



Legal Interests Infringed by Deepfake Pornography and Criminal Law Responses

Jintao Zhao

Zhejiang A&F University, Hangzhou 311300, China

Email: 1875645135@qq.com

Abstract. The misuse of deepfake technology in the pornography sector has evolved from isolated technical pranks into targeted digital sexual violence against specific individuals. Its essence lies in the unauthorized use of artificial intelligence to produce and disseminate false pornographic imagery, thereby imposing psychological coercion and personal dignity violations within virtual spaces. Such acts inflict multiple harms on individual psychological trauma, the foundation of social trust, and legal order. Traditional criminal charges like defamation and dissemination of obscene materials for profit exhibit clear limitations in their applicability. Drawing from the non-contact harm model established in “remote indecent assault” cases, the legal protection of sexual autonomy should extend from physical safeguards to the protection of digital personas. This paper proposes a three-dimensional regulatory framework: interpretatively, expanding the purpose-based scope of the legal interest protected by the crime of insult to incorporate core wrongful acts into existing norms; legislatively, drawing on international experience to establish specialized criminal offenses; and institutionally, building coordinated domestic and international governance mechanisms. This approach aims to strike a balance between safeguarding personal dignity and promoting technological innovation.

Keywords: Deepfakes; Digital Sexual Violence; Sexual Autonomy; Criminal Regulation; Non-Contact Sexual Assault

1 Introduction

The rapid advancement of generative artificial intelligence has transformed “deepfake” technology from a theoretical concept in laboratories into a tangible reality with broad practical applications. However, this technology—originally intended for film production, digital art, and historical reenactment—has spiraled out of control in the production of pornographic content, morphing into a Damocles' sword hanging over the public, particularly women. In China, according to an investigation by the Legal Daily, a gray-market industry has emerged offering “complete tutorials for 8 yuan” and “20-second face-swapping services.” Countless individuals—from ordinary women to prominent public figures—have had their control over their own images stripped away by technology, all without their knowledge or consent.

© The Author(s) 2026

C. F. Peng et al. (eds.), *Proceedings of the 2026 5th International Conference on Humanities, Wisdom Education and Service Management (HWESM 2026)*, Advances in Social Science, Education and Humanities Research 1024,

https://doi.org/10.2991/978-2-38476-593-5_23

The core argument of this paper is that deepfake pornography does not constitute traditional defamation or public indecency offenses. Rather, it represents a form of “digital sexual violence” targeting specific individuals through technological means. Its essence lies in the systematic erosion of individual autonomy and the fundamental degradation of personal dignity. Therefore, classifying such acts as sexual offenses—achieved through interpretive expansion of existing purposes and legislative creation of distinct criminal charges—represents an inevitable response to the legal challenges of the digital age, enabling a transformative upgrade of criminal regulatory paradigms.

The article first examines the underlying technology and its rampant prevalence, revealing deepfake pornography’s nature as “digital sexual violence” and its structural harm to individuals, society, and legal order. Subsequently, it examines the application challenges of traditional offenses—such as defamation, dissemination of obscene materials for profit, and infringement of citizens’ personal information—from a doctrinal perspective, dissecting their deep-seated issues of “evaluation blind spots” and “regulatory inadequacy.” Building on this foundation, it draws upon the non-contact harm model established in “remote indecent assault” cases to argue for the legal justification of extending the protection of sexual autonomy rights from physical safeguards to digital image protection. Finally, it proposes a systematic legal response framework from three dimensions: interpretive theory, legislative theory, and international collaborative governance. Currently, both domestic and international academia have initiated preliminary discussions on criminal regulation of deepfakes. Professor Liu Xianquan advocates adding an “illegal use” category to the crime of infringing on citizens’ personal information^[1]. At the same time, Professor Chen Ran emphasizes shifting the regulatory focus to “protecting genuine sexual privacy” rather than combating “false information.”^[2] These studies provide crucial theoretical foundations for the arguments presented in this paper. However, existing work either focuses narrowly on the interpretation and application of single offenses or remains at the level of macro-level legislative advocacy, failing to develop a systematic discourse spanning from the justification of legal interests to the construction of norms. This paper seeks to fill this gap by systematically constructing the concept of “digital sexual violence” and designing multi-level regulatory pathways, thereby providing an analytical framework for the criminal governance of deepfake pornography that combines theoretical depth with practical validity.

