Criminal-Law Regulatory Pathways for Doxxing in Online Abuse-A Comparative Law Perspective

Zhiyuan Yang
Yantai University, Yantai, Shandong, China

Abstract: This article discusses the criminal-law regulatory pathways of doxxing as online abuse, which involves a comparative-law perspective on the vague definition of doxxing, the structural problems with criminal regulations, and domestic and foreign legislative experiences. Comparing the US, Germany, Netherlands and Hong Kong (China), legislative experiences show regulatory problems in all areas, and some response measures were adopted, including extending offense definitions, creating special provisions, or improving civil remedy enforcement. In China, Article 253-1 of the Criminal Law (the crime of infringing citizens' personal information) should clarify which types of behavior are illegal when disclosing personal information, set separate thresholds and criminal sentences for criminalization, resolve issues of legal application for special circumstances, and form a system of exculpatory grounds consisting of enforcing legal norms, revealing illegal or criminal behavior, news reports, and good faith, in order to follow the principle of relevance and necessity, maintain a balance between individual rights and the public interest, and implement targeted regulation.

Keywords: Doxxing; Online Abuse; Publicly Available Personal Information; Balancing of Interests; Exculpatory Grounds

1. Problem Statement

According to the 56th Statistical Report on the Development of China's Internet issued by CNNIC in June 2025, there were a total of 1.123 billion internet users in China, with a total number of 32.62 million domain names. The cyberspace has become a major channel for hundreds of millions of people to get and spread information[1]. But also there has been a lot of online abuse. Doxxing as an online abuse has been evolving into a problem that poses a serious threat to the citizen's rights and social order, and it has a paradoxical nature of minimal input information but great social harm that is urgent for the criminal law to intervene. In recent years, online abuse has often been mentioned in the media, and has affected people from famous figures to common internet users. Mild cases of personal information being disclosed and individuals experiencing harassment, this violates personality rights and in turn violates the rule of law and public morals; in more serious cases it can even lead to offline violent tragedies [2-3].

2. Dilemmas of Criminal Regulation of Doxxing

Doxxing is an important mode of online abuse. Its concept is hazy in both theory and practice, hampering accurate criminal control. In the 2023 Opinions on Punishing Online Abuse, it is clearly stated that doxxing can constitute criminal punishment, but the document does not express this sufficiently, making the categories of law vague, and the vagueness of categorization results in the absence of standards for judicial application and thus no unification of theory [4]. Observing the pattern of doxxing, we can see that due to the rapid development of the Internet, its forms have shifted on the axis of technological iteration; and the change in evaluative focus on its main purpose has led to a wider divergence in the definition of it.

China's pre-existing norms stress the main difference that, under Article 3(1) of the 2017 Interpretation of the Supreme People's Court and Supreme People's Procuratorate on Several Issues Regarding Application of Law in Dealing with Criminal Cases of Infringement of Citizens' Personal Information, the criminal conduct in doxxing is mainly the disclosure or provision of personal information rather than the acquisition of information [5]. This legislative conception corresponds to a harm-oriented result orientation, but it doesn't define the legal distinction between gaining and disclosing, making it hard

to discern whether internet users who merely collect information should be responsible in actuality, and there are arguments over the question of responsibility [6]. Legal definitions do not provide technical means, stages of conduct, or nature of harm [7], so judicial authorities are unable to carry out normative correction on a case-by-case basis for “doxxing”. As for the present related behavior, it has been addressed only indirectly through invoking other crimes, such as the crime of infringing citizens’ personal information, insult or defamation [8].

Structural Deficiencies in the Current Criminal Regulation of Doxxing: The criminalization of doxxing is a highly complex matter, and its structure contains many deficiencies. In the current legal system, the punishment for doxxing is extremely severe; if someone commits doxxing, they will be charged with multiple offenses including illegal intrusion, unlawful acquisition of citizens' personal information, and provoking trouble. In addition, it is easy to fall into the trap of doxxing under existing laws and regulations[9]. For example, in the case of the "Lanxi High School Student Death," a female student at Lanxi No.2 High School was murdered after her friend, who knew about her situation, spread false information on WeChat. This case is not an isolated incident; there have been numerous similar cases, which can be categorized as doxxing. In summary, there are significant structural deficiencies in the current criminal regulation of doxxing[10].

The current system of criminal-law norms in China shows prominent structural deficiencies and a poor fit between the specific rules when regulating doxxing, which makes it hard to hit exactly on the intricate patterns of conduct and harmful results of doxxing[11].

