



UNIVERSIDADE FEDERAL DE MATO GROSSO DO SUL - CAMPUS
COXIM FACULDADE DE DIREITO

Yuri Apollo da Silva Vasconcelos

DIREITO À PRIVACIDADE: IMPACTOS DA IóE, NA SEGURANÇA DOMÉSTICA

COXIM-MS
2025



UNIVERSIDADE FEDERAL DE MATO GROSSO DO SUL - CAMPUS
COXIM FACULDADE DE DIREITO

Yuri Apollo da Silva Vasconcelos

DIREITO À PRIVACIDADE: IMPACTOS DA IóE, NA SEGURANÇA DOMÉSTICA

Trabalho de Conclusão de Curso apresentado ao Curso de
Direito da Universidade Federal de Mato Grosso do Sul
(CPCX), como requisito parcial para a obtenção do grau de
Bacharel em Direito, sob a orientação da Professor Doutor
Guilherme Sampieri Santinho

COXIM-MS
2025

DIREITO À PRIVACIDADE: IMPACTOS DA IoE, NA SEGURANÇA DOMÉSTICA

Yuri Apollo da Silva Vasconcelos¹

Guilherme Sampieri Santinho²

SUMÁRIO. 1. INTRODUÇÃO. 2. EVOLUÇÃO DA IOE. 3. EVOLUÇÃO DO DIREITO À PRIVACIDADE NO ÂMBITO CONSTITUCIONAL, INFRACONSTITUCIONAL E INTERNACIONAL. 4. ANÁLISE DO ARCABOUÇO JURÍDICO BRASILEIRO EM RELAÇÃO À PROTEÇÃO DA PRIVACIDADE. 5. CONSIDERAÇÕES FINAIS

RESUMO: A Internet of Everything (IoE) representa uma evolução da Internet das Coisas (IoT), conceito introduzido em 2011 pela companhia estadunidense Cisco Systems, traz a ideia de uma transmissão de tudo para tudo; o que antes se limitava à conexão entre dispositivos por meio de sensores, no modelo conhecido como “Machine to Machine” (M2M), caracterizado pela transmissão de dados entre máquinas sem necessariamente utilizar protocolos IP, evoluiu para um ecossistema de conexões inteligentes. Diante desse cenário, esta pesquisa tem como objetivo investigar de que maneira o uso de dispositivos IoE voltados para a segurança doméstica impacta o direito à privacidade, analisando a evolução da IoE, a construção histórica da proteção da privacidade e a adequação do arcabouço jurídico brasileiro vigente, tanto na Constituição como em leis infraconstitucionais, especialmente a LGPD. Essa investigação foi conduzida por meio de revisão bibliográfica e documental, considerando doutrinas, artigos científicos e jurisprudências, verificando se legislação atual é suficiente para garantir uma proteção adequada perante a IoE. O estudo oferece subsídios para compreender as insuficiências do arcabouço jurídico brasileiro relativas à tutela da privacidade diante dos desafios impostos pela IoE e busca demonstrar diretrizes e medidas jurídicas que possam ser implementadas para mitigar os impactos negativos dessa tecnologia sobre os direitos fundamentais dos indivíduos.

Palavras-chaves: internet das coisas; inteligência artificial; arcabouço jurídico; privacidade.

ABSTRACT: *The Internet of Everything (IoE) represents an evolution of the Internet of Things (IoT), a concept introduced in 2011 by the American company Cisco Systems. It brings the idea of everything-to-everything transmission. What was previously limited to connections between devices via sensors, in the model known as "Machine-to-Machine" (M2M), characterized by the transmission of data between machines without necessarily using IP protocols, has evolved into an ecosystem of smart connections. Given this scenario, this research aims to investigate how the use of IoE devices for home security impacts the right to privacy, analyzing the evolution of the IoE, the historical construction of privacy protection, and the adequacy of the current Brazilian legal framework, both in the Constitution and in infra-constitutional laws, especially the LGPD. This investigation was conducted through a bibliographic and documentary review, considering doctrines, scientific articles, and case law, verifying whether current legislation is sufficient to guarantee adequate protection against the IoE. The study provides insights into the shortcomings of the Brazilian legal framework regarding privacy protection in light of the challenges posed by the IoT and seeks to demonstrate legal guidelines and measures that can be implemented to mitigate the negative impacts of this technology on individuals' fundamental rights.*

¹ Discente do curso de Direito, na Universidade Federal de Mato Grosso do Sul – câmpus coxim, E-mail: yuri.apollo@hotmail.com

² Professor Doutor em Direito do Trabalho, docente na Universidade Federal de Mato Grosso do Sul – câmpus coxim, E-mail: guilherme.santinho@ufms.br

Keywords: *Internet of Things; artificial intelligence; legal framework; privacy.*

INTRODUÇÃO

Na perspectiva do Direito Digital, ramo da ciência jurídica que vem sendo bastante discutido, haja vista suas ramificações atingirem inúmeras relações, cresce a importância de verificar se as legislações pertinentes a esse ramo, estão sendo capazes de garantir uma proteção adequada quando o assunto envolve a privacidade em consonância com as tecnologias que utilizam inteligência artificial em ambientes domésticos.

Atualmente, com o avanço da internet das coisas (IoT, do inglês *Internet of Things*), há uma mudança de perspectiva, a começar pela terminologia. A *Internet of Everything* (IoE) representa uma evolução da IoT; esse conceito foi introduzido por volta de 2011, pela companhia estadunidense Cisco Systems³, sediada na Califórnia.

Esse conceito traz a ideia de uma hiperconexão de tudo para tudo, ou seja, o que na visão da IoT se referia à conexão de dispositivos físicos e aplicativos, agora com a IoE, se refere a dispositivos conectados em um sistema amplo e inteligente, uma espécie de conexão de pessoas, processos, dados e coisas em uma mesma rede.

Essa hiperconexão complexa permite a coleta e o cruzamento de informações de diferentes esferas da vida dos indivíduos, criando uma espécie de perfil comportamental mais detalhado. Dessa forma, não apenas aumenta o volume de dados tratados, mas também sua sensibilidade, na medida em que inclui informações pessoais em diversos contextos.

Desse modo surgem incertezas quanto ao alcance dessas conexões na vida privada das pessoas, muitas das quais sequer percebem os riscos a que estão expostas. Todavia, não é generalizar ou rejeitar a utilização dessa tecnologia, mas compreender seus impactos jurídicos, no tocante à proteção da privacidade e à responsabilização legal por eventuais ilícitos praticados por meio desses equipamentos.

Essa perspectiva demonstra a relevância deste trabalho em compreender os impactos sociais nas operações realizadas por esses dispositivos, ao passo que possuem gerenciamento próprio. Essa dinâmica gera preocupações, especialmente em saber se há adequação do

³ A Cisco define a IoE (Internet of Everything, Internet de Todas as Coisas) como a conexão em rede de pessoas, processos, dados e coisas. A vantagem da IoE vem do impacto composto da conexão de pessoas, processos, dados e coisas, além do valor que essa conexão cada vez maior agrega à medida que “todas as coisas” ficam on-line. Disponível em: https://www.cisco.com/c/dam/m/pt_br/ioe/public_sector/pdfs/Public_sector_jurisdiction_faq_final.pdf Acesso em 11 fev. 2025

arcabouço jurídico brasileiro na proteção e regulamentação dessas tecnologias, no que diz respeito ao direito à privacidade em ambientes hiperconectados.

Ocorre que, em ambientes como esse, muitos dispositivos IoE são desenvolvidos com medidas de segurança incongruentes ou até mesmo são usados por terceiros para a prática de golpes e ataques cibernéticos.

