Proceedings of the 3rd International Conference on International Law and Legal Policy
DOI: 10.54254/2753-7048/55/20240096

Digital Privacy Challenges in China: Human Flesh Search

Yuhang Duan[1,a,*]

[1]*School of Arts, University of British Columbia, Vancouver, Canada*
a. duanyuh2@student.ubc.ca
**corresponding author*

Abstract: The advent of digital technology has brought unprecedented convenience but also significant challenges to personal privacy, particularly in China. The phenomenon of "human flesh search" (HFS), facilitated by both legal internet platforms and illicit information trade, has become a source of major privacy violations. This paper explores the effectiveness of China's current legal measures, particularly the Criminal Law as Article 253(A), in safeguarding personal information against these threats. It also examines the implications of these legal shortcomings on individuals' daily lives and privacy. The dangers of human searches and their impact on the reality level are analyzed through detailed profiling of the parties involved in cases related to cyber violence. This report analyzes these legal inadequacies, comparing them with international standards, and suggests enhancements to better safeguard personal privacy in the digital age. By learning from international practices and rigorously adapting and enforcing its laws, China can better safeguard its citizens against privacy violations and set a standard for personal information protection in the digital era.

Keywords: Cyberbullying, Human Flesh Search, Law, China

1. Introduction

The rapid expansion of internet usage in China has been accompanied by increased cybersecurity threats, particularly those affecting personal privacy. According to data from CNNIC (China Internet Network Information Center), as of December 2023, China's internet user base reached 1.092 billion, marking an increase of 24.8 million from December 2022. The significant growth in internet users also mean increase cases of online criminal activities. The various forms of cybercrime can be broadly classified into three categories: attacks on individuals, attacks on property, and attacks on governments. The first category encompasses crimes targeting individuals, including identity theft, cyber-infringement, and credit card fraud. The second category encompasses attacks on property, such as distributed denial-of-service (DDoS) attacks, computer virus installation, and copyright infringement. The third category encompasses attacks on governments, including hacking, cyberterrorism activities, and the dissemination of political propaganda. HFS belongs to the first category, it exemplifies the urgent need for robust legal measures, as it often leads to personal data exposure without consent, resulting in harassment and other harms. The inadequacies of China's Personal Information Protection Law (PIPL) in addressing the pervasive issue of human flesh search (HFS) highlight the urgent need for legal reforms that not only enhance data protection but also ensure the dignity and privacy of individuals. This essay examines the shortcomings of current regulations,

DOI: 10.54254/2753-7048/55/20240096

compares them with international standards, and proposes comprehensive measures to strengthen legal protections and mitigate privacy violations in the digital age.

2. The Phenomenon of Human Flesh Search

Human Flesh Search (HFS) is a unique and often troubling phenomenon that has gained significant attention in the digital age. The designation originating in China, this term refers to a type of collective online activity focused on uncovering facts about specific events or publicizing information about a targeted individual. HFS involves the collective efforts of netizens to track down and expose personal information about individuals who are perceived to have committed social or moral transgressions. This process usually begins on social media platforms where users collaborate to gather and disseminate private details of the targeted individuals. The information uncovered can range from phone numbers and home addresses to intimate photos and personal histories, all of which are shared widely across the internet [1,2]. The motivations behind HFS are varied, including the pursuit of vigilante justice, moral policing, and sometimes mere curiosity or entertainment. Cultural factors also play a significant role in the prevalence and impact of HFS. In collectivist societies like China, where community and social harmony are highly valued, actions that are perceived to disrupt these values can trigger strong collective responses, including HFS. This cultural orientation towards collective action can intensify the effects of cyberbullying, making it more socially acceptable and widespread [2]. Understanding these cultural dynamics is essential for developing targeted interventions that can effectively mitigate the harm caused by HFS and similar practices.

