EVENTO ON-LINE
ConBRepro
XVI CONGRESSO BRASILEIRO DE ENGENHARIA DE PRODUÇÃO
02 a 04 de dezembro de 2026
Inovação e Transformação Digital como Estratégia Competitiva nas Engenharias

Cidades inteligentes e direitos fundamentais: uma análise da integração entre human rights by design e privacy by design

Luiz Fernando Pereira Nunes
Engenharia de Produção - Universidade Tecnológica Federal do Paraná (UTFPR)
João Luiz Kovaleski
Engenharia de Produção - Universidade Tecnológica Federal do Paraná (UTFPR)
Daiane Maria De Genaro Chiroli
Engenharia Têxtil - Universidade Tecnológica Federal do Paraná (UTFPR)

Resumo: A expansão das cidades inteligentes amplia as possibilidades de eficiência na gestão urbana, mas também introduz riscos relacionados à vigilância, ao tratamento massivo de dados e à utilização de sistemas algorítmicos capazes de afetar direitos fundamentais. Diante desse cenário, este artigo analisa de que maneira a articulação entre Privacy by Design e Human Rights by Design pode contribuir para uma governança tecnológica orientada à proteção preventiva desses direitos. Adota-se abordagem qualitativa, exploratória e bibliográfico-documental, apoiada em literatura nacional e internacional, documentos institucionais e na análise ilustrativa dos programas brasileiros Smart Sampa e Muralha BH. Sustenta-se que o Privacy by Design, historicamente anterior e voltado especificamente à incorporação da privacidade à arquitetura dos sistemas, pode ser compreendido como componente de uma abordagem mais abrangente de Human Rights by Design, capaz de considerar também direitos e valores relacionados à igualdade, liberdade, não discriminação, transparência e contestabilidade. No contexto brasileiro, argumenta-se que essa articulação encontra na Lei Geral de Proteção de Dados uma importante base normativa para converter princípios jurídicos em requisitos de concepção, implementação e governança das tecnologias urbanas. Conclui-se que a integração dessas abordagens pode oferecer uma base metodológica para a proteção preventiva de direitos fundamentais em cidades inteligentes, desde que acompanhada por mecanismos efetivos de avaliação de impacto, auditoria independente, transparência, responsabilização e participação social.

Palavras-chave: Cidades inteligentes, Direitos fundamentais, *Human Rights by Design, Privacy by Design*, Proteção de dados.

Smart Cities and Fundamental Rights: an Analysis of the Integration between Human Rights by Design and Privacy by Design

Abstract: The expansion of smart cities increases opportunities for efficiency in urban management, but it also introduces risks associated with surveillance, large-scale data processing, and the use of algorithmic systems capable of affecting fundamental rights. Against this background, this article examines how the articulation between Privacy by Design and Human Rights by Design can contribute to technology governance oriented toward the preventive protection of these rights. The study adopts a qualitative, exploratory, bibliographic, and documentary approach, drawing on national and international literature, institutional documents, and an illustrative analysis of the Brazilian Smart Sampa and Muralha BH programs. It argues that Privacy by Design, historically preceding Human Rights by Design and specifically concerned with embedding privacy into system architecture, can be understood as a component of the broader Human Rights by Design approach,

which also encompasses rights and values related to equality, freedom, non-discrimination, transparency, and contestability. In the Brazilian context, the article argues that this articulation finds an important normative basis in the General Data Protection Law (LGPD) for translating legal principles into requirements for the design, implementation, and governance of urban technologies. It concludes that integrating these approaches can provide a methodological basis for the preventive protection of fundamental rights in smart cities, provided that it is accompanied by effective mechanisms for impact assessment, independent auditing, transparency, accountability, and social participation.

Keywords: *Smart cities, Fundamental rights, Human Rights by Design, Privacy by Design, Data protection*.

1. Introdução

A digitalização da gestão urbana tem transformado progressivamente a prestação de serviços públicos e as formas de interação entre cidadãos, instituições e território. Sensores, câmeras com reconhecimento facial, sistemas automatizados e painéis de dados em tempo real passaram a integrar estratégias de mobilidade, segurança, planejamento e administração urbana. Ao mesmo tempo em que essas tecnologias ampliam a capacidade de processamento de informações e oferecem novas possibilidades de eficiência administrativa, também permitem que deslocamentos, características biométricas e padrões de comportamento sejam registrados, correlacionados e analisados em escala crescente. Nesse contexto, a cidade inteligente não representa apenas um projeto de modernização tecnológica, mas envolve escolhas políticas e institucionais relacionadas ao controle e à utilização dos dados produzidos pela vida urbana (MOROZOV; BRIA, 2020). A expansão dessa infraestrutura de sensoriamento também pode favorecer a formação de perfis comportamentais sem que os indivíduos tenham plena percepção da extensão do monitoramento a que estão submetidos (BEIGUELMAN, 2021).

Esse cenário impõe desafios aos mecanismos tradicionais de proteção de direitos, especialmente quando a tutela jurídica se concentra em medidas posteriores à ocorrência da violação. Em ambientes digitais, decisões tomadas durante a concepção da arquitetura tecnológica podem determinar previamente quais dados serão coletados, por quanto tempo serão armazenados, com quem poderão ser compartilhados e de que maneira serão utilizados para classificar, identificar ou tomar decisões sobre indivíduos. A proteção dos direitos fundamentais, portanto, não pode depender exclusivamente de mecanismos reparatórios, tornando necessária também uma perspectiva preventiva, capaz de incorporar limites e garantias desde as etapas de concepção, desenvolvimento, implementação e governança dos sistemas tecnológicos.

