Economics, Law and Policy
ISSN 2576-2060 (Print) ISSN 2576-2052 (Online)
Vol. 9, No. 1, 2026
www.scholink.org/ojs/index.php/elp

Original Paper

Doxing in China: The "Human Flesh Search" Phenomenon and Its Criminal Law Regulation

Zehao Chen[1]

[1] Law School of Beijing Normal University, Beijing, China

Received: January 13, 2026 Accepted: January 28, 2026 Online Published: January 30, 2026

doi:10.22158/elp.v9n1p84 URL: http://dx.doi.org/10.22158/elp.v9n1p84

Abstract

Doxing constitutes an important manifestation of online violence, and the assessment of its degree of seriousness is a key issue in the formulation of governance rules. Existing standards based on the quantity of personal information fail to accurately reflect the severity of doxing conduct. From the perspective of the dual-layered legal interest theory, and in light of the mosaic theory, the core problem does not lie in the excessive threshold of quantitative standards, but rather in the fact that a single information-quantity criterion is incapable of capturing the "aggregation effect" among multiple pieces of information and the resulting "structural exposure" of the victim's identity. Consequently, information quantity cannot function as an appropriate intermediate factor for assessing the infringement of legal interests caused by doxing. Accordingly, the evaluation of legal interest infringement in doxing cases should shift from a purely quantitative approach to a typological analysis, a more operational normative framework for administrative–criminal coordination can be established.

Keywords

Doxing, Online Violence, Crime of Infringing Citizens' Personal Information, Mosaic Theory

1. Introduction

Doxing is commonly understood as the act of collecting, aggregating and publicly disclosing identifiable personal information about an individual online without that person's consent, with the aim of causing humiliation or other forms of harm (Aghili et al., 2013). In Chinese legal scholarship, doxing has long been analysed primarily as an ancillary phenomenon within the frameworks of civil tort liability, the crime of infringing citizens' personal information, or the broader discourse on online violence. As a result, it has rarely been examined as an autonomous behavioural category with its own distinct risk structure and regulatory logic. With the increasing online and networked evolution of personal information–related offences, China's approach to personal information protection likewise

calls for a shift from generalised governance to more typology-based and differentiated regulation (Ouyang, 2025, pp. 82-83). Against this background, a refined and systematic study of doxing is of pressing practical significance.

In judicial practice, assessing the degree of seriousness of doxing conduct has become a pivotal issue in China's administrative–criminal linkage. Following the 2025 revision of the *Public Security Administration Punishments Law*, which introduced a tiered regulatory scheme for acts infringing citizens' personal information, and in conjunction with Article 253-1 of the PRC Criminal Law, a four-level evaluative structure has gradually taken shape—ranging from "relatively minor" and "ordinary" cases to "serious" and "especially serious" cases. Under this framework, the normative positioning of doxing between administrative sanctions and criminal punishment increasingly depends on a coherent and accurate assessment of its degree of seriousness. However, as a behavioural form directed at specific individuals and characterised by both personal information infringement and online-violence dynamics, doxing cannot be adequately assessed through the mechanical application of pre-existing standards within the current normative system. In different cases, the risk structure, harm outcomes, and governance difficulty generated by doxing vary substantially. Without a clear and operational evaluative approach, the administrative–criminal linkage cannot operate in a stable and predictable manner. Accordingly, it is necessary to develop a systematic analysis of the legal interest infringement caused by doxing and the corresponding method of assessment, so as to respond to the evaluative challenges faced in practice.

2. Normative Challenges in Evaluating Doxing

Since the issuance of the *Guiding Opinions on Punishing Online Violence and Related Illegal and Criminal Conduct According to Law* by China's Supreme People's Court, Supreme People's Procuratorate, and the Ministry of Public Security (hereinafter the "Guiding Opinions on Online Violence"), doxing has been explicitly brought within the horizon of criminal regulation. Yet, in sharp contrast to the urgency of governance needs, doxing remains a non-legal (extra-doctrinal) concept in China: its behavioural boundaries are vague, its manifestations are diverse, and it is difficult to incorporate directly into the existing structure of criminal law. In its early stage, doxing largely took the form of online behaviour driven by curiosity and entertainment(Hao & Zhou, 2013, p. 130). Around 2008, it entered a phase of normalised development and, for a period, was even associated with "justice-oriented" expectations such as truth-seeking and public oversight of governmental power (Liu, 2008, pp. 87-89). It was not until after 2015 that doxing increasingly evolved into a form of online violence characterised by identity exposure, sustained collective attacks, and real-world harassment (Chen & Nian, 2022, p. 28). For this reason, criminal law neither needs nor is able to respond to all instances of doxing. Only those doxing practices that display salient features of online violence and reach a certain threshold of seriousness should fall within the scope of criminal regulation.

