REVISTA DO CAAP
fundada em 1921

EVOLUÇÃO E REGULAÇÃO DA PRIVACIDADE E PROTEÇÃO DE DADOS NO CONTEXTO DA INTERNET DAS COISAS NO CENÁRIO BRASILEIRO

Tales Calaza[1]

RESUMO: Este artigo examina a adequação das legislações de privacidade e proteção de dados face aos desafios impostos pela Internet das Coisas (IoT). O objeto de estudo central é a evolução histórica das regulamentações de proteção de dados, destacando a transição das leis desde os primeiros debates sobre privacidade no final do século XIX até as complexas estruturas regulatórias contemporâneas, como o *General Data Protection Regulation* (GDPR) na União Europeia e a Lei Geral de Proteção de Dados (LGPD) no Brasil. A pesquisa visa identificar as lacunas nas legislações existentes que são ampliadas pela especificidade e pelas exigências da IoT, que incluem a coleta massiva e a interconexão de dados em uma escala sem precedentes. A metodologia adotada envolve uma análise comparativa das legislações de proteção de dados, focando em como diferentes sistemas jurídicos têm respondido aos desafios emergentes trazidos pelas novas tecnologias. Através deste estudo, propõe-se avaliar as respostas legislativas e sugerir adaptações necessárias para a legislação brasileira, considerando as práticas internacionais como referencial. Os resultados indicam que, como existem avanços significativos em algumas jurisdições que podem servir de modelo, há uma necessidade premente de reformas específicas na legislação brasileira para abordar eficazmente os riscos da IoT. As conclusões reforçam a urgência de desenvolver um quadro regulatório que seja capaz de proteger os direitos à privacidade e à segurança dos dados dos cidadãos, facilitando o desenvolvimento tecnológico responsável e sustentável. Este estudo contribui para o diálogo

[1] Mestre em Direito pela Universidade Federal de Minas Gerais (UFMG). Pós-graduado em Processo Civil (UNIDBSCO), em Direito do Consumidor na Era Digital (UNIDBSCO) e em Direito Digital (UNIFTEC). E-mail: tales.calaza@icloud.com. ORCID: https://orcid.org/0000-0003-0370-4065.

Revista do Centro Acadêmico Afonso Pena, Belo Horizonte, Vol. 29, N. 1, 2024

ISSN (impresso): 1415-0344 | ISSN (online): 2238-3840

Editor responsável: Maria Eduarda Adams Andrade | Revisão: Maryanne Pimenta Fargnoli

Data de Submissão: 21/04/2024 | Data de Aceite: 01/07/2024

sobre como harmonizar os avanços tecnológicos com a proteção de direitos fundamentais em um mundo cada vez mais digitalizado.

PALAVRAS-CHAVE: Internet das coisas; Proteção de dados; Privacidade; Regulação.

EVOLUTION AND REGULATION OF PRIVACY AND DATA PROTECTION IN THE CONTEXT OF THE INTERNET OF THINGS IN THE BRAZILIAN SCENARIO

ABSTRACT: This article examines the adequacy of privacy and data protection legislation in the face of challenges posed by the Internet of Things (IoT). The central subject of study is the historical evolution of data protection regulations, highlighting the transition of laws from the first debates on privacy in the late 19th century to the complex contemporary regulatory frameworks, such as the GDPR in the European Union and the LGPD in Brazil. The research aims to identify gaps in existing legislation that are exacerbated by the specificity and demands of the IoT, which include massive data collection and interconnection on an unprecedented scale. The methodology adopted involves a comparative analysis of data protection legislation, focusing on how different legal systems have responded to the emerging challenges brought about by new technologies. Through this study, it is proposed to evaluate legislative responses and suggest necessary adaptations to Brazilian legislation, considering international practices as a benchmark. The results indicate that, while there are significant advancements in some jurisdictions that can serve as models, there is an urgent need for specific reforms in Brazilian legislation to effectively address the risks of the IoT. The conclusions emphasize the urgency of developing a regulatory framework capable of protecting citizens' rights to privacy and data security while facilitating responsible and sustainable technological development. This study contributes to the dialogue on how to harmonize technological advances with the protection of fundamental rights in an increasingly digitalized world.

KEYWORDS: Internet of things; Data protection; Privacy; Regulation.

INTRODUÇÃO

A crescente interconexão digital através da Internet das Coisas (IoT) e outras tecnologias emergentes tem redefinido as fronteiras da privacidade e proteção de dados, desafiando os paradigmas regulatórios estabelecidos. Este texto analisa a evolução histórica da regulação de privacidade e proteção de dados no cenário internacional, destacando como esses marcos legais e doutrinários foram adaptados ao longo do tempo para enfrentar os desafios impostos pela tecnologia moderna. Este estudo não só recapitula a trajetória das legislações e suas implicações para a IoT, mas também propõe um entendimento mais profundo sobre a necessidade de uma legislação dinâmica e adaptativa que possa efetivamente proteger os direitos dos cidadãos na era digital.

