



AN ETHICAL ARTIFICIAL INTELLIGENCE AND CYBER PHYSICAL SYSTEMS FRAMEWORK TO PROTECT GIRL-CHILD RIGHTS IN INDIAN SMART CITIES

Neha Tiwari^{*1}, Dr. Aaratrika Pandey², Ms. Garima Pahwa³, Ms. Asmita Patel⁴, Dr. Medha Tiwari⁵, and Ms. Pankhuri Srivastava⁶

Submission 02.04.2026 Acceptance: 02.06.2026 Publication:04.09.2026

Abstract: Rapid global urbanization, particularly in India, is fueling the expansion of smart cities that integrate AI and CPS to enhance urban living and governance. While these technological advances offer substantial benefits, they also pose complex challenges, particularly for the rights and safety of vulnerable groups, such as girl children. This document addresses the need for an ethical framework to protect the rights of girl children within the intelligent infrastructure of Indian smart cities. It presents a conceptual framework that integrates ethical principles, AI governance, and child protection mechanisms into CPS design and deployment. The approach uses doctrinal case study analysis, drawing on government data, UN reports, and international legal instruments to identify specific vulnerabilities and propose targeted interventions. The analysis considers privacy concerns, the potential for algorithmic bias, and the risk of digital exploitation, set against India's unique socio-cultural context. Furthermore, the paper outlines a methodology for assessing the ethical impact of AI/CPS technologies on children. It offers practical policy recommendations for implementation, emphasizing multi-stakeholder collaboration and a rights-based approach. The proposed framework aims to inform the development of secure, inclusive, and child-centric smart urban environments in India, ensuring that technology serves to uplift rather than jeopardize the fundamental rights of girl children.

Keywords: Ethical AI, Cyber-Physical Systems, Girl-Child Rights, Smart Cities India, Child Protection, Digital Ethics

* **Corresponding author:** Neha Tiwari, PhD scholar, School of Law, Manav Rachana University, Faridabad, Haryana, India

Email: nehavitiwari911@gmail.com ; ORCID: 0009-0000-2541-5438

² Assistant Professor, School of Law, Manav Rachana University, Faridabad, Haryana, India

³ Assistant Professor, School of Law, Manav Rachana University, Faridabad, Haryana, India

⁴ Assistant Professor, School of Law, Manav Rachana University, Faridabad, Haryana, India

⁵ Assistant Professor, Sharda University, Greater Noida, Uttar Pradesh, India

⁶ Research Scholar, Galgotias University, Greater Noida, Uttar Pradesh, India



I. Introduction

Urban centres across the globe are undergoing a transformative period, evolving into "smart cities" through the widespread integration of advanced technologies like Artificial Intelligence (AI), the Internet of Things (IoT), and Cyber-Physical Systems (CPS) (Smita Vempati, 2024; Ahmad *et al.*, 2021). These technological convergences promise enhanced efficiency in urban management, optimized public services, and improved quality of life for residents (Habibzadeh *et al.*, 2019). India, with its ambitious Smart Cities Mission, is at the forefront of this urban revolution, seeking to create sustainable and inclusive urban environments. However, the deployment of such sophisticated digital infrastructure introduces novel ethical and societal considerations, particularly concerning the protection of vulnerable groups (Toll *et al.*, 2020).

Girl children in India face multiple challenges, including issues related to safety, education, health, and protection from various forms of exploitation (Borker, 2021; Suha *et al.*, 2023). The digital sphere, while offering opportunities for connectivity and learning, also presents unique risks such as cyberbullying, exposure to inappropriate content, privacy infringements, and online predation (Livingstone and Third, 2017; Livingstone *et al.*, 2017).

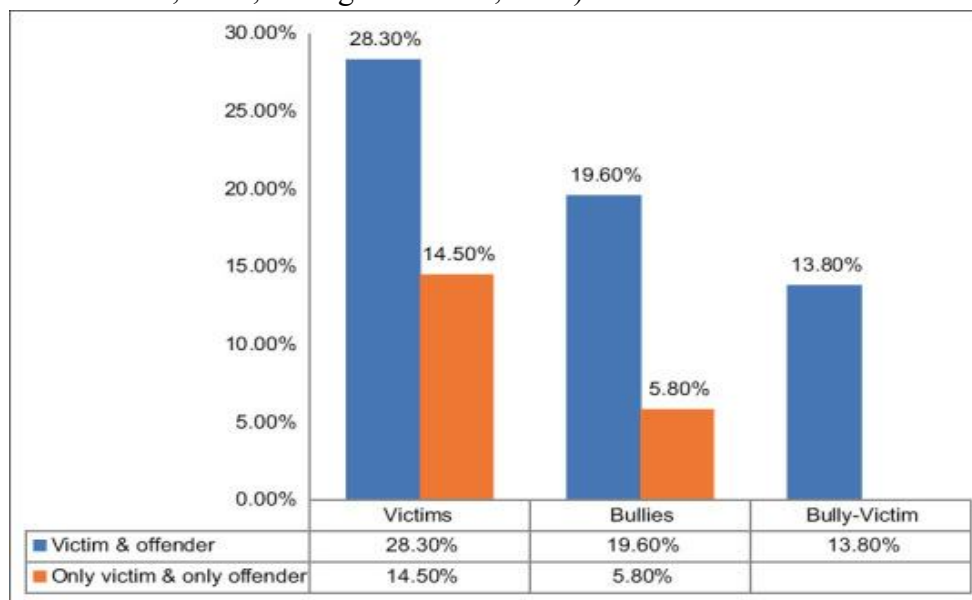


Figure 1 presents the prevalence of cyberbullying among Indian adolescents based on a study of 484 students. The findings show that 28.3% of adolescents were involved in cyberbullying in some form: 14.5% were victims, 5.8% were offenders, and 13.8% were both.

