CENTRO DE EDUCAÇÃO SUPERIOR CESREI LTDA
CURSO DE BACHARELADO EM DIREITO

RUBENILDO PEDRO ACIOLE

HIPERCONECTIVIDADE *VERSUS* PRIVACIDADE: UM ESTUDO SOBRE A INTERNET DAS COISAS NA SOCIEDADE EM REDE

Trabalho de Conclusão de Curso (Artigo) apresentado à Coordenação do Curso de Direito da Cesrei Faculdade, como requisito parcial para a obtenção do grau de Bacharel em Direito, pela referida instituição.

Orientadora: Prof.ª Esp. Sabrina Matias Cavalcante, Cesrei Faculdade

Examinador 1: Prof. Me. Diego Araújo Coutinho, Cesrei Faculdade

Examinador 2: Prof. Esp. Wendley Steffan Ferreira dos Santos, Cesrei Faculdade

Campina Grande - PB
2026

HIPERCONECTIVIDADE *VERSUS* PRIVACIDADE: UM ESTUDO SOBRE A INTERNET DAS COISAS NA SOCIEDADE EM REDE

ACIOLE, Rubenildo Pedro[1]

CAVALCANTE, Sabrina Matias[2]

RESUMO

Com foco em investigar os desafios jurídicos impostos pelo avanço da Internet das Coisas e da hiperconectividade ao direito fundamental à proteção de dados pessoais no Brasil, o presente estudo tem como escopo central analisar a suficiência e as limitações do Marco Civil da Internet e da Lei Geral de Proteção de Dados Pessoais diante das vulnerabilidades sistêmicas e das lacunas normativas do ecossistema de dispositivos conectados. É relevante estudar para compreender a sociedade contemporânea. Profundamente conectada, na qual bilhões de objetos físicos coletam, processam e transmitem informações de forma contínua e autônoma, gerando riscos inéditos de vigilância, controle e exploração comercial sem a devida transparência, o que aprofunda as assimetrias de poder entre corporações de tecnologia e os cidadãos. A análise evidencia que a arquitetura da Internet das Coisas, marcada pela coleta massiva, ininterrupta e automatizada de dados sensíveis e pessoais, fragiliza os pilares do sistema de proteção informacional. Observa-se a configuração do paradoxo do consentimento, em que a autorização do titular se converte em uma ficção jurídica devido à ausência de interfaces físicas nas ferramentas e à extensão abusiva dos termos de uso. O que preocupa são as violações à transparência, falhas estruturais nos requisitos de segurança da informação e dificuldade na atribuição de responsabilidade civil dentro de uma cadeia complexa de fabricantes e operadores. Evidentemente, o modelo normativo vigente é insuficiente frente às especificidades tecnológicas que se alteram o tempo todo. Dada a necessidade de tratar a privacidade não apenas como direito de exclusão, mas de assegurar uma autodeterminação informativa dinâmica, visualizam-se caminhos para o aperfeiçoamento regulatório com a propositura da elaboração de diretrizes específicas pela Autoridade Nacional de Proteção de Dados, a obrigatoriedade da adoção da privacidade desde a concepção na fabricação dos equipamentos, o fortalecimento da responsabilidade solidária entre as empresas envolvidas e o estímulo ao letramento digital dos indivíduos e portanto da sociedade.

Palavras-chave: Internet das Coisas. Proteção de dados. Consentimento informado. Hiperconectividade. Autodeterminação informativa.

ABSTRACT

[1]Concluinte do Curso de Bacharelado em Direito, E-mail: rubennildo@gmail.com;

[2]Professora do curso de Direito da Cesrei Faculdade, Advogada, Mestranda no PPGD/UFPE, Especialista em Direito Civil, Digital, Previdenciário e Inteligência Artificial. E-mail: sabrinamatias@cesrei.edu.br.

This study starts from the focus on investigating the legal challenges imposed by the advancement of the Internet of Things and hyperconnectivity to the fundamental right to personal data protection in Brazil. Thus, it aims to analyze the sufficiency and limitations of the Brazilian Internet Bill of Rights (Marco Civil da Internet) and the General Data Protection Law (Lei Geral de Proteção de Dados Pessoais) in the face of systemic vulnerabilities and normative gaps in the ecosystem of connected devices. This study is relevant for understanding contemporary society, which is deeply connected through billions of physical objects that collect, process and transmit information continuously and autonomously, generating unprecedented risks of surveillance, control, and commercial exploitation without due transparency, culminating in the deepening of the power asymmetries between technology corporations and citizens. The analysis evidences that the architecture of the Internet of Things, characterized by the massive, uninterrupted and automated collection of sensitive and personal data, weakens the bases of the information protection system. In this context, the paradox of consent is observed because the data subject's authorization becomes a legal fiction due to the absence of physical interfaces in the tools and the abusive extension of the terms of use. The concerns are the violations of transparency, structural flaws in information security requirements, and the difficulty in assigning civil responsibility within a complex chain of manufacturers and operators. Evidently, the current regulatory framework is insufficient in the face of constantly changing technological specificities. Given the need to treat privacy not only as a right to opt out, but also to ensure dynamic informational self-determination, possible ways for regulatory improvement are envisioned, including the proposal of specific guidelines by the National Data Protection Authority, the mandatory adoption of privacy from the design stage in equipment manufacturing, the strengthening of joint liability among the companies involved, and the encouragement of digital literacy among individuals and, therefore, society.

Keywords: Internet of Things. Data protection. Informed consent. Hyperconnectivity. Informational self-determination.

1 INTRODUÇÃO

Os avanços tecnológicos transformaram a nossa sociedade e hoje vivemos num tempo em que pessoas e objetos estão sempre conectados. Esse fenômeno é referido como internet das coisas (IoT), que permite que dispositivos comuns como *smartwatches*, eletrodomésticos e carros registrem e transmitam nossos dados incessantemente por conta própria.

Para compreender melhor essa nova realidade, o trabalho se apoia nos conceitos de Manuel Castells, que demonstra que aqueles que controlam as redes de informação detêm o poder hoje, e em Pierre Lévy, que adverte que a internet viabiliza

formas de colaboração, mas também produz novas infra estruturas invisíveis para a vigilância. O próprio risco desse monitoramento constante é o que justifica e torna oportuna esta pesquisa. A acumulação silenciosa de dados por parte das empresas inclina o equilíbrio de poder e avança sobre a privacidade individual, um direito recentemente consagrado e formalmente protegido pela Constituição Federal do Brasil de 1988.

Diante dessa realidade, o principal problema da pesquisa busca responder: a Lei do Marco Civil da Internet e a Lei Geral de Proteção de Dados (LGPD) serão suficientes para proteger os nossos dados na IoT? O desejo de que sim é a hipótese que conduz a pesquisa. Apesar de representar um enorme passo à frente, a LGPD apresenta falhas práticas nesse novo mundo. O modelo da lei está comprometido com o consentimento explícito dos usuários, o conhecido: “ler e aceitar”, o que se revela uma ilusão em dispositivos sem telas que funcionam de forma automatizada e nos quais o controle real das informações se torna impossível.

Para estudar essa questão, o objetivo principal desta pesquisa é analisar os limites e lacunas das leis brasileiras diante dos desafios impostos pela IoT. Em particular, pretende delinear as origens históricas dessas tecnologias, descrever teorias sociológicas sobre a vida em conexão e apresentar os desafios operacionais da LGPD (especialmente articulando mecanismos de consentimento, transparência, segurança e responsabilização). A metodologia é qualitativa, exploratória e descritiva. O método é hipotético-dedutivo, já que o texto parte da hipótese de que a lei hoje é suficiente para verificar essa suposição mediante uma análise de como ela funciona na prática com dispositivos conectados.

Trata-se de um estudo bibliográfico e documental, baseado na leitura de leis (como a LGPD e o Marco Civil da Internet), regulamentos emitidos pela Autoridade Nacional de Proteção de Dados ANPD e em livros escritos por juristas especializados utilizando um referencial teórico ancorado na sociologia das redes e na filosofia da cultura digital para compreender as dinâmicas de poder comunicacional baseadas nos fluxos de informação.