Historicamente, a proteção de dados pessoais e a privacidade têm sido preocupações reguladas por leis que evoluíram ao longo do tempo, desde a publicação dos primeiros estudos publicados abordando o assunto no Século XIX até o desenvolvimento de legislações complexas como o *General Data Protection Regulation* (GDPR) na União Europeia. Essas regulamentações foram concebidas em resposta às mudanças tecnológicas e sociais de suas respectivas eras, refletindo um esforço contínuo para equilibrar os direitos individuais com as capacidades emergentes de coleta e processamento de dados.

No contexto brasileiro, a análise histórico-evolutiva revela uma progressão significativa na abordagem jurídica sobre a privacidade e proteção de dados, desde a Constituição Federal de 1988 até a recente implementação da Lei Geral de Proteção de Dados Pessoais (LGPD). No entanto, essas legislações enfrentam novos desafios com o advento da IoT, que possui características distintas que complicam a aplicação das normas existentes, como a interconexão em massa e a coleta de dados em larga escala.

Este trabalho propõe uma revisão desses marcos legais, explorando como eles se adequam ao novo contexto digital propiciado pela IoT. Também busca traçar um panorama das respostas internacionais a esses desafios, oferecendo uma visão comparativa que pode iluminar caminhos possíveis para uma regulamentação eficaz no Brasil. Ao identificar as lacunas e propor soluções, o estudo visa contribuir para o desenvolvimento de um quadro regulatório que

não apenas proteja os dados pessoais e a privacidade dos usuários mas que também suporte o crescimento sustentável e ético da IoT. Portanto, este texto se dedica a entender e sugerir formas de harmonizar a legislação nacional com as demandas e complexidades introduzidas pelas tecnologias emergentes, garantindo que inovação tecnológica e direitos fundamentais avancem de forma equilibrada e complementar.

1. ANÁLISE HISTÓRICO-EVOLUTIVA DA PRIVACIDADE E PROTEÇÃO DE DADOS NO ÂMBITO INTERNACIONAL

Muito antes de existir qualquer regulação ou norma expressa dedicada à Internet das Coisas, já existiam marcos doutrinários e legais dedicados à privacidade e à proteção de dados pessoais, o que, conforme informado anteriormente, são direitos intrinsecamente ligados à tecnologia objeto deste estudo.

O primeiro marco doutrinário que se tem registro sobre o tema foi um artigo publicado no ano de 1890, por Samuel D. Warren e Louis D. Brandeis. Nessa época, ainda nem se cogitava a produção e o compartilhamento de dados do modo e volume que são feitos na contemporaneidade, vez que as violações de privacidade discutidas pelos autores diziam respeito aos fotógrafos e jornais da época, que publicavam "fofocas" sobre a vida alheia (Warren; Brandeis, 1890, p. 195). Mesmo não envolvendo diretamente uma tecnologia digital, este foi um relevante marco teórico para o início da discussão sobre a privacidade e a proteção de dados a nível global (Calaza, 2020, p. 182).

A primeira legislação sobre o tema viria oitenta anos mais tarde, na década de 1970. A Lei do *Land Hesse*, na Alemanha (1970), inaugurou a discussão sobre a proteção de dados informatizados, inicialmente contemplando somente arquivos de titularidade pública, e posteriormente (1977), tutelando também arquivos de titularidade privada. Em contextos similares, foram editadas as legislações sueca (1973), dinamarquesa (1978) e austríaca (1978). Essas legislações podem ser interpretadas como uma "primeira fase legislativa", a qual é caracterizada pelo rigor na criação dos arquivos informatizados (Limberger, 2008, p. 144).

Em um segundo momento, é vislumbrada a edição de legislações menos rigorosas em relação à criação de arquivos, dedicando maior atenção aos direitos fundamentais. São exemplos desta "segunda fase" as legislações da França (1978), da Suíça (1981), da Islândia (1981) e de Luxemburgo (1979) (Limberger, 2008, p. 144).

Um terceiro momento nesta evolução legislativa é marcado pela unificação do direito europeu, ao passo em que, em 1981, o Conselho da Europa editou a Convenção nº 108 com objetivo de regular o tratamento automatizado de dados pessoais (Council of Europe, [s.d.]). Esse foi o primeiro instrumento internacional juridicamente vinculativo no âmbito da proteção de dados (European Parliament, [s.d.]). Tal Convenção se revela como um importante marco regulatório para o presente estudo, ao passo em que tutela, pela primeira vez, o processamento automático de dados, nos quais podem ser compreendidos os processos realizados pelos dispositivos conectados na IoT.

Neste mesmo recorte temporal (década de 1980), a Organização para a Cooperação e Desenvolvimento Econômicos (OCDE) publicou suas diretrizes para a proteção da privacidade e dos fluxos transfronteiriços de dados pessoais (OECD, [s.d.], p. 3). Este é outro marco regulatório de extrema relevância, vez que tutelou o movimento de dados pessoais além de fronteiras nacionais[2].