Source: From Predictors, prevalence, and patterns of cyberbullying among school-going children and adolescents, by P. J. Ranjith, M. N. Vranda, & M. T. Kishore, 2023, *Indian Journal of Psychiatry*, 65(7), 720–728. https://doi.org/10.4103/indianjpsychiatry.indianjpsychiatry_313_23



The study also reports that threatening messages via mobile phones were the most common victimisation experience, while posting hurtful comments online was the most frequent offending behaviour (James Ranjith *et al.*, 2023). When AI and CPS are embedded within the urban fabric, the scale and complexity of these risks can amplify, creating new avenues for vulnerability that traditional protection mechanisms may not adequately address. For instance, data collected by smart city sensors, if improperly managed or secured, could compromise the privacy of children. Algorithmic biases within AI systems could perpetuate or exacerbate existing societal inequalities, impacting access to services or discriminatory surveillance practices against girl children (Baeza-Yates, 2022). This research articulates a comprehensive ethical framework designed to safeguard girl-child rights within Indian smart cities. It systematically examines the intersection of AI, CPS, and child protection, drawing upon a doctrinal case study approach. The framework proposes specific design principles, architectural considerations, and policy recommendations informed by national and international legal standards, including UN conventions and child rights instruments (Roman-Urrestarazu, Kinsey and van Kessel, 2022). By integrating ethics by design, privacy by design, and child-centric approaches, this work contributes to building smart cities that are not merely technologically advanced but also socially responsible and protective of their youngest and most vulnerable citizens.

II. Literature Review

The Status of Girl-Child Rights in India

The condition of girl children in India is characterized by a complex interplay of socio-cultural norms, economic disparities, and advancements in legal protections. Despite progressive legislative measures, challenges persist across various dimensions of their rights. Educational access, while improving, still faces hurdles such as early marriage, gender-based discrimination, and lack of adequate infrastructure, particularly in rural and marginalized communities (Borker, 2021). Health outcomes for girl children are often compromised due to nutritional deficiencies and limited access to healthcare services. Protection from violence and exploitation remains a significant concern, encompassing issues like child labour, trafficking, and various forms of abuse (Suha *et al.*, 2023). The digital environment introduces additional layers of vulnerability, as children increasingly interact with online platforms without adequate safeguards (Lamsal and Gurung, 2022). Reports from national agencies, such as the National Crime Records Bureau (NCRB), consistently document instances of crimes against children, a subset of which specifically impacts girl children. These statistics underscore the ongoing need for robust protective mechanisms, particularly as urban landscapes become more technologically integrated.

AI, CPS, and Smart Cities: Global and Indian Perspectives

Smart cities represent a paradigm shift in urban development, driven by the integration of advanced digital technologies. At their core are AI and Cyber-Physical Systems (CPS), which enable the



collection, processing, and analysis of vast datasets to optimize urban functions (Smita Vempati, 2024; Habibzadeh *et al.*, 2019). These systems encompass everything from intelligent transportation and waste management to public safety and governance (Wolniak and Stecula, 2024). Globally, smart city initiatives focus on improving efficiency and sustainability. For instance, AI-driven traffic management systems reduce congestion, while IoT sensors monitor environmental quality. However, the interconnected nature of these systems also introduces cybersecurity challenges, as vulnerabilities in one component can have cascading effects across the urban infrastructure (Smita Vempati, 2024).

In the Indian context, the Smart Cities Mission aims to foster economic growth and improve local quality of life through technology-led urban transformation. This involves deploying sensor networks, AI-powered surveillance, and data analytics platforms to manage resources and enhance public services. While the benefits of such integration are clear, the specific socio-economic and infrastructural context of India presents unique considerations. For instance, the large population density, diverse cultural landscape, and varying levels of digital literacy necessitate careful consideration of how these technologies are implemented and governed. The use of AI in urban planning and service delivery, as well as the resilience of these systems against cyber threats, constitutes a significant area of discussion (Hammoumi, Maanan and Rhinane, 2024).

Challenges of Protecting Children in the Digital Age

The pervasive integration of digital media into daily life creates distinct challenges for child protection (Livingstone and Third, 2017). Children, due to their developing cognitive abilities and limited understanding of digital risks, are particularly susceptible to online harms. These include exposure to inappropriate content, cyberbullying, privacy violations, and various forms of commercial and social exploitation (Livingstone *et al.*, 2017; van der Hof *et al.*, 2020). The commercialization of play, for instance, often leverages children's data and psychological vulnerabilities to encourage in-app purchases or engagement with targeted advertising (van der Hof *et al.*, 2020). Furthermore, the collection and processing of children's data by digital platforms raise significant privacy concerns, as these data can be used for profiling and automated decision-making without adequate parental or child consent.

The psychological and behavioural effects of extensive digital technology usage on children also warrant attention, with some studies indicating potential links to aggression, reduced responsiveness, and anxiety (Lamsal and Gurung, 2022). These issues are compounded in smart city environments where children's digital footprints might expand beyond conventional online interactions to include data generated by urban sensors and surveillance systems. The interconnectedness of AI and CPS in smart cities means that a child's interaction with one system could inadvertently affect their privacy or safety across multiple domains, necessitating a holistic approach to protection.



III. Existing Legal and Policy Frameworks

International and national legal frameworks offer foundational principles for safeguarding children's rights in the digital context. The United Nations Convention on the Rights of the Child (UNCRC) provides a comprehensive human rights treaty outlining the civil, political, economic, social, health, and cultural rights of children. Specifically, UNCRC Article 16 addresses children's right to privacy, while Article 19 protects them from all forms of violence, injury, or abuse. General Comment No. 25 on children's rights in the digital environment, adopted in 2021 by the UN Committee on the Rights of the Child, further clarifies states' obligations regarding children's privacy and data protection in the digital era (Roman-Urrestarazu, Kinsey and van Kessel, 2022). This comment emphasizes a rights-based approach, balancing protection with children's capacity to maximize digital opportunities.

