
Criminal Law Regulation of Human Flesh Search and Lessons from Foreign Experience

Lai Wei*

School of Law, Shanghai University of Finance and Economics, No. 777 Guoding Road, Yangpu District, Shanghai 200082, P.R. China

**Corresponding author: Lai Wei.*

Abstract

With the iterative development of network technological tools, “human flesh search” has evolved from scattered individual behavior into organized and industrialized forms of online violence, such as “doxxing and public shaming,” thus posing serious threats to citizens’ personal information rights and interests, human dignity, and even personal safety, becoming a focal point of cyberspace governance. This research, focusing on the criminal law regulation of human flesh search, sorts out the practical dilemmas faced by the application of Chinese criminal law, and proposes plans based on foreign legislative experience, which that China still has application disagreements regarding the criminal law boundary of publicly disclosed personal information, the determination of “serious circumstances,” the application of concurrence of charges, and conditions for exclusion of criminal liability. This paper concludes that publicly disclosed personal information should be subject to typified treatment, the standard of “serious circumstances” should be substantively determined, the logic of concurrence of charges should be clarified, and typified grounds for exclusion of criminal liability should be constructed, thus promoting effective regulation of human flesh search.

Keywords

human flesh search, crime of invading the privacy of people, publicly revealed personal information, agreement on charges

1. Introduction

Over the past few years, online violence has been on the rise. Human flesh search is an example of typical online violence that has evolved over time to be organized and industrialized. The emergence of new forms of online violence like doxxing and public shaming has become frequent due to the advancement of network technology toolkits. Since the 2023 Liu XX case (which included doxxing as part of the crime of infringing on the personal information of citizens) through the 2026 Lin XX and Wang XX case (in which personal information of over 600 million people were obtained illegally and a website known as the social engineering database was created, and this case was listed by the Supreme People's Court as a typical case), numerous human flesh search cases have resulted in severe outcomes, including the mental breakdown of victims and death, thus, they are a serious threat to citizens’ rights to personal information, privacy, human dignity, and personal safety. Legal interests and societal harm have also grown by a large margin.

The initial researchers generally described human flesh search as a combination of information technology as a form of online activity that depends on netizens to conduct a particular type of information search [1]. Due to the appearance of web violence like doxing and public humiliation, the initial definition is no longer able to include the new characteristics. Human flesh search does not cause damage through information acquisition but through the process of disclosure, dissemination, and utilization. In terms of dissemination mechanisms its harmfulness is exactly in the fact that it forces a person to be in the spotlight; increased visibility is already a form of harm, and the victim experiences a constant stream of pressure exerted by spectators and crowds [2].

As per the example of Lin XX and Wang XX issued by the Supreme People's Court, it can be seen that the actors developed a social engineering database to make money and spread private and abusive information as a form of doxxing via encrypted groups, which demonstrates the high level of social harmfulness of the human flesh search in the context of artificial intelligence.

The academic community and judicial practice disagree regarding what legal interests can be violated by human flesh search, which is split between the individual legal interest theory and the composite legal interest theory. The individual legal interest theory assesses its damage through the traditional personality right, including the right to privacy, right to reputation, and right to informational self-determination [3]; the composite legal interest theory claims that the infringed legal interests are pluralistic and dynamic, and they depend on the particular means of acquiring and spreading the information [1]. This paper will take an analytical approach to diffusion, starting with the internal and then moving to the outside, layer by layer. The acquisition of information stage primarily encroaches upon the right to informational self-determination; intrusion into systems also constitutes a threat to the computer information system security. The dissemination of information destroys privacy, human dignity, and reputation; derivative harassment and threats also destroy personal safety. And when it becomes online hunting, it also causes disorder in cyberspace. Consequently, human flesh search is an act that violates composite legal interests that emanate outwards individual rights and interests [4].

The paper will try to clarify the theoretical framework of criminal law regulation of human flesh search, study the implementation problems of the existing regulations, suggest the scheme of the typified treatment of the criminal law border of publicly known personal data, challenge the strict formulation of the concept of serious conditions, explain the issue of concurrence of charges and the number of offenses, and define clear and typified conditions for excluding criminal liability. Meanwhile, it also references and considers the legislative history of Hong Kong, the Netherlands, Germany, and other legal systems, and finally suggests a plan to improve criminal law regulation.