Essas ideias foram então estruturadas de forma lógica em três seções. A primeira apresenta uma travessia no tempo das antigas redes analógicas até a Internet das Coisas dos dias atuais. Agora, a segunda seção estabelece a base teórica com Castells e Lévy, que constroem uma explicação clara das dinâmicas de poder e

controle que operam por trás das redes digitais. A terceira é dedicada à perspectiva jurídica, analisando as insuficiências da LGPD e propondo atualizações, como sistemas que protegem os dados desde o momento em que são fabricados pelas empresas até como usamos no dia a dia.

2 EVOLUÇÃO HISTÓRICA DAS TECNOLOGIAS DE COMUNICAÇÃO E O SURGIMENTO DA INTERNET DAS COISAS

Para entender as limitações da LGPD e os desafios jurídicos que a Internet das Coisas (IoT) traz ao Brasil, precisamos olhar para a história e entender como chegamos à atual fase de "hiperconectividade", isso porque, a forma como nos comunicamos evoluiu e saímos de sistemas analógicos isolados para uma rede global gigante, onde bilhões de objetos físicos ficam conectados à internet o tempo todo, funcionando sozinhos,sendo autônomos e autossuficientes.

Essa grande mudança não envolve apenas máquinas e tecnologia. Ela transformou a sociedade e o próprio Direito, pois cada novo avanço tecnológico alterou quem tem o poder, criou novas formas de consumir e explorar nossos dados, e gerou novos problemas para o Estado tentar regulamentar.

A história das tecnologias de comunicação pode ser compreendida como uma longa trajetória de convergência, orientada pelo imperativo técnico e social de superar as barreiras físicas que separavam as pessoas e as informações. Antes da consolidação das redes digitais, as sociedades industriais se organizavam em torno de sistemas de comunicação analógicos como telégrafo, telefone, rádio e a televisão, cada qual operando em infraestruturas próprias, com padrões técnicos incompatíveis e capacidades de transmissão limitadas.

No Brasil, a trajetória das telecomunicações seguiu os movimentos internacionais com algum atraso estrutural, reflexo das condições econômicas e geográficas do país. A criação da Embratel, em 1965, representou um marco fundamental na organização das telecomunicações nacionais, ao estabelecer uma

infraestrutura estatal capaz de integrar o vasto território brasileiro por meio de redes analógicas de longa distância.[3]

A passagem do paradigma analógico para o digital, iniciada nas décadas de 1970 e 1980, foi impulsionada pelo desenvolvimento dos microprocessadores, pela digitalização dos sinais de voz e dados e, sobretudo, pela criação da ARPANET (*Advanced Research Projects Agency Network*), em 29 de outubro de 1969, quando Charley Kline, estudante da Universidade da Califórnia em Los Angeles (UCLA), estabeleceu a primeira conexão entre dois computadores geograficamente distantes, inaugurando o que viria a ser o embrião da internet moderna (Welivesecurity, 2023).

A ARPANET nasceu de uma necessidade estratégica durante a Guerra Fria: criar uma rede de comunicação descentralizada, capaz de sobreviver a ataques inimigos, que permitisse aos centros de pesquisa da agência ARPA compartilhar informações e recursos computacionais. Seu design descentralizado, baseado na comutação de pacotes, e a posterior adoção do protocolo TCP/IP (*Transmission Control Protocol/Internet Protocol*), desenvolvido em 1973 e publicado em 1974 por Vinton Cerf, Yogen Dalal e Carl Sunshine, estabeleceram os fundamentos técnicos sobre os quais toda a internet seria construída.[4]

Como observa Castells (1999, p. 82), a internet teve origens surpreendentemente específicas:

> A internet nasceu da confluência peculiar entre a grande ciência, a pesquisa militar e a cultura libertária. Sua história revela os meandros de uma sociedade que não podia antecipar as consequências de uma tecnologia que ela mesma havia criado. (Castells, 1999, p. 82).

Neste sentido, a World Wide Web (WWW), desenvolvida pelo físico britânico Tim Berners-Lee no início da década de 1990, transformou a internet de uma rede restrita à comunidade científica em uma plataforma de comunicação e troca de

---

[3] A Embratel (Empresa Brasileira de Telecomunicações) foi criada pela Lei nº 4.769, de 1965, como empresa pública federal vinculada ao Ministério das Comunicações, com a missão de integrar a infraestrutura de telecomunicações do território nacional. Cf. AGÊNCIA BRASIL. De 1500 a 2021: veja como a comunicação evoluiu no Brasil. Disponível em: https://agenciabrasil.ebc.com.br/geral/noticia/2021-05/linha-do-tempo-telecomunicacoes. Acesso em: 01 junho 2026.

[4] Sobre o desenvolvimento do protocolo TCP/IP, ver: MATERIALPUBLIC IMD/UFRN. *História da Internet*. Disponível em: https://materialpublic.imd.ufrn.br/curso/disciplina/4/21/4/2. Acesso em: 01 junho 2026. O protocolo foi publicado como RFC 685 por Vinton Cerf, Yogen Dalal e Carl Sunshine, na Universidade de Stanford.

informações acessível ao público em geral.[5] No Brasil, a internet chegou ao ambiente acadêmico em 1991, por meio da Rede Nacional de Pesquisa (RNP), que conectou dez estados e o Distrito Federal, com uma capacidade inicial de apenas 64 Kb/s.

A abertura comercial veio em maio de 1995, quando o Comitê Gestor da Internet no Brasil (CGI.br) foi criado para gerir as políticas de uso da rede no país e os provedores passaram a oferecer conexões discadas (*dial-up*) de TCP/IP aos usuários (RNP, 2022).[6] Esse processo de massificação progressiva da internet criou as condições infraestruturais para a emergência de um novo paradigma tecnológico: a Internet das Coisas.

2.1 DE ONDE VEM O TERMO “INTERNET DAS COISAS”?

Embora tenha se consolidado como objeto de estudo científico e debate regulatório apenas nas últimas décadas, possui raízes que remontam às primeiras experiências de conexão entre objetos físicos e redes computacionais.

O primeiro dispositivo considerado precursor da IoT foi uma máquina de venda de refrigerantes da Universidade Carnegie Mellon, que, no início da década de 1980, podia ser monitorada remotamente para verificar o estoque e a temperatura das bebidas (Wiki computação/UFPR, 2022). Essa experiência inaugural, aponta o princípio central que norteará o desenvolvimento posterior da IoT, a capacidade de objetos físicos coletar, processar e transmitir dados de forma autônoma, sem necessidade de intervenção humana direta.[7]

---

[5]A World Wide Web foi proposta por Tim Berners-Lee em 1989 e implementada em 1991 no CERN (Organização Europeia para a Investigação Nuclear), na Suíça. Cf. TODA MATÉRIA. História da Internet: quem criou e quando surgiu. Disponível em: https://www.todamateria.com.br/historia-da-internet/. Acesso em: 01 junho 2026.

[6]RNP. Evolução da internet no Brasil. 9 jun. 2022. Disponível em: https://www.rnp.br/comunidades/evoluo-da-internet-no-brasil/. Acesso em: 20 maio 2026. Para um histórico detalhado do surgimento da internet comercial no Brasil, ver também: AGÊNCIA BRASIL. Como era a Internet no Brasil antes da comercialização. 3 maio 2021. Disponível em: https://agenciabrasil.ebc.com.br/geral/noticia/2021-04/como-era-internet-no-brasil-antes-da-comercializacao. Acesso em: 01 junho 2026.

[7]WIKI COMPUTAÇÃO/UFPR. *Internet das Coisas*. Disponível em: https://wiki.inf.ufpr.br/computacao/doku.php?id=i%3Ainternet_das_coisas. Acesso em: 01 junho 2026. Sobre o primeiro dispositivo IoT da história, ver também: ENGENHARIA HÍBRIDA. Você conhece a história da Internet das Coisas (IoT)? 15 jan. 2026. Disponível em: https://www.engenhariahibrida.com.br/post/historia-internet-das-coisas-iot. Acesso em: 01 junho 2026.

O termo *Internet of Things* foi cunhado pelo engenheiro britânico Kevin Ashton, cofundador do Auto-ID Center no Massachusetts Institute of Technology (MIT), em 1999, em uma apresentação realizada para a Procter & Gamble (P&G), apareceu a expressão para chamar a atenção da gerência sênior da empresa para o potencial da tecnologia de identificação por radiofrequência (RFID) como mecanismo de comunicação autônoma entre dispositivos (AVAST, 2019)[8], conforme descreve o criador da expressão supra:

> Eu estava falando sobre a cadeia de suprimentos ser uma 'rede das coisas' e a internet ser uma 'rede de bits' e como a tecnologia de sensores poderia combinar as duas. Depois, eu pensei em uma 'Internet das Coisas' e disse: 'É isso aí'. Era chamativo. E se tornou o título da apresentação. (Ashton apud Avast, 2019).

