

**A REVOLUÇÃO DA INTERNET DAS COISAS (IoT) NA EDUCAÇÃO
CONECTADA: DESAFIOS DE INFRAESTRUTURA, PRIVACIDADE E
INCLUSÃO NO BRASIL**

**THE INTERNET OF THINGS (IOT) REVOLUTION IN CONNECTED
EDUCATION: INFRASTRUCTURE, PRIVACY, AND INCLUSION CHALLENGES
IN BRAZIL**

**LA REVOLUCIÓN DEL INTERNET DE LAS COSAS (IOT) EN LA EDUCACIÓN
CONECTADA: DESAFÍOS DE INFRAESTRUTURA, PRIVACIDAD E
INCLUSIÓN EN BRASIL**



10.56238/sevened2026.001-015

Felipe Menezes de Abreu

Pós-graduado em Gestão de Tecnologia da Informação

Instituição: Universidade do Estado do Pará (UEPA)

E-mail: felipe.md.abreu@aluno.uepa.br

Elias Ramos Quaresma

Graduando em Engenharia de Software

Instituição: Universidade do Estado do Pará (UEPA)

E-mail: eliasramos.educ@gmail.com

Emerson Leandro da Silva Silva

Graduando em Engenharia de Software

Instituição: Universidade do Estado do Pará (UEPA)

E-mail: emersonleandrodss@gmail.com

Glaucia Nunes de Lima Santos

Graduação em Pedagogia – Universidade Paulista (UNIP);

Graduanda em Engenharia de Software

Instituição: Universidade do Estado do Pará (UEPA)

E-mail: glauciaa.nunes@gmail.com

Maria Joselia Mendes das Chagas

Graduanda em Engenharia de Software

Instituição: Universidade do Estado do Pará

E-mail: Maria.chagas@aluno.uepa.br

Paulo Adriano Maciel da Silva

Graduando em Engenharia de Software

Instituição: Universidade do Estado do Pará

E-mail: Paulo.amdsilva@aluno.uepa.br

Paulo Cristiano Abreu de Jesus

Pós-graduado em Matemática, suas Tecnologias e o Mundo do Trabalho

Instituição: Universidade Federal do Piauí

E-mail: paulo.jesus3547@escola.seduc.pa.gov.br

RESUMO

Este artigo analisa o impacto da Internet das Coisas (IoT) na gestão escolar e nas práticas pedagógicas no Brasil. Através de uma revisão bibliográfica e documental de fontes nacionais publicadas entre 2020 e 2025, investiga-se como a interconexão de objetos físicos (sensores, wearables e dispositivos inteligentes) pode transformar o ambiente escolar em ecossistemas de "Smart Schools". Discute-se, concomitantemente, o cenário regulatório brasileiro, com ênfase na Lei Geral de Proteção de Dados (LGPD) e na Estratégia Nacional de Escolas Conectadas, abordando os riscos de vigilância excessiva, a segurança de dados de menores e a disparidade de infraestrutura entre as redes pública e privada.

Palavras-chave: Internet das Coisas. Educação Conectada. LGPD. Gestão Escolar. Desigualdade Digital.

ABSTRACT

This article analyzes the impact of the Internet of Things (IoT) on school management and pedagogical practices in Brazil. Through a bibliographic and documentary review of national sources published between 2020 and 2025, it investigates how the interconnection of physical objects (sensors, wearables, and smart devices) can transform the school environment into "Smart Schools" ecosystems. The Brazilian regulatory landscape is discussed concurrently, with emphasis on the General Data Protection Law (LGPD) and the National Connected Schools Strategy, addressing the risks of excessive surveillance, the data security of minors, and the infrastructure disparity between public and private networks.

Keywords: Internet of Things. Connected Education. LGPD. School Management. Digital Inequality.

RESUMEN

Este artículo analiza el impacto del Internet de las Cosas (IdC) en la gestión escolar y las prácticas pedagógicas en Brasil. Mediante una revisión bibliográfica y documental de fuentes nacionales publicadas entre 2020 y 2025, se investiga cómo la interconexión de objetos físicos (sensores, wearables y dispositivos inteligentes) puede transformar el entorno escolar en ecosistemas de "Escuelas Inteligentes". Se analiza simultáneamente el panorama regulatorio brasileño, con énfasis en la Ley General de Protección de Datos (LGPD) y la Estrategia Nacional de Escuelas Conectadas, abordando los riesgos de la vigilancia excesiva, la seguridad de los datos de los menores y la disparidad de infraestructura entre las redes públicas y privadas.