A referida medida de segurança é incongruente, pois falta nesses dispositivos uma camada de criptografia mais robusta e meios eficazes de autenticação, para impedir que invasores acessem redes domésticas, comprometendo dados pessoais e colocando em risco a privacidade e segurança dos moradores. Em alguns casos, as câmeras armazenam dados em nuvem sem mecanismos de segurança adequados, o que permite o acesso remoto não autorizado. Isso acontece porque os fabricantes negligenciam essas medidas devido à redução de custo ou à facilidade de uso.

Além disso, esses dispositivos coletam frequentemente dados pessoais dos usuários sem consentimento ou transparência. O que levanta preocupações sobre o uso indevido das informações, especialmente quando compartilhadas com terceiros, sem o conhecimento dos proprietários. Quem deverá ser responsabilizado? Seria a fornecedora que desenvolve esses equipamentos ou o lojista que revende, ou nenhum dos dois, e para isso deve seguir um procedimento para investigar de fato quem foi o indivíduo responsável por corromper esse equipamento.

De fato, o uso cada vez mais difundido dessas tecnologias apresenta riscos significativos à segurança dos dados pessoais dos usuários. A facilidade do manuseio e o caráter - aparentemente inofensivo - presente nesses dispositivos ocultam fragilidades técnicas que podem ser exploradas por agentes mal-intencionados para acessar informações privadas de forma indevida. Tais vulnerabilidades evidenciam a necessidade de uma proteção jurídica específica, pois colocam em xeque o direito fundamental à privacidade e à segurança em ambientes domésticos hiperconectados.

Na atual conjuntura, observa-se um grande esforço por parte do judiciário em suprir a lacuna legislativa existente. Buscando, sempre que possível, aplicar a norma vigente e os princípios do Direito como instrumentos capazes de atingir e responsabilizar os agentes que direta e indiretamente são responsáveis pela fabricação, desenvolvimento ou gerenciamento de dispositivos IoE.

Esses princípios incluem: a dignidade da pessoa humana; a legalidade; a inafastabilidade da jurisdição; a proporcionalidade e razoabilidade. A aplicação desses princípios, extraídos da Constituição Federal e da doutrina, serve de base para orientar o intérprete do direito e

preencher as lacunas normativas diante de situações em que a legislação específica ainda não alcança os desafios tecnológicos contemporâneos.

No entanto, tais inseguranças ressaltam a necessidade de equilíbrio entre evolução tecnológica e implementação de medidas robustas de segurança e privacidade, garantindo que os benefícios da IoE sejam aproveitados sem comprometer os direitos fundamentais dos usuários.

Diante dessa perspectiva, questionamos como o direito à privacidade está sendo impactado pelo uso de dispositivos IoE, voltados para a segurança doméstica? Para isso precisamos investigar a evolução e como o uso de dispositivos IoE pode interferir no direito fundamental à privacidade previsto no ordenamento jurídico brasileiro, tanto em nossa constituição quanto em leis infraconstitucionais.

Esse fim será alcançado analisando como foi a evolução da IoE, fazendo uma comparação da evolução do direito à privacidade em um contexto constitucional, infraconstitucional e internacional. A fim de verificar se o arcabouço jurídico brasileiro é capaz de responsabilizar e/ou garantir a segurança em aplicações que utilizam a IoE.

Ao final, vamos entender que a interferência na utilização de inteligência artificial em dispositivos IoE, em ambientes domésticos, amplia significativamente os riscos à privacidade, ao passo que permite a coleta automatizada e contínua de dados sensíveis, muitas vezes sem o consentimento explícito dos titulares. Dessa forma, a ausência de regulamentações específicas voltadas para a fabricação e comercialização de dispositivos IoE, compromete a responsabilização objetiva dos agentes envolvidos em eventuais violações ao direito à privacidade. Contudo, serão propostas algumas diretrizes e medidas jurídicas na intenção de mitigar os riscos diante dessa ausência legislativa.

Portanto, a metodologia empregada no estudo utilizará uma pesquisa teórica descritiva, buscando em fontes secundárias as informações para melhor compreender o objeto cognoscível, a partir de uma abordagem qualitativa, fundamentada em revisão bibliográfica, buscando contribuir para a evolução desse fenômeno.

A pesquisa será conduzida por meio da análise de livros, artigos científicos, doutrina especializada e jurisprudência nacional, podendo, inclusive, incorporar noções do direito comparado, com ênfase nas experiências europeias. As obras e artigos foram selecionados em virtude de sua relevância acadêmica e contemporânea.

O desenvolvimento do trabalho terá como base bibliográfica a biblioteca "Pergamum", da Universidade Federal de Mato Grosso do Sul (UFMS), além de plataformas como o Google Acadêmico e o portal de periódicos, com o objetivo de aprofundar a análise teórica por meio

de fontes qualificadas e atualizadas.

1. EVOLUÇÃO DA IoE

A internet é um veículo crucial utilizado na conexão global de transferências de dados, seu nascimento aconteceu em um momento de instabilidade mundial, pairava a guerra fria em 1957. Os Estados Unidos da América (EUA) de um lado, a União Soviética (URSS) de outro. Nesse contexto, os esforços se concentravam em quem dominava o espaço por meio dos satélites, ao passo que saíria na frente em uma eventual disputa quem detivesse as melhores formas de comunicação.

O nascimento da internet está diretamente relacionado a essa disputa; foi por meio dos peritos militares norte-americanos que o assunto avança: “desenvolveram a ARPANET, rede da Agência de Investigação de Projetos Avançados dos Estados Unidos” (Abreu, 2009, p. 2). Esse desenvolvimento se deu através da agência norte-americana ARPA (*Advanced Research Projects Agency*), responsável pelo desenvolvimento de projetos avançados.

Inicialmente, a ARPANET foi uma rede criada para conectar computadores que armazenavam dados sensíveis do governo americano, com a intenção de garantir a preservação dessas informações em caso de ataques nucleares, haja vista estarem passando pelo período da guerra fria. Posteriormente, tomou outras proporções, fruto dos esforços de Tim Berners-Lee, cientista do Conselho Europeu de Pesquisas Nucleares (CERN), que desenvolveu a *World Wide Web*⁴, marcando uma nova história da Internet. Nesse contexto, “é possível definir a internet como sendo um conjunto de equipamentos interconectados fisicamente, e a *World Wide Web* como sendo um conjunto de aplicações que atuam em uma camada sobre a internet. (Maschietto, 2021, p. 14). Fica evidente que quem reunisse esses elementos participaria desse ciberespaço, impulsionando a evolução da comunicação.

Por volta de 1990, a internet começou a se consolidar, impulsionando diversos benefícios e transformando a maneira como as informações eram compartilhadas. Essa evolução tecnológica impactou diretamente outros setores e, gradualmente, permitiu a transferência de dados entre dispositivos autônomos. Esse cenário, por sua vez, abriu um novo capítulo na história da tecnologia por meio do desenvolvimento e da proliferação da IoT.

⁴ Este sistema nasceu para ligar as universidades entre si para que os trabalhos e pesquisas acadêmicos fossem utilizados mutuamente em um ambiente de contribuição dos lados envolvidos. Este cientista também é responsável pelo desenvolvimento de duas ferramentas indispensáveis para a Internet: o código HTML e o protocolo HTTP. Disponível em: <https://www.tecmundo.com.br/historia/1778-a-world-wide-web-completa-20-anos-conheca-como-ela-surgiu.htm>. Acesso em: 24 maio 2025.

A expressão “internet das coisas” pode ser compreendida como o avanço tecnológico pelo qual aparelhos de uso comum passam a ser dispositivos eletrônicos que se comunicam entre si sem a necessidade do manuseio humano” (Teixeira, 2024, p. 209). Isso vale para veículos, máquinas, eletrodomésticos, eletroportáteis, meios de transporte, entre outros.

Por outra perspectiva, a Agência Europeia para a Segurança das Redes e da Informação (ENISA) define IoT como “um ecossistema ciberfísico de sensores e atuadores interconectados, que permitem tomada de decisão inteligente” (Alves, 2021, p. 102). A grande maioria é de aparelhos interligados pela internet, na medida em que a distância passa a ser ignorada pela função exercida por esses sensores e atuadores. Essa função permite que sistemas mecânicos e de automação efetivem a conversão de energias e sensores em movimento, efetivando a tomada de decisão dinâmica e inteligente.

