Proceedings of the 4th International Conference on Global Politics and Socio-Humanities
DOI: 10.54254/2753-7048/2026.33336

A Study on the Judicial Determination of Online Sexual Grooming and Cyberflashing Targeting Minors

Feiran Jia

Department of Law, Chongqing University, Chongqing, China
2130891667@qq.com

Abstract. With the advancement of digital technologies, online indecency offences targeting minors have become increasingly prevalent. Due to their concealment and lack of physical contact, judicial determination faces persistent difficulties, especially in evidence collection and verification, including unclear proof of infringed legal interests, obstacles to identifying objective conduct and aggravating circumstances, challenges in verifying the offender's identity and distinguishing guilt, as well as disputes over subjective intent and mental coercion. These issues stem from the characteristics of electronic evidence, minors' cognitive and psychological limitations, and internal evaluation and accountability mechanisms. To address them, reforms should focus on improving evidence rules and institutional norms: clarifying standards for verifying legal interest infringements, specifying identification norms for objective elements, perfecting subject identity confirmation mechanisms, and refining rules for assessing subjective elements. On this basis, a complete evidence chain can be established to balance the precise protection of minors' sexual rights and the effective crackdown on such crimes.

Keywords: Virtual Indecent Assault, Protection of Minors, Cybercrime, Electronic Evidence

1. Introduction

With the arrival of the Internet era, conventional forms of criminality have migrated into cyberspace, while novel variants have simultaneously taken shape. Within criminal justice practice, the judicial determination of cyber crimes has become a prominent and persistent problem. Illustrative in this regard is cyber indecent assault on minors. As reported in the "White Paper on Juvenile Prosecution Work (2024)" issued by the Supreme People's Procuratorate in 2024 [1], among cases involving crimes against minors prosecuted in 2024, offences categorized as "rape" and "indecent assault on children" constituted nearly one half of the total. In that same dataset, cases of cyber indecent assault on minors rose by 14.1% year-on-year, displaying emergent traits—wide dissemination, heightened concealment, and continuing harm—that collectively indicate an urgent need to refine both judicial identification and criminal governance.

Within scholarship, a theoretical shift has largely been completed: determinations concerning "indecent assault" have moved from "traditional contact-based indecent assault" toward "non-contact online infringement," that is to say, "cyber indecent assault." The case of "Luo's indecent assault on a child" [2],included as Example No. 43 among guiding procuratorial examples released

© 2026 The Authors. This is an open access article distributed under the terms of the Creative Commons Attribution License 4.0 (https://creativecommons.org/licenses/by/4.0/).

DOI: 10.54254/2753-7048/2026.33336

by the Supreme People's Procuratorate, offers a representative factual pattern. Using a pseudonym, defendant Luo added Xiaoyu—a 13-year-old girl—as a friend via QQ software; during their exchanges he learned that she was a junior high school student and nevertheless employed verbal intimidation to demand nude photographs from her. After Xiaoyu refused and removed him from her QQ contacts list, Luo again pressublue her through Zhou (a schoolmate) so as to re-add her; concurrently he fabricated an additional identity ("Li"), registeblue another QQ account under that name,and added Xiaoyu once more. Thereafter—under the persona of "Li"—Luo threatened and intimidated Xiaoyu during QQ chats while continuing to apply pressure through Zhou; compelled thereby، Xiaoyu took ten nude photographs and transmitted them via QQ for Luo's viewing. Subsequently Luo threatened to publish those images online and demanded an in-person meeting at a hotel for sexual purposes, attempting to commit indecent assault; following Xiaoyu's report to police authorities، Luo was arrested en route to the hotel pursuant to their arrangement.

This matter became the first guiding case affirming criminal liability for cyber indecent assault, and it was followed by issuance of the *Interpretation on Certain Issues Concerning the Application of Law in Cases of Rape and Indecent Assault on Minors* [3] (hereinafter, "the Interpretation"), which further broadened protective coverage while formally establishing—at least at the level of adjudicative concept—the notion of cyber indecent assault within judicial practice. Yet controversies and operational difficulties remain pronounced: disputes concentrate not only upon evidence collection methods and evidentiary authentication but also upon blurblue behavioral boundaries, shifting standards for assessing coercion or compulsion and an uneven demarcation between criminalization and non-criminalization.