Palabras clave: Internet de las Cosas. Educación Conectada. LGPD. Gestión Escolar. Desigualdad Digital.

1 INTRODUÇÃO

A educação brasileira atravessa um momento de redefinição infraestrutural. Se nas últimas décadas o foco estava na informatização básica, traduzida na criação de laboratórios de informática muitas vezes isolados do restante da escola, o cenário contemporâneo aponta para a "computação ubíqua". Neste novo paradigma, a tecnologia não é mais um destino para onde se leva o aluno, mas uma camada invisível e onipresente que permeia todo o ambiente escolar. É neste contexto que a Internet das Coisas (*Internet of Things* - IoT) emerge como uma fronteira tecnológica decisiva.

A IoT refere-se à interconexão digital de objetos cotidianos com a internet (SANTAELLA, 2021). No ambiente escolar, isso se traduz em carteiras que monitoram a postura, sistemas de chamada automatizados por reconhecimento facial ou RFID, laboratórios de ciências com sensores ambientais conectados e bibliotecas inteligentes. Diferente da adoção de tablets ou lousas digitais, a IoT promete uma revolução na gestão de dados físicos e na personalização ambiental do aprendizado.

No entanto, a integração desses dispositivos "inteligentes" no Brasil não ocorre em um terreno neutro. O período de 2020 a 2025 revelou, especialmente após a pandemia de COVID-19, o abismo digital que separa escolas de elite, já imersas na cultura *maker* e na automação, de escolas públicas que ainda lutam por conectividade básica, conforme apontam os dados do Cetic.br (2024).

Ademais, a coleta massiva de dados biométricos e comportamentais de crianças e adolescentes impõe um desafio jurídico sem precedentes. A Lei Geral de Proteção de Dados (Lei n.º 13.709/2018) estabelece, em seu artigo 14, que o tratamento de dados de menores deve ser realizado com o "melhor interesse" da criança. Como conciliar a eficiência administrativa prometida pela IoT, como a redução da evasão através do monitoramento de presença, com o direito fundamental à privacidade e à não vigilância?

Este artigo propõe-se a explorar essa tensão: o potencial da IoT para criar ambientes de aprendizagem eficientes e adaptativos versus os riscos de vigilância, insegurança de dados e aprofundamento das desigualdades regionais no Brasil.

2 OBJETIVOS

2.1 OBJETIVO GERAL

Analisar como as tecnologias de Internet das Coisas (IoT) têm sido aplicadas para modernizar a gestão e a pedagogia nas escolas brasileiras, e quais são as implicações éticas, legais e de infraestrutura dessa adoção no cenário nacional.

2.2 OBJETIVOS ESPECÍFICOS

Mapear as principais aplicações de IoT (sensores ambientais, controle de acesso, wearables) em experimentação ou uso no Brasil entre 2021 e 2025.

Examinar o impacto da Lei Geral de Proteção de Dados (LGPD) na implementação de dispositivos de coleta de dados em ambientes escolares, focando na proteção de menores.

Discutir a viabilidade técnica da implementação de "Escolas Inteligentes" frente à realidade da infraestrutura de conectividade (5G e fibra óptica) nas escolas públicas brasileiras.

3 METODOLOGIA

Sob o prisma metodológico, o presente estudo estrutura-se como uma pesquisa de abordagem qualitativa, essencial para compreender um fenômeno que não é apenas técnico, mas profundamente social e político. A complexidade da introdução de objetos conectados em ambientes de formação humana exige uma análise que ultrapasse métricas de desempenho de hardware, focando nas dinâmicas de privacidade e governança escolar.

Quanto aos seus fins, a pesquisa classifica-se como **exploratória e descritiva**. O caráter exploratório justifica-se pela incipiência da literatura nacional focada especificamente na interseção entre IoT e Educação Básica, muitas vezes eclipsada pelos debates sobre Inteligência Artificial. A dimensão descritiva é necessária para caracterizar o ecossistema regulatório brasileiro e as políticas públicas recentes, como a Estratégia Nacional de Escolas Conectadas.

O procedimento técnico adotado foi a **revisão bibliográfica sistemática e a análise documental**.

Recorte Temporal: Janeiro de 2020 a dezembro de 2025. Esta janela cobre desde a aceleração digital forçada pela pandemia até a consolidação das discussões sobre o leilão do 5G no Brasil e seus reflexos na educação.