É nesse contexto que se aproximam duas abordagens orientadas à incorporação preventiva de direitos ao design tecnológico. O *Privacy by Design*, desenvolvido por Ann Cavoukian, propõe integrar a proteção da privacidade à própria arquitetura dos sistemas, a partir de princípios como prevenção, proteção por padrão, transparência e segurança ao longo do ciclo de vida dos dados (CAVOUKIAN, 2010). Em perspectiva mais abrangente, o *Human Rights by Design* procura incorporar direitos humanos ao desenvolvimento e à governança das tecnologias digitais, buscando traduzi-los em requisitos capazes de orientar escolhas técnicas, institucionais e organizacionais (DIGITAL COOPERATION ORGANIZATION, 2025; MUNJIĆ, 2026).

Embora compartilhem uma orientação preventiva, a articulação entre essas abordagens apresenta desafios conceituais e operacionais quando aplicada às cidades inteligentes. A privacidade constitui apenas uma das dimensões potencialmente afetadas pela digitalização urbana, que também pode produzir impactos sobre liberdade, igualdade, não discriminação, transparência, autonomia e possibilidades de contestação. O desafio consiste, assim, em compreender como princípios jurídicos e direitos fundamentais podem deixar o plano predominantemente abstrato e ser traduzidos em requisitos concretos para a arquitetura e a governança das tecnologias urbanas.

A partir desse problema, questiona-se de que maneira a articulação entre *Privacy by Design* e *Human Rights by Design* pode contribuir para compatibilizar o desenvolvimento de cidades inteligentes com a proteção dos direitos fundamentais e quais são os limites práticos dessa integração. Parte-se da hipótese de que o *Privacy by Design*, historicamente

anterior e especificamente direcionado à privacidade e à proteção de dados, pode ser compreendido como uma dimensão especializada de uma abordagem mais abrangente orientada pelos direitos humanos. Em conjunto com a Lei Geral de Proteção de Dados Pessoais (LGPD), essa articulação pode oferecer fundamentos normativos e metodológicos para incorporar mecanismos preventivos à concepção e à governança das tecnologias urbanas, especialmente diante de riscos relacionados à vigilância excessiva, ao tratamento desproporcional de dados e à discriminação algorítmica. Sua efetividade, contudo, depende também de mecanismos de avaliação de impacto, transparência, auditoria, responsabilização e participação social.

A investigação adota abordagem qualitativa, exploratória e bibliográfico-documental, fundamentada em literatura nacional e internacional e em documentos normativos e institucionais relacionados às cidades inteligentes, aos direitos fundamentais, ao *Privacy by Design* e ao *Human Rights by Design*. A discussão teórica é complementada pela análise ilustrativa de iniciativas brasileiras de vigilância urbana, permitindo examinar possibilidades e limitações da aplicação dessas abordagens ao contexto nacional. O desenvolvimento parte da evolução conceitual das cidades inteligentes e de suas implicações para os direitos fundamentais, avança pelos fundamentos das abordagens de design orientadas à privacidade e aos direitos humanos e, posteriormente, examina sua integração diante da LGPD e das experiências brasileiras selecionadas.

2. Cidades Inteligentes: Conceitos, Promessas e Contradições

2.1 Da eficiência técnica à governança urbana

Não existe consenso acadêmico acerca de uma definição única de cidade inteligente. O conceito assume diferentes significados entre governos, empresas e centros de pesquisa (CARNEIRO et al., 2021). Em uma perspectiva tecnocêntrica, a inteligência urbana é associada à utilização de sensores, Internet das Coisas e sistemas de análise de dados para aumentar a eficiência de serviços como mobilidade, segurança e saneamento. Essa concepção, entretanto, é criticada quando a tecnologia passa a orientar a própria definição dos problemas urbanos, favorecendo interesses comerciais que nem sempre correspondem às necessidades da população (CARNEIRO et al., 2021).

Em uma perspectiva mais ampla, Fernández (2016) compreende a *smart city* como um imaginário sociotécnico, enquanto Morozov e Bria (2020) deslocam o debate da simples adoção tecnológica para as relações de poder que a acompanham. A questão deixa de ser apenas quais tecnologias devem ser utilizadas e passa a envolver quem as controla, quem define suas finalidades e quem exerce poder sobre os dados produzidos pela vida urbana.

Essa abordagem conduz a uma concepção humanocêntrica de cidade inteligente, na qual a tecnologia constitui instrumento de desenvolvimento urbano e deve estar associada à transparência, à participação social e à proteção dos direitos fundamentais. Assim, a inteligência de uma cidade não se mede apenas por sua capacidade de coletar e processar dados, mas também pela forma como utiliza esses recursos para atender às necessidades coletivas sem comprometer os direitos das pessoas.