Em suma, “a Internet das Coisas trata de um ecossistema que conecta objetos físicos, através de um endereço IP³ ou outra rede, para trocar, armazenar e coletar dados para consumidores e empresas através de uma aplicação de *software*” (Carrion; Quaresma, 2019, p. 53).

Para se ter uma ideia, o primeiro equipamento de IoT “foi uma torradeira elétrica criada por John Romkey para ser colocada em exposição, numa feira de tecnologia da informação ocorrida na Inglaterra em 1990”. A partir desse marco inicial, outros dispositivos começaram a ser incorporados, tais como: sistemas de iluminação; geladeiras; máquina de lavar; televisores, etc.

Convém destacar que, em 2024, segundo uma estimativa da IoT Analytics⁵, o número de dispositivos IoT em funcionamento cresceu cerca de 13% chegando a 18,8 bilhões, podendo chegar a 40 bilhões em 2030. Dessa forma, “com o aumento exponencial de utilização desses dispositivos que já existem ou que entrarão em breve no mercado, devemos estar atentos aos riscos que isso pode acarretar para a privacidade e a segurança dos usuários” (Magrini, 2018, p. 24). Atualmente, esses equipamentos estão sofrendo a influência da Inteligência Artificial, surgindo uma nova versão da IoT, a chamada IoE.

A expressão terminológica de IoE (*Internet de Tudo*, do inglês *Internet of Everything*) advém do uso por uma crescente comunidade tecnológica. “Empresas como Cisco e Qualcomm, que trabalham com infraestrutura de redes, vêm difundindo esse termo em convenções e documentos” (Magrini, 2018, p. 73). Estudos na área demonstram que o motivo que destoa esses

⁵ A IoT Analytics, fundada e operando na Alemanha, é uma fornecedora líder global de insights de mercado e inteligência de negócios estratégica para IoT, IA, Nuvem, Edge e Indústria 4.0. Disponível em: <https://iot-analytics.com/number-connected-iot-devices/> Acesso em: 11 fev. 2025

termos está em classificar uma nova versão da internet das coisas para a internet de tudo, haja vista ela ostentar uma característica peculiar que é o aprimoramento da Inteligência Artificial (IA) em sua operabilidade. O que não é observado na IoT.

Vale destacar que a distinção entre IoT e IoE não se resume apenas à presença ou ausência total da IA, mas sim ao nível de integração e complexidade com que essa inteligência opera. Recursos tecnológicos como o *Big Data* e o *Machine Learning*, utilizados nessa nova fase da IoT, contribuíram para expandir o tipo de análise feita por esses dispositivos.

Essa análise, chamada de análise preditiva⁶, é um dos pontos que deixam mais clara essa diferença entre a IoT e IoE. Um exemplo prático dessa técnica é quando esses dispositivos captam dados dos usuários, que são posteriormente utilizados por empresas para direcionar seus anúncios e possivelmente converter em vendas de produtos.

Contudo, com esse aperfeiçoamento, nossas informações - muitas vezes particulares - serão administradas pela IoE, facilitando a entrega de diversos serviços de acordo com nossas necessidades, trazendo mais comodidade. Logo podemos entender que informações colhidas em ambiente doméstico serão utilizadas fora desse ambiente, caracterizando uma espécie de entrada na vida privada das pessoas.

Dentro dessa nova perspectiva, sua influência está principalmente ligada às áreas industriais, agronegócio, medicina, cidades inteligentes e casas inteligentes, tendo essa última um grau de importância maior, explorada no presente texto, pois é nesses ambientes que os direitos fundamentais à privacidade estão sendo impactados.

Dessa forma, cresce uma preocupação pela falta de consentimento explícito dos usuários, haja vista os equipamentos de IoE já fazerem isso no dia a dia, acendendo um alerta quanto à efetiva proteção dos direitos fundamentais, como a privacidade.

Os principais dispositivos que utilizam essa interação entre a IoT e IoE, presentes em ambientes domésticos, são: as fechaduras inteligentes, câmeras inteligentes, sensores inteligentes e os assistentes virtuais presentes em *smart tvs*, *smartphones*, entre outros diversos equipamentos.

As fechaduras inteligentes são dispositivos que utilizam a inteligência artificial para controlar o acesso em ambientes de forma automatizada e eficiente. Elas funcionam por meio de algoritmos que processam dados em tempo real, “podem armazenar e recuperar um registro de acesso, além de se comunicar e sincronizar com calendários para gerenciar o acesso com

⁶ A análise preditiva é o processo de usar dados para prever resultados futuros. O processo usa análise de dados, machine learning, inteligência artificial e modelos estatísticos para encontrar padrões que possam prever comportamentos futuros. As organizações podem usar dados históricos e atuais para prever tendências e comportamentos com segundos, dias ou anos de antecedência, com muita precisão. Disponível em: <https://cloud.google.com/learn/what-is-predictive-analytics?hl=pt-BR> Acesso em 3 set 2025.

base em critérios pré-determinados” (Caballero-Gil et al., 2023, p. 5906).

O que permite seu gerenciamento remotamente, desse modo, ao enviar um comando a essa fechadura (para a entrada de um familiar que veio de visita e a casa encontra-se fechada), esses sistemas permitirão que a pessoa “antes mesmo de chegar à sua residência, possa enviar mensagens para que os próprios dispositivos realizem ações para abrir os portões” (Magrini, 2018, p. 24). Se contar que a maioria delas possui outras formas de abertura, como um painel para digitar a senha de acesso ou até mesmo quem possua uma chave, utilizando o meio tradicional.

Com a integração de sensores, câmeras e sistemas avançados de autenticação, as fechaduras com IA têm como objetivo elevar o nível de segurança, porém existem fechaduras que não utilizam criptografia, umas utilizam apenas o Bluetooth. Contudo, “se nenhuma criptografia for usada para a conexão Bluetooth, a fechadura inteligente não é segura, mas se a criptografia AES⁷ for usada, o nível de segurança é alto” (Caballero-Gil, 2023, p. 5906).

Outro procedimento que ajuda a mitigar tais riscos é a autenticação multifator⁸ (MFA), pois, de maneira simples, adiciona uma camada de proteção em sua porta. Essa autenticação funciona da seguinte forma: ao colocar o login e a senha, o dispositivo segue para a segunda etapa, sendo por meio de uma impressão digital ou até mesmo um código enviado para seu celular.

De acordo com a Coordenadora Nacional de Segurança e Resiliência de Infraestrutura Crítica (CISA⁹), o uso do MFA pode reduzir em 99% os riscos envolvendo os ataques cibernéticos.

As câmeras inteligentes ou câmeras com inteligência artificial são dispositivos de vigilância avançados que utilizam algoritmos para processar imagens e vídeos em tempo real. Esses equipamentos são capazes de analisar o ambiente, identificar comportamentos e compreender contextos visuais.

Seu uso é aplicado em sistemas de segurança, monitoramento urbano, gestão de tráfego e análise comercial. Elas operam seu armazenamento tanto em servidores físicos quanto em

⁷ um método avançado de proteção de dados desenvolvido pelo governo dos EUA no final da década de 1990. Ele usa um algoritmo conhecido como cifra de bloco simétrico para criptografar. Ele é tão seguro, porque os hackers tentam descriptografar os dados experimentando todas as chaves possíveis, quando se deparam com o AES, o espaço de chaves é tão grande que até mesmo os supercomputadores mais rápidos precisariam de bilhões de anos para decifrá-lo. Disponível em: <https://www.avast.com/pt-br/c-what-is-aes-encryption-guide> Acesso em 18 ago. 2025.