É relevante destacar que, embora Kevin Ashton seja apontado como o criador do termo, a ideia subjacente ao conceito foi articulada pela primeira vez por Peter T. Lewis, em setembro de 1985, que definiu a IoT como "a integração de pessoas, processos e tecnologia com dispositivos e sensores conectáveis para permitir o monitoramento remoto, status, manipulação e avaliação de tendências de tais dispositivos" (Lewis apud Dio, 2023).

E de forma bem simplificada significa que a prática de conectar objetos do dia a dia que já existia muito antes de alguém inventar o nome chique “internet das coisas” (IoT), e atualmente o mais difundido é aquele formulado pela Oracle[9] e amplamente adotado pela literatura técnica e jurídica, segundo o qual IoT designa "uma rede de objetos físicos 'coisas' que são incorporados com sensores, software e outras tecnologias com a finalidade de conectar e trocar dados com outros dispositivos e sistemas pela internet", abrangendo desde objetos domésticos comuns a ferramentas industriais sofisticadas (Dio, 2023).

Do ponto de vista técnico, a IoT evoluiu da comunicação máquina a máquina (M2M-*Machine to Machine*), que conectava dispositivos individuais à nuvem, para um

---

[8]AVAST. Como Kevin Ashton batizou a Internet das Coisas? 26 set. 2019. Disponível em: https://blog.avast.com/pt-br/kevin-ashton-named-the-internet-of-things. Acesso em: 01 junho 2026. Kevin Ashton também é cofundador do Auto-ID Center no MIT, responsável pelo desenvolvimento de padrões globais de RFID.

[9] Empresa de tecnologia que fornece a infraestrutura em nuvem necessária para que o ecossistema da IoT exista de forma escalável e inteligente.

ecossistema amplo e interoperável de bilhões de sensores, plataformas e dispositivos inteligentes que conectam pessoas, sistemas e aplicações em tempo real (Chaves, 2022).

Os dados resultantes da hiperconectividade ilustram a dimensão do desafio regulatório que se coloca para ordenamentos jurídicos como o brasileiro, de regular o tratamento de dados gerados por uma rede de dispositivos cujo volume e diversidade superam em muito a capacidade de fiscalização dos mecanismos tradicionais de proteção da privacidade.

2.2 PRESSUPOSTOS DA HIPERCONECTIVIDADE: A GÊNESE DA SOCIEDADE 4.0

A Quarta Revolução Industrial, conceito formulado por Klaus Schwab, fundador e presidente executivo do Fórum Econômico Mundial, em 2016, na cidade de Davos, Suíça, representa o pano de fundo histórico no qual a Internet das Coisas alcança sua expressão mais plena e transformadora, vejamos:

> A quarta revolução industrial, no entanto, não diz respeito apenas a sistemas e máquinas inteligentes e conectadas. Seu escopo é muito mais amplo. Ondas de novas descobertas ocorrem simultaneamente em áreas que vão desde o sequenciamento genético até a nanotecnologia, das energias renováveis à computação quântica. O que torna a quarta revolução industrial fundamentalmente diferente das anteriores é a fusão dessas tecnologias e a interação entre os domínios físicos, digitais e biológicos. (Schwab 2016, p. 6).

No contexto da Sociedade 4.0, expressão que sintetiza os impactos sociais, econômicos e culturais da Quarta Revolução Industrial, a IoT se apresenta como a espinha dorsal de uma nova forma de organização da vida coletiva, caracterizada pela hiperconectividade, a condição na qual pessoas, objetos, sistemas e ambientes estão permanentemente conectados entre si por meio de redes digitais, gerando fluxos contínuos e massivos de dados que alimentam processos automatizados de tomada de decisão.

As aplicações da IoT na Sociedade 4.0 estão inerentes ao cotidiano. No campo da saúde, dispositivos vestíveis (*wearables*) como relógios inteligentes (*smartwatches*) e monitores de sinais vitais coletam continuamente dados biométricos

frequência cardíaca, pressão arterial, saturação de oxigênio, padrões de sono, transmitindo-os a plataformas de saúde digital que permitem o monitoramento remoto de pacientes e a detecção precoce de condições médicas.

No ambiente doméstico, assistentes virtuais como a Amazon Alexa e o Google Home transformaram as residências em ecossistemas conectados (*smart homes*), nos quais eletrodomésticos, sistemas de segurança, iluminação, climatização e entretenimento são controlados por comandos de voz e algoritmos de aprendizagem de máquina que capturam os padrões de comportamento dos usuários.

No espaço urbano, as cidades inteligentes (*smart cities*) integram sensores de tráfego, sistemas de iluminação pública adaptativa, monitoramento ambiental e gestão de resíduos em plataformas centralizadas que otimizam o uso de recursos e melhoram a qualidade dos serviços públicos (Cesar, 2023).[10]

No setor industrial, a IoT viabilizou a fábrica inteligente (*smart factory*), na qual máquinas, robôs e sistemas logísticos comunicam-se entre si de forma autônoma, antecipando necessidades de manutenção, ajustando parâmetros de produção em tempo real e integrando a cadeia de suprimentos em um fluxo contínuo de dados. No campo da mobilidade, veículos conectados coletam dados de geolocalização, padrões de direção e condições de tráfego, comunicando-se entre si e com a infraestrutura viária para otimizar o deslocamento e reduzir acidentes.

Na agricultura de precisão, sensores instalados em plantações monitoram variáveis como umidade do solo, temperatura, luminosidade e presença de pragas, permitindo a aplicação automatizada e eficiente de insumos (engenharia híbrida, 2026). Toda essa arquitetura de conectividade massiva tem como denominador comum um elemento de profunda relevância jurídica: a geração, coleta e transmissão ininterrupta de dados pessoais.

Em cada interação entre um usuário e um dispositivo IoT seja ao vestir um smartwatch, ao conversar com um assistente virtual, ao transitar por uma cidade inteligente ou ao utilizar um veículo conectado, informações de natureza pessoal são capturadas, armazenadas e processadas por agentes econômicos que, na maior parte

---

[10]CESAR. Guia completo sobre Internet das Coisas (IoT) e aplicações. 16 mar. 2023. Disponível em: https://www.cesar.org.br/w/conheca-o-iot-confira-o-guia-do-cesar-sobre-o-assunto. Acesso em: 01 de junho de 2026. Para uma análise das aplicações da IoT em cidades inteligentes, saúde e varejo, ver também: IMMES. *Internet das Coisas (IoT): aplicações, tecnologias e desafios*. Disponível em: https://immes.edu.br/wp-content/uploads/2025/04/Artigo_MATIZ_2023_IOT.pdf. Acesso em: 01 junho 2026.

das vezes, operam de forma assimétrica em relação ao titular dos dados. Essa assimetria informacional é o ponto de tensão central entre a expansão tecnológica da IoT e o direito fundamental à proteção de dados pessoais, cuja análise será aprofundada nas seções subsequentes.[11]

3 IMERSÃO NO IRREVERSÍVEL: CIBERCULTURA E INTELIGÊNCIA COLETIVA

A análise jurídica dos desafios impostos pela Internet das Coisas à proteção de dados pessoais não pode prescindir de um adequado enquadramento teórico que permita compreender as transformações estruturais operadas pelas redes digitais nas sociedades contemporâneas.

O Direito, enquanto sistema normativo que regula relações sociais, precisa compreender a natureza das relações que pretende regular. Nesse sentido, duas tradições teóricas se mostram especialmente fecundas para os propósitos deste trabalho: a Teoria da Sociedade em Rede, desenvolvida por Manuel Castells, que oferece um modelo analítico para compreender como o poder se organiza e circula nas redes de comunicação digital.