2.2 Vigilância, dataificação e riscos aos direitos fundamentais

A mesma infraestrutura que otimiza serviços urbanos também possibilita o rastreamento contínuo de pessoas por meio de câmeras com reconhecimento facial, geolocalização e cruzamento de dados de aplicativos, muitas vezes sem que o cidadão perceba a extensão dessa coleta ou exerça controle efetivo sobre ela (LAPIN, 2021). Beiguelman (2021) relaciona esse fenômeno à vigilância algorítmica, inserida em dinâmicas mais amplas de exploração e controle de dados. Seus riscos ultrapassam a privacidade e alcançam a liberdade, a igualdade, a não discriminação e a transparência, especialmente quando sistemas automatizados reproduzem vieses ou adotam critérios pouco compreensíveis. A concentração dessas informações também amplia riscos de segurança, incentivando arquiteturas descentralizadas de preservação da privacidade (HUANG; SHEN, 2024). No Brasil, iniciativas como Smart Sampa e Muralha BH evidenciam essa tensão, reforçando a necessidade de incorporar a proteção dos direitos fundamentais desde a concepção das tecnologias urbanas.

3. Direitos Fundamentais na Sociedade da Informação

3.1 Dignidade humana como fundamento normativo

Os direitos fundamentais, vinculados à dignidade da pessoa humana e reconhecidos pelas constituições nacionais e pela Declaração Universal dos Direitos Humanos de 1948, constituem parâmetros essenciais para avaliar políticas de digitalização urbana, e não apenas limites considerados após a implementação das tecnologias. A digitalização amplia os desafios à sua proteção: a privacidade pode ser afetada pela coleta massiva de dados; a liberdade, pelo efeito inibidor da vigilância; a igualdade, por possíveis vieses em sistemas automatizados; e a participação social, pela limitada inserção dos cidadãos nas decisões sobre tecnologias que afetam o espaço urbano.

No Brasil, essa discussão relaciona-se à proteção jurídica da intimidade e à Lei Geral de Proteção de Dados Pessoais, que estabelece proteção específica para dados biométricos vinculados a pessoas naturais, classificados como dados pessoais sensíveis (BRASIL, 2018). No campo do design, Buchanan (2001) já defendia a centralidade da dignidade e dos direitos humanos nas práticas projetuais, perspectiva que se aproxima, sem com ele se confundir, dos fundamentos posteriormente associados ao *Human Rights by Design*.

3.2 Da proteção reativa (ex post) à proteção preventiva (ex ante)

A proteção jurídica tradicional dos direitos fundamentais opera, em grande medida, por uma lógica reativa: ocorrida a violação, busca-se identificar o responsável, reparar o dano e aplicar as medidas cabíveis. Esse modelo, embora indispensável, enfrenta limitações em ambientes algorítmicos, nos quais a identificação dos agentes e do nexo entre decisões automatizadas e seus efeitos pode tornar-se mais complexa (AHMAD; ALI; YUSSOF, 2025). Munjić (2026) destaca que a opacidade dos sistemas e a fragmentação da responsabilidade entre diferentes atores reforçam a necessidade de mecanismos preventivos de governança incorporados à própria arquitetura tecnológica, perspectiva associada ao *rights-by-design*.

A proteção preventiva, contudo, não substitui os mecanismos tradicionais de responsabilização e reparação. As perspectivas ex ante e ex post são complementares: a primeira procura antecipar e reduzir riscos durante a concepção e operação dos sistemas, enquanto a segunda permanece necessária diante de violações efetivamente ocorridas. Ahmad, Ali e Yussof (2025) também apontam desafios impostos pela automação de decisões em áreas como contratação, crédito e atuação policial, evidenciando a necessidade de mecanismos capazes de operacionalizar direitos no próprio desenvolvimento tecnológico. Nesse cenário, ganham relevância as abordagens de design orientadas à proteção de valores e direitos.

4. *Privacy by Design*: Fundamentos e Princípios

4.1 Origem e os sete princípios fundacionais

O conceito de *Privacy by Design* foi desenvolvido por Ann Cavoukian na década de 1990, a partir da compreensão de que os instrumentos legais e regulatórios, isoladamente, não seriam suficientes para responder à crescente complexidade das tecnologias da informação (CAVOUKIAN, 2012). A proposta consiste em incorporar a privacidade de forma preventiva à própria concepção e arquitetura dos sistemas, em vez de tratá-la apenas como requisito de conformidade verificado após sua implementação (CAVOUKIAN, 2010). O modelo organiza-se em sete princípios fundamentais: proatividade e prevenção; privacidade como padrão; privacidade incorporada ao design; funcionalidade plena e soma positiva; segurança de ponta a ponta; visibilidade e transparência; e respeito à privacidade do usuário (CAVOUKIAN, 2010), sistematizados na Tabela 1.

Tabela 1 – Os sete princípios fundacionais do Privacy by Design

Nº	Princípio	Descrição síntese
1	Proativo, não reativo; preventivo	Antecipa e previne, em vez de remediar depois.
2	Privacidade como configuração padrão	Proteção máxima automática, sem exigir ação do indivíduo.
3	Privacidade incorporada ao design	Parte integrante da arquitetura e das práticas de negócio.
4	Funcionalidade plena – soma positiva	Acomoda privacidade e outros interesses de forma não excludente.

5	Segurança de ponta a ponta	Segurança desde a coleta até o descarte.
6	Visibilidade e transparência	Componentes e práticas visíveis e verificáveis.
7	Respeito pela privacidade do usuário	Consentimento, acesso e mecanismos de reclamação.

Fonte: elaborado pelo autor com base em Cavoukian (2010).

4.2 Aplicações em ambientes urbanos inteligentes

Cavoukian (2011; 2012) sustenta que a proteção da privacidade não deve ser compreendida como obstáculo à inovação, mas orientada por uma lógica de "soma positiva", na qual diferentes objetivos podem coexistir sem que a privacidade seja necessariamente sacrificada. A partir desses princípios, propõe-se sua aplicação às tecnologias urbanas por meio de decisões de arquitetura e governança, como minimização da coleta de dados, definição de prazos de retenção, descarte seguro, transparência sobre áreas monitoradas e mecanismos de contestação.