Anchoblue in the principle of evidence-based adjudication, this article examines practical obstacles encounteblue when courts determine cyber indecent assaults against minors, traces their underlying causes, and advances corresponding improvement pathways. The objective is threefold: addressing concrete needs arising from adjudicatory practice; strengthening China's criminal justice framework for safeguarding minors' sexual rights; and supplying theoretical as well as practical reference points for precise suppression—and accurate legal qualification—of such network-enabled offences.

2. The practical dilemmas in the judicial determination of online virtual sexual harassment of minors

First, determination of the Object of the Crime: The Concept of Legal Interest Infringement is Vague, and the Certification Standards are Difficult to Unify. The legal interest infringed by the offence of indecent assault against minors is, in essence, the minor's sexual autonomy together with physical and psychological health. Article 237 of the Criminal Law [4] establishes indecent assault on children as an independent offence, and Article 40 of the Law on the Protection of Minors [5] likewise articulates an explicit prohibition on sexual assault against minors. Yet, when contrasted with conventional forms of indecent assault involving in-person conduct, "distance" indecent assaults exhibit two salient attributes: intangibility and temporal latency. The resulting harm to protected legal interests is therefore difficult to evidence in a concrete manner; unified criteria for its proof are also absent. Scholarly commentary has underscored that such offences need not entail direct bodily contact: through online platforms, perpetrators may deceive or coerce minors into transmitting nude images or exposing private parts, thereby impairing the minor's sense of shame and undermining physical and mental health. Even so, the degree to which those legal interests are impaiblue cannot be straightforwardly corroborated by tangible evidentiary materials.From an evidentiary-collection perspective, minors' physical and psychological development remains

DOI: 10.54254/2753-7048/2026.33336

incomplete; correspondingly limited are their capacities to identify sexual misconduct and mount effective resistance. Some victims—fearful or ashamed—fail to notify guardians promptly, with the consequence that indirect indicia of psychological trauma or mental injury cannot be preserved at an early stage. Subsequent reporting does not necessarily cure this deficit: judicial authorities may still be unable to obtain evidence establishing a causal linkage between alleged psychological harm and the offending act itself. Nor can they readily isolate—with any precision—the impact attributable specifically to online indecency from influences arising from other factors.At the level of proof (certification), given that existing statutes and judicial interpretations do not delineate clear standards for determining evidence sufficient to demonstrate impairment of legal interests in this category of offence, practice tends to rely primarily on indirect materials—chat logs or private videos—to substantiate infringement facts. Such sources rarely permit accurate quantification or specification of how particular conduct harmed a minor's physical or mental health. Predictably, divergent approaches have emerged across regions and cases; judicial fairness and uniformity are thereby weakened. As indicated above regarding Luo's case involving indecent assault against a minor, prolonged fear developed after coercion into sending nude photographs; however, because no timely psychological assessment was conducted, consequential harm could only be supported through the victim's statement alone, preventing formation of a complete evidentiary chain.