2. Practical Dilemmas and Reasons Behind Criminal Law Regulation of Human Flesh Search in China

The Criminal Law Regulation of Human Flesh Search Currently Faces Four Practical Dilemmas

2.1 Ambiguous Criminal Law Evaluation of Publicly Disclosed Personal Information

The secondary authorization theory and the purpose compatibility theory are two general analytical directions of academia. Nevertheless, the secondary authorization theory struggles with addressing why primary acquisition and secondary provision are regarded as different phenomena, whereas the purpose compatibility theory struggles with identifying the primary intention at the moment of information disclosure objectively [5]. In the criminal law norms, it is not obvious that the fact that the information was already disclosed eliminates the criminal illegality of its further acquisition, organization, and dissemination by itself. Assuming that the criminal law still covers publicly released personal information, there is no uniform and definite legal determination of the boundaries of reasonable use and unlawful use and the criminal illegality criterion of criminalizing secondary processing [5,6]. Thus, the issue of how the fact that the information is already public influences the decision of illegality in human flesh search cases has become a burning question to be resolved.

2.2 Rigid Determination Standards for “Serious Circumstances”

The 2017 judicial interpretation promulgated by the Supreme People’s Court and the Supreme People’s Procuratorate is largely based on quantitative measures, including the amount of information and illegal profits, to define the term of severe circumstances in the offense of infringement on citizens’ personal information [7]. But the damage caused by human flesh search is mostly in indirect effects that occur after information has been disseminated, including the destruction of the victims’ lives and work, psychological trauma, or even extreme incidents, which do not have to be reflected in the amount of information or illegal profits. Many instances of doxxing can only be prosecuted under the catch-all clause of other circumstances of a serious nature [7]. Nevertheless, the implication of the catch-all clause is unclear, and its overuse contradicts the clarity of the legal principle, which makes numerous instances unable to meet the level of criminalization.

2.3 Confusion in the Application of Concurrence of Charges

Human flesh search consists of various steps, including acquiring information, disseminating information, and further infringement. It may be a violation of the crime of infringing the personal information of citizens, the crime of insult, the crime of defamation, the crime of picking quarrels and provoking trouble, and the crime of illegally using information networks at the same time. The Supreme People’s Court, Supreme People’s Procuratorate, and Ministry of Public Security only give general guidelines of concurrence on the guiding opinions on online violence but do not present specific differentiating criteria of the multi-stage conduct of human flesh search [8]. The main judicial challenge is to define the singularity or plurality of conduct: when it is treated as one act, and imaginative concurrence is used to select the greater penalty, it is effortless to underestimate legal interests; when it is considered as separate acts, and cumulative punishment for several crimes is used, the law prohibiting duplicate assessment is infringed, which puts the court into a dilemma between two options [8].

2.4 Conditions for Exclusion of Criminal Liability are NOT Clearly Stipulated

Human flesh search and monitoring of public opinion share a border that is hard to differentiate between legitimate information flow and human flesh search. The absence of standardized decriminalization regulations is prone to lead to inappropriate criminalization [1]. According to Article 27 of the Personal Information Protection Act and Article 1036 of the Civil Code, the civil-law exception of reasonable processing of personal information available to the general public exists, however, the connection of the prepositive law with the evaluation of human flesh search by criminal law has not yet reached an agreement on the issue in theory and practice [3]. At the same time, public opinions regarding human flesh search are ambivalent and polyphonic [9,10]. Vague decriminalization criteria, coupled with evidentiary and public opinion elements, may allow judges to behave in a bipolar manner of not enough punishment or over-extension of the criminal law, thus, making it hard to strike the right balance between protection of legal interests and restraint in criminal law [6].

3. Solutions to the Problems

3.1 Typified Treatment of Publicly Disclosed Personal Information

Personal information that has been made public is not automatically excluded under criminal law; the fundamental problem is whether later processing behavior presents any new personal or property danger to the person whose information is processed. Human flesh search filters and mixes publicly available data, altering its initial public status, and also has an opportunity to be criminalized. Guiding Case No. 194, the case of Xiong Changheng, explains that alteration in the scope, purpose, and use of publicly disclosed information is not considered reasonable processing, but when the facts are severe, the offense of infringing on the personal information of citizens can be established. Gu and Lu [6], taking the degree of accessibility to accessible subjects as a criterion, initially subdivide publicly disclosed personal information into two major categories that include information disclosed to the general populace and information disclosed to particular individuals; the former is subdivided into personal information with limited access groups and personal information disclosed to family and friends only, and different regulations apply to each category. Disclosure is classified by Douglas [11] into three types based on the nature and effects of disclosure: de-anonymization, target

identification, and delegitimization; Jiang [3] brings this typological model into doctrinal studies to help differentiate among the behavioral patterns of human flesh search.

The paper develops a double standard of the objective level of openness combined with the subjective goal of the processing. In the case of fully public information, the concept of consent is presumed in theory; going beyond reasonable expectations, or provoking online violence, is an exceptional crime. With the expansion of the range of access to limited-open information and the growth of the risk of harm, it also becomes criminally punishable, which balances personal self-determination and the regular flow of information.