2 Behavioral Characteristics and Multiple Harms of Deepfake Pornography

2.1 The Generative Logic of Deepfake Pornography and the Nature of Legal Rights Infringement

The term “deepfake” originated from communities on the Reddit platform^[3]. Although early related chat groups have since disbanded, the technology continues to proliferate in the realm of fabricated pornographic videos^[4]. Within cyberspace, this form of

abuse—mediated by technology and aimed at sexual humiliation—is an inevitable product of the evolution of violence in the digital age. While the anonymity afforded by digital technology grants individuals greater autonomy, it has also catalyzed the “digital transformation” of violent acts, giving rise to “digital sexual violence.” Digital sexual violence refers to acts perpetrated by individuals using technological means within cyberspace to target specific persons with the intent of sexual humiliation, infringing upon sexual autonomy and personal dignity. Requiring no physical contact, such acts can achieve precise and persistent harm through borderless dissemination, posing far greater dangers than ordinary harmful online content. Among these, virtual sexual assault centered on deepfakes represents the most typical manifestation.

Deepfake pornography can be categorized into two types: first, pornographic videos featuring fictional characters without specific targets; second, videos explicitly targeting specific individuals as victims. The former undermines social order and public morality, while the latter directly infringes upon citizens’ personal legal rights. This article focuses solely on virtual sexual assaults targeting specific individuals. Such precise digital violations necessitate redefining “individual sexual autonomy” in the digital age. Fundamentally, this act deprives individuals of control over their sexual image. Natural persons possess the exclusive right to decide the disclosure and presentation of their own sexually related images. Deepfakes illegally bind facial features to obscene scenarios, effectively “stealing” and “redrawing” an individual’s digital body. This goes beyond simple portrait infringement; it forcibly defines victims as sexual objects to be gazed upon and consumed, completely stripping them of control over their self-image. At a deeper level, such acts erode the autonomy of sexual narrative—the core right to interpret and express one’s own sexual experiences and identity. Deepfake videos function as implanted false erotic memories within cyberspace, making it difficult for victims to clarify their experiences. This leads to confusion in self-perception and damage to the integrity of their personality.

Since the emergence of self-referential face-swapped pornographic videos abroad, deepfake pornography has rapidly spread globally. According to the 2023 Deepfake Report by U.S. cybersecurity firm Security Hero, the number of deepfake videos online increased by 550% from 2019 to 2023, reaching over 95,000 instances. Among these, 98% were pornographic content, with 99% of victims being women. Countless women have been subjected to illegal synthetic imagery without their knowledge or consent. This form of “digital sexual assault” poses harm comparable to physical sexual assault^[5], and due to its uncontrollable dissemination, it inflicts more enduring and severe damage.

2.2 Structural Damage to Individuals, Society, and Legal Order Caused by Deepfake Pornography

Professor Tian Hongjie pointed out in an interview with People’s Procurator that “deepfake facial technology” possesses characteristics such as high realism, high efficiency and automation, data dependency, scalability, immediacy, and widespread accessibility^[6]. It is precisely because of its technological nature, distinct from traditional crimes, that the harm caused by deepfake pornography spreads from the indi-

vidual level to the structural level of social trust and legal order, exhibiting an inescapable systemic nature.

For victims, deepfake pornography directly violates sexual autonomy and personal dignity. Unlike traditional sexual assault that relies on physical coercion, this act employs “psychological coercion” by fabricating and disseminating false sexual imagery. Without physical contact, it forcibly fixes victims’ sexual choices—choices they never made—within public spaces, completely nullifying their right to sexual self-determination. Victims consequently suffer severe degradation of their personal dignity, experiencing psychological trauma equivalent to that of actual sexual assault. This includes feelings of stigmatization, PTSD, depression, and even suicidal tendencies, making them highly susceptible to “social death.”