Bases de Dados: Foram consultadas bases nacionais de referência: SciELO Brasil, Portal de Periódicos da CAPES, Biblioteca Digital Brasileira de Computação (BDBComp) e repositórios da Sociedade Brasileira de Computação (SBC).

Estratégias de Busca: Utilizaram-se descritores em português: "Internet das Coisas na Educação", "IoT e Ensino", "Cidades Inteligentes e Escolas", "Privacidade de Dados na Escola", "LGPD e Educação".

CrITÉRIOS de Seleção:

Fontes Primárias: Textos legislativos, especificamente a Lei n.º 13.709/2018 (LGPD), o Decreto n.º 9.854/2019 (Plano Nacional de Internet das Coisas) e relatórios técnicos do Comitê Gestor da Internet no Brasil (CGI.br).

Fontes Secundárias: Artigos publicados em revistas brasileiras qualificadas (Qualis A e B) nas áreas de Educação e Ciência da Computação, teses e dissertações defendidas em programas de pós-graduação nacionais.

A análise seguiu a técnica de análise de conteúdo, triangulando as promessas tecnológicas dos planos governamentais com a realidade descrita nos estudos de caso e nas pesquisas TIC Educação.

4 REFERENCIAL TEÓRICO

4.1 DO COMPUTADOR À COISA CONECTADA: O CENÁRIO BRASILEIRO

A evolução tecnológica na educação brasileira passou por fases distintas. Segundo Valente (2020), superamos a fase do "ciclo do laboratório" para entrar na era da mobilidade. Contudo, a IoT representa um salto para a "computação invisível". No Brasil, o marco regulatório inicial foi o **Plano Nacional de Internet das Coisas** (Decreto n.º 9.854/2019), que, embora foque prioritariamente em agronegócio, saúde, indústria e cidades, coloca a educação como um eixo transversal de capacitação e aplicação.

Pesquisadores da Sociedade Brasileira de Computação (SBC, 2023) argumentam que a IoT na educação brasileira não deve ser vista apenas como "gadgets", mas como infraestrutura. A implementação do 5G é apontada como o catalisador necessário para que dispositivos IoT funcionem com baixa latência em sala de aula, permitindo, por exemplo, o uso de Realidade Aumentada conectada em tempo real.

4.2 O CONCEITO DE ESCOLA INTELIGENTE (*SMART SCHOOL*)

A aplicação da IoT materializa o conceito de *Smart School*. Conforme definem Lemos e Santaella (2021), trata-se de um ambiente onde o espaço físico reage às necessidades dos ocupantes. As aplicações mapeadas na literatura nacional incluem:

Gestão de Ativos e Energia: Sensores que desligam luzes e ar-condicionado em salas vazias, cruciais para a economia de recursos em escolas públicas com orçamentos limitados (SILVA; ALMEIDA, 2024).

Controle de Acesso e Frequência: Uso de etiquetas RFID (*Radio Frequency Identification*) em uniformes ou carteirinhas estudantis para automatizar a chamada, integrando os dados diretamente ao sistema da secretaria de educação e notificando os pais sobre a entrada e saída dos alunos.

Laboratórios Conectados: Experimentos de física e química onde sensores coletam dados (pH, temperatura, velocidade) e enviam gráficos em tempo real para os smartphones dos alunos, modernizando o ensino de ciências (OLIVEIRA et al., 2023).

4.3 REGULAÇÃO E PROTEÇÃO DE DADOS: A LGPD NO CHÃO DA ESCOLA

A coleta passiva de dados pela IoT, onde o aluno muitas vezes não sabe que está sendo monitorado, cria atritos diretos com a LGPD.

A Lei n.º 13.709/2018 classifica dados biométricos (faciais, impressões digitais) como dados sensíveis (Art. 5º, II). O tratamento desses dados requer bases legais robustas.

Segundo Doneda (2022), o uso de reconhecimento facial ou wearables em escolas brasileiras não pode se basear apenas no "consentimento" dos pais, dada a assimetria de poder na relação escola-família. É necessário provar o "legítimo interesse" ou a execução de políticas públicas, sem ferir os direitos fundamentais.

A Autoridade Nacional de Proteção de Dados (ANPD) tem sinalizado cautela. Estudos jurídicos recentes (MENDES; SOUZA, 2024) alertam que escolas que utilizam IoT sem protocolos rigorosos de segurança da informação (criptografia, controle de acesso) estão sujeitas a sanções e responsabilidade civil objetiva em caso de vazamento de dados de menores.