É a filosofia da cibercultura de Pierre Lévy, que ilumina as transformações culturais, cognitivas e políticas produzidas pela expansão do ciberespaço. Articuladas entre si e com o fenômeno específico da IoT, essas perspectivas permitem identificar as tensões estruturais entre conectividade, autonomia informacional e proteção de dados que o ordenamento jurídico brasileiro precisa enfrentar.[12]

Manuel Castells é um dos mais influentes sociólogos do final do século XX e início do século XXI e representa uma contribuição teórica incontornável para a compreensão das transformações estruturais provocadas pelas tecnologias da informação e comunicação nas sociedades contemporâneas. O ponto de partida da

---

[11] A questão da assimetria informacional entre titulares de dados e agentes de tratamento no contexto da IoT é tratada com profundidade por BIONI, Bruno Ricardo. *Proteção de dados pessoais: a função e os limites do consentimento*. 3. ed. Rio de Janeiro: Forense, 2021. p. 112-134.

[12] A necessidade de articulação entre teoria social e análise jurídica para a compreensão dos desafios da proteção de dados digitais é defendida por DONEDA, Danilo. Da privacidade à proteção de dados pessoais: fundamentos da Lei Geral de Proteção de Dados. 3. ed. São Paulo: Thomson Reuters Brasil, 2021. p. 1-27. Disponível em: https://www.lexml.gov.br/urn/urn:lex:br:rede.virtual.bibliotecas:livro:2021;001203055. Acesso em: 01 junho 2026.

sua análise é a tese de que as redes constituem a nova morfologia social da era da informação, substituindo as estruturas hierárquicas verticais típicas das organizações industriais do século XX por arranjos horizontais e descentralizados, nos quais os fluxos de informação, capital e poder circulam de forma simultânea e planetária. Para ele, a relevância da rede como estrutura organizacional não é nova, mas adquire uma dimensão qualitativamente distinta na era digital:

> Redes constituem a nova morfologia social de nossas sociedades e a difusão da lógica de redes modifica de forma substancial a operação e os resultados dos processos produtivos e de experiência, poder e cultura. Embora a forma de organização social em redes tenha existido em outros tempos e espaços, o novo paradigma da tecnologia da informação fornece a base material para sua expansão penetrante em toda a estrutura social. (Castells, 1999, p. 565).

Essa passagem é teoricamente fundamental porque revela que o que distingue a sociedade em rede contemporânea não é simplesmente a existência de redes de comunicação que existem desde a Antiguidade, mas o fato de que as tecnologias digitais de informação forneceram a infraestrutura material que permite que a lógica reticular penetre em todas as esferas da vida social, desde a economia global até as relações interpessoais. Em outras palavras, a rede deixou de ser um meio e tornou-se o próprio ambiente no qual a vida social se organiza.[13]

A análise de Castells sobre o poder é de especial relevância jurídica. Em sua obra posterior, Comunicação e Poder (2009), o autor desenvolve a tese de que o poder na sociedade em rede não é exercido apenas pelo controle de recursos materiais como na sociedade industrial, mas, sobretudo, pelo controle das redes de comunicação e dos fluxos de informação que as atravessam. Aqueles que detêm o poder de programar as redes definindo quais informações circulam, em que formato, para quem e com que velocidade detêm o poder mais fundamental da sociedade contemporânea (Castells, 2009, p. 77).

Essa perspectiva ilumina de forma direta a assimetria de poder que caracteriza a relação entre os grandes operadores de plataformas IoT empresas como Amazon,

[13]A análise de Castells sobre a nova morfologia social das redes é desenvolvida principalmente no Capítulo 1 — "A revolução da tecnologia da informação" — e no Capítulo 6 — "O Estado informacional" — de A Sociedade em Rede. Para uma leitura comentada, cf. UERJ/IFHT. Conceito de Sociedade em Rede. Disponível em: https://ifht.uerj.br/mod/page/view.php?id=10285&forceview=1. Acesso em: 01 junho 2026.

Google, Apple e Samsung e os titulares de dados pessoais que utilizam seus dispositivos e serviços, uma assimetria que o Direito de Proteção de Dados busca, com maior ou menor eficácia, corrigir.

Castells também destaca que a sociedade em rede não é geograficamente uniforme: ela se organiza a partir de nós (rede conectada) e centros de poder que concentram os fluxos de informação, enquanto territórios e populações inteiras são excluídos da rede ou a ela se conectam em posição de extrema dependência e vulnerabilidade.

Esse fenômeno de exclusão que Castells denomina de "espaços de fluxos" versus "espaços de lugares" tem implicações jurídicas diretas no contexto da IoT, especialmente no que diz respeito às populações mais vulneráveis, como crianças, idosos e pessoas de baixa renda, que interagem com dispositivos conectados sem o mesmo grau de consciência e proteção que usuários mais letrados digitalmente.[14] Como sublinha Castells:

> A Nova Economia Informacional/Global é uma economia [...] cujas estruturas e dinâmicas fundamentais são as redes de informação em que estão inseridas [...], e que só pode ser compreendida em seu conjunto mediante a análise de seus fluxos e nódulos. (Castells, 1999, p. 88).

Do ponto de vista metodológico, a contribuição de Castells para o presente trabalho reside, portanto, na demonstração de que a análise jurídica da proteção de dados na IoT não pode ser reduzida a uma abordagem puramente normativa centrada na interpretação de dispositivos legais, mas deve levar em conta as estruturas de poder que determinam como os dados são coletados, processados e utilizados nas redes digitais. A LGPD, nessa perspectiva, é um instrumento de regulação que tenta intervir em relações de poder profundamente assimétricas, cujos determinantes estruturais estão inscritos na própria arquitetura das redes.[15]

---

[14]A distinção entre "espaços de fluxos" e "espaços de lugares" é desenvolvida por CASTELLS (1999, p. 403-467), no Capítulo 6 de A Sociedade em Rede. Para a aplicação desse conceito ao problema da vulnerabilidade digital e da exclusão informacional, ver: BIONI, Bruno Ricardo. Proteção de dados pessoais: a função e os limites do consentimento. 3. ed. Rio de Janeiro: Forense, 2021. p. 145-160.

[15] Sobre a interseção entre teoria das redes e regulação jurídica da internet, ver: REVISTA DA AJURIS. Sociedade em rede, internet e privacidade. Porto Alegre, 2020. Disponível em: https://revistadaajuris.ajuris.org.br/index.php/REVAJURIS/article/download/249/184/347. Acesso em: 01 junho 2026.

Consoante a isso Pierre Lévy é um filósofo tunisiano-canadense, professor da Universidade de Ottawa, especializado em filosofia da informação e em análise das transformações culturais provocadas pelas tecnologias digitais. Alicerçado na obra mais “Cibercultura” em que Lévy desenvolve uma análise filosófica abrangente do ciberespaço como novo ambiente de comunicação e de produção cultural, caracterizam-se três atributos fundamentais.

Eles são: a universalidade sem totalidade, isto é, a capacidade de conectar a todos sem que exista um centro ou uma totalidade de sentido que unifique os conteúdos em circulação; a interatividade generalizada e a inteligência coletiva como forma emergente de organização cognitiva e social. A definição de Lévy para o ciberespaço, frequentemente citada na literatura acadêmica, estabelece que:

> [...] o espaço de comunicação aberto pela interconexão mundial dos computadores e das memórias dos computadores. Essa definição inclui o conjunto dos sistemas de comunicação eletrônicos (aí incluídos os conjuntos de redes hertzianas e telefônicas clássicas), na medida em que transmitem informações. Consiste de uma realidade multidirecional, artificial ou virtual incorporada a uma rede global, sustentada por computadores que funcionam como meios de geração e acesso. (Lévy, 1999, p. 92).

Essa definição, abrangente e precisa, antecipou com notável exatidão o que viria a ser a arquitetura da Internet das Coisas: uma rede global de dispositivos que geram e acessam informações de forma contínua e automática, constituindo um ciberespaço que não se limita ao computador pessoal, mas se expande para os próprios objetos do mundo físico. A virtualização que Lévy descreve como traço central do ciberespaço a capacidade de existir em potência e se manifestar concretamente em diferentes tempos e lugares é exatamente o que ocorre quando um smartwatch coleta dados biométricos do usuário e os transmite a uma plataforma de saúde digital: o dado, antes localizado no corpo físico do indivíduo, virtualiza-se ao ser capturado e circula pelo ciberespaço como informação processável.[16]

[16]O conceito de virtualização em Lévy é desenvolvido em sua obra anterior: LÉVY, Pierre. O que é o virtual? Tradução de Paulo Neves. São Paulo: Ed. 34, 1996. p. 47. A expressão "é virtual aquilo que existe apenas em potência e não em ato" é diretamente citada na resenha de Sebastião e Pesce (2010, p. 67), a partir da edição de 1999 da obra de Lévy.