Through online dissemination, individual violations can escalate into assaults on public legal interests. In South Korea’s 2024 “Nth Room 2.0” incident, numerous participants digitally superimposed familiar female faces onto obscene content, creating a form of digital “gender terrorism” targeting women. This intensified gender polarization and undermined the societal foundation of gender equality^[7]. Simultaneously, highly realistic fake content subverts the cognitive principle of “seeing is believing,” undermining “digital trust” in the information society, increasing the cost of social interaction, and eroding the bonds of trust within the social community^[8]. From a legal order perspective, when citizens’ core personal rights suffer severe digital infringement, existing criminal laws prove ineffective due to a mismatch between elements of offense and lagging legal interest assessments. This deprives victims of dual safeguards—control over their identity and legal protection—erodes public trust in the law, weakens legal authority, and risks societal disorder^[9].

3 Blind Spots in Evaluating Traditional Criminal Offenses and Regulatory Challenges

As discussed in Part I, deepfake pornography inherently constitutes digital sexual violence with severe consequences. However, under the current criminal law framework, traditional criminal charges exhibit significant “evaluation blind spots” and “regulatory inadequacies.” This stems from the fundamental disconnect between the behavioral patterns and legal interests defined by traditional offenses and the novel nature of this illegal activity.

Judicial practice often classifies it as defamation, yet defamation centers on “fabricating facts.” Traditionally, ‘facts’ refer to falsifiable declarative information, whereas deepfakes are algorithmically synthesized electronic visual symbols. Directly labeling them as “fabricated facts” deviates from their essence. From the perspective of protected legal interests, defamation protects reputation rights, whereas deepfake pornography primarily infringes upon sexual autonomy and privacy. The psychological trauma and personal degradation suffered by victims far exceed the scope of “lowered social evaluation.” Regulating such acts under defamation fails to reflect their nature as sexual offenses. The establishment of an independent criminal offense in Taiwan to address these behaviors further underscores the limitations of defamation law.

Classifying this act as the crime of producing and disseminating obscene materials for profit misaligns the legal interests at stake. This offense protects public interests and public morals, whereas deepfake pornography targeting specific individuals uses obscene content as a weapon to perpetrate precise sexual assault and psychological torment, where dissemination serves merely as a means rather than an end. Evaluating such acts solely under this offense overlooks the direct assault on individual sexual autonomy, downgrading the infringement of exclusive personal legal interests to mere disruption of public order. This approach fails to fulfill the function of criminal punishment.

Could we then shift our perspective and classify facial biometric information as sensitive personal data, thereby seeking regulatory grounds under the crime of infringing upon citizens' personal information? This crime regulates the illegal acquisition, sale, and circulation of personal information. However, the core illegality of deepfakes lies in the technical manipulation and character defamation using publicly available or legally obtained facial information—an act that transcends the scope of information crimes and directly infringes upon personal dignity and sexual autonomy. Particularly when such abuse involves complex “technical manipulation” rather than mere “provision,” applying this crime becomes strained.

4 The Criminal Law Implications and Protective Boundaries of Sexual Autonomy in the Digital Age

Traditional criminal charges prove ineffective in regulating deepfake pornography, necessitating an extension of the legal doctrine of sexual autonomy. Conventional sexual offenses are grounded in the “contact theory,” which ties sexual autonomy to physical bodies and real-world coercion. Deepfakes subvert this framework, demanding that protection extend beyond physical bodily safety to encompass control over digital sexual imagery. This extension possesses both legal justification and practical support^[10]. Whether perpetrated through physical violence or digital technology, acts aimed at sexual humiliation or psychological control infringe upon an individual's sexual autonomy and personal dignity^[11].