O *Privacy by Design*, contudo, concentra-se primordialmente na privacidade e na proteção de dados pessoais, enquanto as tecnologias urbanas podem afetar um conjunto mais amplo de direitos, como liberdade, igualdade, não discriminação e garantias relacionadas às decisões automatizadas. Essa ampliação do enfoque conduz ao *Human Rights by Design*, que estende a lógica preventiva do design à proteção mais abrangente dos direitos humanos.

5. Human Rights by Design: da Ética Aplicada à Arquitetura de Sistemas

5.1 Conceito e genealogia

O *Human Rights by Design* pode ser compreendido como uma abordagem voltada à incorporação dos direitos humanos desde a concepção e o desenvolvimento das tecnologias digitais, estendendo essa proteção à sua implementação e governança (DIGITAL COOPERATION ORGANIZATION, 2025; MUNJIĆ, 2026). Munjić (2026) estrutura essa abordagem como um processo de tradução dos direitos em três etapas: tradução normativa, incorporação institucional e garantia operacional, esta última apoiada em mecanismos de monitoramento e remediação (MUNJIĆ, 2026; DIGITAL COOPERATION ORGANIZATION, 2025), conforme representado na Figura 1. A tradução de direitos específicos em requisitos técnicos concretos constitui, por sua vez, uma aplicação desenvolvida neste trabalho.

Figura 1 – Pipeline de tradução de direitos humanos em requisitos de design



Fonte: elaborado pelo autor com base em Munjić (2026).

O rights-by-design não se confunde com o privacy-by-design isoladamente considerado, já que os direitos afetados por sistemas de Inteligência Artificial em contextos urbanos envolvem transparência, não discriminação, privacidade e contestabilidade (MUNJIĆ, 2026), o que sustenta a posição, defendida neste artigo, de que o Privacy by Design funciona como uma das dimensões de um projeto mais amplo.

5.2 Direitos humanos como requisitos de design: Design for Values

O *Design for Values*, de Aizenberg e Van den Hoven (2020), busca aproximar valores abstratos dos direitos humanos das decisões concretas de projeto, traduzindo princípios como dignidade, liberdade, igualdade e solidariedade em requisitos aplicáveis aos sistemas tecnológicos. Essa abordagem procura evitar a "armadilha do formalismo", na qual valores são reconhecidos apenas no plano normativo, sem produzir efeitos concretos sobre o

desenvolvimento da tecnologia. Essa perspectiva também dialoga com a ideia de "aumentação da inteligência" apresentada por Zhou et al. (2023), segundo a qual sistemas de inteligência artificial devem ampliar as capacidades humanas de decisão, em vez de simplesmente substituí-las.

5.3 Experiências correlatas: *Ethics by Design*, *Dignity by Design* e *Child Rights by Design*

O *Human Rights by Design* insere-se em um conjunto de abordagens que compartilham a incorporação de valores e direitos desde a concepção das tecnologias. Entre elas, o *Ethics by Design* diferencia a integração de princípios éticos ao próprio desenvolvimento tecnológico da ética relacionada ao seu uso posterior (DAINOW; BREY, 2021). O *Child Rights by Design* direciona essa lógica à proteção dos direitos de crianças e adolescentes em ambientes digitais (5RIGHTS FOUNDATION, 2023; HENRIQUES; HARTUNG, 2021), enquanto o *Dignity by Design* enfatiza a dignidade humana como princípio orientador do ambiente construído (INSTITUTE FOR HUMAN RIGHTS AND BUSINESS, 2019). Essas abordagens convergem ao reconhecer que valores e direitos devem influenciar as escolhas de projeto desde sua origem, e não apenas funcionar como parâmetros posteriores de avaliação.

Tabela 2 – Experiências correlatas de design orientado a direitos humanos

Abordagem	Organização / autor	Ano	Foco principal
Privacy by Design	Ann Cavoukian	2010	Proteção de dados na arquitetura de sistemas
Ethics by Design / Ethics of Use	Comissão Europeia (Dainow; Brey)	2021	Ética no desenvolvimento e uso de IA
Child Rights by Design	5Rights Foundation	2023	Direitos da criança em produtos digitais
Dignity by Design	Institute for Human Rights and Business	2019	Dignidade no ambiente construído
Rights by Design	Digital Cooperation Organization	2025	Direitos humanos em sistemas de IA
Modelo integrado de HRbD em cidades inteligentes	Sistematização proposta neste artigo	—	Aplicação à governança de tecnologias urbanas

Fonte: elaborado pelo autor (2026).

6. A Integração entre *Human Rights by Design* e *Privacy by Design* em Cidades Inteligentes

6.1 *Privacy by Design* como componente do *Human Rights by Design*

O *Privacy by Design* e o *Human Rights by Design* podem ser compreendidos como abordagens complementares de proteção preventiva. Enquanto o primeiro se concentra na privacidade e na proteção de dados pessoais, o segundo amplia essa perspectiva para outros direitos potencialmente afetados pelas tecnologias digitais. Por ser historicamente anterior e possuir objeto mais específico, o *Privacy by Design* pode ser compreendido como uma dimensão especializada de uma abordagem mais ampla orientada aos direitos humanos, sem que essa interpretação pressuponha uma relação genealógica entre os dois modelos.

