Jonas Valente	Diretor do Coletivo Brasil de Comunicação Social (Intervozes)	Palestrante no Seminário em conjunto da CCTCI com a Comissão Especial realizado em maio de 2018	Ator Sociedade Civil
Senador Ricardo Ferraço	Senado Federal	Relator do PLS 181/2014	Ator político
Senador Vital do Rêgo	Senado Federal	Autor do PLS 181/2014	Ator político
Comissão Nacional das Seguradoras	CNSeg	Contribuições ao debate na reunião	Ator Setor Regulado

		deliberativa da CAE	
Senador Aloysio Nunes	Senado Federal	Relator dos PLs apensados	Ator Político

Fonte: Elaboração própria

Apêndice B – Contribuições ao texto sobre os conceitos de dados sensíveis, Dados Anônimos e consentimento, enviadas à Comissão Especial.

ENTIDADE	DADOS SENSÍVEIS	DADOS ANONIMIZA-DOS	CONSENTI-MENTO
ABES - Associação Brasileira das Empresas de Software	Exclusão do termo "biométricos" no inciso III, passando a contar com a seguinte redação – "dados sensíveis: dados pessoais sobre a origem racial ou étnica, as convicções religiosas, as opiniões políticas, a filiação a sindicatos ou a organizações de	Não enviou contribuição sobre o tema	Não enviou contribuição sobre o tema

	caráter religioso, filosófico ou político, dados referentes à saúde ou à vida sexual e dados genéticos”;		
ANBC - Associação Nacional de Birôs de Crédito	“Dado pessoal: dado relacionado à pessoa natural identificada ou razoavelmente identificável pelo responsável pelo tratamento de dados pessoais, inclusive números identificativos, dados locacionais ou identificadores eletrônicos quando estes estiverem relacionados a uma pessoa;	“Dados anonimizados: dados relativos a um titular que não seja identificado pelo responsável para a finalidade a que se destina o tratamento. A eventual desanonimização, por qualquer pessoa, sujeita-a ao cumprimento desta Lei;”	Não enviou contribuição sobre o tema
CIPL - Centre for Information Policy Leadership	Não enviou contribuição sobre o tema	Acreditamos que os dados anonimizados devem ser excluídos do âmbito de aplicação da lei quando a re-identificação seja possível tão somente através de esforços	Quanto ao consentimento, acreditamos que quando o consentimento expresso não for obrigatório (ex., com relação a dados não sensíveis), meios válidos

	“extraordinários”. Mesmo naqueles casos onde a re-identificação possa ocorrer através de esforços meramente “razoáveis”, os dados ainda deveriam ser considerados anônimos e fora da abrangência da lei se a anonimização se der com base proteções legais, obrigacionais e administrativas, como por exemplo proibições contratuais e regulatórias de re-identificar dados exceto em circunstâncias específicas. Recomendamos que isso seja previsto explicitament	de consentimento deveriam incluir o opt-out e o consentimento implícito para assegurar que os titulares não sejam sobrecarregados com solicitações constantes de consentimento no mundo digital

		e no Artigo 4.	
Seção Americana do Conselho Empresarial Brasil-EUA	A definição de dados sensíveis deveria ser clara e com padrões objeivos. Dados sensíveis podem ser definidos como “dados pessoais que revelem origem racial ou étnica, religião, opiniões políticas, sindicatos, afiliações em entidades políticas/sindicais ou organizações religiosas/filosóficas/políticas, condições de saúde e orientação sexual, assim como dados genéticos expressamente ligados a um registro médico ou individual”.		O consentimento implícito ou informado do consumidor para o uso e transferência de dados, ao invés do consentimento expresso ou afirmativo, é uma opção adequada. Este tipo de consentimento preserva a proteção de dados pessoais, ao mesmo tempo em que permite a inovação.
SENACON - MJ	Não enviou contribuição sobre o tema	Não enviou contribuição sobre o tema	Não enviou contribuição sobre o tema
Câmara de Comércio dos Estados Unidos	Apesar de apoiarmos a criação de diferentes categorias de dados a fim de facilitar uma abordagem de proteção de dados baseada no risco, alguns dos termos desta definição são pouco claros. Primeiramente, sugerimos a retirada do texto da expressão "crenças filosóficas" porque o tipo de dados que se enquadram nesta categoria é muitas vezes bastante subjetivo. Em segundo	Entendemos que merece elogio a linguagem do projeto de lei que reconhece a anonimização como uma ferramenta importante para a	Não enviou contribuição sobre o tema