Na década seguinte, no ano de 1995, o Parlamento Europeu e o Conselho da União Europeia publicaram a Diretiva 95/46/CE (EUR-Lex, [s.d.]), que trouxe o importante princípio da livre circulação dos dados, um importante marco comercial e protetivo para o bloco, vez que veda que os Estados-membros restrinjam ou proíbam a livre circulação dos dados pessoais entre os demais Estados-membros com fundamento na proteção das liberdades e dos direitos fundamentais. Na prática, a Diretiva tratou o bloco econômico como um "território único" no que tange ao tratamento dos dados e à proteção garantida a eles, o que facilita a regulação da Internet das Coisas no âmbito regional.

No ano de 2016, a Diretiva acima foi revogada pelo Regulamento (EU) 2016/679 do Parlamento Europeu[3] (EUR-Lex, 2016), mais popularmente conhecido como Regulamento Europeu de Proteção de Dados ou GDPR (*General Data Protection Regulation*), tido como uma das normas mais relevantes no que tange à proteção de dados internacional, vez que

[2] As diretrizes indicadas trazem importantes princípios básicos de aplicação nacional, de implementação e cooperação internacional.

[3] A Diretiva em questão foi revogada pelo Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, atualmente em vigor. Entretanto, o objetivo deste Regulamento não conflita com o da Diretiva indicada.

impactou diversas empresas atuantes a nível global, compelindo-as a adaptar suas operações aos termos do Regulamento[4].

Em suma, é possível sintetizar os marcos regulatórios mais relevantes no estudo histórico-evolutivo de privacidade e proteção de dados no cenário internacional da seguinte forma:

Ano	Marco regulatório	Relevância
1890	Artigo *The Right to Privacy* (Harvard Law Review)	Marco doutrinário inicial para o debate sobre privacidade
1970	Lei do *Land Hesse* (Alemanha)	Marco legal inicial para o debate sobre privacidade
1980	Diretrizes da OCDE para a Proteção da Privacidade e dos Fluxos Transfronteiriços de Dados Pessoais	Marco regulatório para o compartilhamento internacional de dados
1981	Convenção 108 do Conselho da Europa	Marco regulatório para o processamento automático de dados
1995	Diretiva 95/46/CE do Parlamento Europeu e do Conselho da União Europeia	Marco legal que introduziu o princípio da livre circulação de dados na UE
2016	Regulamento (EU) 2016/679 do Parlamento Europeu e do Conselho da União Europeia	Marco legal sobre a proteção de dados em âmbito internacional

[4] Consequentemente, tal situação também compele os empresários e empresas de menor porte a se adequarem à norma indicada, vez que muitas das empresas de operação com nível internacional, ao realizar negócios com empresas de âmbito nacional ou regional, trazem como um pré-requisito para contratação que haja conformidade com o Regulamento indicado.

2. ANÁLISE HISTÓRICO-EVOLUTIVA DA PRIVACIDADE E PROTEÇÃO DE DADOS NO ÂMBITO NACIONAL

Assim como no contexto internacional, as primeiras normas tangentes à privacidade e proteção de dados no Brasil remontam a cenários anteriores a uma primeira menção expressa sobre o tema.

Desde a instituição do novo Estado Democrático de Direito, com a Constituição Federal de 1988, já era possível vislumbrar a privacidade e a proteção de dados como direitos fundamentais do cidadão[5].

Posteriormente, com a publicação do Código de Defesa do Consumidor, em 1990, a proteção dos dados foi reafirmada em prol do consumidor, ao passo que, em seu artigo 43, o diploma indicado garante o direito de acesso, pelo titular, às informações existentes em cadastros, fichas, registros e dados pessoais e de consumo arquivados sobre ele, assim como suas respectivas fontes[6].

Pouco mais de duas décadas depois, foi publicada a Lei n° 12.965/2014 (Marco Civil da Internet), que se revelou como um importante marco para o presente estudo, vez que: a) disciplinou o uso da internet buscando harmonizar os direitos individuais – principalmente a proteção de dados e a livre expressão – com os interesses do mercado – livre iniciativa, livre

---

[5] Alguns dos incisos constitucionais que comportam normas tangentes à privacidade e proteção de dados:
Artigo 5° da Constituição Federal - Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à *segurança* e à *propriedade*, nos termos seguintes:
V - é assegurado o direito de resposta, proporcional ao agravo, além da indenização por dano material, moral ou à *imagem*;
X - são invioláveis a *intimidade*, a *vida privada*, a honra e a *imagem* das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação;
XI - a casa é *asilo inviolável* do indivíduo, ninguém nela podendo penetrar sem consentimento do morador, salvo em caso de flagrante delito ou desastre, ou para prestar socorro, ou, durante o dia, por determinação judicial;
XII - é *inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas*, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal.
[6] Artigo 43 do Código de Defesa do Consumidor – 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.

concorrência e afins; b) trouxe direitos e garantias fundamentais para o usuário; c) introduziu o princípio da neutralidade de rede; d) disciplinou a proteção aos registros, aos dados pessoais e às comunicações privadas de forma expressa; e) trouxe hipóteses de responsabilidade civil específicas, dentre outros aspectos relevantes para o presente estudo.