The connection between HFS and cyberbullying is profound, as both practices involve the use of digital platforms to inflict harm on individuals. Cyberbullying encompasses various forms of online harassment, such as flaming, exclusion, and cyberstalking. One particularly invasive form of cyberbullying is doxing, which involves publishing private information without consent, closely mirroring the activities involved in HFS [1]. This overlap is significant because it highlights the broader issue of how digital tools are used to invade personal privacy and disrupt lives. Both HFS and cyberbullying leverage the anonymity and reach of the internet to amplify their impact, making it difficult for victims to escape the resulting harassment. The psychological and social impacts of HFS are severe and far-reaching. Victims of HFS often experience a range of negative emotions, including anxiety, depression, and feelings of helplessness. The public exposure and harassment can lead to social ostracization, job loss, and in extreme cases, suicidal thoughts [2]. The anonymity of perpetrators and the viral nature of information dissemination exacerbate these effects, creating a power imbalance where victims feel vulnerable and defenseless against the collective actions of faceless attackers. This aspect of HFS and cyberbullying underscores the urgent need for robust legal protections and effective coping mechanisms to support victims.

Addressing the phenomenon of HFS is crucial not only for protecting individual privacy but also for maintaining societal norms around respect and decency. In many cases, HFS is justified by participants as a form of social justice or moral rectification. However, this perceived justification does not mitigate the harm inflicted on victims. Instead, it often perpetuates a cycle of harassment and retaliation that can escalate quickly and unpredictably [2]. Legal frameworks such as PIPL aimed to curb these practices, but enforcement challenges and legal ambiguities often limit their effectiveness.

3. Types of HFS

The article Human Flesh Search - Facts and Issues by Rui Chen and Sushil K. Sharma examines the phenomenon of HFS in China, discussing its characteristics, implications, and societal impacts. Here is an analysis of distinct types of HFS and how they have harmed individuals or society:

DOI: 10.54254/2753-7048/55/20240096

3.1. Vigilante Justice and Social Punishment

HFS often triggered by perceived social injustices or morally questionable actions by individuals, which catch the public's attention through social media or other online platforms. This form of digital vigilantism arises when netizens collectively decide to take justice into their own hands, bypassing legal processes. These actions are usually fueled by strong emotions and a sense of moral outrage, leading to public shaming and harassment of the targeted individuals.

For example, consider the case of Wang and his mistress. Allegations surfaced about Wang's extramarital affair, which led to his wife's suicide. This scandal quickly garnered public outrage. Incensed by the moral breach and its tragic consequences, internet users mobilized to track down and expose the personal details of Wang and his mistress. Their private information, including addresses, phone numbers, and workplace details, was widely disseminated online. As a result, both individuals faced severe harassment, illustrating how HFS can lead to intense social punishment and personal suffering [3].

3.2. Moral Policing

HFS is also used by social media users to enforce societal norms and values, often targeting individuals whose actions are considered immoral or socially unacceptable, even if they are not illegal. This type of moral policing reflects a collective effort to uphold communal standards and discipline those who violate them. The public exposure serves as a deterrent to others and reinforces societal norms.

A notable example involves a drunk driver who was identified and shamed publicly through HFS. After the driver's actions were made known online, netizens took it upon themselves to gather and publish his personal information. This public shaming led to significant legal repercussions for the driver, including arrest and legal action. Additionally, the backlash from the online community resulted in the driver facing job suspension and enduring widespread social stigma. This case highlights how HFS can act as an extrajudicial mechanism for enforcing moral standards, often with severe consequences for the individuals involved.

3.3. Anti-Corruption and Transparency

HFS can be a powerful tool for exposing corruption or other unethical behaviors by public figures or government officials, thereby pushing for greater transparency and accountability. In such instances, the collective efforts of internet users can bring to light misconduct that might otherwise remain hidden, promoting a culture of accountability and ethical behavior.

