Scientific and Social Research, 2026, Volume 8, Issue 10
https://bbwpublisher.com/journal/SSR
Online ISSN: 2981-9946
Print ISSN: 2661-4332

Reconceptualizing Public Interest in Procuratorial Public Interest Litigation for Personal Information Protection in the Age of AI Deepfakes

Xiuxiu Zhu*

Guilin University of Electronic Technology, Guilin 541000, Guangxi, China

Author to whom correspondence should be addressed.

Copyright: © 2026 Author(s). This is an open-access article distributed under the terms of the Creative Commons Attribution License (CC BY 4.0), permitting distribution and reproduction in any medium, provided the original work is cited.

Abstract: The rapid development of "deepfake" technologies poses new challenges to identifying public interest in procuratorial public interest litigation for personal information protection. The current approach, centered on "infringement upon the rights and interests of multiple individuals" and quantitative thresholds, fails to capture the nonlinear and systemic harms caused by deepfakes. From an epistemological perspective, this article proposes reconstructing the concept of social public interest, establishing a dual-level determination framework, clarifying the criteria for public interest harm, and improving the application of Article 70 of the Personal Information Protection Law, thereby providing a theoretical basis for identifying social public interest in the digital age.

Keywords: Procuratorial public interest litigation for personal information protection; AI-generated deepfake technologies; Social public interest

Online publication: November 25, 2026

1. Introduction

The rapid development of artificial intelligence (AI) generative technologies is reshaping the production and dissemination of information in the digital society. Among these technologies, "deepfake" technologies, represented by AI face-swapping, can be misused to manipulate personal biometric information, such as facial images and voiceprints, at low cost and with a high degree of accuracy through the abuse of AI algorithms [1]. The ability of deepfake technology to produce video or audio content that appears and sounds highly realistic, yet depicts or conveys things that people have never actually done or said, creates unprecedented opportunities for deception [2]. They have thus become tools for large-scale personal information infringement, capable of directly harming individual personality and property interests while

enabling exponential online dissemination. Such dissemination can erode the foundation of public trust in the digital society, threaten cyberspace order, and generate risks for public governance [3]. Accordingly, personal information protection is increasingly extending beyond the protection of individual rights and interests toward the safeguarding of the broader public interest of society.

Article 70 of the Personal Information Protection Law provides the legal basis for procuratorial public interest litigation, but its threshold remains centered on infringement of "the rights and interests of numerous individuals," measured by the amount of information and number of affected individuals. Such quantitative thresholds reveal significant limitations when applied to emerging risks such as deepfakes. Although public interest litigation is used to safeguard personal data, challenges persist [4]. Certain infringements may fall below quantitative thresholds yet substantially disrupt social order, leaving such public interest harm beyond the existing legal framework.

This article examines the tension between judicial practice and existing legal norms concerning deepfakes. It critiques the reductionist paradigm rooted in the classical scientific worldview, draws on epistemological transformation to incorporate social order into public interest, and develops criteria for identifying public interest harm in procuratorial public interest litigation for personal information protection.

2. Practical Challenges of procuratorial public interest litigation for personal information protection in the context of AI-generated "deepfakes"

2.1. Analysis of the Yu case involving AI face-swapping technology

In a civil public interest litigation case involving AI face-swapping, Yu illegally scraped facial information, created and disseminated face-swapped explicit videos, and sold related software and services. Although the information involved fell below relevant quantitative thresholds, the procuratorial organ and court found that the conduct harmed both personal information security and social order, holding that "numerous" should be assessed by its impact on the social public interest rather than the number of individuals affected. The case shows that conduct causing systemic disruption to social order may constitute public interest harm even below statutory quantitative thresholds.