At a national level, India has several laws and policies aimed at child protection, including the Protection of Children from Sexual Offences (POCSO) Act, 2012, and provisions within the Information Technology Act, 2000, addressing cybercrimes. However, these legal instruments were largely conceived before the widespread deployment of AI and CPS in smart cities. Technical standards, such as the IEEE 2089–2021 standard for age-appropriate digital services, serve as a form of soft law to guide developers in designing child-safe technologies, focusing on principles like data privacy, location tracking, and ethical nudging (Michael, 2024). While these frameworks provide a basis, their application to the complex, data-intensive, and often opaque operations of AI and CPS in urban environments requires careful interpretation and adaptation.

IV. Literature Gap

While existing literature thoroughly addresses smart city technologies, AI applications, and child protection in digital spaces, a significant lacuna persists in the integrated conceptualization of ethical AI and CPS frameworks specifically tailored to safeguard girl-child rights within the Indian smart city context. Current literature often examines these domains in isolation or offers generalized ethical guidelines for AI. There is a lack of detailed exploration into how the unique vulnerabilities of girl children in India intersect with the specific functionalities and data flows of AI-driven urban systems. Most discussions on child protection in the digital environment focus on online media practices rather than the embedded, pervasive data collection and algorithmic decision-making inherent in smart city infrastructure (Livingstone and Third, 2017; Livingstone *et al.*, 2017). Furthermore, while some research touches upon the ethical implications of AI in governance, a nuanced understanding of its specific impact on gender-specific child rights, especially in a country with diverse socio-economic strata like India, remains underexplored (Toll *et al.*, 2020). This paper endeavours to bridge this gap by proposing a context-specific, rights-based, and ethically informed framework for the design, deployment, and governance of AI and CPS to ensure the protection and empowerment of girl children in India's evolving smart cities.



V. Problem Statement

The accelerated development of smart cities in India, driven by AI and Cyber-Physical Systems, while promising improved urban living, simultaneously introduces new and amplified risks to the rights and well-being of girl children. Existing child protection mechanisms and digital ethics guidelines are often inadequate to address the pervasive, interconnected, and often opaque nature of AI/CPS technologies deployed in urban environments. This creates a critical challenge: how to harness the benefits of smart city technologies while effectively mitigating their potential for privacy infringements, algorithmic discrimination, and various forms of digital and physical exploitation against girl children in India's socio-cultural landscape. A comprehensive, ethically grounded, and context-specific framework is absent, leaving girl children vulnerable to novel forms of harm within these technologically advanced urban spaces.

VI. Objectives

1. To analyse the specific vulnerabilities of girl children in India within the context of AI and Cyber-Physical Systems deployed in smart cities.
2. To delineate the core components and design principles of an ethical AI and CPS framework that prioritizes the rights and protection of girl children.
3. To assess the implications of national and international legal and policy instruments, including UN conventions, for safeguarding girl-child rights in technology-driven urban settings.
4. To identify potential ethical dilemmas and risks associated with AI/CPS implementation concerning children's rights and to propose corresponding mitigation strategies.
5. To formulate actionable deployment strategies and policy recommendations for Indian smart cities to integrate the ethical framework, fostering safe and inclusive environments for girl children.

Research Objectives for Girl-Child Protection in Smart Cities

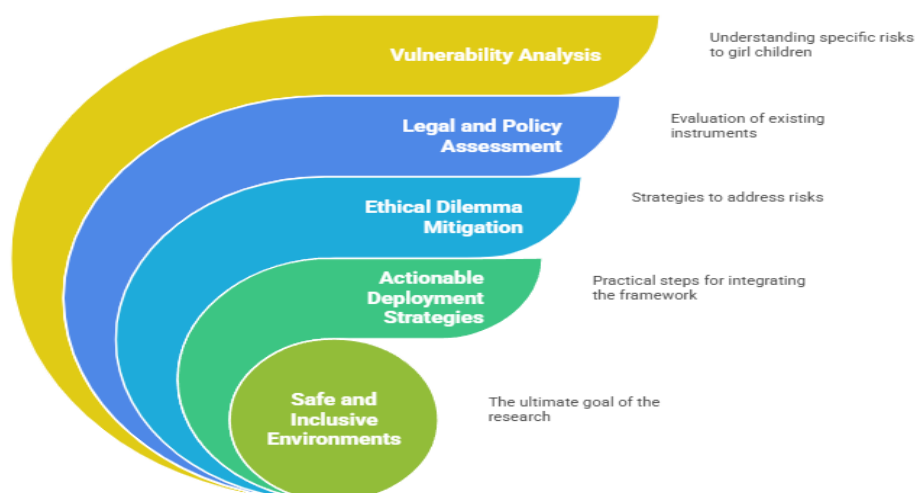




Figure 2: *showing the primary objectives guiding this research*

VII. Detailed System Explanation

The Ethical AI & CPS Framework Design

The proposed Ethical AI & CPS framework for protecting girl-child rights in Indian smart cities is predicated on a multi-layered, rights-based approach. It integrates ethical principles at every stage of the technology lifecycle, from conception and design to deployment and governance.