For example, the exposure of a corrupt official through HFS showcases the potential of this practice to serve as a check on power. Netizens, driven by a desire for justice and transparency, conducted their own investigations and unearthed evidence of corruption. This information was then widely shared online, leading to legal and professional consequences for the official involved. The collective digital scrutiny forced the authorities to take action, demonstrating how HFS can function as a grassroots mechanism to combat corruption and promote transparency in governance

4. Current Legal Inadequacies

4.1. Article 253(A) of Chinese Criminal Law

Article 253(A) [Crime of Infringing Citizens' Personal Information] regulates: “Whoever, in violation of the relevant provisions of the State, sells or provides others with citizens' Personal Information, if the circumstances are serious, shall be sentenced to fixed-term imprisonment of not more than three

DOI: 10.54254/2753-7048/55/20240096

years or criminal detention, and/or be fined; if the circumstances are especially serious, he shall be sentenced to fixed-term imprisonment of not less than three years but not more than seven years, and be fined.

Whoever, in violation of the relevant provisions of the State, sells or provides others with the citizens' personal information obtained during the course of performing duties or providing services shall be given a heavier punishment in accordance with the preceding paragraph.

Whoever illegally obtains the above-mentioned information by theft or otherwise shall be punished in accordance with the provisions of Paragraph 1.

Where an organization commits any of the crimes mentioned in the preceding three paragraphs, it shall be fined, and the persons directly in charge of the organization and other persons directly liable shall be punished in accordance with the respective provisions of the preceding three paragraph."

4.2. China's Current Legal Framework

4.2.1. Vagueness and Enforcement

The laws often contain vague terms that complicate enforcement and lead to inconsistent judicial rulings. This ambiguity undermines the potential for effective legal recourse for victims of privacy breaches [4].

Regarding the scope of the subject of this crime, some scholars argue that it is a special subject, namely, the staff of state organs or financial, telecommunications, transportation, education, and medical institutions. These institutions, whether state organs or service providers, have access to a significant number of citizens' personal information due to their public functions or service responsibilities. However, there are scholars suggest that the legislative process should expand the scope of the crime to include any individual or unit. For example, institutions like online shopping platforms, logistics companies, executive search firms, intermediary organizations, market research companies, and real estate companies, they may also leak citizens' personal information.

The crime currently only stipulates penalties for the act of "selling or illegally providing citizens' personal information," but it neglects the behavior of the staff of the institutions personally disseminating the personal information they have access to. The reason for punishing the act of "selling or illegally providing citizens' personal information" is to prevent personal information from becoming widely known through illegal dissemination, thus damaging the tranquility of private life [4].

4.2.2. Scope of Protection and Platform Responsibility

Current regulations do not fully address the multifaceted nature of privacy, which encompasses not only data protection but also dignity and freedom from harassment. While some laws mandate that platforms protect user data, they do not clearly define the scope of this responsibility, particularly when breaches occur through user-posted content [4]. The internet has provided a convenient platform for the buying and selling of others' personal information. On legitimate platforms such as Taobao, one can find relevant merchants offering human flesh search services. Additionally, on the dark web (including non-real-name registration platforms like Telegram), there are over tens of thousands of cases of various leaked data sold annually, with the total amount of leaked data reaching billions of pieces and transaction amounts exceeding 1 billion yuan. These publicly sold leaked information includes citizen information from government agencies, customer information from financial institutions such as banks and securities, as well as subscriber information from major telecommunications operators and customer/user information from various industries including the internet, express delivery, hotels, real estate, aviation, hospitals, and schools.

DOI: 10.54254/2753-7048/55/20240096

5. Case Study of Jiang Ge

The Jiang Ge case is a poignant example of the complex interplay between privacy, public scrutiny, and cyberbullying. Jiang Ge, a Chinese student in Tokyo, was murdered in 2016. Key individuals involved included Jiang and her roommate, Liu Xin. On the night of the murder, Jiang was attacked by Chen Shi Feng, Liu's ex-boyfriend, after Liu sought refuge in their apartment and allegedly locked Jiang out during the altercation [5]. This case rapidly drew massive media attention and public reaction. Therefore, understanding this phenomenon is crucial as it highlights how public scrutiny can lead to severe invasions of privacy and cyberbullying, illustrating the need for ethical standards in media and online behavior.