2.2. Traditional criteria for identifying public interest litigation for personal information protection

China's current framework for procuratorial public interest litigation in personal information protection largely identifies public interest harm through the aggregation of individual rights and interests and quantifiable thresholds. Article 58(2) of the Civil Procedure Law provides the general basis, while Article 70 of the Personal Information Protection Law applies this approach to unlawful processing affecting "numerous individuals." Procuratorial guidance uses "more than one million individuals" as a reference for major cases, and relevant criminal interpretations adopt tiered standards based mainly on the amount of personal information involved. Such quantitative standards were effective in traditional offline and early online contexts, where public interest harm typically resulted from cumulative individual harms. With digitalization, however, they are increasingly inadequate for systemic and nonlinear risks.

2.3. The limitations of traditional quantitative standards in addressing emerging risks

The harm caused by AI-generated "deepfake" technologies lies not only in the infringement of individuals'

portrait rights and privacy rights, but also in their potential impact on the trust mechanisms of the digital society as a whole [5]. As AI-generated face-swapped content spreads, distinguishing real from fabricated content becomes harder, undermining social trust in ways that extend beyond individual victims and cannot be measured by the number of affected individuals or volume of information involved. All populations exhibit vulnerability to deepfakes, and this vulnerability increases with age and trust in information sources. Adults and educators exhibit greater vulnerability. Vulnerability also increases with exposure to potential deepfakes, suggesting that deepfakes become more pernicious without interventions [6]. In the Yu case, although the facial information fell below the quantitative threshold, disseminating face-swapping tools exposed unspecified users to risks of unauthorized identity manipulation beyond traditional quantitative standards.

Traditional personal information infringements generally involve a linear relationship between the amount of information and individual harm, whereas AI-generated deepfakes exhibit emergence, amplification, and rapid diffusion. A limited amount of facial information, when combined with face-swapping tools, may be transformed into large-scale volumes of fabricated content through automated generation [7]. Deepfakes can spread rapidly through social media, enabling fake news, fraud, and other harms while undermining public trust in digital information. Thus, even limited misuse of personal information may cause widespread social disruption, with its scale bearing no linear relationship to the initial infringement and potentially escaping quantitative thresholds for procuratorial public interest litigation. Traditional quantitative standards, rooted in reductionism, are inadequate to address deepfake-related public interest challenges, requiring a reconceptualization of social public interest for the digital age.

3. Traditional paradigms for conceptualizing social public interest and their limitations

3.1. Theoretical debates over the concept of social public interest

Although "social public interest" is widely used in legislation, its scope remains contested. The "equivalence theory" treats it as synonymous with public order and morality, while the "inclusion theory" regards social order as one component of the broader concept. The debate reflects different understandings of whether public interest possesses holistic value beyond aggregated individual interests; in practice, reductionist approaches have largely treated social order as the aggregation of individual rights and interests.

3.2. The reductionist paradigm of the classical scientific perspective

Rooted in Newtonian mechanics, the classical scientific worldview emphasizes determinism, decomposability, and quantifiability, fostering reductionist approaches that explain complex systems through their constituent parts. Applied to social public interest, reductionism operates ontologically by reducing public interest to aggregated individual interests, causally by assuming linear progression from unlawful conduct to individual and public harm, and adjudicatively by relying on quantitative indicators. This paradigm suited traditional industrial society, where harm was predominantly cumulative and linear.

3.3. The limitations of the reductionist paradigm in the digital age

In the digital age, interconnected social systems make deepfake risks holistic, nonlinear, and emergent, exposing the limits of reductionism. By reducing public interest to individual interests and overlooking social

order as an independent legal interest, it inadequately captures systemic risks such as the rapid amplification of limited facial-information misuse through deepfake dissemination. Quantitative thresholds may therefore underestimate social-order disruption and weaken the preventive function of public interest litigation. These limitations call for a holistic and relational conception of social public interest that recognizes social order as an independent dimension.

4. Reconceptualizing public interest from a quantum-informed epistemological perspective

4.1. The epistemological transformation from classical certainty to complexity and uncertainty

Since the twentieth century, quantum mechanics has challenged the deterministic assumptions of the classical scientific worldview by showing that microscopic phenomena cannot always be explained through fixed causal relationships or complete predictability. A quantum-informed epistemological perspective emphasizes uncertainty, relationality, and the inseparability between a system and its constituent elements [8]. Complex systems cannot always be understood by decomposing their components, as interactions may produce irreducible emergent properties, favoring holistic analysis and greater acceptance of uncertainty in the social sciences.