Traditional criminal law recognizes three tiers of sexual autonomy: the autonomous formation of sexual intent, the specific choice of sexual conduct, and the self-control of one's sexual image and narrative^[12]. Deepfake pornography circumvents the consent process, systematically undermining the latter two tiers of rights through illegal synthesis and dissemination. Unlike conventional defamation offenses, it does not primarily aim to diminish external reputation. Instead, it instrumentalizes victims as sexual objects, imposing profound psychological coercion and personal dignity violations. The resulting trauma is structurally equivalent to sexual assault, rendering it difficult to fully assess under traditional defamation statutes.

This pattern of abuse shares a highly similar legal framework with “remote sexual molestation.” Both abandon the requirement of “physical contact,” establishing “causing sexually related psychological harm” as the standard for criminal liability. Guiding cases from the Supreme People's Court explicitly state that non-physical,

online remote molestation can constitute the crime of molesting a child, shifting the criteria for recognizing sexual offenses from physical contact to the sexual significance of the act and its harmful consequences. Deepfake pornography represents a technological evolution of non-contact molestation. It operates with zero barriers to entry, has a broad scope of harm, and causes irreversible damage. Once posted online, such content persists permanently, creating an indelible “digital scar.”

Extending the protection of sexual autonomy to the digital realm has become a global legislative trend. Countries such as South Korea and the United Kingdom have independently criminalized non-consensual deepfake pornography, explicitly recognizing it as a direct violation of sexual autonomy rather than merely defamation or obscenity. In contrast, domestic cases often lack specific criminal charges, resulting in penalties limited to civil or public order offenses, with regulatory measures proving significantly inadequate.

Of course, upholding the principle of restraint in criminal law requires clarifying that criminal law targets malicious abuse, not the technology itself. Deepfakes hold positive value in legitimate domains, and criminal law should only penalize acts targeting specific individuals with intent to humiliate or demean their character. A reasonable regulatory framework should establish exemption mechanisms for consensual creations, news reporting, academic research, and similar uses, rigorously scrutinize subjective intent, and strike a balance between protecting personal dignity and fostering technological innovation.

5 Collaborative Governance Approaches from Criminal Law Interpretation to Legislation

Therefore, seeking a way forward inevitably requires a systematic response, forming a clearly structured and mutually reinforcing normative matrix that balances the flexible application of hermeneutics, the prudent construction of legislation, and the strengthening of international collaborative governance.

5.1 The Hermeneutic Approach

Article 246 of China’s Criminal Law defines the crime of insult as requiring “publicly insulting another person under serious circumstances.” Traditionally, “insulting” conduct has been understood as direct verbal abuse, defamation, or offensive gestures. However, the Supreme People’s Court, Supreme People’s Procuratorate, Ministry of Public Security, and Ministry of Justice explicitly included “using AI deepfakes” as a circumstance constituting “serious circumstances” for online insults in their “Guiding Opinions on Lawfully Punishing Online Violence Crimes.” In response, the author proposes a “purposive expansion” of the legal provision. This would extend the protection afforded by this crime—which safeguards “personal dignity” and ‘reputation’—to encompass the intrinsic core dignity of an individual’s sexual autonomy and privacy. Unlike the “analogy interpretation” prohibited in criminal law, this expansion constitutes a reasonable extension within the scope of legal principles. First, from a

textual perspective, the core meaning of “insult” lies in “causing damage to another person’s dignity or reputation, or subjecting them to disgrace.” The manner of such conduct is open-ended, not confined to specific forms like verbal abuse or physical assault, and should accommodate new manifestations as society evolves^[13]. Second, from a policy perspective, the “Guiding Opinions on Lawfully Punishing Online Violence Crimes” issued by the Supreme People’s Court, Supreme People’s Procuratorate, and Ministry of Public Security explicitly lists “using generative AI technologies like ‘deepfakes’ to disseminate illegal information” as a circumstance warranting heavier penalties for online insult. The existing judicial stance precisely demonstrates the high degree of alignment between deepfake pornography and the core unlawful essence of the crime of insult.