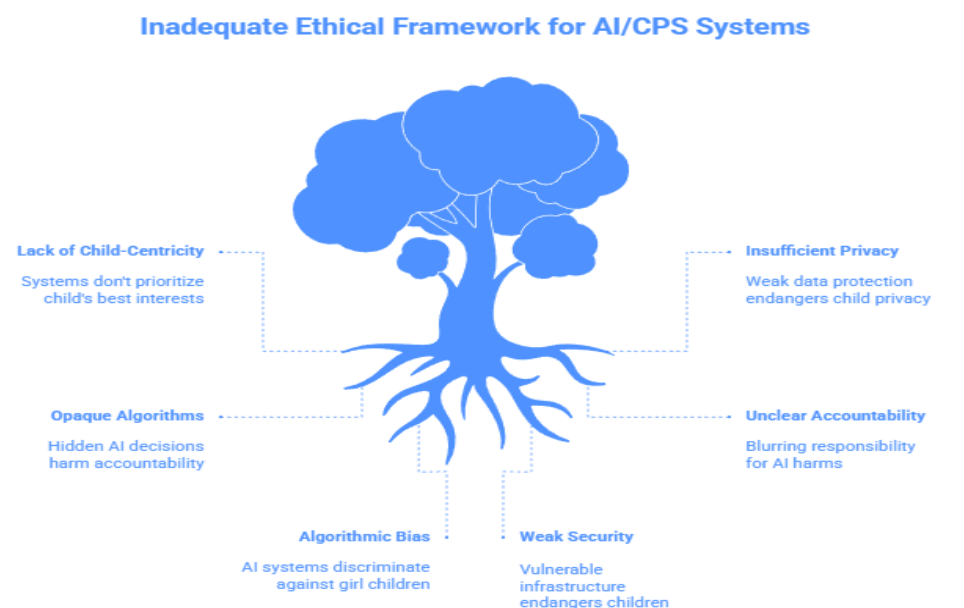


Figure 3: *showing an inadequate ethical framework for AI/CPS system*

The foundation of this framework rests upon an interlocking set of core design principles that collectively reorient AI and CPS away from being neutral tools and toward becoming proactive mechanisms for child protection and empowerment within digital urban ecosystems. The first principle, child-centricity, prioritises children's rights, welfare, and holistic development as the central axis guiding all technological choices, thus operationalising the argument of Livingstone and Third (2017) that digital systems must reflect the UNCRC's 'best interest of the child' standard. Privacy-by-design functions as a second major pillar, requiring that data flows within smart city systems from collection to retention and dissemination adhere to stringent privacy norms, minimising both the quantity and sensitivity of data collected while employing secure encryption, anonymisation, and structural safeguards to prevent misuse. Transparency and explainability constitute a third essential component, ensuring that algorithmic operations remain understandable, auditable, and accountable to regulators, parents, child protection authorities, and,



where appropriate, children themselves. This aligns with the growing ethical demand for algorithmic literacy as articulated by Baeza-Yates (2022).

Accountability forms another critical pillar, establishing unequivocal lines of responsibility among system designers, municipal authorities, technology vendors, and operating personnel. Complementing this is the commitment to non-discrimination and fairness, which requires the proactive identification and mitigation of algorithmic biases that may inadvertently reinforce social inequalities, such as those based on gender, caste, economic status, or geographical location. The final principle is security and resilience, ensuring that AI/CPS infrastructures are protected from cyberattacks, system failures, data tampering, and malicious interference, consistent with Smita Vempati's (2024) recognition of cyber vulnerabilities in high-density digital ecosystems. Ethical Impact Assessments (EIAs) serve as a central mechanism ensuring these principles are systematically implemented. They require developers and city authorities to pre-emptively analyse potential ethical harms, structural inequalities, and unintended consequences before any technological rollout, reinforcing the recommendations put forth by Michael (2024). Collectively, these principles and mechanisms constitute a deeply integrated blueprint for designing child-protective AI systems.

VIII. Architecture Overview

The architecture of the proposed framework is multilayered, interconnected, and meticulously structured to ensure that technological efficiency does not come at the cost of ethical compromise. At its foundation lies the Data Acquisition Layer, consisting of IoT sensors, surveillance cameras, biometric systems, mobility trackers, school-linked digital interfaces, and public service touchpoints. This layer is governed by highly restrictive ethical protocols determining what data may be collected, how frequently, at what resolution, and under what justifications, ensuring that child-related data is collected only when strictly necessary. The Data Processing and Analytics Layer performs the complex functions of data aggregation, pattern recognition, predictive analysis, and anomaly detection. It employs advanced AI techniques including federated learning, differential privacy, and secure computation to ensure that the data remains protected even when used across multiple analytical modalities. Bias-identification algorithms continuously scan machine learning models to detect discriminatory outcomes, reflecting the concerns raised by Baeza-Yates (2022). The CPS Control Layer translates insights into real-world actions through actuators, automated governance mechanisms, and physical infrastructures embedded across transport systems, safety networks, and public services. Ethical checks ensure that automated decisions such as emergency responses, mobility restrictions, or crowd management do not inadvertently endanger children or violate their autonomy. The Interface and Application Layer provide a human-facing dimension, offering dashboards, alerts, parental tools, child-friendly channels, and secure access controls tailored to developmental appropriateness. Finally, the Ethical



Oversight and Governance Layer functions as an overarching safety mechanism integrating regulatory compliance, cross-departmental review boards, auditing systems, accountability protocols, and independent oversight committees to ensure sustained ethical functioning across all components.

IX. Integration with Existing Smart City Infrastructure

Integrating this ethical architecture into India's smart cities, many of which were established under the Smart Cities Mission requires building atop existing capabilities while introducing a stronger rights-based dimension (Ahmad et al., 2021). The Integrated Command and Control Centres (ICCCs), already functioning as urban nerve centres, would evolve to incorporate AI-ethics modules capable of real-time evaluation of algorithmic behaviour affecting children. Child protection dashboards would allow aggregated, anonymised reporting of risk indicators, support proactive interventions while safeguard privacy. Secure data enclaves would segregate child-sensitive information behind multi-tiered authentication barriers, minimising access even among authorised personnel. Standardisation across urban departments ensures uniform protocols for data sharing, algorithmic audits, and privacy compliance. Simultaneously, capacity-building initiatives are critical: municipal officers, law enforcement personnel, health workers, educators, and technologists require sustained training on ethical AI, child safety norms, and data protection. By embedding these ethical systems within existing structural and governance mechanisms, smart cities transition from being technologically driven to becoming ethically calibrated environments designed to protect and empower girl children.

X. Case Study Selection Criteria

The doctrinal case study approach necessitates careful selection of relevant cases and data sources. Selection criteria for cases within Indian smart cities would include:

- **Relevance to Girl-Child Rights:** Cases directly involving issues of safety, privacy, exploitation, or access to services for girl children.
- **AI/CPS Involvement:** Cases where AI or CPS technologies were either directly implicated in the incident or where their absence/misapplication contributed to the vulnerability.
- **Data Availability:** Cases for which official reports, judicial pronouncements, or reputable secondary data (e.g., from NCRB, Ministry of Women and Child Development, UNICEF reports) are publicly accessible.
- **Geographic Diversity:** Cases from different smart cities in India to capture regional variations in technological deployment and socio-cultural dynamics.
- **Illustrative Potential:** Cases that effectively highlight specific ethical dilemmas, policy gaps, or successful mitigation strategies related to AI/CPS and child protection.