Second, objective Element Determination: Lack of Behavioral Delineation Criteria and Challenges in Proving Aggravating Circumstances. The principal obstacles in the objective dimension of determination are concentrated, first, in the paucity of evidentiary support for defining the relevant conduct and, second, in the challenge of locating proof for aggravating circumstances such as "gathering a crowd." At the center lies a definitional problem: the perimeter of online remote indecent conduct resists stable delineation. Article 9 of the Interpretation does set out explicit criminalization thresholds for coercing or enticing minors to expose private parts via the internet and for carrying out obscene acts; yet its language concerning behavioral extension and aggravating factors remains comparatively indeterminate, a feature that has constrained the maturation of judicial practice.To begin with, evidence necessary for determining conduct is difficult to secure. Remote indecency is executed through networked media; accordingly, electronic materials—chat logs being paradigmatic—may be deleted or alteblue with minimal technical effort. Added to this difficulty is an institutional constraint: judicial organs frequently lack specialized capacity to preserve and authenticate digital traces, key items therefore being lost or deemed inadmissible. For borderline forms of behavior—sending pornographic images alone or engaging only in verbal sexual provocation—the adjudicative standard remains unsettled as to whether such acts qualify as "indecent" under criminal law; nor can a clear demarcation be drawn between these behaviors and ordinary sexual harassment. In Jiang's case involving indecent assault on a child [6], some victims' chat records proved irretrievable because accounts had been cancelled and histories deleted; certain infringing acts thus became practically untraceable, preventing full protection of victims' interests.

In addition, evidentiary substantiation of aggravating circumstances presents persistent difficulties. Article 237 of the Criminal Law identifies "gathering a crowd" and acting "in public places when acting publicly" as grounds for aggravated punishment; however, given virtuality and anonymity within online environments, proof corresponding to these circumstances is often elusive [7]. Group-based online indecent acts commonly take place within private groups or niche live-streaming sites. Virtual accounts impede identification not only of joint offending but also—and critically—of shablue intent among three or more participants. Meanwhile, standards used to recognize what constitutes an online public space remain inconsistent: whether live-streaming platforms and analogous venues should be treated as "public places" in the criminal-law sense has

DOI: 10.54254/2753-7048/2026.33336

not been definitively resolved. The result is that aggravating circumstances cannot be established in many cases, thereby undermining sentencing precision.

Third, identification of Perpetrators: Challenges in Identity Tracing and Culpability Assessment.

Perpetrators of online indecent acts against minors exhibit a pronounced capacity for concealment. By exploiting the internet's anonymity, offenders frequently operate under fabricated identities and virtual accounts, a practice that substantially impedes evidentiary collection aimed at establishing the perpetrator's identity [8]. Where offences are carried out by multiple individuals acting in concert, evidentiary clarity regarding the allocation of respective responsibilities is often absent. The principal difficulties are outlined below.

First, reliable identity evidence is difficult to secure. Offenders commonly use social media platforms such as QQ, WeChat, and Douyin to initiate contact with minors through false avatars and nicknames. Once the offence has been committed, accounts may be deleted immediately and login records erased, thereby severing key links in the evidentiary chain needed for attribution. Evidence capable of connecting virtual accounts to real-world identities—such as mobile phone numbers, identification numbers, IP addresses, and device information—typically must be obtained through cooperation from network platforms. Yet certain platforms present practical obstacles including short data-retention periods, incomplete datasets, and low levels of cooperation; under such conditions, judicial authorities cannot accurately ascertain perpetrators' true identities through technical means.

Second, criminal evidence is likewise difficult to obtain. In some cases involving multiple perpetrators using a single virtual account to commit indecent acts against minors (the account having been shablue), even where judicial authorities seize that account it remains challenging to determine precisely what harm was inflicted by each individual offender and what degree of responsibility each should bear. Distinguishing principal offenders from secondary participants thus becomes infeasible on the available record. From an evidentiary standpoint—as reflected in proof structures—indirect indicators such as IP addresses and network traces possess limited probative force and cannot independently function as conclusive evidence for identifying the subject's identity; absent corroboration from other evidence sources (for example), reliance on such material readily leads both to omissions in attributing criminal conduct and to evasion of criminal punishment by perpetrators. Forth, determination of Subjective Elements: Scarcity of Evidence of Criminal Intent and Difficulty in Delineating Psychological Coercion.

The central difficulty in establishing the subjective dimension of online remote indecent assault resides, on the one hand, in evidentiary obstacles to proving a "purpose of sexual stimulation" and, on the other hand, in the absence of a quantitative yardstick for assessing "mental coercion" [9]. With these two elements remaining hard to anchor, controversy recurrently arises when distinguishing between the crime of indecent assault and the crime of indecent assault against children.