From the perspective of legislative structure, China's Criminal Law has no systematic protection system for personal privacy, domestic tranquility, and personal freedom, which is an important obstacle to the regulation of doxxing. In the realm of comparative law, many countries have created independent offenses like “stalking/harassment,” which brings about a type of unauthorized, continuous information tracking and sharing as well as the risk of real-world danger under the purview of criminal regulations[12]. Such offenses can cover subsequent harassment that comes after illegal acquisition of information from doxxing, as well as providing ex-ante protection against any potential infringements [13]. In contrast, the Chinese Criminal Law has not created such specific crimes, leaving the doxxing activities that are solely for the purpose of collection and aggregation, without directly insulting or defaming, without a direct basis for legislation. [14]. In practice, judicial actors will often try to use the offense of xunxin zishi for regulation, but the offense of xunxin zishi requires the offender to commit typical violent acts such as "insulting" or "threatening"[15]; most doxxing participants are only responsible for collecting or spreading information and do not engage in public insults, so it is difficult to satisfy the elements of the offense of xunxin zishi.

3. Comparative-Law Study on Criminal Regulation of Doxxing

3.1 United States

As the first country to develop internet technology, the U. S started to explore how to regulate conduct involving online infringement early on. Yet in the criminal regulation of doxxing, there is a typical pattern of "indirect regulation". On the federal level, there are two statutes limiting extreme behaviors which may include doxxing, but since its constituting elements are strict, and the actual application is hard, the law has a hard time suppressing doxxing in an all-encompassing and effective manner[16].

The Interstate Communications Act (18 U. S. C. § 875(c)) is one of the earliest federal online threat provisions. It provides that any person who in interstate or foreign commerce sends a communication containing a threat to kidnap any other person or to injure the person of another shall be punished by a fine of not more than 0, 000 or by imprisonment for not more than five years, or both. In terms of purpose, it is aimed at fighting against direct threats to one’s personal safety through the internet, and protecting citizens from violent intimidation. And yet there is a striking discrepancy between this provision and what one might expect from a definition of doxxing: the primary harm of doxxing isn’t generally the threat itself, but the possibility of real-world harm resulting from an accumulation and exposure of information. Most doxxing cases don’t involve explicitly saying “kidnap” or “hurt,” but instead, through making public people’s home addresses, contact information, and other private data, they create situations that

enable others to harass or hurt the victims in person.

The Federal Stalking Statute (18 U. S. C. § 2261A(2)) is a federal statute that might also be applicable to the doxxing situation. It makes it a crime when someone does something through the mail or an interactive computer service or an electronic communication service or system and they do it to try to kill, hurt, trouble, or scare another person.

However, the application of this law is difficult to apply. First, it's hard for the police to prove, they have to show that the person had the specific idea to kill, hurt, annoy, or scare someone, and that their actions made the other person feel scared or sad. Second, the scope is too limited: the majority of doxxing cases are not so severe that they cause fear of death or serious bodily harm. They are more likely to cause an inconvenience and disruption to the victim's daily life-a pressure which is unlikely to amount to the statutory requirement of "substantial emotional distress". Third, the enforcement resources are also limited: as federal authorities have a higher priority of investigating major cases such as terrorism and organized crime, individual and dispersed onlineinfringement crimes such as doxxing are less likely to be given sufficient investigation resources.

3.2 Germany

In the past few years, Germany has also faced severe doxxing problems under digitalinfringement. In 2019, there was a nationwide event where the private information of lots of politicians and public figures was shown on the Internet, this became the cause for changing laws. It exposed the severe damage done to people's rights by doxxing and made lawmakers improve specific legal rules, so there was a mix of different tracks like laws about crimes related to data, offenses involving privacy, and newly invented special offenses.

The existing criminal code provision on data crimes in Germany forms the base of regulation of doxxing. Sections 202a (Data Espionage), 202b (Interception of Data), and 202c (Preparation for Data Espionage and Interception) build a gradation against illegal data acquisition; whereas Sections 303a (Data Alteration) and 303b (Computer Sabotage) aim at harmful data tampering and system intrusion. Doxxing scenario, where the perpetrator gains unauthorized access to databases through hacking or breaches privacy protections to obtain non-public personal information such as medical records or communications, directly grounds criminal liability under these provisions. Section 201 of the Criminal Code states that the distribution of images or videos, and other visual material revealing the private life of someone else, as well as other identifiable images, without permission, can be punished with up to two years in prison or a fine; if it significantly lowers the social status of the victim or causes mental suffering, the penalty is increased. When it comes to doxxing, if a perpetrator discloses someone's private life or, through a combination of pieces of information, results in a full exposure of the victim's private life, it could be considered an "invasion of the intimate sphere" under § 201.