Emphasis will be placed on cases that offer clear lessons for framework refinement and policy recommendations, rather than merely descriptive accounts. This helps ensure the analysis is actionable and contributes to practical solutions.

XI. Methodology

This study adopts a doctrinal case study approach to examine the development of an ethical Artificial Intelligence (AI) and Cyber-Physical Systems (CPS) framework for safeguarding girl-child rights in Indian smart cities. The methodology focuses on the systematic analysis of legal principles, statutes, judicial decisions, policy documents, and scholarly literature to understand the normative and regulatory landscape governing child protection in digitally enabled urban environments. The research involves a comprehensive review of national laws, including the Protection of Children from Sexual Offences (POCSO) Act, 2012, the Juvenile Justice (Care and Protection of Children) Act, 2015, the Information Technology Act, 2000, and the Digital Personal Data Protection Act, 2023, alongside international instruments such as the United Nations Convention on the Rights of the Child (UNCRC) and General Comment No. 25 on children's rights in the digital environment. Relevant judicial pronouncements from Indian courts, as well as comparative jurisprudence from other jurisdictions, are examined to assess legal responses to privacy, digital safety, and the ethical implications of emerging technologies affecting children. The study further draws upon secondary sources, including reports from the National Crime Records Bureau (NCRB), the Ministry of Women and Child Development (MWCD), UNICEF, the Office of the United Nations High Commissioner for Human Rights (OHCHR), and other reputable organizations addressing child welfare, digital harms, and smart city governance. Data collection relies exclusively on publicly available secondary materials, while data analysis employs content analysis to identify recurring themes and legal provisions, comparative analysis to evaluate alignment between Indian and international standards, gap analysis to determine deficiencies in existing legal and policy frameworks, and ethical scrutiny based on rights-based, utilitarian, and deontological perspectives. Through the synthesis of legal, policy, and ethical insights, this doctrinal approach facilitates the identification of existing protections and regulatory gaps and supports the formulation of legally grounded and ethically robust recommendations for ensuring the rights, safety, privacy, and well-being of girl children within AI-enabled smart city ecosystems.

XII. Privacy, Legal & Policy Analysis

Privacy Challenges for Girl-Children in Smart Cities

Smart cities create complex privacy challenges for girl children because of the pervasive integration of digital technologies into everyday urban environments. High-resolution cameras, biometric entry systems, continuous mobility tracking, digital school platforms, and sensor-rich public spaces collectively produce a continuous stream of granular data. This data when



aggregated can inadvertently reveal intimate details about a child's daily routines, emotional expressions, social networks, or vulnerabilities. Such extensive data collection operates largely beyond the child's understanding and often without meaningful parental consent, raising serious concerns about autonomy, developmental agency, and exposure to predatory threats (van der Hof et al., 2020). AI-driven profiling systems exacerbate these risks by merging datasets across multiple domains, allowing systems to predict behaviour, identify patterns, or classify children into risk categories. Such classifications can lead to discriminatory treatment, heightened surveillance, or exclusion from opportunities, particularly for marginalised girl children. Cybersecurity vulnerabilities intensify these risks, as breaches of centralised databases could compromise sensitive child data (Smita Vempati, 2024). Algorithmic biases embedded in AI models may disproportionately target children from lower socio-economic backgrounds, particular communities, or specific geographic regions, reinforcing inequalities (Baeza-Yates, 2022). These combined threats demonstrate the urgent need for a robust ethical and legal framework to protect girl children in digitally augmented environments.

Research Analysis Methods

This section elaborates on the specific data collection and analysis methods germane to the privacy, legal, and policy aspects of the framework, expanding on the general methodology.

For privacy analysis, the focus is on identifying how smart city technologies generate, collect, transmit, store, and process data relating to children. This involves Technical Documentation Review for examining publicly available technical specifications and privacy policies of smart city projects in India (e.g., Smart Cities Mission project documents) to understand data flows and security measures. Impact Assessments for analysing existing Data Protection Impact Assessments (DPIAs) or Privacy Impact Assessments (PIAs) conducted for smart city components, if available, to identify assessed privacy risks. Incident Reports for reviewing reports of data breaches or privacy violations, particularly those involving public sector data, to understand practical vulnerabilities.

Further, for legal and policy analysis, the methods extend to Legislative Mapping, for creating a comprehensive map of Indian laws and regulations (e.g., Digital Personal Data Protection Act, 2023, IT Act 2000, POCSO Act) that apply to data privacy, child protection, and technology governance. International Norms Integration was used to systematically integrate the provisions of the UNCRC, especially General Comment No. 25, into the analysis, identifying how these international standards translate into national obligations and policy recommendations for smart cities (Roman-Urrestarazu, Kinsey and van Kessel, 2022). Comparative Legal Research was used to analyse how other jurisdictions (e.g., EU GDPR, California Consumer Privacy Act) address child data privacy and AI ethics to derive comparative insights and best practices.



Analysis techniques applied include detailed textual analysis of legal documents, cross-referencing policy statements with actual technological deployments, and identifying discrepancies or gaps where policy has not kept pace with technological advancements.