To begin with, identifying a "purpose of sexual stimulation" is frequently unworkable. Earlier doctrinal understandings treated this purpose as a necessary subjective component of indecent assault; yet in practice such an internal mental state can be reached only through inference from external conduct. Conduct such as demanding nude photographs or initiating nude chats may be driven by alternative aims—profit-seeking or retaliation against others among them—and no settled criterion exists for separating those motives from sexually oriented intent. Perpetrators, moreover, commonly invoke "joking" or "curiosity" as justificatory pretexts. In Luo's case involving an indecent assault against a child, intent could therefore be affirmed only through an overall appraisal grounded in objective acts—coercing the other party to transmit nude images and requesting an in-

DOI: 10.54254/2753-7048/2026.33336

person meeting for purposes characterized as indecent. A further complication concerns "mental coercion," which resists quantification. In remote forms of indecent assault, coercive means often present themselves primarily as psychological pressure and deception rather than traditional violence-based compulsion; that structural difference makes degrees of coercion difficult to demonstrate evidentially. Although relevant Criminal Law Interpretation provisions list "deception" as one behavioral modality, whether deception should invariably be treated as constituting "coercion" remains contestable. Where adolescents appear to act "voluntarily," their decisions may nonetheless reflect defects in comprehension attributable to developmental immaturity; it is precisely this tension that underlies disputes over cases involving early-romance teenagers who exchange private photographs with one another.

3. Analysis of the causes for challenges in evidence determination in online virtual child molestation of minors

3.1. Internal factors: inherent obstacles stemming from the unique characteristics of online virtual child molestation crimes

1. Inherent Attributes of Electronic Evidence Amplify Difficulties in Collection and Authentication:

(1) The invisibility and separability of electronic evidence render the preservation of originality difficult to secure [10]. Given that such evidence exists as binary-coded data rather than a tangible physical object, extraction typically must be completed through dedicated software tools and appropriate hardware, with operations executed by trained technical personnel. Yet, within many grassroots courts, technological capacity and staffing configurations remain insufficient, such that effective electronic data extraction cannot be reliably implemented. In parallel, the informational content embodied in electronic evidence may exist independently of any particular carrier and can be migrated across media. This condition complicates efforts to anchor an "original" storage device and to demonstrate the integrated consistency of the electronic evidence. Tampering, additionally, is often highly covert: critical items may be deleted or substituted, while superficial traces are readily concealed or modified. Where hash verification and blockchain-based preservation are not performed promptly, recovery of original information becomes difficult; correspondingly, the initial state of the evidence cannot be assublue, which substantially elevates the burden of authenticity verification.

(2) The fragility of electronic evidence, coupled with its finite storage capacity, frequently results in the disappearance of material information. The continued existence of such evidence is contingent on carrier stability and effective retention within the relevant preservation period; it is also markedly shaped by external conditions, user operations, and elapsed storage time. Under Internet-based communication modalities, real-time nude live-streaming chats and synchronous messaging may vanish once a session ends or when mobile application software is deleted if content has not been promptly saved. Third parties [11]—namely social-networking and live-streaming application platforms—often retain data only for limited durations as a cost-control measure; by the time an investigative agency intervenes, critical records may already have been purged. Storage media including mobile phones and USB drives are additionally susceptible to physical damage and malware intrusion. After committing an offence, perpetrators may destroy these media or perform factory resets, thereby amplifying the probability of evidentiary loss. Although certain forms of electronic evidence can be reconstructed, successful recovery depends on residual electromagnetic traces remaining unobscublue. In operational settings, delayed collection commonly renders

DOI: 10.54254/2753-7048/2026.33336

restoration attempts ineffective: success rates are exceedingly low, with substantial portions of core evidence lost irretrievably.