lugar, sugerimos refinar ainda mais o que se entende por dados de "saúde". Por exemplo, deve haver uma diferença entre dados confidenciais relacionados a um exame médico em comparação com a frequência cardíaca gravada em um aplicativo enquanto uma pessoa faz exercícios físicos. Os produtos de consumo e aplicativos móveis de saúde estão preparados para um crescimento exponencial e queremos garantir que os cidadãos brasileiros tenham acesso a essa tecnologia de ponta.

Sugerimos também a qualificação linguística de que os dados genéticos ou biométricos devem estar expressamente ligados a um registo individual ou médico, a fim de incentivar a inovação e a investigação médica contínua. Grandes avanços médicos estão ocorrendo atualmente com o uso dos dados genéticos que são anonimizados frequentemente ou completamente randomizados, e agregados de modo a fazer com que os indivíduos fiquem virtualmente não identificáveis.

proteção de dados. Acreditamos que a anonimização ajuda a diminuir o risco para os indivíduos e deve ser dispensada do projeto de lei.

Os dados não identificados e anonimizados são aqueles que não podem ser razoavelment e identificados e certas medidas foram tomadas para proteger a pessoa contra o anonimato de forma razoável. Dados Descaracteriz ados e anonimizados são aqueles que não podem ser razoavelment e identificados

e certas medidas foram tomadas para proteger a identificação da pessoa de forma razoável. Os dados pessoais deveriam incluir apenas dados ou conjuntos de dados processados relativos a indivíduos razoavelmente identificáveis. Isso elimina a incerteza e permite que as entidades responsáveis realizem avaliações de risco para cenários realistas, em particular beneficiando as pequenas empresas que têm menos recursos. Muitos tipos de dados coletados são descaracteriz

ados e/ou agregados de tal forma que seria necessário um grande gasto e tempo para determinar a identidade do indivíduo. Portanto, embora tecnicamente possível, é altamente improvável que o indivíduo seja identificado. Na verdade, em algumas circunstâncias, os dados adicionais teriam de ser recolhidos e mantidos para cumprirem os requisitos deste projeto. No entanto, limitando-se a linguagem será possível encorajar um maior uso do anonimato.

ITI-Information Technology Industry Council	Diversos países não contemplam uma definição específica para dados sensíveis, reconhecendo o fato de que vários tipos de dados pessoais podem ser considerados mais sensíveis ou menos sensíveis de acordo com o contexto no qual sejam utilizados, e, pelo contrário, adotam uma abordagem baseada em risco, criando obrigações mais rígidas para circunstâncias mais sensíveis de uso dos dados. Essa abordagem proporciona maior flexibilidade e está bem equipada para minimizar seu risco para as pessoas. Contudo, se o Brasil optar pela adoção de uma categoria específica de dados sensíveis, recomendamos que os tipos de dados considerados sensíveis sejam restritos a uma lista fechada, como apresentado na lei, evitando termos demasiadamente vagos e qualquer confusão que poderia categorizar como "sensível" qualquer tipo de informação pessoal, e que as disposições de consentimento relacionadas aos dados sensíveis não se tornem tão restritivas que impeçam o uso desses dados – com salvaguardas apropriadas – para usos benéficos. Isto poderia rapidamente se tornar uma desvantagem competitiva em relação a regimes mais equilibrados e irá não só restringir a capacidade de operação das empresas estabelecidas, como também impedirá o ambiente certo para a inovação no país. Em geral, os legisladores e reguladores brasileiros deveriam	O ITI sugere a seguinte adaptação à definição de "anonimização": "XII - anonimização: qualquer procedimento por meio do qual um dado não pode mais ser razoavelmente associado, direta ou indireta, a um indivíduo identificado ou identificável." Além disso, a ITI sugere que o processamento de dados anônimos seja expressamente excluído do âmbito de aplicação da lei: "Art. 4. Esta Lei não se aplica ao processamento de dados: [...] IV - que é	O consentimento é um modelo importante de proteção de informações pessoais que busca capacitar os titulares dos dados para tomar decisões informadas sobre se e como seus dados são usados. Nos casos em que as transações envolvendo dados estão claramente definidas e existe uma Página | 8 relação direta entre titulares dos dados e as organizações com as quais eles lidam, este modelo é amplamente bem-sucedido e confiável para equilibrar os direitos das