Em 2018, foi publicada a Lei n° 13.709/2018, popularmente conhecida como LGPD (Lei Geral de Proteção de Dados Pessoais), que se revelou como a primeira legislação nacional a tratar especificamente do tema "privacidade e proteção de dados pessoais", vez que, até então, esses direitos eram disciplinados somente de forma esparsa e residual pelas legislações já existentes.

Em suma, é possível sintetizar os marcos regulatórios mais relevantes no estudo histórico-evolutivo de privacidade e proteção de dados no cenário brasileiro da seguinte forma:

Ano	Marco regulatório	Relevância
1988	Constituição da República Federativa do Brasil	Marco legal inicial (geral) para o debate sobre privacidade e proteção da dados
1990	Código de Defesa do Consumidor (Lei n° 8.078/1990)	Estende e reafirma direitos relativos à proteção de dados à figura do consumidor
2014	Marco Civil da Internet (Lei n° 12.965/2014)	Marco legal inicial sobre a interação das pessoas com as redes (internet)
2018	LGPD (Lei n° 13.709/2018)	Marco legal inicial (específico) para o debate sobre privacidade e proteção da dados

3. ATRITOS ADVINDOS DA AUSÊNCIA DE REGULAÇÃO ESPECÍFICA DA IOT NO ESTADO DA ARTE DA LEGISLAÇÃO NACIONAL

A Internet das Coisas representa uma das mais notáveis revoluções tecnológicas do século XXI, redefinindo as fronteiras entre o digital e o físico através de uma rede vasta e integrada de dispositivos conectados. Desde aplicativos domésticos inteligentes até sistemas complexos de gestão urbana, a IoT promete um futuro de eficiência sem precedentes e uma nova onda de inovação em múltiplos setores. No entanto, ao passo que essa tecnologia avança,

surgem também significativas preocupações relacionadas à privacidade e à segurança dos dados pessoais coletados, armazenados e processados por esses dispositivos.

No Brasil, a promulgação da Lei Geral de Proteção de Dados (LGPD) marcou um passo significativo em direção à proteção de dados pessoais. Contudo, a legislação vigente ainda carece de especificidades que abordem os desafios únicos impostos pela IoT. A ausência de uma regulamentação específica para este setor deixa uma lacuna crítica na proteção dos consumidores[7], expondo-os a riscos que vão desde a invasão de privacidade até a exploração indevida de suas informações pessoais.

Esta seção busca analisar a atual situação legislativa brasileira no que concerne à regulação da IoT, destacando a dissonância entre o crescimento tecnológico e as normas de proteção de dados. Este estudo também visa identificar práticas internacionais que poderiam servir de modelo para o aprimoramento da legislação nacional, propondo um caminho legislativo que não apenas proteja os direitos dos consumidores, mas também suporte o crescimento sustentável e ético da IoT no Brasil.

Ao longo deste texto, será explorada a necessidade de uma legislação específica que aborde as particularidades da IoT, considerando a importância de garantir a segurança dos dados pessoais e a privacidade dos usuários em um ambiente cada vez mais conectado. A busca por um equilíbrio entre inovação tecnológica e direitos fundamentais dos cidadãos é o cerne desta discussão, visando estabelecer um marco regulatório robusto que responda eficazmente aos desafios emergentes da era digital.

3.1 A EVOLUÇÃO DA IOT E SUAS IMPLICAÇÕES NA PRIVACIDADE E PROTEÇÃO DE DADOS

A Internet das Coisas, como conceito e prática, tem evoluído de uma ideia futurista para uma realidade palpável e onipresente que permeia vários aspectos da vida hodierna. Essa evolução não se limita à proliferação de dispositivos inteligentes no ambiente doméstico, mas se estende a aplicações industriais, de saúde, urbanismo e além. Estima-se que, até 2030, mais

[7] Não se ignora a existência do Plano Nacional de Internet das Coisas (Decreto nº 9.854/2019). Entretanto, esta norma aborda o assunto de forma incipiente, ou seja, o tema ainda resta carente de uma norma reguladora abrangente.

de 50 bilhões de dispositivos estarão conectados à internet, gerando uma quantidade massiva de dados pessoais e não pessoais a cada segundo (Evans, 2011, p. 4). Esta seção analisa a trajetória de crescimento da IoT, destacando como ela reconfigura as normas de privacidade e proteção de dados.