Foreign Case Law and Comparative Statutes

Comparative legal analysis draws upon foreign case law and statutes to enrich the understanding of robust child protection in technologically advanced environments. For instance, European Union's General Data Protection Regulation provisions, particularly Article 8 concerning children's consent for information society services and the emphasis on a "child-friendly" approach to privacy notices, offer a benchmark for data protection for minors. The explicit requirement for Data Protection Impact Assessments (DPIAs) for high-risk processing activities, which would certainly include many smart city AI/CPS applications, provides a procedural safeguard. Children's Online Privacy Protection Act (COPPA) in the United States specifically regulates the online collection of personal information from children under 13 years of age, requiring verifiable parental consent. While different in scope and application, its clear age-gating and parental consent requirements provide a model for considering child-specific privacy regulations in digital services, including those integrated into smart cities. UK Information Commissioner's Office (ICO) Age-Appropriate Design Code based on the UNCRC, sets 15 standards for online services likely to be accessed by children, mandating "best interests of the child" as a primary consideration. Its principles, such as transparency, data minimization, and geolocation off by default, offer practical guidelines for designing child-safe AI/CPS in urban spaces (Michael, 2024). Jurisprudence from countries like the UK, where legal challenges have been mounted against the use of facial recognition in public spaces, highlights the privacy implications, especially for vulnerable groups like children. These cases underscore the need for strict proportionality and necessity tests when deploying such invasive technologies.

These examples illustrate how other legal systems grapple with the intersection of technology, privacy, and child rights, offering valuable insights for shaping robust legal and policy frameworks in India.

XIII. Ethical Impact Assessment

Assessment of AI & CPS Ethics in Child Protection

Ethical Impact Assessments (EIAs) are essential tools within the proposed framework, enabling systematic evaluation of AI/CPS systems before, during, and after deployment. EIAs examine ethical considerations beyond mere legal compliance, addressing concerns related to fairness, autonomy, dignity, safety, exploitation, and social justice. One major ethical concern is algorithmic bias, where AI systems trained on skewed data produce discriminatory outcomes for girl children or marginalised communities (Baeza-Yates, 2022). EIAs assess training datasets, model architectures, and decision logic to identify and mitigate such biases.



Another concern is autonomy, particularly in environments where surveillance or algorithmic nudging may curtail children's independent decision-making abilities, impacting their personal development. EIAs also examine privacy risks embedded in pervasive data collection and evaluate whether such practices violate children's dignity or expose them to exploitation. Safety threats such as predatory targeting, cyberbullying, or digital manipulation are scrutinised through the lens of digital well-being. Accountability is a significant ethical challenge, especially when responsibilities are distributed across developers, vendors, AI models, and city authorities. EIAs therefore ensure that ethical responsibilities remain traceable, transparent, and enforceable. As Toll et al. (2020) emphasise, EIAs serve as proactive mechanisms that identify ethical risks early, reducing harm and enhancing public trust in AI/CPS systems.

XIV. Potential Risks and Mitigation Strategies

Addressing the identified ethical concerns requires a combination of technical, procedural, and policy-level mitigation strategies:

- 1. Algorithmic Bias Mitigation:** AI systems perpetuate or amplify gender, caste, or socio-economic biases, leading to discriminatory outcomes for girl children. Implementation of rigorous bias detection and correction techniques during AI model development. Use diverse and representative datasets for training. Conduct regular audits of AI systems for fairness and non-discrimination. Employ explainable AI (XAI) tools to understand decision-making processes (Baeza-Yates, 2022).
- 2. Privacy Infringement:** Extensive data collection from smart city sensors and systems compromises the privacy of girl children which can be mitigated by adopting privacy by Design principles. Implementing data minimization, collecting only necessary data. Utilize anonymization and pseudonymization techniques. Employ secure multi-party computation or federated learning for sensitive data processing. Ensure robust encryption for data at rest and in transit.
- 3. Digital Exploitation and Commercialization:** AI-powered targeting or pervasive data collection facilitates commercial exploitation or online grooming of girl children. By prohibiting targeted advertising to children based on smart city data and implementing strict age-gating mechanisms where appropriate, risk can be mitigated. Development of AI systems to detect and flag suspicious online interactions or content related to child exploitation can also help. Collaborate with law enforcement and child protection agencies for rapid responses (van der Hof et al., 2020).
- 4. Lack of Accountability:** There are various ambiguity regarding responsibility for AI/CPS-induced harms. It can be reduced by establishing clear governance structures with defined roles and responsibilities for AI system developers, deployers, and operators. Implementing mandatory Ethical Impact Assessments (EIAs) and Child Rights Impact Assessments (CRIAs) with independent oversight (Michael, 2024) can develop transparent reporting mechanisms for incidents.



- 5. Undermining Autonomy and Development:** Over-surveillance or algorithmic nudges restrict children's freedom and development and hence causes issues. Balance surveillance for safety with children's right to privacy and play can be very useful to mitigate the same. Implement "safe zones" where data collection is minimised and educating children and parents about digital rights and smart city technologies to foster digital literacy programs.

These strategies collectively aim to construct a resilient and ethical ecosystem for girl children within smart cities, ensuring that technological advancements serve as tools for empowerment and protection.

XV. Deployment & Policy Recommendations

Implementation Roadmap for Indian Smart Cities

A structured implementation roadmap is essential for integrating the ethical AI & CPS framework into Indian smart cities. This roadmap should encompass several phases:

Phase 1: Awareness and Capacity Building

Conduct workshops and training programs for city planners, technologists, legal experts, and child protection agencies on AI ethics, child rights in the digital age, and smart city technologies. Develop guidelines and best practices documents, translated into local languages, outlining the ethical framework's principles. Establish multi-stakeholder committees comprising government, industry, academia, civil society, and child advocates to oversee implementation.

Phase 2: Pilot Projects and Framework Integration

Select 2-3 existing smart city projects or a new development for pilot implementation of the ethical framework. Integrate Ethical Impact Assessments (EIAs) and Child Rights Impact Assessments (CRIAs) into the project lifecycle of AI/CPS deployments. Develop and deploy child-centric design principles for new smart city applications, focusing on age-appropriateness, privacy, and safety. Introduce secure data enclaves and privacy-preserving technologies within pilot projects.

Phase 3: Scaling and Standardisation

Based on pilot project learnings, refine the ethical framework and develop standardized protocols for all smart city projects across India. Integrate child-centric ethical considerations into procurement policies for smart city technologies. Establish independent oversight bodies or expand the mandate of existing ones to monitor compliance with the ethical framework. Develop public awareness campaigns to educate citizens, especially parents and children, about their digital rights and safety in smart cities.