(3) Difficulty in ascertaining interrelationships among electronic evidence directly impedes completion of the evidentiary chain [12]. In the present context, electronic evidence is voluminous, fragmented, and widely dispersed. Careful parsing is therefore required to extract probative points and then link them into an intelligible whole. Yet establishing such interrelationships remains exceptionally demanding. "Interrelationships" denotes the connective mapping among heterogeneous clues—network-based virtual identities and real-world individuals, IP addresses and concrete criminal conduct. Across platforms, however, data formats are non-standardized and interfaces remain closed; "data islands" thus emerge. Some platforms, privacy protection having been invoked as justification, decline full cooperation, with the result that identity-traceability chains of proof are prone to rupture. In parallel fashion, no unified standard exists for determining these interrelationships. Marginal acts—such as transmitting pornographic images or engaging in verbal provocation—exhibit varying degrees of linkage to constituent elements of crime; correspondingly divergent assessments arise regarding their associative weight. Added to this difficulty is the susceptibility of auxiliary metadata (including transmission time and location) to manipulation or tampering, a vulnerability that further erodes confidence in inferblue connections. The practical consequence is persistent difficulty in constructing a verifiable closed loop of "behavior–data–trace."

2. The unique characteristics of crimes against minors significantly exacerbate evidentiary challenges:

(1) Minors' cognitive constraints weaken the preservation of evidentiary material. Against the backdrop of developmental immaturity, minors often do not recognise non-contact online sexual advances as abusive conduct. Requests for explicit images, or sexually inappropriate verbal exchanges, may instead be construed as "normal interaction." Material inducements and emotionally manipulative tactics, vigilance having been gradually eroded, can result in minors failing to retain or document key evidence. A limited grasp of evidence-safeguarding practices further narrows the capacity to provide actionable leads, thereby generating discontinuities in the initial chain of evidence.

(2) Psychological stress that drives delayed disclosure frequently ends in evidentiary loss. Victims are commonly coerced through threats—public exposure of private information, retaliation against family members, and cognate forms of intimidation. Alongside these external pressures sit internal constraints: shame, fear, and apprehension about reprimand from guardians also shape reporting behaviour. Under such conditions, disclosure is routinely deferred for months or even years [13]. By then electronic evidence may no longer be available because platforms undertake routine clean-up operations or because perpetrators delete relevant materials. Psychological-injury evidence remains difficult to consolidate and stabilise; with time passing, the causal nexus cannot be established with precision. Time is thus afforded for perpetrators to destroy traces and obscure their identities—a dynamic that compresses the available investigative space.

(3) Language expression disorders can erode testimonial cblueibility [14]. Language and cognitive capacities still being in formation during adolescence, precise details may not be supplied —for example‹ a perpetrator's username at the time of the offence or the duration of an online exchange might not be recalled accurately. Among younger children‹ inconsistencies may emerge from blurblue distinctions between online environments and offline life‹ limited memory consolidation‹ or susceptibility to others' suggestions- Added to this is a contextual constraint: offending often unfolds within digital space rather than at a fixed physical site; consequently‹

DOI: 10.54254/2753-7048/2026.33336

adolescents frequently struggle to reconstruct events in a complete, chronologically coherent manner- These limitations impede police efforts to extract—and then preserve—decisive investigative leads.

(4) The tension between singular verbal proof and corroboration requirements has intensified evidentiary difficulties [15]. In many cases 'minors' oral statements operate as principal evidentiary material, while objective proof sufficient for cross-checking is scarce- Under these conditions, meeting the "interlocking evidence" threshold typically pursued in ordinary criminal proceedings becomes unattainable, with a closed evidentiary chain correspondingly difficult to construct. Beyond this structural constraint lies an additional complication: minors' verbal accounts—vulnerable to distortion through age-linked cognitive development patterns and memory limitations—have triggeblue heightened scrutiny standards; that elevated review threshold, intended both to safeguard victims' rights and avert miscarriages of justice, has in turn narrowed investigative activity.