O conceito de inteligência coletiva é a contribuição mais original de Lévy ao debate contemporâneo sobre tecnologia e sociedade. Para o autor, a inteligência coletiva designa:

> Uma inteligência distribuída por toda parte, incessantemente valorizada, coordenada em tempo real, que resulta em uma mobilização efetiva das competências. [...] O fundamento e o objetivo da inteligência coletiva é o reconhecimento e o enriquecimento mútuos das pessoas, e não o culto de comunidades fetichizadas ou hipostasiadas. (Lévy, 2007, p. 28-29).

Esse ideal emancipatório da inteligência coletiva é uma forma de organização cognitiva distribuída que valoriza cada indivíduo em sua singularidade enquanto o integra a um coletivo mais amplo entra em tensão direta com as dinâmicas de vigilância e extração de dados que caracterizam a economia da IoT.

Se Lévy vislumbrava no ciberespaço um instrumento de empoderamento coletivo e de reconhecimento mútuo das competências individuais, o que se observa na prática da Internet das Coisas é frequentemente o contrário: os dados gerados pelos usuários são capturados por grandes corporações tecnológicas, processados de forma opaca por algoritmos de aprendizagem de máquina e utilizados para fins que os próprios titulares desconhecem, em um modelo que Shoshana Zuboff denominou, com precisão, de "capitalismo de vigilância".[17]

A tensão que Lévy identifica na cibercultura entre a potência emancipatória do ciberespaço e o risco de que ele se converta em instrumento de "novas dominações" é de profunda relevância jurídica. Em sua obra A Inteligência Coletiva, o filósofo já advertia que o projeto de inteligência coletiva poderia ser cooptado por interesses mercadológicos e estatais, transformando-se de instrumento de emancipação em mecanismo de controle (Lévy, 2007, p. 31).

Essa advertência, formulada no final da década de 1990, antes mesmo da consolidação da Web 2.0 e do surgimento da IoT, revela a atualidade e o alcance do

[17]ZUBOFF, Shoshana. A era do capitalismo de vigilância: a luta por um futuro humano na nova fronteira do poder. Tradução de George Schlesinger. Rio de Janeiro: Intrínseca, 2021. A autora define o "capitalismo de vigilância" como a "lógica econômica que reivindica a experiência humana como matéria-prima gratuita para práticas comerciais ocultas de extração, predição e venda" (p. 14). ISBN: 9788551005194.

pensamento de Lévy como ferramenta analítica para a compreensão dos desafios contemporâneos da proteção de dados.[18]

3.1 A INTERNET DAS COISAS NA ERA DA HIPERCONECTIVIDADE: UM DIÁLOGO ENTRE A SOCIEDADE EM REDE E A CIBERCULTURA

A articulação das perspectivas teóricas de Castells e Lévy com o fenômeno específico da Internet das Coisas revela uma convergência analítica de grande relevância: em ambas as tradições, o controle sobre os fluxos de informação e, portanto, sobre os dados é identificado como o locus central do poder e da tensão social na era digital. A IoT, ao multiplicar exponencialmente os pontos de produção e coleta de dados, intensifica as dinâmicas descritas por esses autores a um grau que nenhum deles poderia antecipar plenamente ao escrever suas obras seminais nos anos 1990.

Sob a ótica de Castells, a IoT representa uma expansão radical da lógica reticular que define a sociedade em rede: se antes a rede era constituída por nós identificáveis computadores, servidores, usuários humanos, na era da IoT ela se expande para incorporar bilhões de objetos físicos que coletam, processam e transmitem dados de forma autônoma, aprofundando a penetração da lógica informacional em todas as dimensões da experiência humana.

Os dispositivos IoT são, em essência, novos nós da rede, que ampliam a capacidade de vigilância e de gestão do poder informacional por parte de quem programa e controla as plataformas a que eles se conectam. Essa ampliação dos nós da rede não é neutra do ponto de vista jurídico: ela significa que o alcance potencial da coleta de dados pessoais e, portanto, o campo de incidência das normas de

[18]LÉVY, Pierre. A inteligência coletiva: por uma antropologia do ciberespaço. Tradução de Luiz Paulo Rouanet. 5. ed. São Paulo: Loyola, 2007. p. 28-31. Para uma resenha acadêmica recente dessa obra, cf. SANTOS, Márcio Adriano Costa dos. Resenha: LÉVY, Pierre. A inteligência Coletiva. Convergências: estudos em Humanidades Digitais, v. 1, n. 7, p. 214-219, 2025. DOI: 10.59616/cehd.v1i7.1940. Disponível em: https://periodicos.ifg.edu.br/cehd/article/view/1940. Acesso em: 01 junho 2026.

proteção de dados se expande continuamente, desafiando a capacidade de resposta dos marcos regulatórios existentes.[19]

No olhar de Lévy, a IoT pode ser lida como a materialização mais concreta da virtualização que ele descrevia como traço central do ciberespaço: quando um objeto físico uma geladeira, um termostato, um marcapasso passa a gerar e transmitir dados continuamente, ele se torna parte do ciberespaço, integrando-se ao "universo oceânico de informações" que Lévy descreve como o ambiente característico da cibercultura (Lévy, 1999, p. 17).

A inteligência coletiva, nesse contexto, assume um caráter ambivalente: de um lado, os dados gerados pela IoT alimentam sistemas de inteligência artificial que otimizam serviços urbanos, melhoram diagnósticos médicos e aumentam a eficiência energética realizando, ao menos em parte, o potencial emancipatório que Lévy vislumbrava no ciberespaço; de outro, esses mesmos dados alimentam modelos de negócio baseados na extração e na monetização da informação pessoal, sem o conhecimento ou o consentimento genuíno dos titulares, contrariando o ideal de reconhecimento mútuo e de valorização do indivíduo que fundamenta o conceito de inteligência coletiva.

É precisamente nessa tensão entre o potencial emancipatório da hiperconectividade e os riscos de vigilância, controle e vulneração de direitos fundamentais que ela carrega que reside a justificativa mais profunda para a regulação jurídica da IoT. Como aponta Doneda (2021, p. 143), a proteção de dados pessoais deve ser compreendida como um direito dinâmico de controle informacional, e não como um mero direito de exclusão; e é exatamente essa dimensão dinâmica a capacidade do titular de exercer controle efetivo sobre os dados que os dispositivos IoT geram a seu respeito que os instrumentos regulatórios existentes, como a LGPD, ainda não conseguem garantir de forma satisfatória, como se demonstrará na seção seguinte.

[19] Sobre a expansão da coleta de dados pela IoT e os desafios para a regulação jurídica, ver: UNICAMP. Impactos da LGPD em aplicações da Internet das Coisas. Campinas: UNICAMP, 2021. Disponível em: https://www.ic.unicamp.br/~reltech/PFG/2021/PFG-21-28.pdf. Acesso em: 01 junho 2026.

4 INTERNET DAS COISAS, PROTEÇÃO DE DADOS E DESAFIOS JURÍDICOS: O MARCO CIVIL DA INTERNET E A LGPD NO CONTEXTO DA REGULAÇÃO DIGITAL BRASILEIRA

A regulação digital brasileira se assenta, fundamentalmente, sobre dois instrumentos normativos complementares: o Marco Civil da Internet (Lei nº 12.965, de 23 de abril de 2014) e a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709, de 14 de agosto de 2018). Embora tratem de objetos distintos o primeiro regula o uso da internet no Brasil, enquanto a segunda regula especificamente o tratamento de dados pessoais, esses diplomas formam um conjunto coerente e complementar de normas que estruturam o ambiente jurídico digital brasileiro, sendo frequentemente citados conjuntamente pela doutrina especializada como os pilares do ecossistema regulatório digital nacional (Contábeis, 2025). Como pontua a Agência Brasil:

> O Marco Civil da Internet é o principal marco normativo em relação às plataformas digitais; já a LGPD criou uma regulamentação para o uso, proteção e transferência de dados pessoais. (Agência Brasil, 2023).

Em seu artigo 3º, o Marco Civil estabelece os princípios fundamentais que regem o uso da internet no Brasil, dentre os quais se destacam: a garantia da liberdade de expressão; a proteção da privacidade; a proteção dos dados pessoais; a preservação e garantia da neutralidade da rede; a preservação da estabilidade, segurança e funcionalidade da rede; e a responsabilização dos agentes de acordo com suas atividades (Brasil, 2014, art. 3º).

