

INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS



Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed

www.ijlra.com

DISCLAIMER

No part of this publication may be reproduced, stored, transmitted, or distributed in any form or by any means, whether electronic, mechanical, photocopying, recording, or otherwise, without prior written permission of the Managing Editor of the *International Journal for Legal Research & Analysis (IJLRA)*.

The views, opinions, interpretations, and conclusions expressed in the articles published in this journal are solely those of the respective authors. They do not necessarily reflect the views of the Editorial Board, Editors, Reviewers, Advisors, or the Publisher of IJLRA.

Although every reasonable effort has been made to ensure the accuracy, authenticity, and proper citation of the content published in this journal, neither the Editorial Board nor IJLRA shall be held liable or responsible, in any manner whatsoever, for any loss, damage, or consequence arising from the use, reliance upon, or interpretation of the information contained in this publication.

The content published herein is intended solely for academic and informational purposes and shall not be construed as legal advice or professional opinion.

**Copyright © International Journal for Legal Research & Analysis.
All rights reserved.**

ABOUT US

The *International Journal for Legal Research & Analysis (IJLRA)* (ISSN: 2582-6433) is a peer-reviewed, academic, online journal published on a monthly basis. The journal aims to provide a comprehensive and interactive platform for the publication of original and high-quality legal research.

IJLRA publishes Short Articles, Long Articles, Research Papers, Case Comments, Book Reviews, Essays, and interdisciplinary studies in the field of law and allied disciplines. The journal seeks to promote critical analysis and informed discourse on contemporary legal, social, and policy issues.

The primary objective of IJLRA is to enhance academic engagement and scholarly dialogue among law students, researchers, academicians, legal professionals, and members of the Bar and Bench. The journal endeavours to establish itself as a credible and widely cited academic publication through the publication of original, well-researched, and analytically sound contributions.

IJLRA welcomes submissions from all branches of law, provided the work is original, unpublished, and submitted in accordance with the prescribed submission guidelines. All manuscripts are subject to a rigorous peer-review process to ensure academic quality, originality, and relevance.

Through its publications, the *International Journal for Legal Research & Analysis* aspires to contribute meaningfully to legal scholarship and the development of law as an instrument of justice and social progress.

PUBLICATION ETHICS, COPYRIGHT & AUTHOR RESPONSIBILITY STATEMENT

The *International Journal for Legal Research and Analysis (IJLRA)* is committed to upholding the highest standards of publication ethics and academic integrity. All manuscripts submitted to the journal must be original, unpublished, and free from plagiarism, data fabrication, falsification, or any form of unethical research or publication practice. Authors are solely responsible for the accuracy, originality, legality, and ethical compliance of their work and must ensure that all sources are properly cited and that necessary permissions for any third-party copyrighted material have been duly obtained prior to submission. Copyright in all published articles vests with IJLRA, unless otherwise expressly stated, and authors grant the journal the irrevocable right to publish, reproduce, distribute, and archive their work in print and electronic formats. The views and opinions expressed in the articles are those of the authors alone and do not reflect the views of the Editors, Editorial Board, Reviewers, or Publisher. IJLRA shall not be liable for any loss, damage, claim, or legal consequence arising from the use, reliance upon, or interpretation of the content published. By submitting a manuscript, the author(s) agree to fully indemnify and hold harmless the journal, its Editor-in-Chief, Editors, Editorial Board, Reviewers, Advisors, Publisher, and Management against any claims, liabilities, or legal proceedings arising out of plagiarism, copyright infringement, defamation, breach of confidentiality, or violation of third-party rights. The journal reserves the absolute right to reject, withdraw, retract, or remove any manuscript or published article in case of ethical or legal violations, without incurring any liability.

DIGITAL FUTURES: REDEFINING JUVENILE JUSTICE AND FORENSICS

AUTHORED BY - DR. EKTA PANDEY, ASSISTANT PROFESSOR
(Law) Maa Vaishno Devi Educational Law College, University of Lucknow

CO-AUTHOR - PRABHA SHANKAR CHAUBEY
Student at Maa Vaishno Devi Educational Law College, University of Lucknow

Abstract

Legal systems now have to deal with new types of evidence, new categories of vulnerability, and new governance challenges as a result of the digital revolution of social life, which has also changed how crime is committed and how justice is administered.

As a result of this change, digital forensics has become essential to determining the truth, juvenile justice has had to adjust to minors who are both cybercriminals and cyber victims, and technological governance has emerged as a framework that is required to control the use of AI and data driven tools in criminal justice institutions.

This essay makes the case that an integrated paradigm that incorporates forensic dependability, child-centered legal protection, and responsible regulation of developing technologies is necessary to rethink justice in the digital age. The research demonstrates how their confluence dictates the validity of future justice systems rather than regarding these as distinct entities.