5.2 The Legislative Approach

Although interpretive approaches may offer a temporary solution, they remain constrained by the limitations of existing criminal frameworks and struggle to fully capture the nature of such conduct. These limitations manifest primarily in three aspects: First, the determination of “publicly” within the elements of the offense. If perpetrators send fabricated videos only to the victim themselves or their close relatives and friends, or disseminate them within small encrypted groups to carry out psychological coercion or extortion, yet cannot be held accountable because they fail to meet the “publicly” requirement, does this leave a gap in criminal liability? Second, the core illegality of deepfake pornography lies in its direct violation of an individual’s sexual autonomy—an intrinsic core legal interest. Classifying such acts under defamation essentially disguises “sexual autonomy infringement” as “reputational harm,” failing to reveal its essence as digital sexual violence. Third, focusing on sentencing frameworks, the insult crime—as a private prosecution offense—carries a maximum statutory penalty of three years’ imprisonment. This sentencing range proves inadequate when confronting the systemic harm inflicted by deepfake pornography.

The existence of these limitations means that interpretive approaches can only serve as transitional solutions rather than fundamental remedies. Globally, specialized legislation targeting such conduct has become a prominent trend. The U.S. federal Take It Down Act, passed in 2025, explicitly requires platforms to establish notice-and-takedown mechanisms. At the state level, over thirty states have enacted laws either incorporating AI-generated intimate images into existing “revenge porn” statutes or establishing new offenses. While the EU’s Artificial Intelligence Act adopts a horizontal regulatory approach, it also prioritizes transparency and accountability for deepfake technologies. These legislative practices distinguish “the creation or dissemination of sexually explicit false images without consent” from traditional offenses like defamation or distribution of obscene materials. By establishing independent provisions explicitly criminalizing such acts, they achieve direct and robust protection of the legal interests of “sexual privacy” or “sexual autonomy.”

Regarding the proposed new criminal offense, the author recommends analyzing it through the lens of four essential elements. First, objectively, the law should explicitly define the conduct as “using deepfake technology or other artificial intelligence tech-

niques to create or disseminate false sexual acts or sexually explicit images incorporating another person's genuine facial features, voice, or other biometric characteristics." Second, regarding the subjective element, the law should require that the perpetrator knowingly acted without the victim's consent and with malicious intent to humiliate, degrade, or harass. This distinction clearly separates the offense from general misuse of technology or unintentional dissemination. Third, regarding aggravating circumstances, drawing from international experience and China's practical needs, factors such as "committing the act for the purpose of extorting property," "targeting minors," "causing the victim's suicide or severe mental illness," "causing severe social repercussions through widespread dissemination via information networks," and "forming a black industrial chain" should be established as considerations for increasing statutory penalties^[14]. Fourth, when deepfakes are used in conjunction with subsequent crimes such as extortion or fraud, the relationship between offenses should be determined based on the nature of the legal interests infringed. If multiple acts violate distinct legal interests, they should be treated as either a single offense under the principle of imagined concurrence with punishment for the more severe offense, or as multiple offenses subject to cumulative punishment, ensuring that the total penalty aligns with the overall harm caused^[15].

5.3 Institutional Synergy Pathway

Of course, we must also extend our reach to the very origins of technology generation and expand outward into the vast domains of platform operations and international collaboration, building a collaborative governance network that equally emphasizes prevention, oversight, and accountability.

The primary focus of this network is to strengthen administrative oversight at the source of technology. The key to governance lies in significantly enhancing the enforcement rigor of these regulations: For service providers committing their first violation, with minor circumstances and prompt rectification, reputation penalties such as warnings or public censure may be imposed as deterrents; For those failing to fulfill labeling obligations or security assessment responsibilities as required but without causing severe consequences, corrective actions within a specified timeframe should be mandated alongside corresponding fines; For enterprises that refuse to rectify violations, generate content infringing upon others' rights, or cause severe social repercussions, qualification penalties such as suspension of relevant services or revocation of licenses must be imposed according to law.