Em seu artigo 7º, a lei estabelece dez hipóteses que legitimam o tratamento de dados pessoais, denominadas "bases legais", sendo o consentimento do titular a primeira e mais emblemática delas. O artigo 11, por sua vez, disciplina o tratamento de dados pessoais sensíveis, estabelecendo que essa categoria de dados somente pode ser tratada mediante consentimento específico e destacado do titular, ou nas hipóteses excepcionais ali elencadas, como o cumprimento de obrigação legal, a tutela da saúde e a garantia da prevenção à fraude (ANPD, [s.d.]).[20] A criação da

[20]ANPD. Quais são as bases legais para o tratamento de dados pessoais? Disponível em: https://www.gov.br/anpd/pt-br/acesso-a-informacao/perguntas-frequentes/perguntas-frequentes/2-dados-pessoais/2-6-quais-sao-as. Acesso em: 20 maio 2026. Ver também: LGPD-BRASIL.INFO. Artigo

Autoridade Nacional de Proteção de Dados (ANPD), prevista pela própria LGPD e consolidada pelo Decreto nº 10.474/2020, como órgão da administração pública federal com atribuições de fiscalizar, normatizar e aplicar sanções em matéria de proteção de dados, representou um passo fundamental para a efetividade do sistema regulatório, embora a autoridade ainda enfrenta limitações orçamentárias e operacionais significativas.[21]

4.1 DADOS PESSOAIS, DADOS SENSÍVEIS E VULNERABILIDADES NA INTERNET DAS COISAS

A distinção entre dados pessoais e dados pessoais sensíveis é um dos eixos estruturantes da LGPD e de especial relevância para a análise dos riscos impostos pela Internet das Coisas. O artigo 5º, inciso I, da LGPD define dado pessoal como "informação relacionada a pessoa natural identificada ou identificável" (Brasil, 2018, art. 5º, I), enquanto o inciso II conceitua dado pessoal sensível como aquele referente à "origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural" (Brasil, 2018, art. 5º, II).

A distinção é juridicamente relevante porque os dados sensíveis recebem regime de proteção mais rigoroso exigindo consentimento específico e destacado ou hipótese legal expressa, em razão de seu potencial de causar discriminação, estigmatização ou violação da dignidade humana quando tratados de forma indevida.

No contexto da Internet das Coisas, essa distinção adquire uma dimensão de criticidade sem precedentes, porque os dispositivos IoT são, por sua natureza técnica, instrumentos de coleta simultânea e contínua de múltiplas categorias de dados incluindo dados sensíveis, muitas vezes sem que o usuário tenha plena consciência

---

11-Tratamento de dados pessoais sensíveis. Disponível em: https://lgpd-brasil.info/capitulo_02/artigo_11.Acesso em: 01 junho 2026.

[21]A ANPD foi criada pela MP nº 869/2018, posteriormente convertida na Lei nº 13.853/2019, e consolidada como órgão da administração pública federal direta pelo Decreto nº 10.474/2020. Para uma análise do amadurecimento institucional da ANPD, ver: MAYER BROWN. Um olhar retrospectivo sobre a ANPD e a proteção de dados no Brasil — 2024. Jan. 2025. Disponível em: https://www.mayerbrown.com/pt/insights/publications/2025/01/um-olhar-retrospectivo-sobre-a-anpd-e-a-protecao-de-dados-no-brasil-. acesso em: 01 junho 2026.

da amplitude e da profundidade dessa coleta. A análise de alguns dispositivos paradigmáticos ilustra com precisão a magnitude do problema jurídico, dentre eles, podemos destacar cinco:

a) **Smartwatches e dispositivos vestíveis (*wearables*):** Os relógios inteligentes e pulseiras fitness, como Apple Watch, Samsung Galaxy Watch e Fitbit, coletam de forma contínua e automatizada dados de natureza tipicamente sensível, na definição do artigo 5º, II, da LGPD: frequência cardíaca, pressão arterial, saturação de oxigênio no sangue (SpO2), eletrocardiograma, temperatura corporal, padrões de sono, nível de atividade física e, em modelos mais avançados, dados de glicemia e fertilidade. A legislação classifica os dados relativos à saúde como dados pessoais sensíveis justamente em razão de seu elevado potencial de causar danos ao titular quando utilizados de forma indevida como a discriminação por seguradoras de saúde ou empregadores (Migalhas, 2026).[22] O problema jurídico central, nesse contexto, reside na dificuldade de obter o consentimento específico e destacado exigido pelo artigo 11 da LGPD para cada categoria de dado de saúde coletada, uma vez que o modelo de negócio desses dispositivos se baseia na coleta holística e integrada de todos os dados biométricos disponíveis, sem que o usuário possa facilmente dissociar as finalidades de cada coleta ou exercer seu direito de rejeição seletiva.[23]

b) **Assistentes virtuais (*Amazon Alexa, Google Home*):** Os dispositivos de assistência virtual por voz representam uma das manifestações mais invasivas da IoT do ponto de vista da proteção de dados. Permanentemente em modo de escuta (*always-on listening*), esses dispositivos coletam padrões de voz, hábitos de consumo, rotinas domésticas e preferências

[22]MIGALHAS. Privacidade, LGPD e saúde digital: os desafios na medicina conectada. 24 mar. 2026.Disponível em:https://www.migalhas.com.br/depeso/451923/privacidade-lgpd-e-saude-digital-os-desafios-na-medicina-conectada. Acesso em: 01 junho 2026.

[23]CAFECOMBYTES. LGPD e IoT: como proteger dados em casas inteligentes e dispositivos wearables. 3 maio de 2026. Disponível em: https://cafecombytes.com.br/2026/05/04/lgpd-e-iot-como-proteger-dados-em-casas-inteligentes-e-dispositivos-wearables/. Acesso em: 01 junho 2026.

pessoais dos usuários, gerando perfis comportamentais de alta granularidade que são transmitidos e processados nos servidores das empresas fabricantes. Do ponto de vista jurídico, a coleta contínua de dados de voz configura, em potencial, a captura de dados biométricos classificados como sensíveis pelo artigo 5º, II, da LGPD, bem como dados que revelam opiniões políticas, convicções religiosas e outros atributos sensíveis do titular, a depender do conteúdo das conversações captadas. A ausência de uma interface de consentimento granular nesses dispositivos que permitisse ao usuário definir, com precisão, quais categorias de dados podem ser coletadas e para quais finalidades representa uma violação estrutural dos princípios da transparência e da finalidade estabelecidos pelo artigo 6º da LGPD.

c) **Casas inteligentes (*smart homes*):** A automação residencial por meio de dispositivos IoT câmeras de segurança, sistemas de controle de acesso, termostatos inteligentes, fechaduras digitais, eletrodomésticos conectados transforma o ambiente doméstico em um espaço de coleta sistemática de dados sobre o comportamento cotidiano de seus moradores: horários de entrada e saída, padrões de consumo energético, rotinas alimentares, presença de visitantes e até padrões de movimentação dentro da própria residência. O domicílio, que a tradição jurídica brasileiro-constitucional protege como "asilo inviolável do indivíduo" (Constituição Federal, art. 5º, XI), converte-se, com a adoção de dispositivos IoT, em um ambiente de vigilância permanente, cujos dados são coletados por empresas privadas e armazenados em servidores frequentemente localizados fora do Brasil.

d) **Geolocalização:** Os dados de geolocalização gerados por dispositivos móveis, veículos conectados e dispositivos vestíveis constituem uma das categorias de dados mais sensíveis do ecossistema IoT, pois permitem rastrear com precisão os deslocamentos físicos do titular ao longo do tempo, revelando padrões de comportamento altamente reveladores: local de trabalho, frequência de estabelecimentos religiosos ou políticos, consultas médicas, visitas a advogados ou delegacias. Embora os dados

de geolocalização não sejam explicitamente listados como dados sensíveis pelo artigo 5º, II, da LGPD, a doutrina majoritária, com base nos princípios da finalidade e da não discriminação, defende que eles devem receber proteção equivalente quando tratados de forma combinada um fenômeno que a literatura especializada denomina de "inferência de sensibilidade", pelo qual dados aparentemente não sensíveis tornam-se sensíveis quando agregados e analisados em conjunto.[24]

e) **Dados biométricos e de saúde:** Os dados biométricos impressões digitais, reconhecimento facial, íris, geometria da palma da mão, padrões de voz são expressamente classificados como dados sensíveis pela LGPD e estão na fronteira mais crítica das vulnerabilidades da IoT, porque, ao contrário de senhas ou documentos de identidade, não podem ser alterados em caso de vazamento: uma vez comprometidos, os dados biométricos permanecem comprometidos permanentemente. A ANPD reconheceu essa criticidade ao incluir o reconhecimento facial e o tratamento de dados biométricos entre os temas prioritários de sua agenda regulatória para 2024-2025 (ANPD, 2023).