⁸ é um recurso de segurança que requer que você verifique sua identidade de várias maneiras antes de acessar uma conta. Disponível em: <https://www.staysafeonline.org/pt/articles/multi-factor-authentication> Acesso em 17 ago. 2025.

⁹ A CISA trabalha com parceiros em todos os níveis para identificar e gerenciar e reduzir riscos à infraestrutura cibernética e física. Disponível em: <https://www.cisa.gov/topics/cybersecurity-best-practices/multifactor-authentication>. Acesso em: 18 ago. 2025

nuvem. Sua principal característica é a integração com tecnologias de visão computacional para interpretar imagens de forma autônoma. Segundo Holdsworth e Scapicchio (2024), esse tipo de sistema possibilita que o usuário visualize imagens da câmera ao vivo ou gravadas, contando com o auxílio da inteligência artificial para identificar indivíduos.

Dentre as suas funcionalidades, destacam-se a capacidade de reconhecer rostos, identificar placas de veículos, detectar movimentos suspeitos e diferenciar pessoas, animais ou objetos. Sua tecnologia permite localizar indivíduos com base em características visuais específicas. Além disso, o sistema pode ser programado para acionar alarmes, emitir mensagens automáticas ou interagir com outros dispositivos, como luzes ou fechaduras eletrônicas.

Essas funcionalidades são possíveis graças à aplicação de tecnologias como *deep learning*¹⁰, que utiliza redes neurais¹¹ com múltiplas combinações de entrada para analisar dados e aprender padrões. Conforme Holdsworth e Scapicchio (2024), essas tecnologias são capazes de extrair as características, funcionalidades e relacionamentos necessários para gerar resultados mais precisos a partir de dados brutos e não estruturados. Por vezes, realizam essas tarefas sem a intervenção humana.

Essas aplicações são implementadas por meio da IoE; podem carregar riscos em relação à interferência na vida privada, o uso indevido de informações pessoais, ataques cibernéticos que comprometem a integridade do sistema e erros na identificação de indivíduos, são preocupações relevantes. Para reduzir estes riscos, é essencial adotar medidas de proteção como, por exemplo, a criptografia de dados durante a transmissão e o armazenamento, a implementação de controles rigorosos de acesso, auditorias periódicas de segurança e políticas claras de retenção e anonimização de dados.

Além das fechaduras e câmeras inteligentes, também ganham destaque os sensores inteligentes que monitoram variáveis (movimento, temperatura, umidade ou presença de pessoas) e os assistentes virtuais incorporados nas *smart TVs*, *smartphones*, dentre outros. Contudo, possuem semelhanças na medida em que interpretam comandos de voz e interagem entre si, em ambientes como os residenciais.

Observa-se, portanto, que esse ecossistema de dispositivos inteligentes, quando implementado pela IoE, amplia significativamente as possibilidades de intervenções de terceiros

¹⁰ é um subconjunto do aprendizado de máquina que utiliza redes neurais multicamadas, chamadas redes neurais profundas, para simular o complexo poder de tomada de decisão do cérebro humano. Disponível em: <https://www.ibm.com/think/topics/deep-learning>? Acesso em 18 ago. 2025.

¹¹ tentam imitar o cérebro humano por meio de uma combinação de entradas de dados, pesos e vieses, todos atuando como neurônios de silício. Esses elementos trabalham juntos para reconhecer, classificar e descrever com precisão os objetos contidos nos dados. Disponível em: <https://www.ibm.com/think/topics/deep-learning>? Acesso em 18 ago. 2025.

não autorizados, o que exige uma atenção redobrada quanto à sua utilização.

2. EVOLUÇÃO DO DIREITO À PRIVACIDADE NO ÂMBITO CONSTITUCIONAL, INFRACONSTITUCIONAL E INTERNACIONAL

As noções do direito à privacidade não surgiram de uma construção autônoma, num determinado tempo, veio de uma construção histórica em tempos antigos. Contudo, somente veio a ser bastante influenciada na era moderna pelo “juiz norte-americano Thomas Cooley que, em 1879, identificou a privacidade como o direito de ser deixado sozinho *“the right to be let alone.”*” (Tavares; Alvarez, 2017, p. 456).

A partir de então, casos foram sendo repercutidos na justiça americana; o Estado americano - por sua vez - passou a interferir na vida privada dos estadunidenses. Foi nesse momento, por volta de 1890, que um artigo intitulado *“The right to privacy”* (O direito à privacidade) tornou-se referência no assunto.

Dentro desse artigo, os autores buscavam classificar o direito à privacidade, “distanciando-o da matriz proprietária utilizada como base para proteção de aspectos da vida privada até então, e aproximando-o da intenção de tutela da personalidade humana” (Cancelier, 2017, p. 217).

Segundo Warren e Brandeis (1890), a garantia de resguardar os pensamentos, sentimentos e emoções manifestados por meio da escrita ou das artes, por meio de uma vedação que consiste em impedir a publicação, constitui um exemplo de como esse direito pode ser aplicado. Desse modo, surge a expressão *“right to be let alone”* (direito de ser deixado em paz). Dessa forma, Warren e Brandeis estão afirmando que a proteção de obras intelectuais contra publicações não autorizadas, constitui uma extensão prática do direito à privacidade, evidenciando como o direito de ser deixado em paz se coaduna com o controle sobre suas criações e informações pessoais. Assim, consolida-se como um direito fundamental intrinsecamente relacionado ao direito de personalidade, pois assegura ao ser humano o controle exclusivo sobre sua intimidade e vida privada.

Fazendo um paralelo, esse raciocínio é essencial para entendermos os riscos que estamos passando nos dias atuais por meio das IoE, como por exemplo: as câmeras inteligentes; fechaduras inteligentes; dentre outras formas de captação mencionadas no presente artigo.

Ademais, a noção conceitual de privacidade proposta por esses estudiosos passou a ser reconhecida pela Declaração Universal dos Direitos Humanos em 1948 (DUDH), assim como dispõe o artigo 12: *Ninguém será sujeito a interferências em sua vida privada, em sua família,*

em seu lar ou em sua correspondência, nem a ataques à sua honra e reputação. Todo ser humano tem direito à proteção da lei contra tais interferências ou ataques. Representando uma ampliação e reconhecimento desse instituto.

De lá pra cá, houve várias discussões sobre o assunto, muitas previsões importantes como a do artigo 8 da Convenção para a Proteção dos Direitos do Homem e das Liberdades Fundamentais em 1950, onde que expressa a preocupação com a vida privada e familiar, tanto do domicílio quanto da correspondência, destacando que o direito à privacidade só pode ser limitado em casos excepcionais, tais como: segurança nacional; segurança pública; prevenção de crimes entre outros.

Em maio de 1967, em Estocolmo, uma comissão internacional de juristas elaborou um relatório¹² de conclusão da conferência nórdica sobre o direito à privacidade, relacionado ao direito à privacidade e direitos da personalidade. Esse relatório teve abrangência global, reforçando o papel de Estocolmo, originando em nível internacional a definição do direito à privacidade, como sendo um direito fundamental.

O referido relatório reforça o alinhamento entre o art. 12 da DUDH, no tocante a garantia de não sofrer intromissões em sua vida privada e com o artigo 17 do Pacto das nações Unidas de 1966, que também reforça a proteção sobre as interferências arbitrárias na vida privada, afirmando que toda pessoa tem direito à proteção da lei quando houver tais interferências. Por fim, as conclusões atingidas por essa comissão encontram sua materialização concreta nos dias atuais. O que era uma projeção abstrata dos riscos vira realidade, na medida em que observamos os dispositivos de IoE realizarem coletas, processamentos e transferências de dados, ampliando os riscos de que já haviam sido alertados, como a espionagem e vigilância.