The core difficulty is that China's current legal framework has not yet developed an effective set of criteria capable of distinguishing the degrees of seriousness among different doxing cases. Under the existing normative scheme, doxing is typically subsumed under the evaluative framework of the crime of infringing citizens' personal information. According to the 2017 *Interpretation on Several Issues Concerning the Application of Law in Handling Criminal Cases of Infringing Citizens' Personal Information* issued by the Supreme People's Court and the Supreme People's Procuratorate (hereinafter the "Personal Information Interpretation")—a form of quasi-legislative judicial interpretation that plays an important rule-making role in Chinese criminal justice—the act of publishing citizens' personal information through the Internet or other channels is treated as "providing citizens' personal information" under Article 253-1 of the PRC Criminal Law.

On this basis, judicial practice mainly relies on Article 5 of the Personal Information Interpretation to determine whether the conduct reaches the threshold of "serious circumstances", taking into account factors such as the type and quantity of personal information, the amount of illegal gains, connections with other criminal activities, and prior records. Among these factors, the quantity-based criterion—centred on the number of personal information items—occupies a dominant position in application, while simultaneously constituting the most controversial element of the current approach.

This quantity-centred evaluative approach may have a certain degree of rationality in ordinary personal information crimes, yet it repeatedly fails in doxing cases. Unlike typical offences that involve infringing small amounts of information from a large number of victims, doxing is generally directed at a specific individual. Its conduct is characterised by the systematic collection and public disclosure of identity-related information concerning one or a few targeted victims. Even where the disclosed information appears diverse—such as national identification numbers, contact details, home addresses, workplaces, and social media accounts—the limited number of victims means that a single doxing episode often falls short of the quantitative thresholds required for criminal prosecution under the judicial interpretation.

This structural mismatch results in many doxing practices with significant real-world harms being excluded from the scope of criminal regulation. Only extreme cases—such as those involving repeated doxing or already producing severe consequences—can "barely" enter criminal proceedings. Consequently, although doxing is pervasive in practice, only a very small number of cases are ultimately processed through the criminal justice system (Liu & Zhou, 2023, p. 21).

In response to this dilemma, existing scholarship has argued that doxing is, in essence, an act of "public disclosure" of personal information rather than a mere act of "providing" such information. The two differ fundamentally in terms of the scope of the audience and the mode of dissemination. While "providing" typically presupposes disclosure to a relatively specific recipient, "public disclosure" is directed at an indefinite public. Therefore, subsuming doxing under the category of "providing" personal information may fail to capture its distinctive risk profile (Liu & Zhou, 2023, p. 21).

However, the further question is not simply the conceptual distinction between "providing" and "public disclosure". The more fundamental issue is whether the current evaluative scheme should continue to treat the quantity of personal information as the core criterion for determining the seriousness of doxing conduct. If one merely holds that, under the same amount of disclosed information, doxing entails broader dissemination and higher risks of subsequent third-party harm (Wang, 2025, p. 146), then it may still be possible to accommodate doxing within the existing framework by proportionally lowering the quantitative thresholds. Yet if information quantity itself cannot effectively reflect the real-world danger and the degree of legal-interest infringement produced by doxing, then merely adjusting the thresholds would not address the problem at its root. In that case, it would be necessary to move beyond a single quantitative approach and develop a distinct normative method specifically suited to doxing.

3. The Analytical Logic of Assessing Legal-Interest Infringement in Doxing: A Dual-Layer Perspective

As the preceding chapter has shown, current judicial practice in China typically subsumes doxing under the evaluative framework of the crime of infringing citizens' personal information, and tends to apply the quantitative standards established by the Personal Information Interpretation—most notably the "information type × information quantity" formula—to determine whether the conduct constitutes "serious circumstances". Yet, for doxing as a behavioural form directed at specific individuals and characterised by identity exposure and socially amplified dissemination, it remains to be demonstrated whether the quantitative criterion merely sets the prosecutorial threshold too high, or whether it is methodologically incompatible with the underlying risk structure of doxing itself.