5 DISCUSSÃO E ANÁLISE

A intersecção entre a conectividade da IoT e a realidade educacional brasileira gera um cenário de tensões dialéticas, onde a modernização administrativa colide com a precarização estrutural e os riscos aos direitos digitais.

5.1 EFICIÊNCIA VERSUS VIGILÂNCIA: O DILEMA DO PANÓPTICO DIGITAL

Dados analisados por pesquisas da Revista Brasileira de Informática na Educação (2024) indicam que a automatização de tarefas via IoT (como a chamada automática) pode recuperar até 15% do tempo de aula. Para gestores educacionais, a IoT oferece um painel de controle inédito sobre o fluxo escolar, consumo de merenda e uso de espaços.

Contudo, críticos como Amiel (2023) alertam para a naturalização da vigilância. Ao instrumentar a escola com câmeras inteligentes e sensores de rastreamento, corre-se o risco de criar um "Panóptico Digital", onde o aluno aprende, desde cedo, que ser monitorado constantemente é normal. A discussão pedagógica desloca-se da autonomia para o controle. A tecnologia, em vez de libertadora, torna-se uma ferramenta de disciplinamento comportamental automatizado.

5.2 O FOSSO DA INFRAESTRUTURA E A DESIGUALDADE

A discussão sobre IoT no Brasil é inseparável da infraestrutura de telecomunicações. O relatório TIC Educação (Cetic.br, 2023) aponta que, embora a maioria das escolas tenha acesso à internet, a qualidade da conexão é insuficiente para suportar um ecossistema de IoT.

Enquanto escolas privadas de elite em capitais como São Paulo e Rio de Janeiro implementam laboratórios maker com sensores Arduino e impressoras 3D conectadas, escolas rurais e periféricas sofrem com conexões instáveis de baixa velocidade.

A análise dos dados sugere que, sem a efetivação de políticas como a Estratégia Nacional de Escolas Conectadas, a IoT servirá como um acelerador de desigualdades. Cria-se um cenário de "Apartheid de Conectividade":

De um lado, alunos que interagem com o mundo físico-digital, desenvolvendo competências para a Indústria 4.0.

De outro, alunos excluídos da literacia digital material, limitados ao consumo passivo de conteúdo em telas pequenas.

5.3 A SEGURANÇA COMO CALCANHAR DE AQUILES

Dispositivos de IoT são historicamente conhecidos por vulnerabilidades de segurança (senhas padrão, falta de atualizações). Inserir esses dispositivos em redes escolares, que guardam dados acadêmicos e pessoais sensíveis, aumenta exponencialmente a superfície de ataque para cibercriminosos. No Brasil, onde a cultura de segurança da informação nas escolas ainda é incipiente, isso representa um risco crítico. Um ataque *ransomware* que sequestre o sistema de gestão de uma escola através de um sensor de temperatura vulnerável não é um cenário de ficção científica, mas uma possibilidade técnica real discutida por especialistas em segurança da RNP (Rede Nacional de Ensino e Pesquisa).

6 CONCLUSÃO

A análise realizada permite concluir que a Internet das Coisas representa uma evolução inevitável, porém crítica, para a infraestrutura educacional brasileira. As tecnologias desenvolvidas e testadas entre 2020 e 2025 demonstram capacidade real de otimizar a gestão de recursos (água, energia, merenda) e de enriquecer a experiência de aprendizado prático (STEAM).

Contudo, a "revolução" da IoT nas escolas brasileiras esbarra em dois grandes obstáculos: a desigualdade estrutural e a imaturidade na cultura de proteção de dados.

A literatura e a legislação nacional (LGPD) indicam que a escola é um ambiente de dados sensíveis. A eficiência administrativa não pode se sobrepor à privacidade dos estudantes. Conclui-se que a adoção de IoT não deve ser guiada pelo tecnocionismo (a tecnologia pela tecnologia), mas por projetos pedagógicos claros que justifiquem a coleta de dados.

O futuro da IoT na educação brasileira não depende apenas da compra de sensores, mas da garantia de conectividade robusta (fibra/5G) para a rede pública e da formação de gestores capazes de lidar com a governança desses novos fluxos de informação.

7 CONSIDERAÇÕES FINAIS

A trajetória percorrida ao longo deste estudo revela que a integração da Internet das Coisas na educação brasileira é um processo em disputa, situado entre a promessa de modernização e o risco de exclusão.

Não se trata apenas de conectar objetos, mas de conectar saberes e garantir direitos. A visão de uma "Escola Inteligente" deve ser, antes de tudo, a visão de uma escola humana, onde a tecnologia serve ao bem-estar da comunidade e não apenas ao controle métrico.