Social public interest itself represents an open-textured legal concept; AI-generated deepfakes intensify the uncertainty of social public interest, whose interests extend from individual rights to social trust and public order and whose beneficiaries range from identifiable groups to society at large, requiring a holistic and relational approach to its scope and meaning [9].

4.2. Public interest as a composite whole of individual rights and interests and social order

Quantum superposition suggests that a whole may possess properties irreducible to its components, indicating that individual interests and social order constitute an integrated whole. Individual rights and interests support traditional quantitative thresholds, while social order provides a structural foundation with holistic value; neither alone exhausts public interest, and deepfake-related conduct may harm both by infringing on personal information, portrait, and privacy rights through unlawful collection of facial information. On the other hand, through the dissemination of fabricated content and the distribution of infringement-enabling tools, such conduct directly disrupts the authenticity order of digital information and the social trust order in cyberspace, thereby constituting harm at the level of social order [10]. These harms are simultaneous and mutually reinforcing; the Yu case reflects this holistic approach by recognizing both individual information-related interests and broader disruption to social order.

Quantum entanglement illustrates correlations that challenge conventional linear causality and, as an epistemological analogy, helps explain the nonlinear relationship between deepfake-related conduct and social-order disruption. Once biometric information is misused and disseminated online, even limited misuse may undermine digital trust and impose broader social verification costs, with harm not necessarily proportional to the number of individuals affected.

Thus, deepfake-related conduct may disrupt social order holistically and immediately, without requiring widespread individual harm. Conduct posing a substantial risk of such disruption should therefore be

recognized as a public interest threat before large-scale harm materializes, reinforcing the preventive function of public interest litigation. While traditional social order centered on physical safety and interpersonal rules, digital society depends increasingly on information integrity and trust, which deepfakes can disrupt by blurring the line between authentic and fabricated content and amplifying deception, false narratives, and governance risks. What makes digital misinformation distinctly threatening is its ability to circumvent and undermine common knowledge-producing institutions, including the sciences, courts, medicine and other professions, and the media [11]. Such disruption cannot be measured by individual infringements or adequately addressed through individual litigation, but requires the collective and preventive protection of procuratorial public interest litigation.

5. Approaches to improving the framework of procuratorial public interest litigation for personal information protection

5.1. Recognizing social order as an independent legal interest

Article 70 authorizes procuratorial public interest litigation for unlawful processing affecting "numerous individuals" but does not expressly recognize social-order disruption as public interest harm; purposive and systematic interpretation should therefore encompass substantial disruption even below quantitative thresholds.

5.2. Constructing a dual-tiered framework for public interest determination

A dual-tiered framework should retain quantitative criteria for large-scale ordinary infringements while applying a social-order-disruption model to high-risk conduct such as deepfake-related misuse of biometric information. Under the latter, public interest harm should be assessed by substantial actual or potential disruption of social order rather than quantitative thresholds alone.

5.3. Establishing a four-element determination framework

5.3.1. The actor element

Relevant actors include AI developers and service providers, large-scale biometric-information processors, and those unlawfully providing or disseminating biometric data or content-fabrication tools; liability should require intent or gross negligence. Malicious actors exploit deepfakes to spread misinformation, manipulate public perception, and threaten information integrity [12]. Direct intent covers knowingly unlawful processing or deepfake creation and dissemination despite awareness of its social-order risks; conditional intent covers recognizing and accepting the risk that supplied tools or data may facilitate such violations, as in Yu's sale of face-swapping software and tutorials. Gross negligence applies where actors foresee serious risks from technology misuse or data leakage but fail to take necessary preventive measures despite violating statutory security duties; ordinary negligence is excluded to avoid undue expansion of liability.