(5) Obstacles stem from the concealment of criminal conduct and the resulting paucity of objective evidence. Within virtual environments, such offences occur in settings where the "scene" remains effectively hidden. Witnesses are generally absent; likewise, conventional physical traces—injury marks, fingerprints, and related indicia—do not exist. Proof of occurrence therefore depends largely on electronic data, a category of evidence that can be readily rendeblue invalid or destroyed. When perpetrators are "familiar offenders," victims may decline to report out of courtesy, thereby reducing the probability that cases will be detected. Testimonial evidence is also difficult to obtain, witnesses being reluctant or otherwise unable to provide statements.

3.2. External factors: systemic and environmental constraints in judicial practice

1. The performance-assessment orientation embedded within procuratorial organs induces distortions in both evidence collection and prosecutorial decision-making. Under a stringent internal evaluation regime—whose core indicators include the non-prosecution rate, acquittal rate, and charge-withdrawal rate, with the acquittal rate operating as a "one-vote veto"—case handling is readily pulled into an "emphasizing prosecution over evidence" logic. Where evidentiary acquisition is arduous and the factual basis remains contestable, procuratorial organs may opt for a doubtful non-prosecution disposition; as a result, numerous harmful acts are prevented from entering judicial proceedings, while associated evidence is irretrievably lost. Even when cases proceed into the judicial process, grassroots procuratorial organs typically lack the specialized technical capacity and material resources requiblue for proper fixation of electronic evidence.

With case-handling targets exerting constant pressure, investigators often forego an exhaustive examination of pivotal proof. Transfer decisions are instead made on the strength of preliminary oral statements or scattered electronic data. Supplementary investigations that would complete an evidentiary chain are not undertaken; nor are authenticity and relevance subjected to full verification. The trial stage is thereby burdened with latent risks, generating a self-reinforcing cycle: insufficient evidence collection → diminished prosecution quality → heightened difficulty in trial adjudication.

2. The evaluation and accountability mechanisms within the court system constrain the rationality of evidence determination. Internal court performance metrics and judicial accountability mechanisms narrow the scope for evidence assessment, leading judges to adopt a conservative approach in their review and adjudication:

(1) The evaluation regime for judicial efficiency has effectively elevated the evidentiary threshold. In grassroots courts, retrial and reversal rates are tied directly to judges' performance appraisals and promotion prospects. Yet the cases implicated in such metrics frequently rest on

DOI: 10.54254/2753-7048/2026.33336

intrinsically fragile proof: they depend largely on victim statements and partial electronic materials, while lacking probative physical traces closely connected to the alleged conduct as well as eyewitness testimony. The evidentiary chain, therefore, is often difficult to complete. With reversals capable of adversely affecting assessment outcomes, a stringent standard of evidence review is commonly applied; even where infringement facts could be inferblue under applicable evidentiary rules, acceptance may still be denied when the proof does not attain a "definitely sufficient" level that substantially exceeds what is requiblue in ordinary cases.

(2) The lifelong accountability regime generates a pronounced "fear of judgment." Under this judicial accountability arrangement, judges are rendeblue personally responsible, on a permanent basis, for the quality of cases they adjudicate. Yet many such cases resist evidentiary consensus—whether mental coercion occurblue or whether subjective intent was present being illustrative—and therefore require the exercise of discretion. With potential wrongful judgments in view, judges tend to privilege "unambiguous" evidentiary standards and to refrain from applying principles associated with free evaluation of evidence and experience-based reasoning. As a result, even where an underage defendant's statements appear reasonable, they cannot be treated as the sole foundation for conviction in the absence of corroborating objective evidence, leaving the case unable to achieve a decisive breakthrough.

(3) The court president indicated that the system has further intensified its administrative character. In cases involving intricate evidentiary questions, discussion and determination are required to be undertaken by the court president after a report has been submitted by the presiding judge. Greater weight is placed on considerations such as assessment-related risks and social repercussions, rather than on adjudication strictly anchored in evidentiary rules and applicable legal provisions. Even where no procedural space exists for adducing additional evidence, judges are still instructed to supplement the evidentiary record. Cases, accordingly, are frequently left pending for extended periods or claims are dismissed on grounds of insufficient proof, thereby decoupling evidentiary determination from the core logic of judicial adjudication.