Phase 4: Continuous Review and Adaptation

Implement mechanisms for continuous monitoring and evaluation of the framework's effectiveness. Conduct regular reviews of emerging AI/CPS technologies to anticipate new risks and adapt the framework accordingly. Foster research and innovation in child-safe AI/CPS development, potentially through government grants or public-private partnerships.



XVI. Policy Guidelines and Best Practices

Effective deployment of the ethical framework requires concrete policy guidelines and the adoption of best practices. These recommendations are based on a synthesis of international standards and contextual needs:

- 1. Legislate Child-Centric AI Governance:** Enact specific amendments or new legislation that mandates ethical AI development and deployment for children within smart city contexts, aligning with principles of the UNCRC and General Comment No. 25 (Roman-Urrestarazu, Kinsey and van Kessel, 2022). This should include provisions for algorithmic transparency and accountability when systems impact children.
- 2. Mandate Child Rights and Privacy Impact Assessments:** Make CRIAs and DPIAs compulsory for all smart city projects involving AI/CPS that could affect children, with independent review and public reporting of findings (Michael, 2024).
- 3. Enforce Data Minimization and Purpose Limitation:** Implement strict policies ensuring that smart city systems collect only the minimum necessary data about children, for specified, legitimate purposes, with clear retention periods.
- 4. Prohibit Discriminatory Profiling:** Explicitly ban AI systems that create profiles of children for commercial exploitation or that could lead to discriminatory practices based on sensitive attributes.
- 5. Promote Digital Literacy and Empowerment:** Develop national programs for digital literacy and critical thinking for children, parents, and educators, enabling them to navigate smart city technologies safely and responsibly.
- 6. Establish Independent Oversight and Redress Mechanisms:** Create or designate an independent regulatory body with the authority to audit AI/CPS systems, investigate complaints, and provide effective redress for children whose rights are violated by smart city technologies.
- 7. Foster Multi-stakeholder Collaboration:** Encourage sustained dialogue and partnerships among government agencies, technology developers, civil society organizations, academic institutions, and international bodies to share knowledge and best practices (Ekie and Ekie, 2022).

These policy guidelines collectively aim to cultivate a resilient and protective digital ecosystem for girl children in India's evolving urban landscape, ensuring that technological progress is underpinned by ethical imperatives and human rights.

Stakeholder Engagement Strategies

Effective implementation of an ethical AI and CPS framework necessitates robust engagement with a diverse array of stakeholders. A bottom-up approach, emphasizing community involvement, yields more sustainable and contextually appropriate solutions (Ekie and Ekie, 2022). Key strategies include:

- 1. Community Consultation:** Organize regular town hall meetings, focus group discussions, and online forums with parents, guardians, local community leaders, and



children themselves to understand their concerns, perceptions, and priorities regarding smart city technologies and child safety. Employ child-friendly consultation methods to ensure children's voices are heard and incorporated into policy design, as advocated by UNCRC principles.

- 2. Collaboration with Child Rights Organizations:** Partner with national and international NGOs specializing in child protection and digital rights. These organizations possess expertise in identifying vulnerabilities and advocating for children's best interests. Involve them in the design, review, and oversight of smart city projects to ensure a rights-based perspective is maintained.
- 3. Engagement with Technology Developers and Industry:** Establish dialogues with AI and CPS developers to promote ethical design principles, privacy-by-design, and child-safe features as standard practice. Incentivize the development of responsible AI solutions through grants, recognition, or preferred procurement status for companies adhering to ethical guidelines.
- 4. Government Agencies and Policy Makers:** Facilitate inter-ministerial coordination (e.g., Ministry of Urban Development, Ministry of Women and Child Development, Ministry of Electronics and Information Technology) to ensure a unified approach to ethical AI and smart city governance. Provide policy briefs and evidence-based recommendations to inform legislative processes and regulatory frameworks.
- 5. Academic and Research Institutions:** Collaborate with universities and research centers to conduct independent ethical audits, impact assessments, and studies on the effectiveness of implemented safeguards. Foster research into new privacy-enhancing technologies and ethical AI development specifically tailored for child protection.

This comprehensive engagement model ensures that the ethical framework is not only technically sound but also socially legitimate and responsive to the real-world needs and concerns of all affected parties, particularly girl children.

XVII. Conclusion

The convergence of Artificial Intelligence and Cyber-Physical Systems within India's burgeoning smart cities presents both unprecedented opportunities for urban enhancement and significant ethical challenges, particularly for the protection of girl children. This research outlines an ethical AI & CPS framework, grounded in a doctrinal case study approach, to systematically address these concerns. The analysis reveals that while existing legal and policy instruments provide a foundational layer of protection, they often fall short in anticipating and mitigating the complex, pervasive, and often opaque risks introduced by advanced urban technologies. Privacy infringements, algorithmic biases, and new forms of digital exploitation represent substantial threats to the rights and well-being of girl children in these evolving urban environments.



The proposed framework emphasizes child-centric design, privacy by design, transparency, and accountability as non-negotiable principles. It integrates these principles into a multi-layered architectural overview, detailing how ethical considerations can be embedded from data acquisition to application interfaces within smart city infrastructure. By drawing upon national data (e.g., NCRB reports) and international standards (e.g., UNCRC General Comment No. 25), the framework offers a contextually relevant and globally informed approach. The ethical impact assessment identifies critical risks such as algorithmic discrimination and compromised autonomy, providing clear mitigation strategies. Finally, the deployment roadmap and policy recommendations call for proactive legislation, mandatory impact assessments, robust stakeholder engagement, and continuous adaptation to ensure that smart cities in India truly serve as safe and inclusive spaces for all children. Implementing this framework can help ensure that technological progress in urban development genuinely contributes to the empowerment and protection of girl children, rather than inadvertently creating new vulnerabilities.

Funding: This research received no external funding.