7.1 O DESAFIO DA SOBERANIA DE DADOS

Um ponto crucial que emerge é a questão da soberania nacional sobre os dados educacionais. Muitos dispositivos IoT utilizam plataformas em nuvem hospedadas fora do Brasil. É imperativo questionar: para onde vão os dados comportamentais das crianças brasileiras? A dependência de soluções proprietárias estrangeiras pode comprometer a segurança estratégica nacional a longo prazo. Políticas de incentivo ao desenvolvimento de hardware e software nacional para IoT educacional são urgentes.

7.2 SUSTENTABILIDADE E LIXO ELETRÔNICO

A massificação da IoT traz consigo o problema do descarte. Sensores têm vida útil, baterias degradam-se. As escolas brasileiras estão preparadas para gerir o lixo eletrônico gerado por essa revolução? A educação ambiental precisa integrar o currículo tecnológico, discutindo o ciclo de vida dos objetos conectados.

7.3 O PAPEL DO EDUCADOR NO MUNDO HIPERCONECTADO

Por fim, a IoT reconfigura o papel docente. O professor deixa de ser apenas o transmissor de conteúdo para se tornar um mediador de experiências em um ambiente rico em dados. A formação docente precisa incorporar o letramento em dados (*data literacy*), capacitando o professor a interpretar os *dashboards* gerados pelos sensores e a discutir criticamente com os alunos as implicações de viver em um mundo vigiado. A tecnologia deve ser transparente, compreensível e auditável pela comunidade escolar.

7.4 AGENDA PARA PESQUISAS FUTURAS

Identificam-se lacunas para a comunidade acadêmica brasileira:

Estudos de Caso Longitudinais: Acompanhar escolas piloto com IoT para verificar se a economia de recursos (energia/água) paga o investimento na tecnologia.

Impacto Psicológico: Pesquisar como o uso de wearables e monitoramento constante afeta a sensação de liberdade e criatividade dos alunos.

Auditoria de Algoritmos em IoT: Desenvolver metodologias nacionais para verificar a segurança dos dispositivos vendidos para escolas públicas.

Em suma, a IoT na educação brasileira deve ser implementada sob o paradigma do *Privacy by Design* e da equidade social, evitando que a escola do futuro seja um privilégio de poucos.

REFERÊNCIAS

AMIEL, Tel. **Educação, vigilância e privacidade:** perspectivas críticas sobre a tecnologia na escola. Revista Brasileira de Educação, Rio de Janeiro, v. 28, 2023.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018.** Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília: Diário Oficial da União, 2018.

BRASIL. **Decreto nº 9.854, de 25 de junho de 2019.** Institui o Plano Nacional de Internet das Coisas. Brasília: Diário Oficial da União, 2019.

CETIC.BR. **Pesquisa sobre o uso das tecnologias de informação e comunicação nas escolas brasileiras: TIC Educação 2023.** São Paulo: Comitê Gestor da Internet no Brasil, 2024.

DONEDA, Danilo. **A proteção de dados pessoais de crianças e adolescentes na era digital.** Revista de Direito Civil Contemporâneo, São Paulo, v. 30, 2022.

LEMONS, André; SANTAELLA, Lucia. **Internet das Coisas e a nova ordem dos objetos.** São Paulo: Estação das Letras e Cores, 2021.

MENDES, L. S.; SOUZA, C. A. P. **Responsabilidade civil e proteção de dados nas escolas: desafios da IoT.** Revista dos Tribunais, São Paulo, v. 1045, 2024.

OLIVEIRA, G. H.; SILVA, M. A.; COSTA, R. F. **Internet das Coisas no ensino de ciências: experiências com sensores de baixo custo.** Revista Brasileira de Ensino de Ciência e Tecnologia, Curitiba, v. 16, n. 2, 2023.

SBC (Sociedade Brasileira de Computação). **Grandes Desafios da Pesquisa em Computação no Brasil: 2020-2030.** Porto Alegre: SBC, 2023.

SILVA, F. J.; ALMEIDA, R. T. **Eficiência energética em escolas públicas através da IoT: um estudo de caso.** Revista Brasileira de Computação Aplicada, Passo Fundo, v. 16, n. 1, 2024.

VALENTE, José Armando. **A sala de aula e as tecnologias digitais: do laboratório de informática à mobilidade.** In: ALMEIDA, M. E. B. (Org.). Educação e tecnologias: novos cenários. São Paulo: EDUC, 2020.