3.2 Substantive Determination of “Serious Circumstances”

The foreign laws on the crime of human flesh search mainly aim at assessing the substance of harm: Dutch criminal law, the two-tier offense system under Hong Kong law, and the Protection against Harassment Act in Singapore do not only consider the amount of information or unlawful profits, but regard harassment, intimidation, and disruption of working life due to the behavior, with certain provisions providing tiered punishment [1]. Similarly, Chinese court decisions like the Liu XX case and the Wu XX and Chen XX case also verify that other serious circumstances can be fully judged based on subjective intent, range of distribution, and real damage [7]. The level of illegality of human flesh search varies depending on how the information is spread and also the likelihood of secondary damage occurring. It is proposed that judicial interpretation should incorporate seriously harassing the lives and jobs of victims and hindering the professional activities as a separate severe situation [1].

3.3 Establishing Unified Application Rules for Concurrence of Charges

The human flesh search is a combination of several links including information acquisition, information transmission and ultimately harm. In assessment, there must be differences based on the stages of behavior and fundamental guidelines and exceptions in the case of concurrence of charges should be set. [8]

In the context of the existing legislation, this paper suggests certain regulations on the use of charges: the crime of violating the personal information of citizens can be used as the core charge to regulate human flesh search. If the distribution of personal information and insult or defamation belongs to one natural act, it is considered as an imaginative concurrence and the punishment is applied based on the heavier crime; the seriousness of the insult or defamation may be regarded as a mitigating factor in sentencing. In case the insult or defamation is a separate independent act, it is assessed individually [8]. In case the insult or defamation action that follows is relatively independent with respect to time and space and is of the severity of an independent crime, the cumulative punishment of several crimes should be applied.

The case of Chen XX, Lu XX, et al. in the act of starting quarrels and inciting trouble as issued by the Supreme People’s Procuratorate is a good example. In this case, after the information was obtained via doxxing, the participants engaged in a sequence of online violence and intimidation actions, and finally received a cumulative sentence on account of the crime of starting quarrels and inciting trouble and the crime of infringing the personal information of citizens [7].

It should be mentioned that the existing stage of human flesh search has developed into the creation of so-called social engineering databases, websites, or the creation of encrypted communication groups to industrialize “doxxing”. Such activity could be treated as the front-end form of criminal conduct of violating the rights to the personal information of citizens and goes beyond the limits of the constitutive elements of the infringement of the rights to the personal information of citizens and breaks the infringement of illegal use of information networks. It also indicates that in the case of criminal behavior that was performed by the perpetrator at various stages and has relative independence, it must be assessed individually based on its particular constituent elements; in case both stages are mutually independent and meet the constituent elements, it should be punished as a combination of several crimes.

3.4 Typified Provisions on Conditions for Exclusion of Criminal Liability

There is a crossover between the concepts of human flesh search and the monitoring of public opinion, and it is acceptable to remove information disclosure conducted in the name of the public interest from criminal liability [1,6]. According to Article 64(4) of the Hong Kong Personal Data (Privacy) Ordinance, there are

several exceptions, including criminal investigation, court order, consent of the data subject, legal news, and disclosure in the public interest [1]. The German Criminal Code Article 126a(3) refers to the social adequacy clause and considers civic education, news reporting, scientific research, and teaching as reasons to exclude liability under the law [1].

Based on the experience of other countries, four forms of exclusion of criminal liability can be identified: in the form of public interest, in the form of consent of the data subject, in the form of enforcement of legal norms, and in the form of lawful news reporting [1,8]. Nevertheless, two restrictive principles of relevance and necessity need to be formulated: the information disclosed should be directly relevant to the interests of the public to be preserved, and the extent of the information communicated should be restricted to the essential amount to check the unlawful behavior. The disclosure of information behaviour is justifiable only when it satisfies the conditions; it does not make the pattern of human flesh search behaviour legal. The author proposes clarifying the different reasons behind exclusion of criminal liability through judicial interpretation, and how they apply in order to defend the area of expressing public interest and avoid the incorrect expansion of decriminalization standards [1,8].

4. Conclusion

The peculiarity of the Internet era is the ability of each person in society to be a producer and distributor of information on the Internet and a carrier of online violence. The study of legal regulation of human flesh search under criminal law involves not only the preservation of cyberspace order, but most importantly, the legal protection of fundamental rights like human dignity and the personal safety of citizens. In accordance with the existing criminal law framework, to address the practical challenges of the criminal law regulation of human flesh search, it was decided to type criminal law assessments of publicly available personal data, determine the substance of serious situations, and create uniform guidelines on concurrence of charges, and create type conditions to exclude criminal liability. Judicial interpretations under the principle of legality can be employed to hone adjudication principles, ensure that the behavior of human flesh search is rationally regulated, and give future judicial practice some sort of a blueprint that is clear and inclusive.