Acknowledgements: I would like to thank my supervisor for her valuable inputs and guidance and for her constant support throughout the work. I also acknowledge the work of the authors and scholars who have worked in this field; their literature has greatly helped and contributed to developing this study. Lastly, I extend my thanks and gratitude to my family and friends for their constant support and encouragement.

Conflicts of Interest: The authors declare no conflicts of interest.

AI Usage Statement: ChatGPT (OpenAI, GPT-5.5) and Grammarly were referred to solely for language support, including translation, grammar correction, language refinement, and improving the clarity and readability of the manuscript. No AI tool was used to determine the research methodology, legal analysis, or conclusions.

References

1. Ahmad, Md.O. *et al.* (2021) "Cyber-Physical Systems and Smart Cities in India: Opportunities, Issues, and Challenges," *Sensors*. MDPI AG. Available at: <https://doi.org/10.3390/s21227714>.
2. Baeza-Yates, R. (2022) "Ethical Challenges in AI," *Proceedings of the Fifteenth ACM International Conference on Web Search and Data Mining*. ACM. Available at: <https://doi.org/10.1145/3488560.3498370>.
3. Borker, H. (2021) "Inside a Residential Girls' Madrasa in India," *Current Anthropology*. University of Chicago Press. Available at: <https://doi.org/10.1086/714346>.
4. Ekie, J. and Ekie, T. (2022) "Delivering together: A framework for sustainable ownership of early warning and health emergency surveillance technologies in low- and middleincome



- countries,” *Journal of Public Health in Africa*. AOSIS. Available at: <https://doi.org/10.4081/jphia.2022.2168>.
5. Habibzadeh, H. *et al.* (2019) “Smart City System Design,” *ACM Computing Surveys*. Association for Computing Machinery (ACM). Available at: <https://doi.org/10.1145/3309545>.
 6. Hammoumi, L., Maanan, M. and Rhinane, H. (2024) “Characterizing Smart Cities Based on Artificial Intelligence,” *Smart Cities*. MDPI AG. Available at: <https://doi.org/10.3390/smartcities7030056>.
 7. <https://pmc.ncbi.nlm.nih.gov/articles/PMC10461578/>
 8. James Ranjith, P., Vranda, M.N. and Kishore, M.T. (2023) ‘Predictors, prevalence, and patterns of cyberbullying among school-going children and adolescents’, *Indian Journal of Psychiatry*, 65(7), pp. 720–728. [doi: 10.4103/indianjpsychiatry.indianjpsychiatry_313_23](https://doi.org/10.4103/indianjpsychiatry.indianjpsychiatry_313_23).
 9. Lamsal, A. and Gurung, G. (2022) “Impact of Digital Technology Usage on Children’s Behavior: A Case Study,” *Nepalese Journal of Business and Management Studies*. Nepal Journals Online (JOL). Available at: <https://doi.org/10.3126/njbms.v1i1.66173>.
 10. Livingstone, S. and Third, A. (2017) “Children and young people’s rights in the digital age: An emerging agenda,” *New Media & Society*. SAGE Publications. Available at: <https://doi.org/10.1177/1461444816686318>.
 11. Livingstone, S. *et al.* (2017) “Global Perspectives on Children’s Digital Opportunities: An Emerging Research and Policy Agenda,” *Pediatrics*. American Academy of Pediatrics (AAP). Available at: <https://doi.org/10.1542/peds.2016-1758s>.
 12. Lok Sabha Secretariat (India) (2024) ‘Number of Crime Cases including Rape (Girls under 18 years) Parliamentary Reply’, Annexure to Unstarred Question 1119, Lok Sabha. Available from: https://sansad.in/getFile/annex/266/AU1119_bGpZrf.pdf?source=pqars
 13. Michael, K. (2024) “Mitigating Risk and Ensuring Human Flourishing Using Design Standards: IEEE 2089–2021 an Age Appropriate Digital Services Framework for Children,” *IEEE Transactions on Technology and Society*. Institute of Electrical and Electronics Engineers (IEEE). Available at: <https://doi.org/10.1109/tts.2024.3453396>.
 14. Roman-Urrestarazu, A., Kinsey, J. and van Kessel, R. (2022) “A Bill of Children’s Digital Rights Is Required to Improve and Sustain Children’s Futures Globally,” *JAMA Pediatrics*. American Medical Association (AMA). Available at: <https://doi.org/10.1001/jamapediatrics.2022.3418>.
 15. Smita Vempati (2024) “Securing Smart Cities: A Cybersecurity Perspective on Integrating IoT, AI, and Machine Learning for Digital Twin Creation,” *Journal of Electrical Systems*. Science Research Society. Available at: <https://doi.org/10.52783/jes.3052>.



16. Suha, S.M. *et al.* (2023) “COVID-19 Risks and Vulnerabilities of Street-Connected Children: A Qualitative Study in Bangladesh,” *Journal of Social Service Research*. Informa UK Limited. Available at: <https://doi.org/10.1080/01488376.2023.2277305>.
17. Toll, D. *et al.* (2020) “Values, Benefits, Considerations and Risks of AI in Government,” *JeDEM - eJournal of eDemocracy and Open Government*. JEDEM Journal of e-Democracy and Open Government. Available at: <https://doi.org/10.29379/jedem.v12i1.593>.
18. van der Hof, S. *et al.* (2020) “The Child’s Right to Protection against Economic Exploitation in the Digital World,” *The International Journal of Children’s Rights*. Walter de Gruyter GmbH. Available at: <https://doi.org/10.1163/15718182-28040003>.
19. van Rooijen, M. *et al.* (2020) “Stakeholder engagement from problem analysis to implementation strategies for a patient-reported experience measure in disability care: A qualitative study on the process and experiences,” *Health Expectations*. Wiley. Available at: <https://doi.org/10.1111/hex.13147>.
20. Wolniak, R. and Stecula, K. (2024) “Artificial Intelligence in Smart Cities—Applications, Barriers, and Future Directions: A Review,” *Smart Cities*. MDPI AG. Available at: <https://doi.org/10.3390/smartcities7030057>.