O conceito de "coisas" na IoT abrange uma gama diversificada de dispositivos, desde eletrodomésticos comuns, como refrigeradores e assistentes de voz, até complexos sistemas de monitoramento industrial. A habilidade desses dispositivos de coletar, transmitir e processar dados em tempo real oferece conveniências inegáveis, mas também introduz numerosas vulnerabilidades de segurança e privacidade. A expansão da IoT é alimentada por avanços significativos em tecnologias de sensoriamento, capacidade de armazenamento em nuvem, velocidades de processamento e, especialmente, padrões de conectividade como 5G, que facilitam uma comunicação quase instantânea e contínua entre dispositivos.

A natureza intrinsecamente invasiva da IoT, que se baseia na coleta contínua de dados, lança desafios significativos para a privacidade e a segurança dos dados. Cada dispositivo IoT pode ser visto como um ponto de coleta de dados pessoais, muitas vezes sem o conhecimento explícito do usuário: (i) Coleta de Dados Pessoais – Muitos dispositivos IoT coletam informações detalhadas sobre os hábitos pessoais, preferências e até a saúde dos usuários. Por exemplo, um relógio inteligente pode monitorar informações sobre a saúde do usuário, enquanto um refrigerador inteligente pode rastrear hábitos alimentares; (ii) Segurança dos Dados – A segurança dos dados coletados por dispositivos IoT é uma preocupação crescente. Muitos desses dispositivos possuem protocolos de segurança insuficientes, o que os torna vulneráveis a ataques cibernéticos, resultando em potenciais vazamentos de dados pessoais; (iii) Consentimento e Transparência – A complexidade e a opacidade com que os dados são coletados, processados e compartilhados por dispositivos IoT muitas vezes tornam difícil para os usuários dar um consentimento verdadeiramente informado. Além disso, a falta de transparência sobre como os dados são utilizados pelos fabricantes ou terceiros agrava a situação.

A regulação atual, incluindo a Lei Geral de Proteção de Dados brasileira, enfrenta dificuldades para abordar especificamente as questões que emergem no contexto da IoT. A legislação existente foi projetada primariamente para ambientes digitais mais tradicionais e não para ecossistemas interconectados e automatizados que caracterizam a IoT. Especificamente, a

LGPD e regulamentos similares focam na proteção de dados pessoais com base em princípios de transparência, consentimento e segurança da informação. No entanto, a aplicabilidade desses princípios à IoT é complexa devido à sua arquitetura distribuída e à natureza automatizada da coleta de dados.

A crescente integração da IoT em todos os aspectos da vida cotidiana e profissional traz consigo enormes benefícios em termos de conveniência e eficiência. No entanto, esses avanços não devem ocorrer às custas da privacidade e segurança dos dados pessoais. É crucial que os desenvolvimentos regulatórios acompanhem o ritmo das inovações tecnológicas, assegurando que os direitos à privacidade e à proteção de dados sejam preservados na era da IoT. A próxima seção deste capítulo abordará os desafios regulatórios específicos e proporá caminhos para o fortalecimento da legislação, garantindo que a proteção de dados e a privacidade sejam efetivamente mantidas no contexto brasileiro, frente aos desafios únicos impostos pela IoT.

3.2 DESAFIOS REGULATÓRIOS E A PROTEÇÃO DE DADOS NA IOT

A expansão da Internet das Coisas introduz um panorama complexo para a regulamentação de proteção de dados, uma vez que os dispositivos conectados permeiam uma diversidade de setores e atividades. Embora determinadas normas atuais, como a LGPD, representem marcos significativos na proteção de dados pessoais, enfrentam desafios específicos quando aplicadas ao contexto da IoT. Esta seção discute os principais desafios regulatórios impostos pela IoT e avalia a adequação das normas vigentes para proteger efetivamente a privacidade e os dados dos usuários.

A LGPD foi elaborada com base em princípios gerais de proteção de dados, inspirados largamente pelo Regulamento Geral de Proteção de Dados (GDPR) da União Europeia. Esses princípios incluem a transparência, o consentimento informado, a limitação de finalidade, a minimização de dados, a segurança, a não discriminação, entre outros. No entanto, a aplicação desses princípios no contexto da IoT apresenta desafios particulares.

Dentre estes desafios, aponta-se as dificuldades em operar a transparência e efetivar a obtenção do consentimento do usuário, vez que muitos dispositivos IoT operam de maneira contínua e automática, coletando dados sem interação direta com o usuário. Isso faz com que

seja uma tarefa penosa para o fornecedor garantir que o consentimento seja informado e específico, como exigido pela lei.

Outros desafios ocorrem em relação à minimização dos dados, vez que, dada a vasta quantidade de dados que dispositivos IoT podem coletar, muitas vezes é complexo aplicar o princípio da minimização de dados, que preconiza que apenas os dados necessários para a finalidade especificada sejam coletados.