The scope of platform liability should be appropriately expanded by establishing a tiered liability system for online service providers and strengthening technical governance obligations. For large platforms, drawing on the regulatory approach for "gatekeeper" platforms under the EU's Digital Markets Act, they should be required to deploy deepfake content detection systems. For small and medium-sized enterprises, however, given their practical constraints in terms of funding and technical expertise, it is inappropriate to demand the same level of proactive review as large platforms. Instead, compliance efforts should focus on fulfilling the entity information verification obligations stipulated in the E-Commerce Law and establishing and implementing the

cybersecurity incident emergency response mechanisms required by the Cybersecurity Law. In response, China's Regulations on the Management of Deep Synthesis in Internet Information Services explicitly mandate that deep synthesis service providers establish robust fact-checking mechanisms. Those who use deep synthesis technology to create, publish, or disseminate false information must promptly take corresponding measures to refute such claims.

However, we must also recognize that the industrial chain and servers of deepfake crimes are often distributed across different jurisdictions. Therefore, the scope of institutional coordination must be elevated from the domestic to the international level. Countries can actively promote and leverage multilateral legal frameworks such as the United Nations Convention on Cybercrime at the international level. This includes streamlining judicial assistance procedures for cross-border electronic evidence collection, establishing standardized request formats, and clear response timelines. Simultaneously, regional cooperation should explore the creation of specialized joint investigation and rapid response mechanisms targeting cyber sexual violence crimes. Through close law enforcement collaboration, this approach ensures that criminal activities in the virtual world cannot evade legal prosecution due to physical geographical boundaries.

6 Conclusion

The criminal regulation of deepfake pornography fundamentally addresses how law in the digital age responds to new infringements on personality rights arising from technological alienation. Beginning with the conceptual definition of “digital sexual violence,” this paper demonstrates how such acts systematically erode individual sexual autonomy—including control over one’s sexual image, freedom to choose sexual conduct, and even the right to self-narrate one’s sexuality—while structurally undermining gender equality, the foundation of social trust, and the legal principle of reliance interest. Through doctrinal examination of defamation, dissemination of obscene materials for profit, and infringement of citizens’ personal information, it reveals the traditional criminal framework’s triple predicament: mismatched elements of offense, inaccurate assessment of protected interests, and inadequate penalty configuration. Building upon this foundation, drawing from the non-contact harm model established by “remote indecent assault,” this study provides a legal justification for extending the protection of sexual autonomy from physical safeguards to digital image protection. It also lays a solid theoretical groundwork for incorporating deepfake pornography into the evaluation framework of sexual crimes.

Faced with this new form of crime spawned by technological alienation, clinging to traditional regulatory paradigms is tantamount to carving a mark on a boat to find a sword. The systematic response framework proposed in this paper addresses the current regulatory vacuum through interpretive expansion of purpose—by extending the legal interest of “personal dignity” in defamation offenses, it incorporates the core unlawful acts of deepfake pornography into the evaluative scope of existing norms; Legislatively, it addresses long-term institutional needs by establishing a distinct criminal

offense—drawing from international precedents such as the U.S. TAKE IT DOWN Act, the EU AI Act, and South Korea’s Special Act on Punishment of Sexual Violence Crimes. This involves adding provisions to China’s criminal law specifically regulating non-consensual deepfake pornography, with elements and aggravating circumstances precisely calibrated to the severity of the harm; Establish a collaborative governance network emphasizing prevention, oversight, and accountability through a three-pronged approach of administrative supervision, platform responsibility, and international cooperation.