Introduction

By increasing the involvement of networks, devices, platforms, and algorithmic systems in both harmful behaviour and legal inquiry, digital technologies have changed the architecture of crime. As a result, in order to prove facts and assign blame, court systems are depending more and more on electronic records, metadata, communications logs, biometric technologies, and AI-assisted investigation techniques. The inadequacies of traditional juvenile justice frameworks, which were designed for a previous social and technological environment, have also been made clear by the increasing involvement of juveniles in cyberbullying, sextortion, hacking, online fraud, and digital victimization.

The current discussion increasingly focuses on how digital technologies should be approved, regulated, and limited rather than just whether or not they should be utilized in legal systems. Because juvenile justice is based on rehabilitation, dignity, and reintegration rather than just punishment, this dilemma becomes particularly pressing when young people are involved. Therefore, the combination of digital forensics, juvenile justice, and technology governance poses a constitutional and ethical test for contemporary legal systems in addition to a policy problem.

Research Problem and Thesis

This paper focuses on the fundamental issue that justice institutions are digitizing more quickly than its doctrinal, procedural, and ethical protections. Investigators are expected to recover and authenticate digital evidence, courts are increasingly confronted with AI-supported analysis, and juvenile justice systems must respond to technologically mediated offending without abandoning child-rights principles. However, the existing institutional and legal frameworks are still disjointed, with cyber law, child protection law, evidentiary procedure, and AI governance frequently functioning independently.

The idea put forth in this paper is that justice in the digital age should be organized around three interrelated pillars: first, strict and open digital forensic procedures; second, a distinct and rehabilitative juvenile justice approach to cyber behaviour; and third, technological governance frameworks that require AI and digital decision-support systems to be validated, monitored, transparent, and accountable. In a legal system increasingly influenced by data and technology, only such a combination model can maintain due process, child welfare, and public legitimacy.

Digital Forensics as a Justice Function

Since many modern crimes leave evidence in phones, computers, cloud storage, social media platforms, surveillance systems, and messaging apps, digital forensics has developed from a technological expertise into a fundamental judicial function. Justice today largely depends on institutions' capacity to gather, retain, analyse, and display electronic material in dependable and repeatable ways due to the increasing reliance on digital evidence. Investigation delays and a lack of specialized forensic expertise can directly undermine evidentiary integrity and impede fair adjudication, particularly in juvenile cyber cases.

Digital forensics is important for both evidence recovery and epistemic discipline since it establishes protocols for chain of custody, authenticity, integrity, and traceability. Electronic evidence is susceptible to manipulation, contamination, or exclusion in the absence of these protections, weakening the rights of both the prosecution and the defense. Therefore, forensic systems should be viewed as institutional guarantees of legal credibility in digital contexts rather than as neutral technical add-ons.

Juveniles in Digital Spaces

Juveniles are becoming more prevalent in digital justice systems as both offenders and victims, according to recent legal research on India's cybercrime scene. Cyberbullying, online fraud, hacking, identity theft, sextortion, grooming, harassment, and sexual exploitation via digital platforms are among the behaviours that have been reported. Because juveniles may need protection, accountability, and rehabilitation at the same time, this dual positioning makes the task of juvenile justice more difficult.

According to the information that is currently available, a large number of adolescent cyber offenders are between the ages of 16 and 18, and they are frequently characterized as being more tech-savvy and exposed to harmful online conduct. Girls between the ages of 12 and 17 are found to be especially susceptible to online grooming, harassment, and exploitation. These patterns show that digital-era juvenile justice must move beyond narrow delinquency models and instead address online behaviour as a mix of developmental vulnerability, technological exposure, and social context.

Limits of Existing Juvenile Justice Frameworks

Based on rehabilitative concepts, the Juvenile Justice (Care and Protection of Children) Act, 2015 prioritizes care, protection, reintegration, counselling, and social assistance over incarceration. But when it comes to significant but unconventional cybercrimes, the same framework allows minors between the ages of 16 and 18 to be tried as adults. When there is significant digital injury but the offender's maturity, intent, and comprehension are still up for debate, this ambiguity becomes very challenging.

Weak coordination between juvenile law, internet law, and investigative practice exacerbates the issue. Inadequate forensic infrastructure, inconsistent application of legal principles in cases involving children, and shortcomings in cyber literacy among law enforcement officers are all

highlighted in the literature that is currently accessible. A legal system that handles child misbehaving on the internet using structures intended for offenses committed in the real world runs the risk of both overcriminalization and under protection.

Technological Governance and Criminal Justice

The rules, regulations, oversight procedures, and institutional controls that influence the use of digital and artificial intelligence (AI) systems in legal contexts are referred to as technological governance. Four main application areas are identified in the Department of Justice's new framework for AI in criminal justice: risk assessment, forensic analysis, identification and surveillance, and predictive policing. The primary governance issue in all of these areas is not just whether AI is beneficial, but also if its application is precise, equitable, comprehensible, reviewable, and compliant with due process and human rights.