A Tabela 3 sistematiza essa relação a partir de três categorias: convergência, complementaridade e extrapolação. Há convergência quando ambas as abordagens compartilham objetivos semelhantes, como prevenção, incorporação de direitos ao design e transparência. A complementaridade ocorre quando um princípio de privacidade precisa ser ampliado por mecanismos institucionais ou de participação. Por fim, determinadas dimensões, como não discriminação e liberdade de expressão e de reunião, extrapolam o escopo específico do *Privacy by Design* e evidenciam a abrangência adicional proporcionada pelo *Human Rights by Design*.

Tabela 3 – *Privacy by Design* e *Human Rights by Design*: convergências e extrapolações

Princípio do *Privacy by Design*	Dimensão do *Human Rights by Design*	Natureza da relação
Proatividade / prevenção	Governança preventiva e avaliação de impacto ex ante	Convergência direta
Segurança de ponta a ponta	Accountability institucional no ciclo de vida	Complementaridade
Incorporação ao design	Tradução normativa em requisitos de sistema	Convergência direta
Visibilidade e transparência	Transparência e explicabilidade algorítmica	Convergência direta
Respeito pela privacidade do usuário	Participação e vias de contestação	Complementaridade
(sem correspondente direto)	Não discriminação e mitigação de viés	Extrapolação (dimensão própria do HRbD)
(sem correspondente direto)	Liberdade de expressão e de reunião	Extrapolação (dimensão própria do HRbD)

Fonte: elaborado pelo autor com base em Cavoukian (2010) e Munjić (2026).

A comparação evidencia que a integração não depende de uma equivalência direta entre os princípios das duas abordagens. O *Privacy by Design* oferece mecanismos consolidados de prevenção relacionados ao tratamento de dados, enquanto o *Human Rights by Design* amplia a análise para impactos que não podem ser reduzidos à privacidade. Essa complementaridade permite avaliar uma tecnologia não apenas pela forma como protege os dados, mas também pelos efeitos que sua arquitetura pode produzir sobre outros direitos.

Essa diferença pode ser observada em um sistema hipotético de transporte público. Uma arquitetura orientada exclusivamente à eficiência pode coletar e armazenar grandes volumes de dados de deslocamento, permitindo rastreamento e perfilamento dos usuários. Uma arquitetura orientada por direitos, por outro lado, pode alcançar objetivos operacionais semelhantes utilizando minimização da coleta, anonimização, transparência e mecanismos independentes de controle. A Tabela 4 sintetiza como diferentes escolhas de projeto podem produzir configurações distintas a partir de uma mesma finalidade tecnológica.

Tabela 4 – Transporte público: arquitetura com e sem orientação por direitos

Sem orientação explícita por direitos	Orientada por Human Rights by Design
Rastreamento integral dos usuários	Anonimização contextual dos dados de deslocamento
Coleta excessiva de dados pessoais	Minimização da coleta ao estritamente necessário
Perfilamento comportamental sistemático	Transparência ativa sobre dados coletados e finalidades
Ausência de fiscalização externa	Auditoria contínua e independente

Fonte: elaborado pelo autor.

A Tabela 4 demonstra que a proteção de direitos não depende necessariamente da rejeição da tecnologia, mas das escolhas realizadas em sua arquitetura e governança. Técnicas como pseudonimização, k-anonimato e privacidade diferencial, combinadas a arquiteturas descentralizadas, podem contribuir para reduzir riscos de identificação e concentração de informações, preservando a utilidade dos dados para determinadas finalidades urbanas (HUANG; SHEN, 2024).

6.2 Governança algorítmica, LGPD e o caso brasileiro

No contexto brasileiro, a integração entre proteção de dados e design preventivo encontra importante fundamento normativo na Lei Geral de Proteção de Dados Pessoais. A LGPD estabelece princípios como finalidade, adequação, necessidade, transparência, segurança, prevenção, não discriminação e responsabilização, além de conferir proteção específica aos dados biométricos vinculados a pessoas naturais, classificados como dados pessoais sensíveis (BRASIL, 2018).

Alguns desses princípios apresentam aproximações relevantes com o *Privacy by Design*. A necessidade relaciona-se à minimização da coleta; a segurança, à proteção durante o ciclo de vida dos dados; a transparência, à visibilidade das práticas de tratamento; e a prevenção, à antecipação dos riscos antes da ocorrência de danos. O *Human Rights by Design* amplia essa lógica ao incorporar dimensões que ultrapassam a proteção de dados, considerando os efeitos das tecnologias sobre igualdade, liberdade, participação e não discriminação.

A relação entre LGPD, *Privacy by Design* e *Human Rights by Design* pode, portanto, ser compreendida como complementar: a legislação estabelece princípios, direitos, obrigações e mecanismos de responsabilização, enquanto as abordagens de design contribuem para traduzir essas exigências em escolhas técnicas e institucionais. Essa articulação assume especial relevância diante da expansão de tecnologias de reconhecimento facial e vigilância urbana, cujos riscos demandam mecanismos preventivos de avaliação, controle e fiscalização (LAPIN, 2021).

