Privacy Protection and Criminal Regulation in the Digital Era: An Analysis of Online Personal Information Disclosure

Jiashuo Wang
[1]*Nursing, School of Nursing, He University, Shenyang, Liaoning, China*

Keywords: Online Personal Information Disclosure, Crime of Infringing on Citizens' Personal Information, Platform Liability.

Abstract: The disclosure of personal information online has become increasingly rampant in the digital era. Such behaviour infringes upon citizens' rights, posing numerous challenges for criminal regulation. Centring on the Crime of Infringing on Citizens' Personal Information under the Criminal Law of the People's Republic of China, this article employs doctrinal legal analysis and comparative law methods to systematically explore the judicial difficulties and governance paths concerning this behaviour. The study reveals that the key dilemmas in judicial practice involve defining the illegality of the secondary use of publicly available information, the absence of a substantive standard for determining serious circumstances, and the challenges of ascertaining joint criminality and platform liability in collective actions. The paper further posits that a singular model of criminal punishment has functional limitations and necessitates a balance between combating crime and safeguarding rights, as well as between public supervision and privacy protection. Therefore, future governance should transcend traditional criminal law thinking. A comprehensive governance framework should be constructed by refining judicial standards, clarifying platform liability, and drawing on foreign experiences. This framework should integrate criminal, administrative, civil, and social co-governance to achieve the long-term governance of cyberspace.

1 INTRODUCTION

While the wave of digital technology in the modern era reshapes social life, it has also given rise to the malicious disclosure of personal information online. This behaviour often manifests in extreme forms such as human flesh searches, severely infringing upon the personal dignity and privacy rights of citizens. The instantaneous and pervasive nature of the information's dissemination extends online harm into the real world, causing irreparable social trauma and posing a severe challenge to online order and the rule of law.

To address this issue, China has progressively established a legal framework that includes the Personal Information Protection Law. Within this framework, Article 253-1 of the Criminal Law, the Crime of Infringing on Citizens' Personal Information, is regarded as the final line of defence for personal information security due to its severe punitive nature. However, applying this charge to the complex and volatile online environment presents numerous dilemmas and controversies in judicial practice, necessitating further scholarly inquiry (Wang, 2025).

Chinese academia has extensively discussed this topic, yet there remains scope for deeper analysis in three areas. Firstly, existing research lacks a systematic doctrinal legal analysis of several of the most intractable controversies in judicial practice. These controversies include the illegality of the secondary use of publicly available information, the substantive standards for serious circumstances, and the determination of online joint criminality. Secondly, the scope of current research is often confined to domestic law, lacking a detailed comparison with foreign models like the EU's GDPR and relevant US laws. This limitation makes it difficult to scrutinise the characteristics of the Chinese model within an international dialogue. Thirdly, the prevailing research approach tends to emphasise calls for criminal sanctions, with insufficient reflection on the inherent limitations of criminal punishment, thus failing to propose a systematic governance solution that transcends a

Wang, J.
Privacy Protection and Criminal Regulation in the Digital Era: An Analysis of Online Personal Information Disclosure.
DOI: 10.5220/0014389300004859

In *Proceedings of the 1st International Conference on Politics, Law, and Social Science (ICPLSS 2025)*, pages 534-539
ISBN: 978-989-758-785-6

singular criminal law perspective (Bradford, Aboy & Liddell, 2020).

To address the research gaps, this article combines doctrinal legal analysis, case analysis and comparative law to examine the criminal regulation of online personal information disclosure. The discussion moves from theoretical foundations to practical difficulties, then to institutional reflection and finally to proposals for improvement, and is presented in three chapters. Chapter One will directly confront the core dilemmas in judicial practice. This chapter examines the illegality of collecting and republishing publicly available information. It considers how to establish a multi-dimensional standard for serious circumstances that reflects qualitative factors and provides an adaptive interpretation of joint criminality theory to clarify the liability of key participants and platforms in collective online actions. Building on this analysis, Chapter Two will offer an institutional reflection, critically examining the functional limitations and internal value conflicts of the singular criminal punishment model. Finally, Chapter Three will focus on future paths, proposing a systematic and comprehensive governance solution based on the preceding analysis.