Agencies should keep AI inventories, establish clear roles, carry out thorough testing, guarantee human control, and promote transparency both before and after implementation, according to the DOJ guidelines. Because criminal adjudication entails coercive power, reputational injury, and liberty concerns, these measurements are particularly pertinent to justice systems. Therefore, inadequate governance in this area can result in constitutional harm in addition to technological errors.

The Forensic Governance Nexus

Due to the growing use of AI in forensic workflows, the convergence of digital forensics and technology governance is especially significant. Biometric comparison, mixed-sample DNA interpretation, drug tracing, and digital analysis of images, videos, and communications—including the identification of potentially AI-generated content—are examples of current applications. These techniques increase the need for dataset quality, validation, explainability, and independent auditing, even while they may also increase efficiency, reproducibility, and scale.

This implies that forensic modernization cannot be approached as a straightforward procurement issue. Evidentiary dependability depends on governance decisions on training data, mistake rates, license limitations, expert supervision, and continuous monitoring when AI is used in the creation or interpretation of evidence. Therefore, rather than treating forensic governance as a back-end administrative concern, reimagined justice in the digital age must

tackle it as a due-process issue.

Why Juveniles Need Special Protection

Due to children's unique normative status in the legal system, juvenile justice cannot simply adopt digital technologies on the same conditions as adult criminal justice. Responses to children in legal trouble must be dignified, age-sensitive, and reintegration-focused in accordance with international child rights standards and the rehabilitative rationale of juvenile law. Governance regulations must take this higher standard of care into account when using digital tools to look into, classify, or evaluate minors.

There are various ramifications to this criterion. First, child-sensitive procedures that safeguard privacy and lessen secondary harm should be used when handling digital evidence involving kids. Second, because these systems may encode prejudice, compress developmental complexity, and encourage early punitive labelling, using predictive or risk-based tools on juveniles should be done extremely carefully. Third, legal institutions must to make a distinction between teenagers' impulsive or ignorant online behaviour and organized intentional cybercrime.

Institutional Gaps

Several institutional deficiencies are revealed by the convergence examined in this research. Inadequate cyber awareness in schools, inadequately educated investigators, poor coordination between cyber cells and child protection systems, and delays in recovering admissible electronic evidence are all documented in the literature. However, the DOJ governance framework cautions that before deploying high-impact AI systems, justice agencies must have stronger regulations, greater worker training, community supervision, and clearer organizational structures.

All of these results point to the existence of both legitimacy and capacity gaps in current systems. While legitimacy gaps erode public trust by leaving automated or technologically intensive acts unregulated, capability gaps impair the actual ability to investigate and adjudicate digital harm. These mistakes are amplified in juvenile settings since they have an impact on children's growth, reputations, and long-term social integration.

Reimagining Justice

Integration, not compartmentalization, should be the foundation of a redesigned justice model for the digital age. Technological governance should guarantee that digital and AI systems continue to be transparent, reviewable, and rights-compatible; juvenile justice should offer a child entered normative framework; and digital forensics should provide disciplined evidential techniques. By itself, none of these pillars is adequate.

Practically speaking, such a model would call for explicit guidelines for AI procurement, validation, and audit in justice institutions, school-based cyber awareness programs, stronger digital-forensic capabilities, specialist juvenile cyber units, and child-specific standards for digital evidence. Additionally, significant human judgment would need to be maintained at every level when automated systems could affect classification, investigation, or decision-making. The goal is to domesticate technology within constitutional, evidential, and developmental safeguards rather than to oppose it.

Normative Implications

The basic definition of justice is altered by the merging of these domains. Fairness in a digital world depends not just on substantive legal rights but also on the governance and design of technical systems that determine what is known, verifiable, predictable, and punishable. This means that when it comes to juveniles, justice must continue to pay attention to context, maturity, reform potential, and the imbalance between institutional power and young experimentation.

Accountability is also reframed in this way. Institutions must be held responsible for both the final judgments and the technical processes that lead to them, such as vendor selections, algorithmic models, evidence processing procedures, and supervision frameworks. In this way, technology governance is now an integral aspect of justice rather than existing outside of it.

Conclusion

Analogous legal presumptions applied to digitally mediated injuries and facts cannot support justice in the digital age. Digital forensics is essential to contemporary adjudication, juvenile cyber involvement necessitates a more tailored rehabilitative response, and AI-enabled criminal justice tools require strong governance based on validation, transparency, and human

oversight, according to the available research and policy analysis. Therefore, reimagining justice necessitates a cohesive framework wherein accountable technological governance, child-centered safety, and evidential integrity function as prerequisites of legitimacy.

Select Analytical Points

- Digital evidence has become central to modern investigations, making forensic integrity a precondition of legal fairness.
- Juveniles occupy a dual role in cyber contexts as both offenders and victims, requiring responses that combine accountability with protection and rehabilitation.
- AI can enhance criminal-justice efficiency and analysis, but its use must remain bounded by testing, transparency, auditing, and human supervision.
- Child-sensitive justice in digital contexts requires more than statutory reform; it also requires institutional coordination, education, and technical capacity.