References

1. Liu XQ. (2025). The criminal regulation of deepfake behavior in the era of artificial intelligence. *Politics and Law*, (11), 59. <https://doi.org/10.15984/j.cnki.1005-9512.2025.11.004>(In Chinese).
2. Chen R. (2024). Criminal regulation of deepfake sexually explicit information. *Law Science*, (3), 80. Retrieved March 13, 2026, from <https://lawscience.ruc.edu.cn/>(In Chinese).
3. Ding F, Kuang RS, Zhou Y, Sun L, Zhu XG, Zhu GP. (2024). A survey of deepfake and related digital forensics. *Journal of Image and Graphics*, 29(2), 295–317. Retrieved March 13, 2026, from <http://www.cjig.cn/> (In Chinese).
4. Dunn S. (2024). Legal definitions of intimate images in the age of sexual deepfakes and generative AI. *McGill Law Journal*, 69, 1–15. <https://doi.org/10.26443/law.v69i4.1626>.
5. Deng S, Dong J, Cao XF. (2025). The application of AI face-swapping technology in pornography crime and its investigative response. *Journal of Sichuan Police College*, (4), 63. <https://doi.org/10.16022/j.cnki.cn51-1716/d.2025.04.011>(In Chinese).
6. Tian HJ, et al. (2025, June 20). The application risks and governance of AI face-swapping. *Supreme People’s Procuratorate of the People’s Republic of China*. Retrieved March 5, 2026, from https://www.spp.gov.cn/llyj/202506/t20250620_698776.shtml(In Chinese).
7. Wang G. (2024, June 17). South Korea’s “Nth Room” incident reappears: Digital sex crimes are becoming increasingly rampant. *Legal Daily*. Retrieved March 13, 2026, from http://www.legaldaily.com.cn/international/content/2024-06/17/content_9010284.html(In Chinese).
8. Wang ZB, Wu XL. (2025). Research on deepfake technology in the digital era: Mechanism characteristics, functional alienation, and optimization paths. *Journal of Beijing University of Aeronautics and Astronautics (Social Sciences Edition)*, (2), 51. <https://doi.org/10.13766/j.bhsk.1008-2204.2022.0148>(In Chinese).
9. Wang C. (2025). Misconceptions correction and application approaches of the legal interest of trust in criminal law. *Hebei Law Science*, (8), 194–195. <https://doi.org/10.16494/j.cnki.1002-3933.2025.08.010>(In Chinese).
10. Eisele J, Duman I. (2025). Criminal liability of deepfake pornography under Turkish and German criminal law. *Zeitschrift für Internationale Strafrechtswissenschaft*, 4(1), 69–82. Retrieved from <https://www.zfis-online.de/index.php/zfis/issue/view/12>.
11. Shen CH. (2025). The right to bodily integrity approach to sexual harassment infringement. *Journal of Human Rights Law*, (3), 122–127. Retrieved March 13, 2026, from <http://gzzy.cbpt.cnki.net/>(In Chinese).
12. Jia J. (2018). What exactly does rape violate? – A review of the legal interest of “sexual autonomy” as a common theory. *Science of Law (Journal of Northwest University of Po-*

- litical Science and Law), (5), 96–105. <https://doi.org/10.16290/j.cnki.1674-5205.2018.05.060>(In Chinese).
13. Wei C. (2025). From external reputation to inner dignity: Reconstruction and development of the legal interest protected by the crime of insult. *China Legal Science*, (3), 123. <https://doi.org/10.14111/j.cnki.zgfx.2025.03.004>(In Chinese).
 14. Zhang MK. (2021). The functional transformation of aggravating circumstances. *Tsinghua Law Journal*, (1), 29–44. Retrieved March 13, 2026, from <http://qhfl.cbpt.cnki.net/>(In Chinese).
 15. Krasnodar University of the Ministry of Interior of Russia. (2025). The study of criminal liability for extortion in the digital space under foreign legislation. *Bulletin of the Kaliningrad branch of the St. Petersburg University of the Ministry of Internal Affairs of Russia*, (2), 31–38. <https://doi.org/10.5281/zenodo.16203433>.

Open Access This chapter is licensed under the terms of the Creative Commons Attribution-NonCommercial 4.0 International License (<http://creativecommons.org/licenses/by-nc/4.0/>), which permits any noncommercial use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license and indicate if changes were made.

The images or other third party material in this chapter are included in the chapter's Creative Commons license, unless indicated otherwise in a credit line to the material. If material is not included in the chapter's Creative Commons license and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder.