Ademais, temos em 1969, mais uma vez a ratificação e preocupação com o direito à privacidade no Pacto de São José da Costa Rica, quando definiu obrigações aos Estados-membros, uma delas é de estabelecer como direito e liberdade fundamental, o direito à privacidade previsto no artigo 11, inciso 2 da referida convenção, onde os Estados-membros passam a respeitar e garantir tais direitos.

Uma vez reconhecido no plano internacional, o direito à privacidade foi ganhando amplitude a partir do momento em que os países membros foram aderindo. Contudo, sua definição não se restringe a um conceito único e consolidado, existindo - por conseguinte - diversos conceitos sobre esse direito.

¹² Relatório de conclusão da Conferência Nórdica sobre o direito à privacidade. Disponível em: <https://www.icj.org/wp-content/uploads/2013/06/Right-to-privacy-seminar-report-conclusions-1967-eng.pdf> Acesso em 16 ago. 25.

A começar pela Constituição Federal de 1988, que em seu artigo 5, inciso X, classifica a privacidade como um direito fundamental, determinando que: “são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurando o direito à indenização pelo dano material ou moral decorrente de sua violação”. Nota-se que o direito à privacidade está implícito nesse inciso em um contexto amplo e genérico, o que preocupa alguns doutrinadores.

Em normas infraconstitucionais, a Lei Geral de Proteção de Dados (LGPD) é a que mais busca proteger os direitos de liberdade e privacidade (art. 1º, *caput*). O ponto a ser explorado é saber se a LGPD é suficiente para englobar a camada de proteção aplicável aos dispositivos IoE, haja vista serem uma porta de entrada na vida privada das pessoas, só que inúmeras vezes entram sem pedir licença ou até mesmo são colocados pelos próprios usuários, a fim de cumprirem finalidades específicas, porém acabam colhendo informações de maneira silenciosa sem o consentimento de seus titulares.

Observa-se que a Lei 13.709 de 2018 (LGPD) não prevê tratamento jurídico específico para as aplicações de Inteligência Artificial contidas em dispositivos de IoE, utilizados em ambientes domésticos. Embora o artigo 20 da referida lei se refira ao “tratamento automatizado de dados pessoais”, sua redação não é suficiente para abranger a real complexidade das situações que envolvem essas aplicações. Nesse sentido, não se mostra adequado suprir essa lacuna apenas por meio de uma hermenêutica jurídica extensiva ou analógica, ainda que se invoque o princípio da inafastabilidade da jurisdição. Isso porque, quando se realiza uma hermenêutica lógica, deve-se respeitar a intenção do legislador no momento de elaboração da norma, o que evidencia a ausência de forma expressa acerca das particularidades em dispositivos de IoE.

Assim como leciona o professor Tarcísio Teixeira, “a inclusão desse artigo pelo legislador revela a sua preocupação com o limite de influência da decisão de uma máquina sobre as vidas das pessoas” (Teixeira, 2022, p. 33). Em diversas situações, o tratamento das informações ocorrerá por meio de análise de dados, que se dará de forma automatizada, o que pode levar a resultados equivocados e, conseqüentemente, a discriminações e abusos por parte do agente de tratamento, finaliza o professor. Dessa maneira, é possível concluir que a intenção do legislador em relação a esse artigo não tinha como escopo atingir os dispositivos de IoE.

Havendo tal omissão legislativa, fica evidente o papel doutrinário e jurisprudencial em dar um entendimento mais fundamentado, na tentativa de equilibrar a balança entre a evolução legislativa e a evolução tecnológica, nesse caso, ao conflito existente entre a liberdade de expressão e o direito à privacidade, ambos direitos fundamentais previsto em nossa constituinte.

“Entretanto, considerando-se a inexistência de norma brasileira que discipline a questão, mister se faz o equilíbrio entre os direitos assegurados pela Constituição” (Teixeira, 2008, p. 63).

Esse equilíbrio é dado pelo Supremo Tribunal Federal (STF) quando se depara com antagonismos cada vez mais inerentes a fatos contemporâneos, atraídos pelas tecnologias. Hoje, o STF utiliza a técnica de ponderação dos interesses, a fim de “fazer concessões recíprocas, de modo a produzir um resultado socialmente desejável, sacrificando o mínimo de cada um dos princípios ou direitos fundamentais em oposição” (Barroso, 2012, p. 332).

A decisão judicial que chegou mais perto está no REsp 2.135.783, julgado em 2024. O caso envolvia um motorista de aplicativo que estava sendo descredenciado pela prestadora de serviço. O propósito recursal era decidir *se é possível a exclusão definitiva de perfil de motorista de aplicativo sem contraditório e ampla defesa durante o processo de descredenciamento e notificação prévia à exclusão do perfil profissional* (STJ, 2024, p. 9).

A ministra Nancy Andrighi, em seu voto, ressaltou que as análises de perfil realizadas pelas plataformas digitais decorrem de decisões automatizadas, haja vista o protagonismo das tecnologias com inteligências artificiais. Desse modo, o perfil do motorista que continha seus dados atrai a proteção da LGPD, mais precisamente em seu artigo 20, artigo esse que a doutrina ressalta preocupante, tendo em vista a sua generalização. Ao final, a ministra, ao conjugar esse dispositivo, entendeu que o titular dos dados (o motorista) deve ser informado, deve ter seu direito de revisão, pois isso garantirá o seu direito de defesa.

Ainda que se trate de uma relação contratual, observa-se o esforço que o judiciário vem demonstrando por meio da aplicação da LGPD, a fim de fiscalizar ou até mesmo restringir as decisões geradas por inteligência artificial, reforçando a proteção da privacidade em diferentes contextos sociais e tecnológicos.

Ademais, na doutrina brasileira, a mesma preocupação por essa lacuna normativa, evidenciada pelo professor Tarcísio Teixeira supramencionado, é a mesma dos demais especialistas da área.

À luz do direito comparado, diversos especialistas da área têm apontado que essa questão ampla e genérica trazida em nossa constituinte e nos conceitos supramencionados preocupa a evolução desse instituto. Nesse sentido, Solove¹³ (2006) ressalta a necessidade de apresentar uma explicação fundamentada e bem articulada, a fim de demonstrar que os problemas relacionados à privacidade são prejudiciais. Embora seus argumentos tenham sido formulados antes da popularização da IoE, eles permanecem pertinentes, pois os princípios em discussão são universais e aplicáveis em contextos onde os dados pessoais são processados.

No entanto, não basta apenas invocar o direito, precisa-se desenvolver as nuances entre o

¹³ Professor de direito da George Washington University Law School - Daniel J. Solove - especialista no direito à privacidade.

direito e o caso em concreto. Solove (2006) acredita que essa falta de clareza conceitual gera tanto dificuldades na formulação de políticas como na resolução de casos concretos, uma vez que legisladores e juízes não conseguem articular facilmente o dano à privacidade. O que pode corroborar para o arquivamento de processos e comprometer a elaboração de normas adequadas de proteção.

Desse modo, dizer apenas que a IoE está interferindo sem trazer as circunstâncias materiais, os problemas, não vai ajudar na evolução legislativa. Cresce de importância o aprofundamento argumentativo na hora de invocar essa pretensão perante o Estado, pois é um direito relativamente novo e que precisa ser melhor regulamentado, a fim de que cheguemos a um consenso social.

Em síntese, a evolução do direito à privacidade evidenciada nessa seção demonstrou um avanço significativo na legislação e na forma como é interpretado o direito à privacidade, em seus diversos contextos. Muito embora tenha sido observado o avanço desse instituto, sendo alcançada a condição de direito fundamental no âmbito constitucional e ratificado por normas infraconstitucionais e tratados internacionais, sua aplicação protetiva continua sendo precária, diante da complexidade trazida pelo avanço tecnológico.

3. ANÁLISE DO ARCABOUÇO JURÍDICO BRASILEIRO EM RELAÇÃO À PROTEÇÃO DA PRIVACIDADE

A partir dessas considerações, passamos a adentrar com mais profundidade nas complexidades existentes nesses dispositivos de IoE, verificando a capacidade de proteção do arcabouço jurídico brasileiro, frente ao que esses dispositivos são capazes de fazer.