This study aims to clarify the theoretical controversies surrounding the application of the Crime of Infringing on Citizens' Personal Information in the digital era, provide more operational guidance for judicial practice, and ultimately construct a comprehensive governance framework that transcends a singular reliance on criminal justice. The theoretical significance of the research lies in advancing the criminal law theory on cybercrime and contributing Chinese perspectives to the global comparative study of platform governance. Its practical significance is to offer a plan, possessing both theoretical depth and real-world feasibility, for China's judicial bodies, legislators, and all sectors of society to collaboratively govern cyberspace and protect the core rights of citizens in the digital age.

2 CHALLENGES IN JUDICIAL APPLICATION

2.1 Determining the Illegality of the Secondary Use of Publicly Available Information

One of the most contentious issues in Chinese judicial practice is whether the act of collecting, consolidating, and republishing personal information that is already scattered and publicly available online constitutes illegal acquisition.

Since the information is already in the public domain and accessible to anyone, the act of collecting and consolidating this information through technical means essentially only alters its presentation. Therefore, this act should not be classified as illegal acquisition. This perspective emphasises the public attribute of the information.

However, the illegality of such an act lies precisely in exceeding the purpose and scope of the data subject's original consent for the disclosure. According to the principles of purpose limitation and informed consent established in China's Personal Information Protection Law, when an individual shares life updates on social media, the implied scope of consent is for social interaction, not to allow others to compile all their information into a digital file for public shaming online. Therefore, this malicious act of collection and consolidation, which goes beyond reasonable expectations, substantively infringes upon an individual's right to self-determination over their information processing. The methods and purposes of the act lack a legitimate basis, thereby fully meeting the constituent elements of illegal acquisition by other means.

The European Union's General Data Protection Regulation (GDPR) provides a clear reference on this point. The GDPR strictly adheres to the purpose limitation principle, meaning that the processing of personal data must not be incompatible with the specific, explicit, and legitimate purposes for which it was collected. The core of this rule is that control over information always remains with the data subject; the public status of information does not equate to an unlimited waiver of rights (Gal & Aviv, 2020).

2.2 The Multi-Dimensional Standard for Determining Serious Circumstances

Serious circumstances serve as the threshold for criminalisation. Yet current judicial interpretations rely mainly on quantitative criteria, which are insufficient for online disclosure cases where the main harm lies in psychological damage and loss of social reputation.

This paper argues that future judicial practice, while considering traditional quantitative factors, should construct a comprehensive judgment framework that is more focused on substantive harm and includes multiple qualitative dimensions. Firstly, the sensitivity of the information should be fully

considered. The disclosure of highly sensitive information that directly relates to an individual's personal security and dignity, such as home addresses, medical records, or private conversations, should in itself be assigned a higher evaluation of social harm. Secondly, the scope and impact of the information's dissemination online is another key indicator. Judicial bodies need to assess factors such as whether the information was reposted across multiple platforms and whether it triggered widespread online scrutiny, in order to evaluate the impact on online order.

More centrally, the focus of the judgment must return to the actual harmful consequences for the victim. Whether the victim suffered real-world harassment or threats, lost their employment, developed severe psychological trauma such as depression, or experienced a social death should be the most critical basis for evaluating serious circumstances. Finally, an examination of the perpetrator's subjective malice and purpose is also indispensable. Whether the perpetrator acted out of malicious revenge, to engage in cyberbullying, or for other illegal purposes directly determines the degree to which the behaviour warrants criminal punishment (Shi, 2022).

2.3 Ascertaining Platform Liability and Joint Criminality

The collective perpetration characteristic of online personal information disclosure presents two major difficulties in ascertaining criminal liability: how to hold dispersed individual participants accountable, and how to define the liability of centrally positioned online platforms.

Regarding the former, the ascertainment of joint criminality among individual participants, the dilemma lies in the fact that spontaneous online incidents often lack the prior conspiracy required by traditional theory. To address this, legal doctrines that allow for accountability without prior, explicit agreement provide a feasible path. When an online disclosure incident is ongoing, a subsequent participant who is aware that the acts are infringing upon the victim's rights, yet still actively provides key information, consolidates data, or maliciously disseminates the information, establishes a causal link with the preceding acts. This forms a tacit understanding, allowing the participant to be identified as a joint perpetrator.