6.3 Aplicação ilustrativa: Smart Sampa e Muralha BH

Os programas Smart Sampa, em São Paulo, e Muralha BH, em Belo Horizonte, permitem observar de forma ilustrativa as tensões entre eficiência tecnológica, segurança pública e proteção de direitos. O Smart Sampa foi lançado com meta de integração de 40 mil câmeras e alcançava cerca de 50 mil pontos em 2025, com resultados oficialmente divulgados de 2.956 capturas de procurados, 4.170 prisões em flagrante e 195 localizações de pessoas desaparecidas (SÃO PAULO, 2025a). O Muralha BH, anunciado em 2025, prevê aproximadamente 12 mil câmeras, incluindo recursos de reconhecimento facial e leitura de placas (O TEMPO, 2025; BELO HORIZONTE, 2025).

Esses indicadores demonstram a escala e os objetivos operacionais dos programas, mas não são suficientes, isoladamente, para avaliar sua compatibilidade com direitos fundamentais. Os resultados do Smart Sampa são divulgados pela própria administração pública (SÃO PAULO, 2025a, 2025b), enquanto a literatura crítica registra questionamentos relacionados à avaliação prévia de impactos e a episódios de identificação equivocada (PONTE JORNALISMO, 2025). A Tabela 5 organiza os elementos identificados nas fontes utilizadas, diferenciando escala, tecnologia, resultados divulgados e mecanismos de controle.

Tabela 5 – Comparativo dos programas Smart Sampa e Muralha BH

Critério	Smart Sampa (São Paulo)	Muralha BH (Belo Horizonte)
Escala	40 mil previstas; ~50 mil pontos (2025)	~12 mil previstas (out. 2025)
Tecnologias	Reconhecimento facial e IA analítica	Reconhecimento facial e leitura de placas
Resultados (autodeclarados)	2.956 capturas, 4.170 prisões, 195 desaparecidos	Em implantação; sem dados consolidados
Auditoria independente	Não identificada; só interna	Não identificada; fase inicial
Avaliação prévia de impacto	Não identificada	Não identificada

Fonte: elaborado pelo autor com base em São Paulo (2025a, 2025b), Ponte Jornalismo (2025), Belo Horizonte (2025) e O Tempo (2025).

A Tabela 5 evidencia uma assimetria relevante entre a disponibilidade de indicadores operacionais e as informações relacionadas à governança e à proteção de direitos. Enquanto escala, tecnologias utilizadas e resultados de segurança são divulgados de

maneira objetiva, aspectos como auditoria independente e avaliação prévia de impacto não puderam ser identificados nas fontes analisadas. Essa ausência de informação não permite concluir, por si só, que tais mecanismos inexistam, mas limita a possibilidade de avaliar externamente a adequação dos programas aos parâmetros de proteção preventiva.

Sob a perspectiva integrada de *Privacy by Design* e *Human Rights by Design*, a avaliação dessas iniciativas não deveria se restringir à quantidade de câmeras instaladas ou de ocorrências registradas. Critérios como necessidade, proporcionalidade, minimização de dados, transparência, segurança, riscos de discriminação, mecanismos de contestação e fiscalização independente também integram uma análise orientada à proteção dos direitos fundamentais.

6.4 Limites técnicos, institucionais e político-econômicos

A integração entre *Privacy by Design* e *Human Rights by Design* oferece instrumentos para antecipar riscos, mas encontra limitações técnicas, institucionais e político-econômicas. No plano técnico, a complexidade e a opacidade de determinados sistemas algorítmicos podem dificultar auditorias e a compreensão dos critérios empregados em decisões automatizadas, especialmente em instituições com limitada capacidade técnica.

No plano institucional, existe o risco de que a incorporação de direitos ao design se converta em procedimento meramente formal, sem influência efetiva sobre as decisões tecnológicas. Aizenberg e Van den Hoven (2020) discutem esse problema a partir da denominada “armadilha do formalismo”, enquanto Munjić (2026) destaca a importância de mecanismos capazes de transformar princípios normativos em requisitos efetivamente incorporados às estruturas institucionais. No contexto brasileiro, assimetrias técnicas entre fornecedores de tecnologia e administrações públicas podem ampliar esse desafio (LAPIN, 2021).

No plano político-econômico, decisões sobre tecnologias urbanas também são influenciadas por interesses comerciais, modelos de contratação e relações de poder entre governos, empresas e cidadãos. Morozov e Bria (2020) demonstram que a governança das cidades inteligentes não pode ser dissociada do controle sobre infraestruturas e dados. *Privacy by Design* e *Human Rights by Design*, portanto, podem fortalecer a proteção preventiva dos direitos fundamentais, mas não substituem fiscalização independente, capacidade institucional, responsabilização, participação social e controle democrático sobre as tecnologias urbanas.

7. Considerações Finais

A digitalização das cidades amplia possibilidades de eficiência administrativa, integração de serviços e utilização estratégica de dados, mas também modifica as condições em que direitos fundamentais são exercidos e protegidos. Sistemas de reconhecimento facial, infraestruturas de sensoriamento e mecanismos automatizados de análise demonstram que decisões aparentemente técnicas podem produzir consequências sobre privacidade, liberdade, igualdade, não discriminação e autonomia. Nesse cenário, a proteção jurídica exclusivamente posterior à ocorrência do dano mostra-se insuficiente, tornando necessária sua complementação por mecanismos preventivos incorporados à própria concepção e governança das tecnologias.

A análise desenvolvida permite sustentar que *Privacy by Design* e *Human Rights by Design* constituem abordagens complementares. O *Privacy by Design*, historicamente anterior e concentrado na privacidade e na proteção de dados pessoais, oferece princípios consolidados para incorporar essas garantias à arquitetura tecnológica. O *Human Rights by Design*, por sua vez, amplia essa perspectiva ao considerar um conjunto mais abrangente de direitos potencialmente afetados pelos sistemas digitais. A relação entre ambos não pressupõe equivalência entre seus princípios nem uma relação genealógica, mas permite compreender o *Privacy by Design* como dimensão especializada de uma abordagem mais ampla de proteção preventiva orientada pelos direitos humanos.