A segurança dos dados coletados é outra preocupação significativa. A diversidade e o número de dispositivos conectados ampliam a superfície de ataque, expondo os dados pessoais a riscos consideráveis de segurança. Embora a LGPD exija a adoção de medidas técnicas e administrativas apropriadas para proteger os dados, a implementação efetiva dessas medidas pode ser complexa devido à heterogeneidade tecnológica e à ausência de padrões de segurança especificamente voltados para IoT.

Além das questões já apontadas, existem lacunas na legislação que não foram projetadas para abordar as peculiaridades tecnológicas da IoT. Uma dessas lacunas é a classificação dos dados coletados, que nem sempre podem ser claramente identificados como pessoais ou anonimizados, o que implica complicações práticas para a aplicação das normas de proteção de dados.

Outro ponto diz respeito à responsabilidade pelos dados. Na IoT, a cadeia de responsabilidade é muitas vezes difusa; fabricantes de dispositivos, desenvolvedores de software, provedores de serviços e até os usuários têm papéis que podem sobrepor-se na gestão de dados, tornando a atribuição de responsabilidades complexa e ambígua.

A internacionalização da IoT, que envolve frequentemente o fluxo transfronteiriço de dados, adiciona outro nível de complexidade, exigindo conformidade com múltiplas jurisdições e suas respectivas leis de proteção de dados. Isso representa um desafio adicional para empresas nacionais e internacionais que operam no Brasil.

Dada a necessidade de ajustes na legislação para abordar especificamente os desafios da IoT, é imperativo desenvolver normas e diretrizes técnicas que contemplem as particularidades desta tecnologia. Isso incluiria a elaboração de padrões de segurança para dispositivos IoT, a clarificação das regras de consentimento para torná-las aplicáveis no contexto da IoT, e o fomento a modelos de governança de dados que reforcem a transparência e o controle do usuário sobre seus dados.

Os desafios regulatórios impostos pela IoT exigem uma resposta legislativa que esteja à altura das complexidades tecnológicas e operacionais desta nova era digital. As leis atuais, embora fundamentais, necessitam de ajustes e ampliações para enfrentar eficazmente os riscos à privacidade e à proteção de dados na IoT. A próxima seção explorará práticas regulatórias internacionais que podem servir como referência para o aprimoramento da legislação nacional no contexto da IoT, garantindo que a proteção de dados e a privacidade sejam efetivamente mantidas.

3.3 RESPOSTA INTERNACIONAL E LIÇÕES PARA O BRASIL

A abordagem de diversos países em relação à regulamentação da Internet das Coisas oferece perspectivas valiosas para o aprimoramento da legislação brasileira neste setor. Enquanto o Brasil ainda lida com a adequação de normas gerais de proteção de dados ao contexto específico da IoT, várias jurisdições internacionais já implementaram diretrizes específicas que abordam os desafios únicos desta tecnologia. Este segmento analisa as práticas regulatórias adotadas por algumas dessas jurisdições e explora como essas experiências podem informar e inspirar reformas legislativas no Brasil.

Nos Estados Unidos, a abordagem para a regulamentação da IoT tem sido caracterizada por um modelo de governança que envolve tanto legislação específica quanto iniciativas de padrões lideradas pela indústria. Por exemplo, a legislação da Califórnia, conhecida como a Lei de Privacidade do Consumidor da Califórnia (CCPA), impõe obrigações rigorosas sobre a transparência e o controle do consumidor em relação aos dados pessoais, aplicando-se de maneira significativa aos dispositivos de IoT. Além disso, agências como o Instituto Nacional de Padrões e Tecnologia (NIST) dos EUA desenvolveram diretrizes específicas que abordam a segurança da IoT, focando na necessidade de proteção robusta desde o design até o uso final dos dispositivos.

Na União Europeia, o Regulamento Geral sobre a Proteção de Dados (GDPR) estabelece um quadro regulatório abrangente que inclui disposições aplicáveis à IoT. O GDPR enfatiza princípios como a minimização de dados, onde apenas os dados necessários para fins específicos devem ser coletados, e a proteção por padrão, exigindo que medidas de segurança sejam integradas ao design dos produtos e serviços de IoT. Esses princípios são complementados por diretrizes emitidas por órgãos como o Grupo de Trabalho do Artigo 29

(agora o Comitê Europeu de Proteção de Dados), que oferece recomendações específicas para a aplicação do GDPR no contexto da IoT.

A experiência dessas jurisdições demonstra a importância de um quadro legal claro e específico para a IoT, que não apenas protege os dados pessoais, mas também fortalece a confiança do consumidor na segurança dos dispositivos conectados. Para o Brasil, a adoção de um modelo similar poderia envolver várias estratégias legislativas e regulatórias: (i) Desenvolvimento de Normas Técnicas Específicas – Assim como nos EUA, o Brasil poderia beneficiar-se da elaboração de normas técnicas que detalhem os requisitos de segurança para dispositivos de IoT, garantindo que a proteção de dados seja incorporada desde a fase de design; (ii) Legislação Específica para IoT – Inspirando-se em premissas do GDPR, o Brasil poderia considerar a implementação de uma legislação específica (ou seções dedicadas em legislações específicas) para IoT que aborde de maneira explícita questões como consentimento, transparência, direitos de acesso e retificação, e a eliminação de dados, adaptando esses conceitos para o contexto tecnológico da IoT; (iii) Fomento à Autorregulação e Padrões de Indústria – Incentivar a indústria a desenvolver e aderir a padrões de segurança e privacidade pode ser uma maneira eficaz de complementar a legislação, assegurando que as práticas de mercado evoluam para acompanhar as mudanças tecnológicas.