4. Pathways for enhancing evidentiary standards in online sexual grooming of minors

First, clarifying the Logic of Criminal Object Identification and Strengthening Evidentiary Support for Legal Interest Violations. Establish a specialized system for preserving evidence of infringements on legal rights. Relevant units should record the entire questioning process with audio and video, strictly adhering to the "one-time questioning principle" to avoid interfering with the truthfulness of verbal evidence. For those who delay reporting, a long-term psychological tracking mechanism should be established, combining assessment data, guardian and school feedback to form a supporting chain. Certification rules for legal interest violations must be unified. Special judicial interpretations should be issued to define core types of evidence. In cases relying solely on circumstantial evidence, a "preponderance of evidence + investigative experience" model should be adopted. A case retrieval mechanism for similar offenses should be established to standardize certification criteria across jurisdictions. Second, refining Standards for Objective Elements to Address Evidentiary Challenges in Conduct and Aggravating Circumstances. The doctrinal boundaries of remote indecent conduct should be clarified. Typical manifestations may be enumerated: coercive or deceptive acts inducing minors to transmit nude photos or engage in video-based nude chatting; and compelling minors to view obscene materials via remote exposure. The analytical fulcrum lies in whether the minor's will is violated and whether the minor's sexual sense of shame is infringed. A unified mechanism should be instituted for the tracing and remediation of electronic evidence. At the grassroots level, judicial authorities should be equipped with specialized

DOI: 10.54254/2753-7048/2026.33336

equipment and personnel to enable immediate fixation of digital materials. For critical categories of electronic evidence, authenticity should be secured via hash verification and blockchain storage. Third-party platforms should be required to retain minors' data for no less than one year, with a judicial "green channel" for expedited evidence collection. Evidence thresholds for determining aggravating circumstances should be strengthened. "Group-based" circumstances are to be corroborated through group-member lists and chat logs. Live-streaming platforms directed at an unspecified majority and publicly accessible group chats fall within the category of "public space." It is also clarified that "online live-streaming of indecency" and "dissemination of a victim's private images revealing identifying information" constitute "serious circumstances. Third, Improving the Mechanisms for Identifying Criminal Subjects and Clarifying the Pathways for Identity Tracing and Liability Differentiation. Rules for differentiating criminal responsibility of co-conspirators require role-specific evidentiary reconstruction. Participants should be categorized as principal or accessory offenders based on account-management authority and leadership remarks. A responsibility-allocation rule premised on "who operates bears responsibility" should be applied. Technical evidence collection and preservation mechanisms for establishing the subject's identity should be refined. Through IP addresses, mobile phone feature codes, and QQ-number linkages, identity information should be queried. Where an account is used by multiple individuals, differentiation may proceed through cross-analysis of login timestamps, IP trajectories, and chat-language tone features. The duty of third-party platforms to assist with evidence collection should also be strengthened. Assistance obligations arise when key electronic evidence is being collected, when it is major or technically difficult, or when it implicates public interests. The platform's assistance role should be specified, and consequences for refusal to act must be stipulated. Fourth, clarifying Criteria for Determining Subjective Aspects to Resolve Disputes over Intentionality and Coercion. The presumption rule for subjective intent shall be established. The prerequisite presumption of a "purpose of sexual stimulation" for indecent assault against a child shall be abolished. Based on objective conduct—including repeated demands for nude photos, dissemination of private images, and evidence destruction—intent shall be presumed through integrated inference. The identification of "mental coercion" should rest on a threat-centred evidentiary core. Decisive materials are chat records containing threats and the victim's statements, read in conjunction with contextual factors to assess whether the conduct substantially goes against the will. "Deception" falls within "coercion," with its defining criterion being whether deceptive means capitalize on minors' cognitive deficiencies. Refine the "innocent love" exemption rule. Where an individual under 18 voluntarily transmits private images to the counterpart within an intimate relationship, and the age gap does not exceed three years, such conduct should not be characterized as criminal provided the images are not disseminated. Where dissemination occurs, conviction should proceed in accordance with law.