No contexto brasileiro, essa articulação encontra importante fundamento normativo na Lei Geral de Proteção de Dados Pessoais. Princípios como finalidade, necessidade, transparência, segurança, prevenção, não discriminação e responsabilização oferecem parâmetros jurídicos que podem ser traduzidos em requisitos técnicos e institucionais. A proteção dos direitos fundamentais, entretanto, não decorre automaticamente da existência de normas ou da adoção formal de princípios de design. Sua efetividade depende de

mecanismos capazes de acompanhar todo o ciclo de vida das tecnologias, incluindo avaliação prévia de impactos, minimização de dados, transparência, auditoria independente, responsabilização, mecanismos de contestação e participação social.

A análise ilustrativa do Smart Sampa e do Muralha BH evidencia a importância dessa dimensão de governança. As fontes consultadas permitem identificar informações relacionadas à escala, às tecnologias empregadas e, no caso do Smart Sampa, aos resultados operacionais divulgados pela administração pública. Entretanto, não forneceram elementos suficientes para avaliar de maneira conclusiva aspectos como auditoria independente, avaliação prévia de impacto, proporcionalidade da retenção de dados e mecanismos de participação e contestação. Essa limitação demonstra que indicadores de eficiência operacional, isoladamente, não são suficientes para determinar a compatibilidade de uma tecnologia urbana com a proteção dos direitos fundamentais.

A principal contribuição da análise está, portanto, na sistematização da relação entre *Privacy by Design* e *Human Rights by Design* sem reduzir uma abordagem à outra ou estabelecer correspondências artificiais entre seus princípios. A integração proposta combina dimensões convergentes, complementares e específicas, permitindo deslocar a discussão da simples conformidade normativa para uma perspectiva na qual direitos possam influenciar escolhas concretas de arquitetura e governança. Mais do que perguntar se determinada tecnologia é juridicamente admissível depois de implementada, essa perspectiva introduz uma questão anterior: quais requisitos devem orientar sua concepção para prevenir violações antes que seus efeitos se materializem?

O caráter qualitativo, exploratório e bibliográfico-documental da pesquisa, contudo, estabelece limites aos resultados alcançados. Não foram realizadas auditorias técnicas, entrevistas com gestores, fornecedores ou cidadãos, nem avaliações empíricas dos sistemas analisados. Além disso, parte das informações disponíveis sobre as iniciativas brasileiras decorre de dados divulgados pelas próprias administrações responsáveis. As conclusões devem, portanto, ser compreendidas como uma sistematização teórico-analítica, e não como avaliação definitiva da conformidade ou da efetividade dos programas considerados.

Essas limitações também abrem possibilidades para pesquisas futuras. Estudos empíricos podem desenvolver e validar indicadores mensuráveis de *Human Rights by Design*, permitindo avaliar em que medida direitos fundamentais são efetivamente convertidos em requisitos técnicos e institucionais. Outra possibilidade consiste na aplicação do modelo integrado a sistemas reais de reconhecimento facial, mobilidade urbana e decisões algorítmicas no setor público, comparando diferentes arquiteturas e modelos de governança. Pesquisas futuras também podem investigar metodologias de avaliação de impacto em direitos fundamentais, mecanismos de auditoria algorítmica independente e formas de participação social capazes de incorporar cidadãos às decisões sobre tecnologias urbanas. A comparação entre diferentes cidades e marcos regulatórios nacionais constitui, ainda, caminho relevante para identificar práticas de governança que conciliem inovação, eficiência administrativa e proteção de direitos.

Construir cidades inteligentes, portanto, não significa apenas ampliar a capacidade tecnológica da administração pública. Significa definir, desde a concepção das infraestruturas digitais, quais limites orientarão a coleta de dados, quais mecanismos permitirão controlar o exercício do poder tecnológico e quais direitos permanecerão protegidos diante da busca por eficiência. A integração entre *Privacy by Design* e *Human Rights by Design* não oferece solução isolada para esses desafios, mas fornece uma perspectiva preventiva capaz de aproximar inovação tecnológica, governança e proteção de direitos. A inteligência de uma cidade, nesse sentido, não deve ser medida apenas pela quantidade de dados que consegue processar ou pela eficiência de seus sistemas, mas também por sua capacidade de utilizar a tecnologia sem comprometer a dignidade, a liberdade e os direitos das pessoas que nela vivem.

Referências

5RIGHTS FOUNDATION. **Child Rights by Design**: guidance for innovators of digital products and services used by children. London: 5Rights Foundation, 2023.

AHMAD, Nehaluddin; ALI, Aqilah Walin; YUSSOF, Mohammad Hilmy Baihaqy bin. The challenges of human rights in the era of artificial intelligence. **UUM Journal of Legal Studies**, v. 16, n. 1, p. 150-169, jan. 2025.

AIZENBERG, Evgeni; VAN DEN HOVEN, Jeroen. Designing for human rights in AI. **Big Data & Society**, v. 7, n. 2, p. 1-14, jul./dez. 2020.

BEIGUELMAN, Giselle. **Políticas da imagem**: vigilância e resistências na dataesfera. São Paulo: Ubu Editora, 2021.