3.3 Hong Kong (China)

In the face of the more and more rampant doxxing, the Hong Kong SAR China legislature responded. In 2021 it amended the Personal Data (Privacy) Ordinance, adding a specific target for doxxing, which provides a solid legal basis for combating doxxing.

Amended Sec 64(3A)(3B): Without the data subject's consent, disclosing that person's personal data with the intent that the subject or a family member suffer a specified harm upon conviction, is punished by a level-6 fine and 2 years imprisonment. The provision specifies the exactness of the illegality of doxxing, both subjectively and objectively. Subjectively, it means whether he intends to cause damage to the object or to the family of the victim, or is indifferent to it. Objectively, it is disclosure without consent, combined with the possibility of harm-the defining characteristics of doxxing. Personal data that has been disclosed online can lead to serious consequences for a person's life and reputation, which is the intention of these provisions and to prevent people from punishing them.

3.4 Netherlands

In July 2023, with help from the Minister of Justice, the Dutch Parliament agreed to make doxxing against someone a crime, which was a big step toward stopping people from being mean on the internet. It came into force on January 1, 2024, with Article 285d added to the Criminal Code to establish an independent

offense aimed at doxxing, thus providing a clear legal basis for enforcement.

Article 285d new Article states that anyone who gets someone else's or a third party's personal information and spreads or does something to make this information public has committed a crime if they have certain subjective goals or objective bad results. Combining subjective and objective elements, the provision takes in the core of doxxing-unlawful disclosure plus some concrete harm-while also keeping from wrongly judging mere acquisition or harmless spreading.

4. Summary

China's criminal-law regulation of doxxing needs to be improved through its domestic situation and the comparison with other countries to establish a correct and reasonable legal framework. The US indirectly constrains doxxing via the Interstate Communications Act and the Federal Stalking Statute, but their elements are exacting and coverage limited, making them unsuited to complex situations. Germany makes use of data-crime and privacy offenses to target unlawful acquiring and invading of privacy; leaving a gap for mere aggregation and disclosing. In Hong Kong (China), it amended the Personal Data (Privacy) Ordinance, with the disclosure without consent + intention + harm as the standard for criminalisation, thus identifying the key characteristics of doxxing. The Netherlands added Article 285d, criminalizing "acq. plus disc. with specified harms" as a separate offense, offering a model for specialized legislation.

On the other hand, China's current Criminal Law relies on indirect regulation such as the criminal offence of infringement of citizens' personal information, which is still confronted with gaps in the coverage of the behavior, and structural protection. Moving forward, Article 253-1 should specify the elements of criminalization, and a system of exculpatory grounds must be created to strike a balance between personal-information protection and freedom of expression. To establish a special offense+judicial interpretation+exculpatory mechanisms integration, and strengthen the rule of law foundation for governing onlineinfringement.

5. Enhancing the Current Criminal-Law Framework of China

Some scholars have proposed making a new offense to target doxxing specifically, such as a "crime of disclosing another's privacy," so that when it is done maliciously, the act can be addressed as a separate offense from the underlying crime. This view sees doxxing's main feature as the systematic gathering and disclosure of other people's private information using technology. Its harmfulness is different from privacy torts that have traditionally existed and from regular leaks of personal information; it takes advantage of the openness of cyberspace and people's joint participation to place someone's privacy under the public eye, which causes ongoing mental stress and actual-world risks. Compared to this, regulating doxxing by amending or adding elements to Article 253-1 (the crime of illegally obtaining citizens' personal information), is a more appropriate fit for China's current legal framework and judicial needs. To clarify the types of behaviors that qualify as "unlawful disclosure of personal information," to modify the standards for "serious circumstances," and to differentiate between information categories and levels of malicious intent are the most realistic and effective ways forward. This approach is both conducive to effective control of doxxing and the maintenance of the simplicity and integrity of the criminal law system. It meets the needs of protecting privacy and governing the internet in the digital age.