Primeiramente, em que pese termos um arcabouço robusto, constituído principalmente por nossa constituição, pelo Marco Civil da Internet, pela LGPD e pelo Código de Defesa do Consumidor (CDC). O mesmo não consegue ser efetivo, pois não possui a capacidade de atingir as novas operações algorítmicas.

Convém destacar que esse arcabouço jurídico não é totalmente insuficiente diante das questões trazidas pela IoE, mas apresenta limitações decorrentes da ausência de especificidade normativa.

A Constituição Federal em seu artigo 5º, incisos X e XII, juntamente com a LGPD, já oferece bases sólidas de proteção à privacidade e aos dados pessoais. Todavia, esses instrumentos foram concebidos em um contexto anterior ao avanço de operações algorítmicas mais sofisticadas (por exemplo, a análise preditiva). Essa opacidade e complexidade acabam por escapar dos

contornos normativos existentes.

O direito à privacidade, como já observado, evoluiu e hoje consegue ter uma proteção mais profunda, garantida por esse pacote normativo envolvendo nossa constituinte, o marco civil da internet, LGPD e o CDC. Contudo, quando confrontada com os desafios contemporâneos gerados por essa interferência na vida privada das pessoas, seja por essa coleta desenfreada de dados ou pelo direcionamento - sem consentimento explícito - da compra de determinado produto, gerando riscos não apenas à privacidade, mas também à autonomia dos consumidores.

Em que pese o CDC ter se atualizado para essa situação, o mesmo ainda carece de profundidade, ao passo que ainda é difícil ao intérprete adequar um raciocínio hermenêutico, a fim de abranger esse novo modelo de transação comercial.

O CDC em seu artigo 6, inciso 3, trata de uma proteção muito importante que é o dever de ser informado de forma clara e precisa. Dessa forma, “o direito à informação visa a assegurar ao consumidor uma escolha consciente, permitindo que suas expectativas em relação ao produto ou serviço sejam de fato atingidas” (Gaio Júnior; Mello, 2025, p. 116).

Entretanto, a insegurança jurídica se manifesta principalmente na ausência de consentimento informado. Muitos dispositivos não oferecem essa opção, até porque, se houvesse, o usuário/consumidor poderia questionar para onde os dados estão sendo enviados e, conseqüentemente, poderiam impedir interferências em sua vida privada, garantindo sua autonomia de vontade.

Algo que atualmente poderia ser feito, na tentativa de mitigar violações ao direito à privacidade por meio desses dispositivos de IoE, seria o acionamento da Agência Nacional de Proteção de Dados (ANPD). Na medida em que a ANPD busca também desenvolver diretrizes sobre as IAs. Porém, é um órgão ainda pequeno que não consegue suprir essa imensidão de transferências de dados, observadas pelo fenômeno do *Big Data*.

A LGPD foi inspirada pelo Regulamento Geral de Proteção de Dados (RGPD); ambos têm como escopo a tutela sobre direitos fundamentais, mais especificamente sobre os direitos relacionados ao processamento de dados. Essa proteção abrange as pessoas físicas e jurídicas, tanto em âmbito do direito privado como público.

Essa inspiração fica evidente, por exemplo, quando analisamos o direito ao acesso previsto no art. 19, §1 da LGPD e o art. 15 da RGPD. Logo, podemos identificar essa preocupação em saber se os dados estão sendo objeto de tratamento ou não. Caso estejam, o titular poderá exigir o fim do tratamento dos dados, assim como dispõe o art. 18, IV da LGPD, tendo uma certa semelhança com o direito ao esquecimento, previsto no art. 17 da RGPD.

Contudo, a União Europeia (UE) observou que precisaria de uma lei que assegurasse o

desenvolvimento técnico e o uso seguro das tecnologias envolvendo as inteligências artificiais. Para tanto, criou-se o EU AI ACT¹⁴ (Ato de Inteligência Artificial da União Europeia), que é considerado um marco regulatório global sobre a IA, porém não rege especificamente direitos fundamentais; em essência, ele dispõe sobre as diretrizes para o desenvolvimento e uso desses novos modelos tecnológicos, a fim de prevenir potenciais abusos decorrentes do uso da IA. Nesse contexto, a lei estabelece regras técnicas e jurídicas por meio da classificação de riscos, prevista no art. 6 e seguintes da referida lei. A combinação da GDPR com a lei EU IA ACT foi a solução dada pela UE para solucionar o problema da privacidade em países europeus.

O Brasil está caminhando no mesmo sentido; hoje temos um projeto de lei da inteligência artificial tramitando no Congresso Nacional, o PL. 2.338 de 2023. Ao que tudo indica, a resposta para esse conflito influenciado pela IoE em relação ao direito à privacidade está nesse projeto de lei, pois nele está contido um tratamento mais robusto em relação às mais variadas circunstâncias observadas por essas tecnologias.

Ao analisar o texto final do PL. 2.338/23, podemos identificar uma série de proteções e medidas que servirão não só para proteger a privacidade das pessoas em ambientes domésticos, como também favorecer o consentimento daquele usuário, tendo em vista que a importância desse projeto de lei se dá pela centralidade no ser humano, ou seja, a importância da supervisão humana prevista no artigo 6, III do PL. 2.338. O capítulo 2 do referido projeto traz consigo essa centralidade, inclusive já demonstra em seu artigo 5º, inciso II, a garantia de proteção a essa pessoa ou grupo afetado por um sistema de IA, perante sua privacidade e a seus dados.

No tocante às fechaduras inteligentes presentes na 1ª seção desse artigo, a questão que se aflora é como o PL consegue, de certa forma, mitigar essa intromissão na vida privada das pessoas?

Primeiro, conforme analisado anteriormente acerca das fechaduras inteligentes, estas possuem características como: acesso remoto e abertura automatizada por biometria; tais características podem ser avaliadas como sendo um sistema de alto risco. Essa avaliação preliminar é um “processo simplificado de autoavaliação, anterior à utilização ou disponibilização de sistemas de IA no mercado, para classificação de seu grau de risco, com o objetivo de determinar o cumprimento das obrigações definidas nesta Lei” (Zanatta; Rielli, 2024). Com o intuito de proporcionar a correção de falhas na segurança e transparência. Já que tem o condão de

¹⁴ A EU IA ACT é uma legislação proposta pela Comissão Europeia com o objetivo de estabelecer um quadro legal abrangente para a regulamentação do uso e desenvolvimento da IA na União Europeia. Este ato é considerado uma das primeiras e mais significativas tentativas de regulamentação legal de IA em uma grande região econômica. Disponível em: <https://www.migalhas.com.br/depeso/399513/entendendo-o-eu-ai-act-uma-nova-era-na-regulamentacao-da-ia-na-europa> Acesso em: 16 jun. 2025.

identificar e responsabilizar quem fez parte daquela operação, podendo ser: os desenvolvedores, distribuidores e aplicadores.

Os desenvolvedores são considerados como pessoas naturais ou jurídicas, de natureza pública ou privada, que “desenvolvam um sistema de inteligência artificial, diretamente ou por encomenda, com vistas à sua colocação no mercado ou à sua aplicação em serviço por ela fornecido, sob seu próprio nome ou marca, a título oneroso ou gratuito”. (Zanatta; Rielli, 2024).

Já os distribuidores são considerados “pessoas naturais ou jurídicas, de natureza pública ou privada, que disponibilizam e distribuem sistemas de IA para que terceiros apliquem a título oneroso ou gratuito” (Zanatta; Rielli, 2024).

Fechando essa tríade de responsáveis pelo manejo dos sistemas de IA, temos os aplicadores como também sendo pessoas naturais ou jurídicas, de natureza pública ou privada “que empregue ou utilize, em seu nome ou benefício, sistema de inteligência artificial, inclusive configurando, mantendo ou apoiando com o fornecimento de dados para a operação e o monitoramento do sistema de IA” (Zanatta; Rielli, 2024).