reconhecer que o tratamento de dados categorizados como sensíveis pode ter resultados incrivelmente benéficos não só para o indivíduo como para a sociedade (como, por exemplo, no setor de saúde). As informações sobre saúde já têm sido utilizadas para metas maiores de política pública, buscando monitorar a disseminação de doenças no Brasil, como no caso do Zika vírus e dengue, bem como para reduzir significativamente o número de óbitos resultantes de infecções em hospitais brasileiros2 . Para garantir que esses potenciais benefícios sejam usufruídos, aos legisladores cabe evitar qualquer perspectiva muito abrangente, habilitando diversos mecanismos ou fundamentos jurídicos para o tratamento de dados sensíveis. Exigir consentimento expresso para o processamento de dados sensíveis impediria um grande número de usos benéficos de dados, onde o responsável pelo tratamento não está em condições de obter o consentimento ou quando o consentimento é negado sem um bom motivo em casos onde não há danos, por exemplo. Assim, incentivamos permitir o interesse legítimo como base para o processamento de dados sensíveis. Uma vez que as razões de interesse legítimo para que processamento exigem avaliação de riscos, bem como mitigações adequadas, em muitos casos, isto pode ser uma proteção maior dos	anonimizado. ”	pessoas interessadas com organizações que desejam usar os dados. No entanto, com o surgimento de inovações que dependem dos últimos desenvolvimentos em cloud computing, big data e internet das Coisas (IoT), o ambiente é radicalmente diferente. Intercâmbios tradicionais e isolados de dados estão sendo substituídos por fluxos de dados por meio de sistemas distribuídos, dificultando a compreensão de quais organizações estão processando seus dados e para quais

dados pessoais do que o consentimento expresso pode ser. Além dos interesses legítimos, a base jurídica prevista nos incisos II (obrigação legal do responsável pelo tratamento) e VII (proteção da vida e segurança física) do Artigo 7º deve ser a fundamentação jurídica para o processamento de dados pessoais sensíveis. Da mesma forma, o processamento deve ser permitido nos casos em que o titular dos dados tenha fornecido dados voluntariamente como expressão de sua liberdade de expressão, consciência ou crença – por exemplo, quando alguém voluntariamente deseja divulgar sua religião ou orientação de gênero.

fins.

Isso levou os reguladores de privacidade a repensar a ênfase colocada no consentimento como um fundamento legal para a proteção de dados e um desejo crescente de buscar soluções que evitem o ônus excessivo que os regimes focados em consentimento podem impor tanto em organizações como em indivíduos[4]. Uma solução importante é a inclusão de razões de interesse legítimo para o processamento de dados, o que coloca o ônus da responsabiliz

ação e transparência nas organizações que usam os dados. Por isso, elogiamos tanto a redação proposta para o consentimento inequívoca e informadae a inclusão do "interesse legítimo" como fundamentação jurídica para o processamento de dados pessoais no Projeto de Lei nº 5276/2016. Por um lado, garante que os direitos dos usuários sejam protegidos. Por outro lado, permite flexibilidade suficiente para garantir que a natureza dinâmica

da internet não seja, de forma alguma, limitada. Também recomendamos que quaisquer ajustes aos requisitos de consentimento feitos pela autoridade competente como parte de suas funções estabelecidas no Art. 9º, § 7º, reflitam de forma semelhante essa flexibilidade e evitem impor obrigações gerais para tipos específicos ou métodos de coleta de consentimento.

BRASSCOM - Associação Brasileira das Empresas de Tecnologia da Informação e Comunicações	III - dados sensíveis: dados pessoais sobre a origem racial ou étnica, as convicções religiosas, as opiniões políticas, a filiação a sindicatos ou organizações de caráter religioso, filosófico ou político, dados relacionados à condição médica do titular, referentes à saúde ou a vida sexual, e dados genéticos e referentes à orientação afetiva e de gênero e biométricos;	ARTIGO 4º Art. 4º Esta Lei não se aplica ao tratamento de dados: [...] 3 IV - anonimizados, desde que não seja razoavelmente possível identificar o titular, ou na hipótese de uso de dados pessoais de forma anonimizada. V – que estão meramente em trânsito no território nacional. Art. 13 Os dados desanonimizados, assim compreendidos como aqueles dados que em sua origem eram anônimos, mas que, para uso específico e utilizando qualquer técnica,	CONSENTIMENTO ARTIGOS 5º, 7º E 9º Art. 5º [...] [...] VII - consentimento: manifestação livre, informada e inequívoca, fornecida por qualquer meio que o certifique, inclusive quando o tratamento se der mediante o uso da internet, pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada; [...] Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:

mecanismo ou procedimento, razoavelmente disponível, tenham efetivamente voltado a identificar os seus titulares terão a mesma proteção dos dados pessoais, aplicando-se aos responsáveis pelo tratamento o disposto nesta Lei. § 1º Poderão ser igualmente considerados como dados pessoais, para os fins desta Lei, os dados utilizados para a formação do perfil comportamental de uma determinada pessoal natural, ainda que não identificada.	I - mediante o fornecimento pelo titular de consentimento livre, informado e inequívoco, por qualquer meio que o certifique; [...] Art. 9º O consentimento previsto no art. 7º, inciso I, inclusive quando o tratamento se der mediante o uso da internet, deverá ser livre, informado e inequívoco e fornecido por escrito ou por qualquer outro meio que o certifique. [...] § 4º O consentimento deverá se referir a finalidades determinadas propósitos legítimos, sendo nulas as

			autorizações genéricas para o tratamento de dados pessoais.
Dra. Cíntia Rosa Pereira de Lima - USP	Não enviou contribuição sobre o tema	Não enviou contribuição sobre o tema	Não enviou contribuição sobre o tema
BSA - The Software Alliance	Não enviou contribuição sobre o tema	Não enviou contribuição sobre o tema	Apesar de reconhecermos que o consentimento do titular é uma forma válida de

legitimar o tratamento de dados pessoais, o mesmo não deve ser a única forma. Outras bases legais para o tratamento de dados devem ser consideradas igualmente válidas. A exigência de consentimento como forma primária de legitimar o processamento é problemática, pois pode haver casos em que a obtenção do consentimento não seja adequada ou apropriada. Por exemplo, se uma instituição financeira precisar coletar informações sobre uma

dívida pendente para autorizar procedimentos de cobrança, pode não ser adequado solicitar a autorização do titular dos dados para fazê-lo. Entretanto, existe um interesse comercial legítimo que justificaria a coleta de dados neste caso (vide seção abaixo para mais detalhes sobre interesse legítimo).

Modificações recomendadas

Aplaudimos as mudanças que já foram incorporadas ao projeto de lei reconhecendo outros meios de legitimar o tratamento de dados, incluindo o

legítimo interesse. Essas mudanças devem ser mantidas. Em situações nas quais o consentimento for necessário, é importante que a legislação foque nos fins e não nos meios através dos quais o consentimento é fornecido. Contanto que o consentimento seja dado de forma livre, específica, informada e de maneira inequívoca, o mesmo deverá ser aceito.

ABEMD - Associação Brasileira de Marketing Direto	III – dados sensíveis: dados pessoais sobre a origem racial ou étnica, as convicções religiosas, as opiniões políticas, a filiação a sindicatos ou a organizações de caráter religioso, filosófico ou político, dados referentes à saúde ou à vida sexual e dados genéticos ou biométricos, salvo quando a utilização destes últimos for exclusivamente para identificação de pessoas naturais, hipótese em que o dado será considerado pessoal, nos termos do inciso I.	Não enviou contribuição sobre o tema	Em caso de alteração de informação referida nos incisos I, II, III ou V do art. 8º, o responsável deverá informar o titular a respeito".
SindiTelebrasil - Sindicato Nacional das Empresas de Telefonia e Serviço Móvel Celular e Pessoal	Não enviou contribuição sobre o tema	Dados anonimizados ou dissociados: dados relativos a um titular que não possa esteja identificado; Justificativa: Retirar da definição de dados anonimizados a menção a impossibilidade de de associação do dado ao titular. Entendemos como fundamental a adoção de uma definição de	Não enviou contribuição sobre o tema