6. Elements of Criminalization for Doxxing

Once the path of revising Article 253-1 to regulate doxxing is selected, it will be necessary to refine the specific norms to guarantee a correct and effective protection of the protected interests. The first task will be to define clearly that doxxing occurs when the disclosure, release, or dissemination of personal information results in infringement, or the risk of infringement. The real harm that doxxing causes is not just obtaining, but it is making such personal information known to the public or disclosing it, lawfully or unlawfully obtained, and leading to a series of infringements or risks for the victim. the norms should clarify what sort of conduct this is. "Disclosure" means exposing someones personal info on open channels like social platforms and online forums, plus sending it out through groups or communities which are relatively limited but still reach many people. "Dissemination" means spreading it

around-think about sharing the stolen personal info across lots of different channels and layers so more and more people know about it. the following ones are different kinds of infringement or risks: being harassed directly (such as repeated calls, personal harassment, etc.); receiving threats (such as threats of infringement or revealing more privacy); and receiving attacks (verbal abuse, online infringement to spread rumors and so on). For instance, if a perpetrator publishes someone's home address or workplace online and the victim then begins to receive many calls from strangers or even in-person threats, that conduct should be covered by doxxing norms. When the elements are clearly delineated, judicial practice has clear standards for judgment, and it doesn't let certain doxxing behaviors through because they don't know what the conduct is.

7. Building up a System of Grounds for Excluding Criminal Liability in Doxxing

7.1 Acts in Execution of Legal Norms

Law-enforcement organs' collection and disclosure of personal information when they are performing their statutory duties is aimed at carrying out the law and serving the public interest, and usually does not constitute a breach. As an example, based on the Civil Procedure Law and related interpretation provisions, when a judgment debtor refuses to perform their obligation to fulfill a legal instrument that has been declared valid or a condition specified by law is satisfied, the people's court can use public channels to publish some personal information to urge performance. Though it may have implications with regard to privacy, publicity of such is still justified with respect to protecting the authority of judiciary and realization of creditor's rights. Also, the public security organ may publish wanted notices or bulletins during criminal investigation to catch the suspects or find the facts, and they may disclose some important clues including photo, physical appearance and ID number.

7.2 Unlawful or criminal conduct disclosure

If someone collects and divulges the personal details of a criminal or wrongdoer, and if the revealing aids to promptly halt wrongdoing and safeguard the public's interests, then-though the disclosure involves privacy-it could be justifiable through the principle of legal proof or a weighing of interests.

7.3 Objective, Neutral News Reporting

As a key part of the public watch, news reporting usually enjoys advantages to collect and spread news even when personal information is concerned. For example, when investigating the environmental pollution of an enterprise, the media can obtain and publish the responsible person's name, position, and photos of the polluted area through legal means to expose the illegal act and promote rectification. So long as it is not for personal gain and it doesn't break journalist codes, it's most likely fine. But if reporting veers from normal practice and is open to be malicious, partial, and partial, the gathering and dissemination of private data is likely to be forfeit justification.

7.4 Justification by Good Faith

Cyberspace ordinary user find hard to judge whether the truth and legality of information in cyberspace. Where an individual is acting in good-faith belief that they fit within the aforementioned justifications to search for and release information, no criminal liability should be imposed unless it can be demonstrated that the individual was aware that the objective criteria for exculpation would not be met. For example, after a missing child report, a person may post a photo of what they believe is the child and the contact information for the presumed parents in a neighborhood group to help. Though this involves another person's personal information, the subjective purpose is helpful, and the way is not obvious beyond the reasonable limit; if the situation fails to conform to the legal standards of exculpation in the end, the actor's intention and the low degree of harmfulness of the conduct still need cautious weighing before criminal liability is imposed. This ground for exclusion shows criminal law's principle of restraint: if the conduct has no serious malice and only minor harm, civil remedies or administrative penalties are better than too many criminal laws.

8. Basic Principles Governing Exculpation in Doxxing Cases

Principle of Relevance is the primary consideration for applying exculpatory grounds to doxxing cases. Doxxing can only gain justification if and to the extent that it directly serves to protect or realize a legitimate interest.

Like whistleblowing, the point is the disclosure of some specific information about wrongdoing, it must tightly connect to that wrongdoing and be closely tied to the protection of a legal interest. And that's the same for doxxing. For example, in the widely talked about "Chengdu woman dropping a dog" incident, the woman's behavior is said to have broken the law, and the police had already gotten involved. In such circumstances, the proper course was to wait for a fair judicial resolution, and continued, severe doxxing by some users was not directly conducive to the protection of rights or public interest, but rather gravely disrupted the individual's life and infringed upon her lawful rights, and so there was no justification.