References

- [1] Huawei Wang. (2025). The criminal law regulation of doxing in the context of cyber violence. *Comparative Law Research*, (3), 136–150. https://kns.cnki.net/kcms2/article/abstract?v=sb6TFb_dKprfDT4NygsYxzjeOjiGTB85B6xLupy4tJpr7tg86-CiSa52xSi1-XDjB-0r0ngcMySzbWqBBGpA5KEuopGRbodO-1lyvWPQW8G4AQQar0K6aSGH33Cp2dBW2rUIE3oHh0yAcN81O_HAAvx9BA7mp8Z-vRDpWSBSU_QCPFw-9y9nw==&uniplatform=NZKPT&language=CHS.
- [2] Trottier, D. (2017). Digital vigilantism as weaponisation of visibility. *Philosophy and Technology*, 30 (1), 55–72. <https://doi.org/10.1007/s13347-016-0216-4>
- [3] Xiaodong Ding. (2024). The Chinese approach to legal protection of non-confidential personal information. *Law Science*, (3), 3–16. https://kns.cnki.net/kcms2/article/abstract?v=sb6TFb_dKpoAJycl7ri4fb10bFyt9dv_Se26_HZiNsCiqfMds1Jozv_ia60WR7JjIfyRoa7_wtBh8RPIawJQyv4mwZxar6ql2qrOPvhQVW1H0F_x23Lg_AvfmiLY7SBXomQTWDMiUVIRAI-xdXnWimdpP9NvyYf8X2rVsO9LhEd1PhX22m--Q==&uniplatform=NZKPT&language=CHS.
- [4] Haiyang Jiang. (2024). Criminal law doctrinal analysis of “doxing” disclosed personal information. *Journalism World*, (10), 64–75. <https://doi.org/10.15897/j.cnki.cn51-1046/g2.20241104.001>.
- [5] Huawei Wang. (2022). Criminal law protection of publicly disclosed personal information. *Chinese Journal of Law*, 44 (2), 191–208. https://kns.cnki.net/kcms2/article/abstract?v=sb6TFb_dKppXZ_dUBkthFz1Dgtz95jS-MbfmITq8b_gHA64aoiy5YXQlzoQYKXj8eMyPi5NUX-

[oTpn3aMJ7jaoDLQqhP9SzMa6D6cj0cQXN9RF5umzxpMuxcSW68-Rq8H1-NfbUFQILfrHwRjIv3-j4PfPJcGcXsiEhSPzL2U=&uniplatform=NZKPT.](https://doi.org/10.20034/j.cnki.hxfxp.2025.05.003)

- [6] Jianghong Gu & Jiahong Lu. (2026). The criminal law boundary and typified regulation of processing publicly disclosed personal information. *People's Procuratorate*, (10), 87–89.
- [7] Zhiheng Li. (2025). Criminal law regulation of doxxing-type online violence: A commentary on the first doxxing online violence case, Liu XX's crime of infringing on citizens' personal information. *Huxiang Law Review*, 5 (5), 23–35. <https://doi.org/10.20034/j.cnki.hxfxp.2025.05.003>.
- [8] Xiang Luo. (2024). Choices and reflections on the path of criminal law regulation of cyber violence: From the perspective of disaggregating the crime of insult. *Peking University Law Journal*, 36 (2), 285–306. <https://link.cnki.net/urlid/11.2447.D.20240319.1059.002>.
- [9] Chang, L. Y. C., & Poon, R. (2017). Internet vigilantism: Attitudes and experiences of university students toward cyber crowdsourcing in Hong Kong. *International Journal of Offender Therapy and Comparative Criminology*, 61 (16), 1912–1932. <https://doi.org/10.1177/0306624X16639037>.
- [10] Trotter, D., Huang, Q., & Gabdulhakov, R. (2024). Digital media, denunciation and shaming: The court of public opinion. Routledge. <https://doi.org/10.4324/9781003453017>.
- [11] Douglas, D. M. (2016). Doxing: A conceptual analysis. *Ethics and Information Technology*, 18 (3), 199–210. <https://doi.org/10.1007/s10676-016-9406-0>.

Funding

This research received no external funding.

Conflicts of Interest

The authors declare no conflict of interest.

Acknowledgment

This paper is an output of the science project.

Copyrights

Copyright for this article is retained by the author (s), with first publication rights granted to the journal. This is an open-access article distributed under the terms and conditions of the Creative Commons Attribution license (<http://creativecommons.org/licenses/by/4.0/>).