4.2 “QUEM CONTROLA OS MEUS DADOS?” A PERGUNTA QUE TODO USUÁRIO/TITULAR NÃO DEVERIA PRECISAR SE FAZER

Embora a LGPD represente um avanço significativo na proteção de dados no Brasil, ela ainda enfrenta dificuldades para se adaptar às novas demandas da IoT, que inclui a coleta contínua de dados e a necessidade de garantir a segurança da informação em ambientes de dispositivos restritos. Essas dificuldades se manifestam em pelo menos seis dimensões analíticas distintas, que serão examinadas a seguir.

O consentimento do titular, consagrado como a primeira das bases legais para o tratamento de dados pessoais pelo artigo 7º, inciso I, da LGPD, é definido pelo artigo 5º, inciso XII, como "manifestação livre, informada e inequívoca pela qual o titular

[24]O conceito de "inferência de sensibilidade" é discutido em: UNICAMP. Impactos da LGPD em aplicações da Internet das Coisas. Campinas: UNICAMP, 2021. p. 18-24. Disponível em: https://www.ic.unicamp.br/~reltech/PFG/2021/PFG-21-28.pdf. Acesso em: 01 junho 2026.

concorda com o tratamento de seus dados pessoais para uma finalidade determinada", é o fundamento axiológico central do modelo de proteção de dados instituído pela lei. Esse modelo pressupõe um sujeito consciente, informado e capaz de exercer uma escolha genuína sobre o tratamento de suas informações pessoais. O problema é que esse pressuposto é estruturalmente incompatível com a arquitetura técnica da Internet das Coisas.

Bruno Bioni, ao analisar o que denomina "paradoxo do consentimento", identifica a contradição fundamental que acomete o modelo baseado na autonomia da vontade informada em ambientes de coleta massiva e automatizada de dados:

> O consentimento, apesar de ocupar o protagonismo no cenário de proteção de dados pessoais, não é suficiente, por si só, para garantir a efetiva proteção dos indivíduos em um ambiente em que a coleta e o tratamento de dados ocorrem de maneira massiva, automatizada e, muitas vezes, imperceptível para o próprio titular." (Bioni, 2021, p. 89).

Na prática da IoT, o consentimento opera como uma ficção jurídica, formalmente presente no momento da configuração inicial do dispositivo, mas substancialmente ausente na realidade cotidiana da coleta automatizada de dados, então resta claro que a LGPD não oferece respostas específicas para essa realidade, pois foi elaborada a partir de um modelo de interação usuário-plataforma que pressupõe interfaces digitais explícitas e momentos identificáveis de coleta de dados, premissa que não se aplica à arquitetura difusa e contínua da IoT.

Neste viés, o princípio da transparência, estabelecido pelo artigo 6º, inciso VI, da LGPD, pressupõe a existência de um canal de comunicação efetivo entre o agente de tratamento e o titular, por meio do qual informações relevantes sobre a coleta e o processamento de dados possam ser transmitidas de forma inteligível. No contexto da IoT, esse pressuposto enfrenta um obstáculo técnico fundamental: grande parte dos dispositivos conectados sensores industriais, dispositivos médicos, equipamentos de automação urbana, etiquetas RFID não possui interface de usuário (*user interface*), o que torna materialmente impossível a apresentação de informações sobre o tratamento de dados no momento de sua coleta.

Essa limitação técnica compromete não apenas o cumprimento do princípio da transparência, mas também o exercício efetivo dos direitos do titular previstos no artigo 18 da LGPD: o direito de confirmação da existência de tratamento; o direito de

acesso aos dados; o direito de correção; o direito de anonimização, bloqueio ou eliminação; o direito de portabilidade; e o direito de revogação do consentimento. Em ambientes de IoT caracterizados pela multiplicidade de dispositivos, pela interoperabilidade entre plataformas e pela ausência de interfaces de usuário, o exercício desses direitos é, na prática, extremamente difícil, senão impossível para o usuário médio, desprovido de conhecimento técnico especializado.

O artigo 6º, inciso VII, da LGPD estabelece o princípio da segurança, determinando a utilização de "medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão" (Brasil, 2018, art. 6º, VII). O artigo 46 reforça essa obrigação. O problema é que os dispositivos IoT, por suas características técnicas intrínsecas, apresentam restrições que dificultam a implementação dos padrões de segurança exigidos pela lei. Vejamos que:

> Para atender a estas questões é necessário transpor barreiras como a garantia da privacidade dos dados, as restrições de capacidade de processamento, memória e consumo de energia de dispositivos restritos, os desafios normativos e regulatórios. (Unifor/Revista Tec, 2024).

A LGPD, em seu artigo 48, estabelece a obrigação de comunicação à ANPD em caso de incidente de segurança que possa acarretar risco ou dano relevante aos titulares. Contudo, a lei não prevê requisitos técnicos mínimos de segurança específicos para dispositivos IoT lacuna que países como o Reino Unido já começaram a surgir com o *Product Security and Telecommunications Infrastructure Act* de 2022, que proíbe senhas universais padrão e impõe obrigações de suporte de segurança aos fabricantes.[25]

O artigo 42 da LGPD determina que "o controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo" (Brasil, 2018, art. 42).

No contexto da IoT, a responsabilidade civil apresenta desafios adicionais de grande complexidade. O primeiro é a dificuldade de identificação do controlador: em

[25] REINO UNIDO. Product Security and Telecommunications Infrastructure Act 2022. Disponível em: https://www.legislation.gov.uk/ukpga/2022/46/contents/enacted. Acesso em: 20 maio 2026.

um ecossistema IoT típico, os dados de um usuário podem ser coletados pelo fabricante do dispositivo, transmitidos por um operador de telecomunicações, processados por uma plataforma de nuvem e compartilhados com parceiros comerciais, criando uma cadeia de agentes de tratamento de difícil identificação para o titular lesado.

O segundo desafio é a comprovação do dano: a jurisprudência brasileira ainda não consolidou entendimento uniforme sobre a configuração do dano moral em hipóteses de vazamento ou tratamento irregular de dados pessoais, oscilando entre posições que exigem comprovação de dano efetivo e concreto, e posições que reconhecem o dano *in re ipsa* isto é, presumido pela própria violação do direito fundamental à proteção de dados, independentemente de comprovação de prejuízo material.

Em 2025, a ANPD instaurou 81 processos de fiscalização e respondeu a 12.701 requerimentos de titulares, conforme seu 1º Relatório Integrado de Gestão, publicado em 5 de maio de 2026. A Medida Provisória nº 1.317/2025, convertida na Lei nº 15.352, transformou a ANPD em agência reguladora, ampliando sua autonomia de gestão, criando a carreira de Regulação e Fiscalização de Proteção de Dados e atribuindo competências de proteção digital de crianças e adolescentes pelo Decreto nº 12.622/2025 avanços institucionais expressivos.

Contudo, a principal limitação operacional da ANPD diante da IoT permanece, que é a ausência de regulamentação específica para o ecossistema de dispositivos conectados. O processo normativo avança em ritmo diferente da velocidade de expansão da IoT no Brasil, deixando o ecossistema submetido apenas às normas gerais da LGPD, que como se demonstrou ao longo desta seção foram concebidas para um modelo de coleta de dados centrado em interfaces digitais explícitas, e não na arquitetura difusa e automatizada da hiperconectividade.

5 CONSIDERAÇÕES FINAIS

Ao olharmos para a jornada que traçamos da comunicação analógica até o mundo atual, fica claro que a Internet das Coisas (IoT) deixou de ser apenas uma inovação tecnológica para se tornar o próprio ambiente em que se vive e respira.