To address this question, the analysis must return to the starting point of normative evaluation: what legal interest does the crime of infringing citizens' personal information protect, and through what legal-interest structure does criminal law transform "information infringement" into a legally assessable "real-world risk"? On this basis, this chapter first clarifies the protected legal interests of the offence, and then examines whether information quantity can function as an appropriate intermediate factor for assessing the degree of legal-interest infringement in doxing cases, thereby laying the foundation for the subsequent argument.

3.1 Reassessing the Protected Legal Interests of the Crime of Infringing Citizens' Personal Information

With regard to the protected legal interests of the offence of infringing citizens' personal information, Chinese scholarship has developed several representative positions. These include: (1) a private-law–oriented view that conceptualises the protected interest as an individual right, typically framed as the right to informational self-determination (Liu, 2019, pp. 19-33); (2) a public-law–oriented individual-right view that identifies the protected interest as the right of citizens' personal information to be protected (Jiang, 2021, pp. 37-55); (3) a supra-individual view emphasising the "security of information circulation" (or "flow security") as the core protected interest (Chen, 2022,

pp. 73-80); and (4) a composite-interest approach that treats the offence as protecting a combination of multiple legal interests (Xu, 2022, pp. 119-125).

This paper argues that a purely individual-right/self-determination approach cannot adequately explain the structurally intensified risks faced by individuals in the digital society. Conversely, a purely public-interest or flow-security approach tends to dilute the concrete position of victims and risks reducing the offence to an abstract governance instrument. By contrast, defining the protected legal interest of this offence as the "right of citizens' personal information to be protected" better accommodates the dual demands of individual-right protection and risk control.

As research in this area has deepened, scholarly understandings of the legal-interest structure of this offence have gradually shifted from a single, flat conception to a multilayered and more three-dimensional analytical framework. Whether scholars define the protected legal interest as personal information rights, or as the right of personal information to be protected, or even as personal information security, there is a growing consensus on one point: criminal law does not ultimately protect "information as such". Rather, it protects information (or the right of information to be protected) as a *shielding-layer legal interest*, thereby preventing substantive infringements of deeper legal interests—such as damage to human dignity, or threats to personal and property security—arising from the loss of informational control. The former functions primarily as the means of protection (the shielding layer), whereas the latter constitutes the ultimate object of protection (substantive legal interests).

As research in this area has deepened, scholarly understandings of the legal-interest structure of this offence have gradually shifted from a single, flat conception to a multilayered and more three-dimensional analytical framework. Whether scholars define the protected legal interest as personal information rights, or as the right of personal information to be protected, or even as personal information security, there is a growing consensus on one point: criminal law does not ultimately protect "information as such". Rather, it protects information (or the right of information to be protected) as a *shielding-layer legal interest*, thereby preventing substantive infringements of deeper legal interests—such as damage to human dignity, or threats to personal and property security—arising from the loss of informational control. The former functions primarily as the means of protection (the shielding layer), whereas the latter constitutes the ultimate object of protection (substantive legal interests) (Ouyang, 2025, pp. 99-100).

In this sense, the degree of legal-interest infringement in cases involving the unlawful handling of citizens' personal information should ultimately be assessed by reference to the extent of harm to, or risk imposed upon, the victim's substantive legal interests. Yet, in most cases, the degree of impairment of such substantive interests cannot be directly quantified. For instance, doxing may simultaneously endanger a victim's human dignity, tranquillity of private life, and even personal safety, but the *extent* of such harm is rarely susceptible to straightforward measurement.

For this reason, normative assessment requires the introduction of an intermediate evaluative factor—a proxy through which the seriousness of substantive-interest infringement may be indirectly reflected. To qualify as a legitimate intermediate factor, two conditions must be satisfied. First, it must be formally measurable, or at least capable of being categorised into distinct types with qualitatively different characteristics. Second, it must exhibit a relatively stable correspondence with the degree of substantive harm or risk. Only when both the formal and substantive requirements are met can changes in the intermediate factor serve as a reliable basis for evaluating the degree of infringement of the victim's substantive legal interests, thereby providing objective and consistent standards for conviction and sentencing.