Necessity is also a necessity. In considering the justification of doxxing one must consider whether it was necessary for a legitimate aim. Among all sorts of ways to protect lawful interests and realize public goals, doxxing should be the last resort-it is only after we exhaust all other, milder methods that cause lesser infringement on personal rights that we can use it to accomplish the purpose.

9. Conclusion

Doxxing as a principal modality of online infringement faces tough challenges for criminal regulation. According to an in-depth research of China's current situation of criminal law and a comparative study of laws in the US, Germany, the Netherlands, and HK (C), it is concluded that China should regulate doxxing by modifying Article 253-1 (the offense of disclosing the private affairs of citizens). The definition of the offense must specify that the act of disclosing or disseminating personal information that subsequently leads to an infringement or poses a risk of such an infringement constitutes the main offense, i.e., it includes both the act of disclosing or disseminating and the harassment, threats, or attacks that result therefrom. Set independent criminalization and sentencing thresholds; consider the actor's mental state; adopt a low threshold for obvious malice and gross negligence resulting in serious consequences; clarify the standards for attributing responsibility. And building a system of grounds for exculpation is also crucial-including the acts of executing legal norms, disclosing unlawful and criminal behavior, neutral and objective news reporting, and good faith justification. The application of such grounds is subject to the principles of relevance and necessity, and doxxing can only be used when closely connected with the aim of achieving legitimate interests, as a last resort, when milder measures are not sufficient.

Criminal regulation of doxxing must find a fine line between protecting personal-information rights and safeguarding the public interest and freedom of speech. Improving criminal law, establishing an effective exculpation system, and the law can properly regulate doxxing and protect the rule of law and public order and good morals in cyberspace.

References

[1] Wang, H C. (2025) Regulation of Human-flesh Search in the Context of Cyberinfringement. J. Comparative Law Studies, 03: 136-150

[2] Li, F. (2025) Research on Investigation Strategies for Cyberbullying Crimes Based on SWOT Analysis. J. Journal of Hebei Public Security Police Vocational College, 02: 27-30

[3] Guo, Z, Xu, H. (2024) Criminal Law Evaluation of "Human-Flesh Search" Leading to Suicide from the Perspective of a Pan-Moralist Society. J. Juvenile Delinquency Issues, 06: 55-69

[4] Jiang, H. (2024) Dogmatic Analysis of the Criminal Law Regarding the Disclosure of Personal Information through Human-Flesh Search. J. Journalism, 10: 64-75

[5] Liu, H. (2024) Research on the Criminal Regulation of Cyberinfringement. D. Jiangxi University of Finance and Economics, 20: 24-32.

[6] He, J, Jing, P. (2024) Research on criminal acts involving human flesh search from the perspective of protecting publicly disclosed personal information. J. Huazhang, 03: 140-143.

[7] Li, Y. (2024) "Human-flesh Search" Behavior in the Netherlands Will Be Classified as a Crime. J. JiaoChan FengYun, 01: 50-51

[8] Chen, Q. (2023) Semantic Evolution of "Human-Flesh Search": An Exploration Based on Raymond Williams' "Keywords" Approach. J. Modern Communication (Journal of Communication University of China), 09: 36-45

[9] Nian, F, Liu, X, Zhang, Y. (2022) Human flesh search based on information coupling.

J. International Journal of Modern Physics B, 36: (3):

[10] Wang, J. (2022) Research on "Human-powered Search" and Privacy Protection in the New Media Era. J. News Culture Construction, 02: 50-52

[11] Cui, X. (2022) On the Legal Liability of "Human-Flesh Search". J. Heilongjiang Human Resources and Social Security, 02: 131-134

[12] Dong, J. (2019) On the Protection of Civil Rights in "Human-flesh Search" -- From the Perspective of the Conflict between Privacy and Freedom of Speech. J. Journal of Yancheng Institute of Technology (Social Science Edition), 04: 31-35

[13] Baasanjav, Undrah B. (2019) A critical discourse analysis of the human flesh search engine[J]. Media Asia, 46: 18-34.

[14] Manea, T. (2020). Considerations regarding the regulation of body search and physical examination in the code of criminal procedure, including the relationship between the two evidentiary proceedings in connection with the possibilities of investigating the body. J. Conferința Internațională de Drept, Studii Europene și Relații Internaționale, 8: 216-223.

[15] Ciobanu, F. C. (2025). The participation of specialists in carrying out body search in criminal proceedings. J. Legea şi Viaţa,7: 352-363.

[16] Hardcastle, R.(2019) Law and the human body: property rights, ownership and control. Bloomsbury Publishing, 2007.