Regarding the latter, the boundary of a network platform's criminal liability, the key lies in proving the platform's subjective knowing state of mind. The platform's liability does not arise from its status as a neutral technology provider, but from its failure to fulfil its statutory network security management obligations under specific conditions. With reference to relevant provisions in the Criminal Law, if a platform, after receiving a clear notice of infringement, is fully aware of the existence of serious and persistent illegal information disclosure on its service but still adopts a passive and permissive attitude by not taking necessary measures such as deletion or blocking, its failure to act can be evaluated as a form of assistance with indirect intent. Such an omission could even lead to the platform being considered an accomplice to the primary offence.

On the issue of platform liability, the legal paths of China and the United States show a stark contrast. Unlike the increasingly strict security management obligations imposed on platforms under Chinese law, Section 230 of the Communications Decency Act in the United States grants online platforms extensive immunity. In principle, platforms are not held legally responsible for content published by third-party users. The original intent of this legislative choice was to protect the innovative vitality and freedom of speech of the nascent internet industry. However, this has also made the legislation less effective in regulating problems such as cyberbullying and false information (Hocott, 2021).

3 VALUE BALANCING AND INSTITUTIONAL REFLECTION

3.1 Boundaries and Balance in Criminal Regulation

The expansion of penal power is naturally accompanied by the curtailment of citizens' fundamental rights, particularly freedom of speech. An overly broad application of the Crime of Infringing on Citizens' Personal Information could lead to a chilling effect, suppressing normal criticism and exchange in cyberspace. In this context, the principle of the subsidiarity of criminal law, also known as the last resort principle, becomes particularly important.

This means that criminal intervention must strictly adhere to the principle of proportionality. The initiation of criminal proceedings is only justifiable when the infringement of legal interests caused by the disclosure, in both nature and degree, significantly outweighs any expressive value the disclosure may

have, and when other legal measures such as civil tort claims or administrative penalties are insufficient to provide effective remedy.

3.2 The Boundary of Public Supervision and Privacy Rights Protection

The key to demarcating the two lies in the relevance to the public interest. For public officials who hold public power or public figures who influence the public sphere, some of their information, such as financial status or professional conduct, is closely related to the public interest, and their expectation of privacy should be appropriately lowered. But this supervision is by no means without boundaries. When the disclosed content exceeds the scope of public interest and extends to purely private domains such as family members, health conditions, or personal relationships, it degenerates from legitimate public supervision into illegal privacy infringement. The legitimacy of online supervision depends not only on its purpose but also on the legality and necessity of its means. No one has the right, in the name of supervision, to conduct human flesh searches that transgress legal boundaries or to subject others to extra-legal punishment through privacy violation.

3.3 Balancing the Right to Privacy and Freedom of Speech

The model represented by the US, under the strong influence of the First Amendment, places freedom of speech in a position of priority, and the scales of judicial practice tilt significantly in its favour. Particularly in cases involving public figures or public issues, courts adopt the strict actual malice standard, which greatly protects the content of the speech itself; only by proving that the publisher acted with actual malice can legal liability be pursued. To avoid creating a chilling effect on speech, US law is more inclined to regulate the intrusive act of acquiring information rather than directly restricting the content of the speech, reflecting a profound trust in the free market of ideas (MacKinnon, 2020).

In contrast, the European legal tradition, especially in the practice of the European Court of Human Rights (ECHR), places more emphasis on the equal dialogue and proportionality analysis of the two rights. European law considers both the freedom of expression and the right to a private life guaranteed by the European Convention on Human Rights to be fundamental rights requiring protection, with no absolute hierarchy between them. Therefore, in individual cases, the court will conduct a detailed value assessment, carefully weighing a series of factors such as whether the disclosure serves a debate of public interest, the public status of the individual concerned, and the degree of privacy of the information, ultimately reaching a proportionate judgment in the specific context. The establishment of the right to be forgotten in Europe further embodies the particular emphasis placed on the dignity of personal information and the right to privacy control in the digital age (Mchangama & Alkiviadou, 2021).