3.2 The Logic of Using Information Quantity as an Intermediate Factor

It is evident that the quantity of personal information infringed can directly reflect "more or less" in numerical terms, and therefore satisfies the *formal requirement* of an intermediate evaluative factor. Whether it can genuinely perform the function of reflecting the degree of legal-interest infringement, however, depends on the more crucial *substantive requirement*: namely, whether information quantity can stably map onto the extent of substantive harm (or risk) suffered by the concrete victim(s).

For analytical convenience, let **X** denote the overall infringement of substantive legal interests caused by a given act of infringing citizens' personal information; let **a** denote the substantive-interest infringement suffered by an individual victim; and let **N** denote the number of victims. The following relationship can then be expressed:

$$X=a\times N$$

In this basic relationship, neither information quantity nor information sensitivity/type has yet been explicitly incorporated. If information quantity is to serve as an intermediate evaluative factor for assessing the degree of legal-interest infringement, it is necessary to further decompose the variable **N** (the number of victims). In general, the number of victims can be understood as the ratio between the total volume of personal information infringed (**S**) and the amount of personal information infringed per victim (**s**). Accordingly:

$$N=\frac{S}{s}$$

By substituting the above relationship into the previous equation, we obtain:

$$X=a\times\frac{S}{s}$$

This derivation indicates that information quantity **(S)** can function as an intermediate proxy for assessing the overall degree of substantive legal-interest infringement only if there exists a relatively stable correspondence between the substantive harm suffered by each individual victim (**a**) and the amount of information infringed with respect to that victim (**s**).

In practice, this prerequisite can be satisfied in some paradigmatic forms of personal information crimes. Take, for example, real-estate intermediary cases, where offenders unlawfully obtain large volumes of housing-related information (including homeowners' names, telephone numbers, national identification numbers, unit numbers, and floor areas) (Note 1). In such cases, the content and amount of information infringed per victim are broadly uniform.

Under these circumstances, both the substantive harm borne by an individual victim (**a**) and the amount of information infringed with respect to that victim (**s**) remain relatively fixed. As the total volume of infringed information (**S**) increases, the number of victims (**N**) and the aggregate degree of substantive legal-interest infringement (**X**) will increase in a roughly linear manner. Accordingly, in this type of case, using information quantity as a criterion for assessing the seriousness of legal-interest infringement has a certain degree of rationality.

When the content and structure of the infringed information vary across cases, however, the relationship among the above variables becomes unstable. For example, in an automobile insurance company case, the information provided or sold by the offender included names, national identification numbers, home addresses, contact details, and various vehicle-related data (Note 2). The amount and types of personal information infringed per victim in such cases differ significantly from those in real-estate intermediary cases.

In this context, if one still attempts to compare seriousness by information quantity, it becomes necessary to assume that the substantive harm suffered by an individual victim (**a**) can be reduced to the simple sum of harms associated with each individual piece of information—namely an *additivity assumption*:

$$a=a_1+a_2+a_3+\ldots+a_s=\bar{a}\times s$$

Combining this assumption with the foregoing formula yields the following further derivation:

$$X=\bar{a}\times S$$

Within this evaluative framework, the aggregate degree of legal-interest infringement is treated as a linear function of information quantity, while the harm associated with each individual data point is assumed to be determined by its level of sensitivity. Following this logic, judicial practice operationalises seriousness by distinguishing between ordinary personal information, generally sensitive information, and highly sensitive information, and by setting corresponding quantitative thresholds. This yields the familiar "information type × information quantity" model, which remains workable in most forms of information-trading crimes.

It must be stressed, however, that the above additivity assumption—namely, that the harm to an individual victim can be linearly decomposed into the sum of harms generated by each item of information—does not hold in doxing cases. The legal-interest infringement caused by doxing cannot be adequately understood as a mere accumulation of discrete informational harms. Even a small amount of sensitive information, or even seemingly ordinary or already public information, may—once combined into a particular configuration—enable the precise identification of the victim and generate a

highly concentrated and significant real-world risk. Explaining this phenomenon requires the introduction of the mosaic theory.