5.3.2. The object element

The "social order" should be defined through three dimensions—digital-information trust and interaction security, authentic and orderly cyberspace information dissemination, and public order and morality—so the object element is satisfied only when conduct undermines one or more of them.

5.3.3. The normative element

The social-order-disruption model applies only to conduct violating mandatory requirements for personal information processing or deep synthesis services, including unlawful biometric processing, failure to label deep synthesis content, noncompliance with service obligations, and unlawful disclosure or dissemination of biometric data; lawful conduct should not constitute public interest harm merely because it affects social order.

5.3.4. The practical element

Without requiring quantitative thresholds or actual harm, the practical element is satisfied when any concrete circumstance indicates a substantial risk of social-order disruption or significant social impact, assessed by dissemination scope, risk replicability, or potential severity, thereby reflecting the preventive function of procuratorial public interest litigation.

6. Conclusion

AI-generated deepfakes expose the limits of reductionist, quantitative approaches to personal information protection and procuratorial public interest litigation, as their nonlinear disruption of social order may occur without cumulative individual harm. A holistic perspective, therefore, recognizes social public interest as encompassing interconnected individual interests and social order.

Accordingly, a purposive and systematic interpretation of Article 70 of the Personal Information Protection Law should recognize substantial social-order disruption as public interest harm within a dual-tiered framework of individual-interest aggregation and social-order disruption. The latter should be assessed through the four elements of "actor–object–norm–practice," balancing personal information protection, technological innovation, and social public interest.

Funding

Innovation Project of GUET Graduate Education (Project number: 2026YCXS172)

Disclosure statement

The author declares no conflict of interest.

References

[1] Peng CL, Li JY, Liu DC, et al., 2026, Deepfake Detection in the Era of Large Models. Science China Information Sciences, 56(1): 1–22.

[2] De Ruiter A, 2021, The Distinct Wrong of Deepfakes. Philosophy & Technology, 34(4): 1311–1332.

[3] Patarlapati N, 2023, Unmasking Reality: Exploring the Sociological Impacts of Deepfake Technology. International Journal for Research in Applied Science and Engineering Technology, 11(XI): 882–889. https://doi.org/10.22214/ijraset.2023.56639

[4] He M, Chen Y, 2025, Personal Data Protection in China: Progress, Challenges and Prospects in the Age of Big

Data and AI. Telecommunications Policy, 103076.

[5] Sheikh MA, Tariq M, Farrukh M, et al., 2026, Deepfake Dilemma: A Profound Threat to Trust and Authenticity in Media and Society. Journal of Social Sciences Research & Policy, 4(2): 66–79.

[6] Doss C, Mondschein J, Shu D, et al., 2023, Deepfakes and Scientific Knowledge Dissemination. Scientific reports, 13(1): 13429.

[7] Shahzad HF, Rustam F, Flores ES, et al., 2022, A Review of Image Processing Techniques for Deepfakes. Sensors, 22(12): 4556.

[8] Jussi L, Jukka L, 2020, The Heisenberg Uncertainty Principle as an Endogenous Equilibrium Property of Stochastic Optimal Control Systems in Quantum Mechanics. Symmetry, 12(9): 1533.https://doi.org/10.3390/sym12091533

[9] Lewis CW, 2006, In Pursuit of the Public Interest. Public Administration Review, 66(5): 694–701.

[10] Vaccari C, Chadwick A, 2020, Deepfakes and Disinformation: Exploring the Impact of Synthetic Political Video on Deception, Uncertainty, and Trust in News. Social Media + Society, 6(1): 2056305120903408.

[11] Abiri G, Buchheim J, 2022, Beyond True and False: Fake News and the Digital Epistemic Divide. Michigan Technology Law Review, 2022(29): 59.

[12] Boediman EP, 2025, Exploring the Impact of Deepfake Technology on Public Trust and Media Manipulation: A Scoping Review. Jurnal Komunikasi, 19(2): 313–334.

Publisher's note

Bio-Byword Scientific Publishing remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.