BELO HORIZONTE (Cidade). Prefeitura de Belo Horizonte. **Muralha BH**. Belo Horizonte: Prefeitura de Belo Horizonte, 2025. Disponível em: https://prefeitura.pbh.gov.br/seguranca/muralha-bh. Acesso em: 19 ago. 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, DF, 15 ago. 2018.

BUCHANAN, Richard. Human dignity and human rights: thoughts on the principles of human-centered design. **Design Issues**, v. 17, n. 3, p. 35-39, 2001.

CARNEIRO, Leandro Alves et al. (org.). **Cidades inteligentes**: uma abordagem humana e sustentável. Brasília: Câmara dos Deputados, Edições Câmara, 2021. (Série Estudos Estratégicos, n. 12).

CARVALHO, Grazielle. **Cenários futuros para cidades inteligentes**. 1. ed. São Paulo: Trilha Treinamentos e Consultoria, 2019.

CAVOUKIAN, Ann. **Privacy by design**: the 7 foundational principles — implementation and mapping of fair information practices. Ontario: Information and Privacy Commissioner of Ontario, Canada, 2010.

CAVOUKIAN, Ann. **Privacy by design in law, policy and practice**: a white paper for regulators, decision-makers and policy-makers. Toronto: Information and Privacy Commissioner of Ontario, Canada, 2011.

CAVOUKIAN, Ann. Privacy by design [Leading Edge]. **IEEE Technology and Society Magazine**, v. 31, n. 4, p. 18-19, dez. 2012.

DAINOW, Brandt; BREY, Philip. **Ethics by design and ethics of use approaches for artificial intelligence**. Brussels: European Commission, Directorate-General for Research and Innovation, 2021.

DIGITAL COOPERATION ORGANIZATION. **Rights by design**: embedding human rights principles in AI systems. [S. l.]: DCO, 2025.

FERNÁNDEZ, Manu. **Descifrar las smart cities**: ¿qué queremos decir cuando hablamos de smart cities? [S. l.]: Megustaescribir, 2016.

HENRIQUES, Isabella; HARTUNG, Pedro. Children's rights by design in AI development for education. **International Review of Information Ethics**, v. 29, mar. 2021.

HUANG, Cheng; SHEN, Xuemin (Sherman). **Decentralized privacy preservation in smart cities**. Cham: Springer, 2024. (Wireless Networks).

INSTITUTE FOR HUMAN RIGHTS AND BUSINESS (IHRB). **Dignity by design**: human rights and the built environment lifecycle. London: IHRB, 2019.

LAPIN – INSTITUTO DE PESQUISA EM DIREITO E TECNOLOGIA DO RECIFE. **Vigilância automatizada**: uso de reconhecimento facial pela administração pública no Brasil. Recife: LAPIN, 2021. Disponível em: https://lapin.org.br/2021/07/07/vigilancia-automatizada-uso-de-reconhecimento-facial-pela-administracao-publica-no-brasil/. Acesso em: 19 ago. 2026.

MOROZOV, Evgeny; BRIA, Francesca. **A cidade inteligente**: tecnologias urbanas e democracia. Tradução: Humberto do Amaral. São Paulo: Boitempo, 2020.

MUNJIĆ, Janko. Rethinking human rights protection in the age of AI: from ex-post remedies to rights-by-design. **Facta Universitatis: Series Law and Politics**, v. 24, n. 1, p. 23-36, 2026.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS. **Declaração Universal dos Direitos Humanos**. Paris: ONU, 1948.

O TEMPO. BH terá sistema com reconhecimento facial e monitoramento de placas. Belo Horizonte: O Tempo, 6 out. 2025. Disponível em: https://www.otempo.com.br/cidades/2025/10/6/bh-tera-sistema-com-reconhecimento-facial-e-monitoramento-de-placas. Acesso em: 19 ago. 2026.

PONTE JORNALISMO. Sem resultados efetivos, Prefeitura já gastou mais de R$100 milhões com o Smart Sampa. São Paulo: Ponte Jornalismo, 1 out. 2025. Disponível em: https://ponte.org/sem-resultados-efetivos-prefeitura-ja-gastou-mais-de-r-100-milhoes-com-o-smart-sampa/. Acesso em: 19 ago. 2026.

SÃO PAULO (Cidade). Prefeitura de São Paulo. **Smart Sampa chega a 50 mil câmeras e já supera em 25% o previsto no programa de metas**. São Paulo: Prefeitura de São Paulo, 2025a. Disponível em: https://prefeitura.sp.gov.br/web/se/w/smart-sampa-chega-a-50-mil-cameras-e-ja-supera-em-25-o-previsto-no-programa-de-metas. Acesso em: 19 ago. 2026.

SÃO PAULO (Cidade). Prefeitura de São Paulo. **Taxa de reconhecimento facial do Smart Sampa é de 99,5%, sem registro de prisão de inocentes**. São Paulo: Prefeitura de São Paulo, 18 jun. 2025b. Disponível em: https://prefeitura.sp.gov.br/w/taxa-de-reconhecimento-facial-do-smart-sampa-e-de-99-5-sem-registro-de-prisao-de-inocentes. Acesso em: 19 ago. 2026.

ZHOU, Lina et al. From artificial intelligence (AI) to intelligence augmentation (IA): design principles, potential risks, and emerging issues. **AIS Transactions on Human-Computer Interaction**, v. 15, n. 1, p. 111-135, 2023.