5.1. Moral Policing in Jiang Ge Case

As been said, the incident sparked extensive media coverage in China, with many blaming Liu for not aiding Jiang. The public reaction was intense, leading to widespread scrutiny and cyberbullying against Liu, driven by emotional and sensationalized reporting. Moreover, Jiang Ge's mother was also harmed by the human flesh search, as her personal information was exposed, making her a target of online harassment. The intensity of this digital mob justice highlights the urgent need to address privacy concerns and establish ethical guidelines for online conduct in the age of social media. The media played a significant role in shaping public opinion during the Jiang Ge case. Extensive coverage focused heavily on Liu Xin, critiquing her for not aiding Jiang during the attack and for not contacting Jiang's mother promptly. Sensationalist reports and emotional storytelling fueled public anger, leading to cyberbullying and moral judgment against Liu. This media-driven narrative shifted the focus from Chen Shi Feng, the accused murderer, to Liu, exacerbating public scrutiny and digital harassment [5]. The online gatherings of netizens gradually lead to offline actions, their real-world influence is significant and has a high potential to trigger actual actions. For example, Jiang Ge's mother posted online petition for the death penalty of Chen Shi Feng. Statistics show that 1.5 million netizens participated in the petition. Meanwhile, the public remained dissatisfied with the possibility that Liu Xin might not face the same legal consequences as the murderer, leading to a surge of online violence against her. For instance, her and her family's home addresses, workplaces, and license plate numbers were exposed [6]. Netizens not only hurled insults and curses at Liu Xin on online platforms but also extended these threats into real life, with many people making threatening and abusive phone calls to Liu Xin and her family. This collective online behavior exacerbated the cyberbullying against Liu, leading to severe consequences such as losing her job and being forced to change her name.

5.2. Reflection on the Phenomenon of Media Trials in Criminal Case

It is worth to mention that the case underscores the need for responsible journalism that balances factual reporting with ethical considerations. The press often identifies criminal suspects early in the judicial process, driven by a public interest in crime news and a constitutional commitment to press freedom. This practice, however, can harm suspects' privacy and reputations and challenge the presumption of innocence. Legal protections exist but are limited, and ethical guidelines vary widely among media outlets. The press should exercise greater caution in identifying suspects, protecting individuals' privacy and reputation until guilt is proven. This cautious approach helps maintain a balance between transparency and personal rights, ensuring that individuals are not prematurely judged by the court of public opinion. Credible media should also avoid publishing exaggerated, sensational, and biased information to prevent social dysfunction. Ultimately, online public opinion cannot determine court verdicts. The internet provides a channel for the public to express their emotions, and the power of public opinion, as an "invisible tool" to criticize criminal suspects, can only exert psychological pressure on them.

DOI: 10.54254/2753-7048/55/20240096

6. Analysis of Personal Data Protection between EU and China

In the European Union, data protection is considered a fundamental right, reflecting a strong cultural emphasis on privacy. The General Data Protection Regulation (GDPR), which came into effect in May 2018, sets stringent standards for data protection, ensuring that personal data is processed lawfully, transparently, and for specific purposes. The GDPR grants extensive rights to individuals, including the right to access, rectify, and erase their data, and limits governmental surveillance. This regulation emphasizes strong data protection, holding organizations accountable for data breaches with significant fines, up to 4% of global annual turnover. The GDPR's strict enforcement mechanisms and the role of the European Data Protection Board ensure uniform application across the EU, fostering a high level of trust in digital transactions [7].

In contrast, China prioritizes national security and social stability over individual privacy, exercising strict control over the Internet through aggressive surveillance measures. The concept of cyber-sovereignty is central to China's approach, requiring both domestic and foreign companies to comply with stringent Internet regulations and surveillance standards. China's personal data protection framework is evolving, with laws such as the Cybersecurity Law and the upcoming Personal Information Protection Law aiming to regulate data handling practices. However, these laws often lack the comprehensive coverage and enforcement mechanisms seen in the GDPR. Penalties for data breaches in China are relatively lenient, and the focus remains more on state security than on protecting individual privacy rights [7].