A implementação dessas medidas no Brasil requer uma análise cuidadosa das especificidades jurídicas e tecnológicas locais, bem como um diálogo contínuo entre reguladores, legisladores, a indústria de tecnologia e a sociedade civil. A harmonização das leis de proteção de dados com as exigências da IoT é crucial para que o país possa aproveitar plenamente os benefícios dessa tecnologia emergente, ao mesmo tempo em que salvaguarda os direitos fundamentais de privacidade e proteção de dados dos cidadãos.

3.4 PROPOSTAS PARA UMA REGULAMENTAÇÃO EFICAZ DA IOT NO BRASIL

Diante do avanço tecnológico representado pela Internet das Coisas e das respostas regulatórias internacionais analisadas, torna-se imperativo para o Brasil desenvolver um arcabouço jurídico que enderece especificamente as singularidades dessa tecnologia. Esta seção propõe um conjunto de medidas legislativas e regulatórias destinadas a estabelecer uma proteção para os dados pessoais e a privacidade dos usuários no contexto da IoT, refletindo

sobre a integração de práticas bem-sucedidas globalmente com as particularidades jurídicas e sociais brasileiras.

A primeira medida proposta envolve a elaboração de legislação específica para a IoT. Tal legislação deve abranger disposições detalhadas sobre a coleta, o armazenamento, o processamento e a transferência de dados, assegurando que todos esses aspectos sejam realizados de forma transparente e com o consentimento informado dos usuários, considerando sempre o volume, a velocidade e a variedade de dados coletados neste contexto. É crucial que esta legislação incorpore princípios de proteção de dados por design e por padrão, exigindo que fabricantes e desenvolvedores de sistemas IoT integrem medidas de segurança apropriadas em todas as etapas do desenvolvimento e operação dos dispositivos.

Além disso, é essencial que o Brasil desenvolva e adote padrões técnicos específicos para a IoT. Esses padrões devem estabelecer requisitos mínimos de segurança e privacidade, incluindo diretrizes para a atualização segura de software, autenticação robusta de usuários e dispositivos, e criptografia de dados sensíveis. A adoção de tais padrões não apenas fortaleceria a segurança dos dispositivos IoT, mas também facilitaria a interoperabilidade e a compatibilidade entre diferentes sistemas e dispositivos.

Uma terceira medida relevante seria incentivar a autorregulação por parte da indústria de IoT. Isso poderia ser alcançado por meio do fomento a iniciativas de certificação e selos de qualidade que atestem o cumprimento de normas de privacidade e segurança por produtos e serviços IoT. A autorregulação, acompanhada de supervisão e fiscalização adequadas por parte do Estado, poderia proporcionar flexibilidade suficiente para acomodar a rápida evolução tecnológica, ao mesmo tempo em que assegura o respeito aos direitos dos consumidores.

A promoção de campanhas educativas e de conscientização também desempenha um papel fundamental na proteção de dados e na segurança da IoT. Tais campanhas deveriam visar tanto os consumidores, para que estes possam fazer escolhas informadas e seguras, quanto as empresas, reforçando a importância da implementação de práticas de segurança avançadas e do respeito à legislação de proteção de dados.

Por fim, o estabelecimento de um diálogo contínuo entre o governo, a academia, a indústria e a sociedade civil é essencial para a criação de uma legislação adaptativa e responsiva às necessidades tecnológicas e sociais. Esse diálogo pode facilitar a atualização constante da

legislação e das normas técnicas, além de permitir que diferentes perspectivas sejam consideradas na formulação de políticas públicas relacionadas à IoT.

A implementação dessas medidas exigirá um compromisso assumido pelo governo brasileiro, bem como uma colaboração efetiva entre todos os setores envolvidos. Somente por meio de uma abordagem integrada e multidisciplinar será possível garantir que a regulamentação da IoT no Brasil proteja efetivamente os dados pessoais e a privacidade dos usuários, ao mesmo tempo em que fomenta a inovação e o desenvolvimento tecnológico.

CONCLUSÃO

A análise detalhada da evolução regulatória e dos desafios impostos pela Internet das Coisas demonstra a urgência de uma resposta legislativa ajustada às peculiaridades desta tecnologia disruptiva. As legislações existentes no Brasil, incluindo a Lei Geral de Proteção de Dados, proporcionam uma base sólida para a proteção de dados pessoais; contudo, elas precisam ser expandidas e especificadas para abarcar as complexidades introduzidas pelos dispositivos IoT.