Agora, a relação do humano com a tecnologia tornou-se profundamente íntima: abrimos as portas das nossas casas para assistentes virtuais que nos ouvem, colocamos em nossos pulsos relógios que monitoram nossos batimentos cardíacos e andamos por cidades que rastreiam nossos passos.

Evidentemente, a hiperconectividade traz consigo uma promessa maravilhosa de "inteligência coletiva", capaz de melhorar a saúde, otimizar recursos e conectar a humanidade de formas antes inimagináveis, mas essa mesma conexão esconde uma realidade preocupante, presente em nossos hábitos mais corriqueiros e nossos dados mais sensíveis estão sendo continuamente sugados de forma silenciosa, afinal, no mundo invisível e automático da Internet das Coisas, o "consentimento" acabou se tornando uma ilusão, uma verdadeira ficção jurídica, pois é humanamente impossível ler milhares de páginas de termos de uso ou sequer perceber tudo o que está sendo coletado ao nosso redor.

Este estudo não é um convite ao medo ou à rejeição da tecnologia, mas um chamado urgente para o respeito à privacidade desde a fabricação dos aparelhos (o chamado *privacy by design*). Acima de tudo, o futuro da privacidade humana depende de um amadurecimento e aprimoramento dos conhecimentos sobre o ciberespaço, para garantir que a tecnologia seja, de fato, uma ferramenta de evolução e liberdade para a humanidade, e não uma prisão invisível construída com os próprios dados dos titulares.

REFERÊNCIAS

A8 SERGIPE. **O silencioso e crescente mercado de IoT**. *A8 Sergipe*, Aracaju, 1 dez. 2025. Disponível em: https://a8se.com/blogs/economia-e-inovacao/o-silencioso-e-crescente-mercado-de-iot/. Acesso em: 01 junho 2026.

AGÊNCIA BRASIL. **Marco Civil da Internet e LGPD**: leis que regulamentam o Brasil digital. *Rádio Agência Nacional*, Brasília, 28 mar. 2023. Disponível em: https://agenciabrasil.ebc.com.br/radioagencia-nacional/geral/audio/2023-03/marco-civil-da-internet-e-lgpd-leis-que-regulamentam-. Acesso em: 01 junho 2026.

ANPD. **Quais são as bases legais para o tratamento de dados pessoais?** gov.br, Brasília, [s.d.]. Disponível em: https://www.gov.br/anpd/pt-br/acesso-a-

informacao/perguntas-frequentes/perguntas-frequentes/2-dados-pessoais/2-6-quais-sao-as. Acesso em: 01 junho 2026.

ANPD. **Resolução CD/ANPD nº 10, de 27 de dezembro de 2023**. Aprova o Regulamento de Comunicação de Incidente de Segurança com Dados Pessoais. *Diário Oficial da União*, Brasília, dez. 2023. Disponível em: https://dspace.mj.gov.br/bitstream/1/11995/1/RES_ANPD_2023_10.pdf. Acesso em: 01 junho 2026.

ASHTON, Kevin. **Como Kevin Ashton batizou a Internet das Coisas**. [Entrevista]. *AVAST Blog*, 26 set. 2019. Disponível em: https://blog.avast.com/pt-br/kevin-ashton-named-the-internet-of-things. Acesso em: 01 junho 2026.

BIONI, Bruno Ricardo. **Proteção de dados pessoais:** a função e os limites do consentimento. 3. ed. rev. Rio de Janeiro: Forense, 2021. ISBN: 9788530994082.

BRASIL. **Constituição da República Federativa do Brasil de 1988**. Brasília: Senado Federal, 1988. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 01 junho 2026.

BRASIL. **Lei nº 12.965, de 23 de abril de 2014**. Marco Civil da Internet. *Diário Oficial da União*, Brasília, 24 abr. 2014. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 01 junho 2026.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais — LGPD. *Diário Oficial da União*, Brasília, 15 ago. 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 01 junho 2026.

BRAZIL TOWER COMPANY. Até 2025, o mundo terá cerca de 27 bilhões de dispositivos IoT conectados. Brazil Tower Company, 18 maio 2025. Disponível em: https://braziltowercompany.com.br/ate-2025-mundo-tera-cerca-de-27-bilhoes-de-dispositivos-iot-conectados/. Acesso em: 01 junho 2026.

CASTELLS, Manuel. **A sociedade em rede**. Tradução de Roneide Venâncio Majer. 6. ed. São Paulo: Paz e Terra, 1999. (A era da informação: economia, sociedade e cultura, v. 1). ISBN: 9788521903291.

CASTELLS, Manuel. **Comunicação e poder**. Tradução de Vera Lúcia Mello Joscelyne. São Paulo: Paz e Terra, 2009. ISBN: 9788577530601.

CESAR. **Guia completo sobre Internet das Coisas (IoT) e aplicações**. CESAR, Recife, 16 mar. 2023. Disponível em: https://www.cesar.org.br/w/conheca-o-iot-confira-o-guia-do-cesar-sobre-o-assunto. Acesso em: 01 junho 2026.

CHAVES. **Você conhece a história da Internet das Coisas (IoT)?** *Engenharia Híbrida*, 12 agosto. 2022. Disponível em: https://www.engenhariahibrida.com.br/post/historia-internet-das-coisas-iot. Acesso em: 01 junho 2026.

CONTABEIS. **Marco Civil da Internet e LGPD:** como se complementam? *Contabeis*, 24 fev. 2025. Disponível em: https://www.contabeis.com.br/artigos/69555/marco-civil-da-internet-e-lgpd-como-se-complementam/. Acesso em: 01 junho 2026.

DIO. **História da Internet das Coisas**. *DIO*, 28 maio 2023. Disponível em: https://www.dio.me/articles/historia-da-internet-das-coisas. Acesso em: 01 junho 2026.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais:** fundamentos da Lei Geral de Proteção de Dados. 3. ed. São Paulo: Thomson Reuters Brasil, 2021. ISBN: 9786559917969.

LÉVY, Pierre. **A inteligência coletiva:** por uma antropologia do ciberespaço. Tradução de Luiz Paulo Rouanet. 5. ed. São Paulo: Loyola, 2007.

LÉVY, Pierre. **Cibercultura**. Tradução de Carlos Irineu da Costa. São Paulo: Ed. 34, 1999. (Coleção TRANS).

McDONALD, Aleecia M.; CRANOR, Lorrie Faith. The cost of reading privacy policies. ***I/S****:* A Journal of Law and Policy for the Information Society, v. 4, n. 3, p. 543-568, 2008.

MIGALHAS. **Privacidade, LGPD e saúde digital**: os desafios na medicina conectada. *Migalhas*, 24 mar. 2026. Disponível em: https://www.migalhas.com.br/depeso/451923/privacidade-lgpd-e-saude-digital-os-desafios-na-medicina-conectada. Acesso em: 01 junho 2026.

REPOSITÓRIO ENAP. **Histórico e conceitos relacionados à IoT**. Disponível em: https://repositorio.enap.gov.br/jspui/bitstream/1/7690/1/Módulo 1 - Histórico e conceitos relacionados à IoT.pdf. Acesso em: 01 junho 2026.

REVISTA TEC/UNIFOR. Desafios regulatórios da LGPD para a IoT. v. 14, n. 2, 2024. Disponível em: https://ojs.unifor.br/tec/article/view/13998. Acesso em: 01 junho 2026.

RNP - Rede Nacional de Pesquisa. **Evolução da internet no Brasil**. 9 jun. 2022. Disponível em: https://www.rnp.br/comunidades/evoluo-da-internet-no-brasil/. Acesso em: 01 junho 2026.

SCHWAB, Klaus. **A quarta revolução industrial**. Tradução de Daniel Moreira Miranda. São Paulo: Edipro, 2016.

WELIVESECURITY. **ARPANET**: o nascimento da internet moderna. *WeLiveSecurity*, 29 out. 2023. Disponível em: https://www.welivesecurity.com/pt/we-live-progress/arpanet-o-nascimento-da-internet-moderna/. Acesso em: 01 junho 2026.

WIKI COMPUTAÇÃO/UFPR. **Internet das Coisas**. Curitiba: Universidade Federal do Paraná, 2022. Disponível em: https://wiki.inf.ufpr.br/computacao/doku.php?id=i%3Ainternet_das_coisas. Acesso em: 01 junho 2026.