Logo, devem sempre adotar medidas necessárias quando estiverem manejando os sistemas de IA, para que esses sistemas não interfiram no comportamento da pessoa natural, assim como dispõe o artigo 13, §1º do PL. 2.338/23.

Da mesma forma acontece com as câmeras inteligentes e os sensores inteligentes, ou seja, uma implementação perfeita para serem utilizadas contra os usuários (donos de dispositivos IoE), pois essas tecnologias juntas podem realizar diversas ações que poderão contribuir no futuro para a prática de crimes. Nesse sentido, a proposta determina que serão vedadas o desenvolvimento, implementação e uso de sistemas de IA, quando esses sistemas ostentarem características “de identificação biométrica à distância, em tempo real e em espaços acessíveis ao público” (art. 13, IV do PL. 2.338/23), determinando um rol de exceções que basicamente estabelece limites claros e garantias processuais para o uso de tecnologias de vigilância e monitoramento, especialmente em contextos como investigações criminais, buscas e situações de flagrante.

Nessa linha, o projeto de lei traz um passo muito importante para o combate a essa interferência na privacidade, pois classifica tal conduta como de risco excessivo. Desse modo, o art. 13 proíbe que sejam desenvolvidas ou implementadas aplicações que vão instigar ou induzir o comportamento daquela pessoa natural, de maneira a lhe causar danos à saúde, à segurança ou a outros direitos fundamentais.

Outra figura que ganhará reforço com a vigência da lei de IA brasileira é a Autoridade Nacional de Proteção de Dados (ANPD). O projeto de lei propõe que o Sistema Nacional de Regulação e Governança de Inteligência Artificial (SIA) seja integrado pela ANPD, que por sua

vez o coordenará; além de contar com autoridades setoriais (Anvisa, Banco Central, etc.); Conselho Permanente de Cooperação Regulatória de Inteligência Artificial (CRIA) e o Comitê de Especialistas e Cientistas de Inteligência Artificial (CECIA).

Dessa forma, o sistema contribuirá para a regulamentação dos sistemas de alto risco. Permitindo que as autoridades setoriais estabeleçam regras para o uso das IAs, no âmbito de suas competências. Assim, a implementação da regulação da Inteligência Artificial no Brasil poderá ser implementada de maneira eficaz, assegurando que seus efeitos não comprometam os direitos e interesses da sociedade civil.

Paralelamente, outra ferramenta que reforçará e fomentará a inovação é o Sandbox regulatório, assim como vem fazendo no âmbito econômico. Essa ferramenta está prevista no art. 4, XVIII, do PL. 2.338/23:

“Conjunto de condições especiais estabelecidas para desenvolver, treinar, validar e testar, por tempo limitado, um sistema de IA inovador, bem como modelos de negócio e políticas públicas inovadoras e técnicas e tecnologias experimentais que envolvam IA, mediante o cumprimento de critérios e de limites previamente estabelecidos e por meio de procedimento facilitado”.

A principal vantagem do Sandbox é flexibilizar a aplicação normativa que possa engessar o desenvolvimento de sistemas de IA. Podemos entendê-lo como sendo um ambiente neutro e temporário que permitiu a inovação com menos burocracia. Nesse ambiente, as empresas ou instituições poderão desenvolver, testar e validar novas soluções de IA, antes de lançá-las oficialmente no mercado ou colocá-las em uso.

Por fim, diante desse cenário, o PL. 2.338/23 surge como uma resposta concreta ao limbo existente entre a legislação e o avanço tecnológico, estruturando mecanismos anteriormente que promoverão a inovação, salvaguardando medidas robustas contra os abusos já existentes, presentes não apenas em dispositivos de IoE, mas também em outros sistemas de IA.

CONSIDERAÇÕES FINAIS

A presente pesquisa buscou analisar a evolução da IoE e seus impactos no direito à privacidade; essa análise se deu no âmbito do ordenamento jurídico brasileiro vigente e no contexto internacional.

Observou-se que a transição da IoT para a IoE representa um desafio significativo para a proteção dos direitos fundamentais, especialmente o direito à privacidade.

O objetivo principal da pesquisa foi investigar a evolução da IoE, relacionando-a à evolução do direito à privacidade no arcabouço jurídico brasileiro, tanto em âmbito

constitucional e infraconstitucional, como no âmbito internacional, com o intuito de verificar se o arcabouço jurídico é capaz de assegurar uma proteção adequada diante dos desafios tecnológicos trazidos por essa evolução.

Por meio de uma revisão teórica baseada na doutrina, legislação e jurisprudência, bem como no direito comparado, especialmente a partir da experiência europeia, foi possível alcançar os objetivos propostos, demonstrando que apesar de existir um conjunto normativo robusto, o mesmo tem baixa capacidade de enfrentar os desafios emergentes, no tocante aos crescentes sistemas e dispositivos de inteligência artificial. Desse modo, a legislação vigente não consegue acompanhar essa transição.

A pesquisa respondeu à questão-problema inicialmente colocada, ao evidenciar que a evolução tecnológica da IoE impacta diretamente o direito à privacidade, ao ampliar a coleta automatizada e contínua de dados pessoais em ambientes privados, muitas vezes sem o consentimento explícito dos titulares.

Contudo, a ausência de regulamentação específica para dispositivos inteligentes gera uma lacuna que dificulta a responsabilização efetiva dos agentes envolvidos, dentre eles: os desenvolvedores, distribuidores e aplicadores.

Tal dificuldade não decorre de uma ausência normativa, mas da limitação prática de sua aplicação, até porque o CDC em seu artigo 18 c/c o art. 25 §1, estabelece a responsabilidade solidária entre todos da cadeia de fornecimento, permitindo que o consumidor acione qualquer um deles, cabendo a aquele que suportar o ônus, buscar eventual ação de regresso.

O problema surge em situações específicas, quando uma câmera inteligente vaza imagens em razão de falhas na segurança ou quando uma assistente de voz - como a Alexa - grava conversas privadas sem autorização. Nessas hipóteses, como o lojista poderá demonstrar se o dano decorreu de falha no algoritmo ou de mau uso pelo consumidor? Essa incerteza gera obstáculos adicionais e tende a desequilibrar as relações de consumo.

Por outro lado, observou-se que o Projeto de lei que tramita no congresso nacional, fortalece a ANPD e oferece um caminho para mitigar os riscos existentes em sistemas de IA, por meio da implementação de diretrizes claras, focado na supervisão humana, nos sistemas de alto risco e mecanismos que vão incentivar a inovação tecnológica ética e responsável, como é o caso do Sandbox.

Conclui-se que apesar do direito à privacidade estar consolidado em nosso ordenamento jurídico, o mesmo não é suficiente e não está adequado às demandas urgentes envolvendo os dispositivos de IoE. Pois não basta apenas invocá-lo, a uma necessidade de uma explicação mais elaborada, entretanto, a falta de clareza cria uma dificuldade na resolução de litígios dessa

natureza.

Por tanto, essa clareza é observada no texto da proposta de lei da IA, onde pode inclusive servir de exemplo, assim como mencionado por especialistas da área, como: Danilo Doneda e Laura Schertel, que pontuam no sentido de que a lei de IA, trará um equilíbrio entre a proteção dos direitos fundamentais e a inovação tecnológica, além de impactar positivamente o desenvolvimento econômico do país.

REFERÊNCIAS

ABREU, Karen Cristina Kraemer. **História e usos da Internet** [recurso eletrônico]. 2009. p. 2 Disponível em: <https://pt.scribd.com/document/728654257/Historia-e-usos-da-internet>. Acesso em: 22 mai. 2025.