		dados anonimizados abrangendo qualquer dado que não esteja associado a um titular, mesmo que ele possa ser identificado por algum artifício. A definição constante do PL restringe em demasia os casos de dissociação.	
FEBRABAN	§ Quando tratados somente para fins de identificação e cadastro do titular, os dados sensíveis serão considerados apenas como dados pessoais (ex. Biometria coletada para prover segurança e eficiência das transações bancárias com o intuito de prevenção á fraudes); § Inclusão da possibilidade de tratamento dos dados sensíveis se justificado por cumprimento de legislação específica, no exercício regular de direito do responsável ou quando for necessário como meio de prova (art. 11, §2º)	Não enviou contribuição sobre o tema	Indicação expressa de que os tratamentos de dados realizados até a revogação do consentimento são válidos (art. 9º, § 5º); § inclusão da dispensa do consentimento do titular para as hipóteses de transferência de dados mencionados no art. 26; § o consentiment

			o deverá ser livre, informado e inequívoco, fornecido por qualquer meio que possibilite a manifestação de vontade do titular dos dados (Art. 9º).
FACEBOOK	Devem ser previstas exceções claras às formalidades para o tratamento de dados sensíveis, em especial quando o seu tratamento for voltado a trazer benefícios aos titulares ou quando os titulares houverem voluntariamente disponibilizado os dados	Dados Anonimizados devem ser claramente excluídos do escopo da lei	A regra do consentimento livre, informado e inequívoco deve prevalecer sobre regras de consentimento expresso
IRIS e GNET - UFMG	Não enviou contribuição sobre o tema	Não enviou contribuição sobre o tema	Não enviou contribuição sobre o tema
Comissão Europeia	Não enviou contribuição sobre o tema	Não enviou contribuição sobre o tema	Não enviou contribuição sobre o tema
ABRANET	Não enviou contribuição sobre o tema	dados relativos a um titular que não possa ser identificado no nível individual pelo responsável	manifestação inequívoca realizada pelo titular de dados de maneira livre e informada para autorização

		pelo tratamento, tendo em conta o conjunto de meios suscetíveis de serem razoavelmente utilizados para identificar o referido titular, ou desde que os responsáveis pelo tratamento estejam sob obrigação contratual, administrativa ou legal de manter os dados anonimizados.	do tratamento de seus dados pessoais.
ABINEE	Não deve conter menção aos dados relacionados à saúde - por impactar diretamento o uso de dados para fins de fitness.	Não enviou contribuição sobre o tema	Defendem o consentimento de maneira informada

AMCHAM Brasil	Riscos similares, oriundos de uma definição muito ampla, se percebem na definição oferecida pelo inciso III do Art. 5 que define dados sensíveis. A definição de dados sensíveis precisa deixar claro a ligação com o titular, a fim de evitar ônus ao próprio, em sua gestão de seu histórico cotidiano de saúde ou prática esportiva, por exemplo. Para tanto sugerimos a seguinte redação: "III – dados sensíveis: dados pessoais sobre a origem racial ou étnica, as convicções religiosas, as opiniões políticas, a filiação a sindicatos ou a organizações de caráter religioso, filosófico ou político, dados referentes à saúde ou à vida sexual e dados genéticos ou biométricos, que estejam expressa e efetivamente vinculados a um indivíduo ou ao seu histórico médico."	A definição de anonimização proposta pelo inciso XII do Art.5 é de extrema importância para o desenvolvimento do ambiente brasileiro de redes. Mesmo assim, sua atual redação entende este processo como definitivo e irreversível. Este tipo de entendimento se torna preocupante pois leva os responsáveis e operadores do tratamento de dados a buscarem esforços inexequíveis nos procedimentos de anonimização ,além de desincentivar boas práticas e compromisso	Não

		s contratuais para que estes dados se mantenham anônimos, por exemplo por terceiros e prestadores de serviço. Uma redação alternativa a este cenário seria a seguinte: "XII – anonimização: qualquer procedimento por meio do qual determinado dado não possa ser efetivamente associado, direta ou indiretamente, a um indivíduo titular dos dados"	
ABRASEM	Não enviou contribuição sobre o tema	Não enviou contribuição sobre o tema	O consentimento deverá se referir a dados e finalidades determinadas ou conexas, sendo nulas as autorizações

			excessivamente genéricas para o tratamento de dados pessoais em descrumprimento da lei.
Instituto Alana - Programa Prioridade Absoluta	Não enviou contribuição sobre o tema	Não enviou contribuição sobre o tema	Não enviou contribuição sobre o tema