4 IMPROVEMENT SUGGESTIONS AND FUTURE PATHS

4.1 Refining the Standard for Serious Circumstances

To solve the current problem in judicial practice of having a surplus of quantitative but a deficit of qualitative assessment, this paper suggests that the Supreme People's Court, by issuing a new judicial interpretation or guiding case, should refine the standard for determining serious circumstances and construct a dual quantitative and qualitative judgment system.

Specifically, the new judicial interpretation should clearly guide judicial officers to move beyond simple quantitative calculations during judgment and instead conduct a comprehensive assessment of a series of qualitative factors. These factors include the sensitivity of the information, the consequences of psychological harm and reduced social standing for the victim, the scope and speed of the information's dissemination, and the perpetrator's subjective malice and motive. It is particularly important that when handling cases involving highly sensitive information such as personal privacy, health, finance, and home addresses, the quantitative threshold should be significantly lowered or even eliminated. A judicial approach where one piece of information could be enough to constitute a crime should be clarified, in order to reflect the special and prioritised protection of core personality rights.

4.2 Clarifying the Boundaries of Platform Liability

Platforms play a core role in the dissemination of online information. Defining their liability must

balance incentives with punishment, guiding them to transition from a passive safe harbour role to that of an active gatekeeper.

To this end, this paper suggests constructing a hierarchical liability system. On the one hand, a procedural safe harbour from criminal liability should be established for all platforms. This means explicitly stipulating that if a platform establishes and effectively implements clear and convenient channels for infringement complaints, deals with illegally disclosed information in a timely manner within a reasonable period after receiving a valid notice, and lawfully preserves relevant records while cooperating with judicial investigations, it can be exempted from the most severe criminal liability. This mechanism aims to incentivise platforms to fulfil their basic content management obligations through positive reinforcement, rather than through the constant threat of criminal punishment.

On the other hand, for large social media platforms with significant social mobilisation capacity, a higher level of special preventive duty should be imposed. This requires them not merely to passively notice and takedown, but to use their technological advantages to proactively provide warnings and identify trending events that could trigger large-scale human flesh searches or cyberbullying. They should also actively take intervention measures such as traffic limitation and pop-up warnings to prevent the uncontrolled escalation of harmful consequences (Kiritchenko, Nejadgholi & Fraser, 2021).

4.3 Establishing a Coordinated System of Governance and Multi-Stakeholder Participation

Given the limitations of criminal punishment, it is essential to construct a governance network in which multiple legal instruments and social forces act in concert to achieve the comprehensive prevention and control of online personal information disclosure.

This system first requires breaking down internal barriers between the state's legal instruments by strengthening the effective connection between administrative penalties and criminal justice. A fluid mechanism for case referral and information sharing should be established among the Cyberspace Administration, public security organs, and procuratorial organs. For acts that are clearly illegal but do not yet constitute serious circumstances, the Cyberspace Administration should impose timely administrative penalties in accordance with laws such as the Personal Information Protection Law. This would form a tiered and smoothly connected public law liability system. At the same time, civil remedy channels must be vigorously expanded. This can be achieved by lowering the threshold for victims to defend their rights, explicitly supporting their claims for emotional damages, and exploring the establishment of fast-track adjudication mechanisms for online tort cases. Civil compensation can provide victims with the most direct economic relief and psychological solace, a function that criminal punishment cannot replace (Calzada, 2022).

Finally, the effective operation of legal instruments must be supplemented by broad social co-governance. The work of governance must extend to the societal level. Through sustained rule of law publicity and digital literacy education, public awareness of the importance of personal information protection and the harms of cyberbullying must be raised. This will cultivate a healthy and rational online culture at its source and reduce the occurrence of infringing acts (Mandrescu, 2025).

5 CONCLUSIONS

As a complication of the digital era, the malicious disclosure of personal information online has become a substantive threat to citizens' rights and social order. Through a systematic study of the Crime of Infringing on Citizens' Personal Information within the Chinese Criminal Law, this paper finds that although criminal law provides a core regulatory tool, its judicial application still faces profound theoretical dilemmas.