5. Conclusion

The recurrent incidence of online offences involving the indecent assault of minors has brought into sharp relief a structural mismatch: traditional criminal evidentiary rules do not readily satisfy the governance demands posed by contemporary cybercrime. The complexity of judicial determination arises from electronic evidence attributes, minors' physiological and psychological characteristics, and institutional features of the judicial system. Such difficulties are concentrated in the four constituent elements: unclear standards for assessing infringement of legally protected interests; obstacles to conduct identification and circumstance evaluation; problems in establishing identity and liability; and divergent conclusions on intent and mental coercion. Rectifying these problems calls for an integrated and system-level evidentiary framework. By establishing specialized evidence

DOI: 10.54254/2753-7048/2026.33336

and uniform certification mechanisms, a foundation can be laid for object-related determinations; by fine-tuning evidentiary rules for conduct and aggravating circumstances, proof burdens may be eased; by strengthening technical traceability and platform coordination, obstacles to subject identification can be reduced; and by developing objective presumption criteria, divergences over subjective elements can be narrowed. This framework adheres to evidence-based adjudication while acknowledging minors' vulnerability and the distinctive features of such cases. It helps balance the precise suppression of online indecent-assault offences and stronger protection of minors' sexual rights, providing a practical approach to improving criminal justice safeguards for minors in the digital age.

References

[1] Supreme People's Procuratorate. White Paper on Juvenile Procuratorial Work (2024) [R]. Beijing: Supreme People's Procuratorate, 2024.
[2] Supreme People's Procuratorate. Case No. 43: Luo's Case of Child Sexual Abuse [Z]. 2018.
[3] Supreme People's Court, Supreme People's Procuratorate. Interpretation on the Application of Law in Handling Cases of Rape and Child Sexual Abuse [Z]. 2023.
[4] Criminal Law of the People's Republic of China [Z]. 2020.
[5] Law of the People's Republic of China on the Protection of Minors [Z]. 2020.
[6] Supreme People's Court. Case of Jiang Chengfei's Child Sexual Abuse [Z]. 2019.
[7] Zhu Guangxing. Research on the Criminalization of Network Remote Child Sexual Abuse: An Analysis from the Perspective of Protecting Children [J]. Journal of China University of Political Science and Law, 2022(04): 206-217.
[8] Li Chuan. Normative Principles and Identification Standards of Network Remote Child Sexual Abuse Crimes [J]. Legal Forum, 2024(01): 51-62.
[9] Li Minglu, Pi Yong. The Networked Development of Child Sexual Abuse Crimes and Their Criminal Evaluation [J]. Journal of the People's Public Security University (Social Sciences Edition), 2025(05): 62-72.
[10] Zi Zhengfa. The Theory of Electronic Evidence Trace Effect and Its Application [J]. Political and Legal Forum, 2023(02): 45-58.
[11] Chu Fumin. Three Aspects of the Authenticity of Electronic Evidence: An Analysis from the Perspective of Criminal Litigation [J]. Legal Research, 2022(01): 123-138.
[12] Zi Zhengfa. The Normative Construction Theory of Third-Party Network Platform Cooperation in Electronic Evidence Extraction [J]. Dongfang Legal Studies, 2025(05): 35-46.
[13] Xiang Yan. Review on the Examination and Judgment of Victim Testimonies in Cases of Sexual Assault against Children [J]. Global Legal Review, 2018(06): 138-152.
[14] Zhang Hongwei, Yu Tianshi. On the Dilemma and Solution of Applying Verbal Evidence of Children in the Determination of "Child Sexual Abuse Crime" [J]. China Youth Social Sciences, 2021(03): 113-123.
[15] Xiang Yan. Research on Difficulties in Proving Cases of Sexual Abuse of Minors - Also Discussing the Institutional Transformation of Criminal Proving Mode from Verification to Multiple "Seeking Truth" in China [J]. Jurist, 2019(04): 160-175.