3.3 Critiquing Information Quantity as an Intermediate Factor

The mosaic theory originally emerged in the fields of national security and intelligence as a criterion for determining whether state secrets have been unlawfully disclosed, and was later incorporated into privacy analysis (Ai, 2020, p. 2). In *United States v. Jones*, some Justices of the United States Supreme Court, in their concurring opinions, suggested that the one-off or short-term collection of location information does not necessarily constitute a privacy infringement. However, the long-term and systematic aggregation of seemingly fragmented location data can reveal an individual's patterns of life, behavioural habits, and even value orientations, thereby amounting to a substantive invasion of privacy. Within the context of electronic tracking, the mosaic theory can thus be understood as follows: although the monitoring of any single movement trajectory may not constitute a "search", once multiple trajectories are aggregated, the resulting location pattern becomes qualitatively different and may constitute a search—precisely because what it reveals goes beyond the information contained in each discrete trajectory (Ostrander, 2011, p. 1735).

The central insight of mosaic theory lies not in whether each isolated piece of information is individually highly sensitive, but in the structural exposure risk produced through aggregation. The theory demonstrates that informational harm does not necessarily accumulate in a linear and additive manner: a set of data points that appear harmless in isolation may, once combined in a particular configuration, disclose far more than the sum of their individual components. This logic directly undermines the assumption that overall infringement can be assessed by simply adding up the harm of each discrete item of information.

When introduced into the analytical context of doxing, mosaic theory reveals that the harmfulness of doxing is not determined by the sheer quantity of disclosed information. Rather, its core risk lies in the "structural exposure" of the victim's identity through aggregation. Even when the amount of disclosed information is limited, once it becomes sufficient to precisely identify the victim, it may trigger persistent harassment, mass online attention, and real-world risks, thereby generating a pronounced sense of insecurity and serious infringements of dignity and personal autonomy.

From the perspective of harm dynamics, in typical forms of crimes involving the infringement of citizens' personal information, aggregate legal-interest infringement tends to increase linearly with the quantity of information involved. In doxing cases, by contrast, there is no stable linear correspondence between information quantity and legal-interest infringement. The relationship is better approximated by a logistic function. Where the disclosed information remains insufficient to identify the victim, the harms associated with different data points are relatively independent, and legal-interest infringement rises only slowly as more information is disclosed. Once aggregation reaches a critical threshold at which the victim's identity can be locked in, the infringement exhibits a marked qualitative leap and accelerates sharply. After the victim's identity has already been fully exposed, further increases in the

quantity of disclosed information generate diminishing marginal increments in infringement.

Accordingly, the degree of legal-interest infringement in doxing cannot be modelled as a linear function of information quantity. Rather, it constitutes a form of *structural risk* jointly shaped by information aggregation, identity exposure, and socially amplified dissemination. Under such conditions, continued reliance on a quantity-centred quantitative approach not only fails to capture the concrete risks faced by victims, but also normatively obscures the fundamental differences among doxing incidents in terms of their modes of infringement and risk structures. This indicates that the core difficulty in assessing the seriousness of doxing does not lie in whether the numerical thresholds are set too high or too low. Instead, it stems from a more basic problem: a structural mismatch between the prevailing evaluative method and the distinctive characteristics of doxing as a behaviour type.

4. A Methodological Turn in Assessing the Legal-Interest Infringement of Doxing

Having shown above that information quantity cannot serve as a stable criterion for evaluating the degree of legal-interest infringement in doxing, it becomes necessary to further reconsider the adequacy of the prevailing evaluative approach. This chapter does not seek to exhaustively list substantive factors relevant to seriousness. Rather, it addresses a methodological question: in doxing cases, once the quantity-based standard exhibits structural failure, what evaluative pathway should be adopted to assess the degree of legal-interest infringement? On this basis, this article argues that typological analysis should replace a single quantitative metric and become the primary method for assessing the seriousness of doxing.

Doxing is a complex behavioural form constituted by multiple interacting elements, and its harmfulness cannot be reduced to any single variable. On the one hand, it is difficult to use absolute quantitative indicators—such as the number of disclosed data points—to precisely measure legal-interest infringement across heterogeneous cases. On the other hand, if evaluation relies only on broad value judgements to include or exclude entire categories of doxing from criminal regulation, the resulting boundary between criminal and non-criminal conduct tends to depend on highly abstract "exception clauses", offering little operational guidance for judicial practice. By contrast, typological analysis based on variations in behavioural elements can both avoid the distortions produced by mechanical quantification and distinguish different structures of risk within an abstract normative framework. It is also more conducive to building a layered interface between administrative sanctions and criminal enforcement. Where the quantity-based standard has already demonstrated structural failure, typological analysis is not merely one option among many; it is the only feasible approach capable of reconciling general normative assessment with case-specific heterogeneity.