A interconexão e a capacidade de comunicação dos dispositivos IoT oferecem oportunidades inéditas para a melhoria da qualidade de vida, eficiência empresarial e gestão de recursos urbanos. No entanto, essas mesmas características apresentam riscos significativos à privacidade e segurança dos dados dos usuários. Sem regulamentações adequadas, os indivíduos ficam vulneráveis a violações de privacidade, usos indevidos de dados pessoais e ataques cibernéticos. Assim, o desenvolvimento de uma legislação específica para IoT é imperativo para equilibrar os benefícios da tecnologia com a proteção dos direitos fundamentais dos cidadãos.

As experiências internacionais, como as práticas adotadas na União Europeia e nos Estados Unidos, oferecem modelos valiosos de como legislações e diretrizes podem ser estruturadas para enfrentar os desafios da IoT. A partir desses modelos, o Brasil pode construir um regime regulatório que não apenas proteja dados e privacidade, mas também estimule a inovação e a adoção tecnológica de forma responsável e segura.

Portanto, propõe-se uma abordagem regulatória holística que inclua: a elaboração de legislação específica para IoT, o desenvolvimento de normas técnicas de segurança, a promoção da autorregulação através de certificações de conformidade, a realização de campanhas de

conscientização para consumidores e empresas, e a manutenção de um diálogo constante e produtivo entre todos os *stakeholders* envolvidos.

Conclui-se que a regulamentação eficaz da IoT no Brasil é crucial para garantir que essa revolução tecnológica seja integrada à sociedade de maneira que respeite os valores éticos e jurídicos estabelecidos, ao mesmo tempo em que aproveita o potencial de transformação que a IoT promete. A legislação que responda adequadamente aos desafios da IoT fortalecerá a confiança pública na digitalização crescente de diversos setores, assegurando que o desenvolvimento tecnológico avance de mãos dadas com a proteção dos direitos individuais e coletivos.

REFERÊNCIAS

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

BRASIL. Lei n° 8.078, de 11 de setembro de 1990. *Código de Defesa do Consumidor*. Diário Oficial da União, Brasília, DF, 12 set. 1990.

BRASIL. Lei n° 12.965, de 23 de abril de 2014. *Marco Civil da Internet*. Diário Oficial da União, Brasília, DF, 24 abr. 2014.

BRASIL. Lei n° 13.709, de 14 de agosto de 2018. *Lei Geral de Proteção de Dados Pessoais (LGPD)*. Diário Oficial da União, Brasília, DF, 15 ago. 2018.

CALAZA, Tales. 2020. O direito à privacidade: origem histórica e jurídica. *In:* LONGHI, João Victor Rozatti; FALEIROS JÚNIOR, José Luiz de Moura; BORGES, Gabriel de Oliveira Aguiar; REIS, Guilherme (Coords.). *Fundamentos do direito digital*. Uberlândia: LAECC, 2020, p. 169-183.

Treaty No. 108: Council of Europe. (1981). *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Treaty No. 108)*. Disponível em: https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=108. Acesso em: 9 jul. 2022.

Directiva 95/46/CE: Parlamento Europeu e Conselho. (1995). *Directiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de outubro de 1995, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados*. EUR-Lex. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A31995L0046. Acesso em: 9 jul. 2022.

Diretrizes da OCDE: OECD. (1980). *Diretrizes da OCDE para a proteção da privacidade e dos fluxos transfronteiriços de dados pessoais*. Disponível em: https://www.oecd.org/en/topics/digital.html. Acesso em: 9 jul. 2022.

EVANS, Dave. A Internet das Coisas: Como a próxima evolução da Internet está mudando tudo. *Cisco Internet Business Solutions Group (IBSG)*. 2011. Disponível em: https://www.cisco.com/c/dam/global/pt_br/assets/executives/pdf/internet_of_things_iot_ibsg_0411final.pdf. Acesso em: 21 abr. 2024.

LIMBERGER, T. Da evolução do direito a ser deixado em paz à proteção dos dados pessoais. *Revista do Direito*, n. 30, p. 138-160, 15 jul. 2008.

Proteção de dados pessoais: European Parliament. (2022). *Proteção de dados pessoais*. Disponível em: https://www.europarl.europa.eu/factsheets/pt/home. Acesso em: 9 jul. 2022.

Regulamento (UE) 2016/679: União Europeia. (2016). *Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados*. EUR-Lex. Disponível em: https://eur-lex.europa.eu/legal-content/pt/TXT/?uri=CELEX%3A32016R0679. Acesso em: 9 jul. 2022.

WARREN, Samuel D.; BRANDEIS, Louis D. The right to privacy. *Harvard Law Review*, Cambridge, v. 4, n. 5, p. 193-220, dez. 1890.