This research has reached the following core conclusions. Firstly, regarding the illegality of the secondary use of publicly available information, the determining factor is not the public status of the information itself, but rather whether its processing exceeds the legitimate and proper principle of purpose limitation, thereby infringing upon the individual's right to informational self-determination. Secondly, the determination of serious circumstances must shift from traditional, quantitatively-biased standards towards a substantive judgment framework that also considers qualitative factors such as the sensitivity of the information and the harmful consequences for the victim. Finally, in confronting collective online behaviour, the liability of core actors can be pursued through an adaptive interpretation of joint criminality theory, and the criminal liability of platforms can be ascertained by defining the platform's knowing state of mind.

However, the most important conclusion is that a singular model of criminal sanctions has functional

limitations; it cannot eradicate cyberbullying, nor can it effectively restore the rights and interests of the victim. The use of criminal sanctions must be exercised with restraint amidst the conflict of values between safeguarding freedom of speech and protecting personal privacy. Therefore, effective future governance is by no means a matter of treating criminal law as a panacea; instead, it must follow a comprehensive path of multi-stakeholder governance.

The significance of this research is that it not only systematically clarifies the internal jurisprudential controversies of the criminal regulation of online personal information disclosure and provides more operational guidance for judicial practice, but more importantly, it constructs a paradigm-shifting framework from punishment to governance. By introducing a comparative law perspective, this paper places China's governance challenges in the context of a global dialogue. The research provides a logically coherent and forward-looking solution for the division of liability, the positioning of the role of platforms, and the construction of a comprehensive governance system. The work holds positive theoretical and practical value for advancing the process of building the rule of law in China's cyberspace.

Future research could be expanded in the following areas. Firstly, large-sample empirical research could be conducted, using quantitative analysis of judicial precedents to test the practical validity of the theoretical viewpoints proposed in this paper. Secondly, interdisciplinary research should be strengthened, combining sociology, communication studies, and computer science to deeply explore the socio-psychological causes behind cyberbullying and the technological inducements of algorithmic recommendations. Thirdly, with the evolution of technology, the legal regulation of new issues, such as the use of artificial intelligence for the automated collection and disclosure of information, will become a new field urgently requiring exploration. This research can serve as a starting point for the legal analysis in these future inquiries.

REFERENCES

Bradford, L., Aboy, M., & Liddell, K. (2020). International transfers of health data between the EU and USA: a sector-specific approach for the USA to ensure an ‘adequate’ level of protection. Journal of Law and the Biosciences, 7(1), lsaa055.

Calzada, I. (2022). Citizens’ data privacy in China: The state of the art of the Personal Information Protection Law (PIPL). Smart Cities, 5(3), 1129-1150.

Gal, M. S., & Aviv, O. (2020). The competitive effects of the GDPR. Journal of Competition Law & Economics, 16(3), 349-391.

Hocott, A. (2021). The partisan Samaritan: The Communications Decency Act and the modern internet. Ave Maria Law Review, 19, 238.

Kiritchenko, S., Nejadgholi, I., & Fraser, K. C. (2021). Confronting abusive language online: A survey from the ethical and human rights perspective. Journal of Artificial Intelligence Research, 71, 431-478.

MacKinnon, C. A. (2020). Weaponizing the First Amendment. Virginia Law Review, 106(6), 1223-1283.

Mandrescu, D. (2025). Designing (restorative) remedies for abuses of dominance by online platforms. Journal of Antitrust Enforcement, 13(2), 353-389.

Mchangama, J., & Alkiviadou, N. (2021). Hate speech and the European Court of Human Rights: Whatever happened to the right to offend, shock or disturb? Human Rights Law Review, 21(4), 1008-1042.

Shi, J. (2022). Artificial intelligence, algorithms and sentencing in Chinese criminal justice: Problems and solutions. Criminal Law Forum, 33(2), 121-148.

Wang, H. (2025). Criminal regulation of doxxing under the context of cyber violence. Comparative Law Studies, 3, 136-150.