Existing scholarship has recognised the need to differentiate the unlawfulness of doxing by reference to variations in its constituent elements. For instance, one study argues that the degree of illegality in doxing is largely shaped by the manner in which personal information is disclosed or disseminated, the scope of its circulation, and the likelihood that it will trigger subsequent harms or risks of harm in

particular contexts (Wang, 2025, p. 146). This approach is instructive in that it treats doxing as an element-sensitive phenomenon rather than a homogeneous behavioural category. Overall, however, much of the literature remains at the level of generalised assessment. It rarely specifies how different elements function within the structure of legal-interest infringement, and thus cannot be readily translated into an operational evaluative pathway for judicial application.

Among existing typological studies, David M Douglas' typology is particularly influential. He distinguishes doxing into three types—deanonymising doxing, targeting doxing, and delegitimisation doxing—highlighting how different modes of exposure generate different levels of real-world risk and social-evaluative harm for victims (Douglas, 2016, p. 199). The principal contribution of this typology does not lie in the labels of the categories themselves, but in the methodological move it represents: by adopting typological reasoning, Douglas rejects an "all-or-nothing" assessment of doxing and instead proposes a more flexible normative framework capable of mediating between freedom of expression, privacy protection, and real-world security. Substantively, *deanonymising doxing* refers to disclosing identity information that was previously anonymous or semi-anonymous, thereby linking an online persona to an identifiable real-world individual. *Targeting doxing* focuses on disclosing information that directly, or with a high probability, enables the localisation of the victim in real-world space—such as home or workplace address or contact details—thereby shifting online conflict into offline life. *Delegitimisation doxing* involves the assemblage and recontextualisation of personal information so as to drive sustained negative moral judgement and social stigmatisation. Taken together, this typology provides a useful reference point for understanding behavioural heterogeneity in doxing from the perspective of legal-interest infringement.

It should be noted, however, that the "degree of legal-interest infringement" is itself an overarching evaluative concept. A typology that merely classifies doxing by reference to the object of disclosure or the mode of disclosure remains insufficient to fully capture the heterogeneity of infringement across different behavioural forms. Typological reasoning, in this context, should not be pursued for the sake of constructing a purely formal classification scheme. Rather, its purpose is to enable a normatively meaningful assessment of legal-interest infringement. Accordingly, when typological analysis is adopted as the evaluative approach, the criteria for classification must themselves be carefully selected and constrained.

More specifically, typological classifications should satisfy at least three requirements. First, normative relevance. The selected criteria must be capable, at the normative level, of reflecting differences in the extent to which the conduct infringes protected legal interests; they should not hinge on non-normative considerations such as the actor's moral character or self-professed motivations. Where a classificatory criterion lacks an internal connection to legal-interest infringement, the resulting typology cannot advance the purpose of normative evaluation. Second, objective ascertainability. The attributes used for classification should be identifiable and provable through external behavioural manifestations and objective facts, rather than inferred from internal mental states or speculative assessments of subjective

intent. Otherwise, even a theoretically appealing typology would be difficult to operationalise under evidentiary rules in judicial practice. Third, salient differentiation. Provided that the criteria are normatively relevant, the resulting categories must exhibit substantial differences in the nature of infringement or in their underlying risk structures, rather than merely reflecting minor variations in degree. Without clear categorical boundaries, typological analysis risks undermining—rather than enhancing—determinacy in legal judgement.

5. Conclusion

In the digital environment, doxing has evolved from an episodic form of informational misconduct into a structurally intensified mode of online violence. Its harmfulness no longer derives from the sheer volume of disclosed data, but from the aggregation of dispersed information and the ensuing exposure of personal identity within an open and socially amplified network. Under such conditions, traditional quantitative standards centred on information quantity are ill-suited to capture the actual degree of legal-interest infringement caused by doxing conduct.

By adopting a dual-layer theory of legal interests, this article clarifies that the criminal law's concern with personal information does not terminate at informational interests themselves. Rather, personal information functions as a shielding layer through which criminal law ultimately protects substantive legal interests such as human dignity, tranquillity of private life, and personal security. From this perspective, the assessment of seriousness must focus on how informational handling translates into concrete risks to these substantive interests. The analysis grounded in mosaic theory further demonstrates that informational harm does not accumulate in a linear manner. Instead, once aggregated information crosses an identification threshold, legal-interest infringement may undergo a qualitative leap—rendering information quantity an unreliable proxy for seriousness in doxing cases.