ALVES, David; PEIXOTO, Mario; ROSA, Thiago. **Internet das Coisas (IoT): Segurança e privacidade de dados pessoais**. Rio de Janeiro: Editora Alta Books, 2021. Disponível em: <https://app.minhabiblioteca.com.br/reader/books/9786555202793/>. Acesso em: 22 mai. 2025.

BRASIL. **Declaração Universal dos Direitos Humanos de 1948**. Disponível em: https://brasil.un.org/sites/default/files/2025-03/ONU_DireitosHumanos_DUDH_UNICRio_20250310.pdf . Acesso em 22 mai 2025.

BRASIL. Senado Federal. **Projeto de Lei n.º 2338, de 2023**, Senador Rodrigo Pacheco. Brasília: Senado Federal, 2023. Disponível em: <https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2487262>. Acesso em: 14 jun. 2025.

BRASIL. **Superior Tribunal de Justiça. Recurso Especial nº 2135783 – DF (2023/0431974-4). RECURSO ESPECIAL. AÇÃO DE OBRIGAÇÃO DE FAZER C/C AÇÃO INDENIZATÓRIA. NEGATIVA DE PRESTAÇÃO JURISDICIONAL. OMISSÃO. NÃO DEMONSTRADA. DESCRENCIAMENTO PERFIL. MOTORISTA APLICATIVO. DECISÃO AUTOMATIZADA. NOTIFICAÇÃO PRÉVIA. DESNECESSÁRIA. DEVER DE INFORMAÇÃO. SEGURANÇA DOS USUÁRIOS. CONTRADITÓRIO. AMPLA DEFESA. Recorrente: Eliomar Evangelista de Souza. Recorrido: 99 TECNOLOGIA LTDA. Relatora: Min. Nancy Andrighi, 18 de junho de 2024. Disponível em: https://processo.stj.jus.br/SCON/GetInteiroTeorDoAcórdão?num_registro=202304319744&dt_publicação=21/06/2024. Acesso em 15 jun. 2025.**

BARROSO, Luís R. **Interpretação e Aplicação da Constituição**. 7. ed. Rio de Janeiro: Saraiva, 2012. E-book. pág.332. ISBN 9788502075313. Disponível em: <https://app.minhabiblioteca.com.br/reader/books/9788502075313/>. Acesso em: 25 jul. 2025.

CARRION, Patricia; QUARESMA, Manuela. **Internet da Coisas (IoT): Definições e aplicabilidade aos usuários finais**. *Human Factors in Design*, Florianópolis, v. 8, n. 15, p. 049–066, 2019. DOI: 10.5965/2316796308152019049. Disponível em: <https://revistas.udesc.br/index.php/hfd/article/view/2316796308152019049>. Acesso em: 15 mar. 2025.

CABALLERO-GIL, Cândido; ÁLVAREZ, Rafael; HERNÁNDEZ-GOYA, Candelaria; MOLINA-GIL, Jezabel. **Research on smart-lock cybersecurity and vulnerabilities**. *Wireless Networks*, v. 30, n. 6, p. 5905–5917, 27 de maio de 2023. Disponível em:

<https://link.springer.com/article/10.1007/s11276-023-03376-8> Acesso em: 17 jul. 2025.

CANCELIER, Mikhail Vieira de Lorenzi. **O Direito à Privacidade hoje: perspectiva histórica e o cenário brasileiro**. Sequência (Florianópolis), pp. 213-239, 2017. Disponível em: <https://doi.org/10.5007/2177-7055.2017v38n76p213>. Acesso em 19 jul. 2025.

CONSELHO DA EUROPA. **Convenção para a Proteção dos Direitos do Homem e das Liberdades Fundamentais**. Roma, 4 de novembro de 1950. Disponível em <https://www.hrea.org/erc/Library/hrdocs/coe/echr_pt.pdf>. Acesso em: 20 jul. 2025.

GAIO JÚNIOR, Antônio Pereira; MELLO, Cleyson de Moraes. **Código de defesa do consumidor comentado**. 4. ed. Rio de Janeiro: Freitas Bastos, 2025. *E-book*. p. 116 Disponível em: <https://plataforma.bvirtual.com.br>. Acesso em: 31 jul. 2025.

HOLDSWORTH, Jim; SCAPICCHIO, Mark. **What is deep learning?** IBM Think. 17 jun. 2024. Disponível em: <https://www.ibm.com/think/topics/deep-learning>. Acesso em: 18 ago. 2025.

MAGRINI, Eduardo. **Internet das Coisas**. Rio de Janeiro: FGV Editora, 2018. p. 192 ISBN 978-85-225-2005-3. Disponível em: <https://repositorio.fgv.br/items/ec1ac3f7-9f6d-479a-930d-1b62183d7af1>. Acesso em: 12 abr. 2025.

MASCHIETTO, L. G.; VIEIRA, A. L. N.; TORRES, F. E.; et al. **Arquitetura e Infraestrutura de IoT**. Porto Alegre: SAGAH, 2021. *E-book*. p. 14. ISBN 9786556901947. Disponível em: <https://app.minhabiblioteca.com.br/reader/books/9786556901947/>. Acesso em: 25 mai. 2025.

ORGANIZAÇÃO DOS ESTADOS AMERICANOS. **Convenção Americana sobre Direitos Humanos**, San José, Costa Rica, em 22 de novembro de 1969. Disponível em: https://www.cidh.oas.org/basicos/portugues/c.convencao_americana.htm Acesso em: 16 jul. 2025.

SOLOVE, Daniel J. **A taxonomy of privacy**. University of Pennsylvania Law Review, v. 154, p. 477-555, 2006. Disponível em: https://scholarship.law.upenn.edu/penn_law_review/vol154/iss3/1/. Acesso em: 28 jul. 2025.

TEIXEIRA, Tarcísio. **Direito Digital e Processo Eletrônico**. 8. ed. Rio de Janeiro: Saraiva Jur, 2024. *E-book*. pág. 209. ISBN 9788553622344. Disponível em: <https://app.minhabiblioteca.com.br/reader/books/9788553622344/>. Acesso em: 09 fev. 2025.

TEIXEIRA, Tarcísio; GUERREIRO, Ruth M. **Lei Geral de Proteção de Dados Pessoais: Comentada Artigo por Artigo**. 4. ed. Rio de Janeiro: Saraiva Jur, 2022. *E-book*. pág. 33. ISBN 9786555599015. Disponível em: <https://app.minhabiblioteca.com.br/reader/books/9786555599015/>. Acesso em: 29 jul. 2025.

TAVARES, Letícia Antunes e ALVAREZ, Bruna Acosta. **Da proteção dos dados pessoais: uma análise comparada dos modelos de regulação da Europa, dos Estados Unidos da América e do Brasil**. In: BALDANI, Thiago Gomes de Fillipo; ONODERA, Marcus Vinicius Kiyoshi (Coord.). Brasil e EUA: temas de direito comparado. São Paulo: Escola Paulista da Magistratura, 2017. Disponível em: <https://www.tjsp.jus.br/download/EPM/Publicacoes/ObrasJuridicas/ii%204.pdf?d=636680444556135606>. Acesso em: 15 jun. 2025.

WARREN, S. D.; BRANDEIS, L. D. **The right to privacy**. Harvard Law Review, v. 4, p. 193-220, 1890. Disponível em: <https://www.cs.cornell.edu/~shmat/courses/cs5436/warren-brandeis.pdf>. Acesso em: 19 jul. 2025.

ZANATTA, Rafael A. F.; RIELLI, Mariana. **A construção da legislação de inteligência artificial no**

Brasil: análise técnica do texto que será votado no plenário do Senado Federal. Data Privacy Brasil, São Paulo, 2 abr. 2024. Disponível em: <https://www.dataprivacybr.org/a-construcao-da-legislacao-de-inteligencia-artificial-no-brasil-analise-tecnica-do-texto-que-sera-votado-no-plenario-do-senado-federal>. Acesso em: 10 ago. 2025.