On this basis, the article argues that the core difficulty in current practice lies not in whether quantitative thresholds are set too high or too low, but in a structural mismatch between quantity-based evaluation and the distinctive risk profile of doxing. Where identity exposure, social amplification, and sustained harassment constitute the primary sources of harm, seriousness cannot be meaningfully assessed through numerical accumulation alone.

Accordingly, this article advances a methodological shift from single-factor quantification toward a typological mode of normative assessment. Rather than prescribing rigid categories or expanding the scope of criminalisation, this approach seeks to identify evaluative dimensions that are normatively relevant, objectively ascertainable, and capable of differentiating distinct risk structures. Such a methodological reorientation provides a more coherent basis for distinguishing administrative violations from criminal offences in doxing cases, thereby enhancing the predictability and rationality of administrative–criminal coordination.

Ultimately, the proposed framework does not aim to intensify punitive intervention. Its normative ambition is more modest but more precise: to restore proportionality and coherence in the assessment of doxing by aligning evaluative methods with the actual mechanisms through which harm is produced. In doing so, it contributes to a more balanced accommodation between personal information protection, the maintenance of cyberspace order, and the principle of restraint in criminal law.

References

Aghili, S., Mathews, R., & Lindskog, D. (2013). *A study of doxing, its security implications and mitigation strategies for organizations*. Concordia University of Edmonton. https://doi.org/10.7939/r3-nh05-7x95.

Ai, M. (2020). From mosaic theory to perfect surveillance theory: Theoretical evolution of legal regulation of big data investigations. *Peking University Law Review*, *21*(1), 1-20.

Chen, Q. X., & Nian, X. (2022). Changes in the information dissemination mechanism of human flesh search (2001-2021). *Shanghai Journalism Review*, (11), 16-30.

Chen, X. B. (2022). Determining the protected legal interest of infringing citizens' personal information and its judicial application: From the perspective of quantifying personal information. *Journal of People's Public Security University of China (Social Sciences Edition)*, (2), 73-80.

Douglas, D. M. (2016). Doxing: A conceptual analysis. *Ethics and Information Technology*, *18*(3), 199-210.

Hao, Y.H., & Zhou, F. (2013). The first decade of "human flesh search" (2001-2012): An empirical study based on collective behaviour theory. *Modern Communication (Journal of Communication University of China)*, (3), 129-134.

Jiang, T. (2021). The justificatory rules for protected legal interests of new offences: Taking the protected legal interest of the crime of infringing citizens' personal information as an example. *Chinese Journal of Criminal Law*, (3), 37-55.

Liu, R. (2008). Distinguishing "human flesh search" from public opinion supervision and online violence. *Shanghai Journalism Review* , (9), 87-89.

Liu, X.Q., & Zhou, Z.J. (2023). The regulatory dilemma of online violence in criminal law and its solution. *Rule of Law Research*, (5), 16-27.

Liu, Y. H.(2019). The protected legal interest of the crime of infringing citizens' personal information: Affirming individual legal interest and emerging rights—An analysis from the perspective of the Draft Personal Information Protection Law. *Chinese Journal of Criminal Law*, (5), 19-33.

Ostrander, B. M. (2011). The mosaic theory and Fourth Amendment law. *Notre Dame Law Review*, 86(4), 1735.

Ouyang, B.Q. (2025). *Criminal law dogmatics of cyber and data crimes* (pp. 82-83). Beijing: Law Press China.

Wang, H. W. (2025). The criminal law regulation of doxing in the context of cyber violence. *Journal of Comparative Law*, (3), 136-150.

Xu, Y. M. (2022). Re-analysis of the protected legal interest of the crime of infringing citizens' personal information: A discussion based on the enactment of the Personal Information Protection Law. *Social Scientist*, (8), 119-125.

Notes

Note 1. Real Estate Intermediary Case of Yang Liuzhong for Infringing Citizens' Personal Information, Xinzheng People's Court of Henan Province, Criminal Judgment, (2021)豫 0184 刑初 162 号.

Note 2. Automobile Insurance Company Case of Bao Wei for Infringing Citizens' Personal Information, Tongzhou District People's Court of Nantong City, Jiangsu Province, Criminal Judgment, (2020)苏0612刑初593号.