6.1. Data Protection as a Fundamental Right vs. State Security Priority

In the European Union, the General Data Protection Regulation (GDPR) reflects a commitment to privacy as a fundamental human right. It emphasizes the protection of personal data and limits governmental surveillance, demonstrating a cultural preference for privacy over security [6]. In contrast, China prioritizes state security and social stability, implementing extensive surveillance and control measures. Privacy is often secondary to national interests, and data protection laws are primarily designed to maintain state control [7].

6.2. Regulatory Framework and Enforcement

The EU's GDPR provides a detailed regulatory framework with clear guidelines and robust enforcement mechanisms. Significant fines for non-compliance serve as a strong deterrent, ensuring that organizations prioritize data protection [6]. On the other hand, China's data protection laws, though evolving, often lack specific operational requirements and strong enforcement. Penalties for violations are relatively mild, and enforcement is inconsistent, reducing the effectiveness of data protection measures [7].

6.3. Public Awareness and Cultural Emphasis

There is a strong cultural emphasis on privacy in the EU, supported by public awareness campaigns and education. The implementation of the GDPR has been accompanied by efforts to inform citizens about their privacy rights and the importance of data protection [7]. In China, public awareness about privacy rights is growing but remains limited compared to the EU. The focus on state security and control often overshadows efforts to educate citizens about personal data protection [7].

7. Recommendations for Legal Reforms

To mitigate the risks associated with HFS and enhance privacy protection, China should consider several strategies. Firstly, the clarification and strengthening of laws are essential. Specific terms and

DOI: 10.54254/2753-7048/55/20240096

provisions within existing legal frameworks need to be clearly defined to ensure consistent application and enforcement. Moreover, the scope of legal protection must be expanded to cover all aspects of an individual's privacy. Current Chinese laws, such as the Constitution, Civil Law, and Labor Law, mention privacy concerns but are often ambiguously stated and provide limited substantial protection.

Enhanced penalties and enforcement mechanisms are also crucial. Introducing stricter penalties for privacy violations and implementing robust enforcement mechanisms can serve as effective deterrents. The lack of accountability in current human flesh search practices highlights the need for a system where individuals face consequences for privacy breaches and unethical behavior [8]. This can be seen in the disparity between the consequences faced by journalists in traditional media versus the anonymity and lack of accountability in HFS practices.

Public awareness and education play a pivotal role in reducing the incidence of HFS. Increasing public awareness about the importance of privacy and the legal tools available for its protection can foster a more informed and conscientious online community. Education campaigns can emphasize the ethical responsibilities inherent in freedom of expression and the potential harms of violating others' privacy [8]. As observed, the chaotic and often irresponsible dissemination of information in HFS practices can lead to severe consequences for individuals, underscoring the need for a more educated and responsible approach to online behavior.

8. Conclusion

The phenomenon of Human Flesh Search (HFS) underscores the urgent need for robust legal measures to protect personal privacy in the digital age. The rapid expansion of internet usage in China has heightened the vulnerability of individuals to cybercrimes, including the invasive practices of HFS. Current legal frameworks, such as the Personal Information Protection Law (PIPL) and Article 253(A) of Chinese Criminal Law, fall short in addressing the complex and multifaceted nature of privacy violations that HFS entails. These inadequacies are further highlighted by the severe psychological, social, and economic impacts on victims, as illustrated by high-profile cases like that of Jiang Ge. Comparing China's legal protections with international standards, particularly the European Union's General Data Protection Regulation (GDPR), reveals significant gaps. The GDPR's comprehensive and enforceable framework serves as a model for balancing privacy rights with technological advancements. China's focus on state security and control needs to be recalibrated to place greater emphasis on individual privacy rights. Legal reforms in China should include clearer definitions of privacy violations, expanded scope of protection, enhanced penalties, and stronger enforcement mechanisms. Public awareness and education are equally vital in fostering a culture that respects privacy and discourages unethical online behavior. By adopting these measures, China can better safeguard its citizens' privacy, uphold human dignity, and mitigate the pervasive threats posed by HFS and similar cybercrimes.

References

[1] *Chen, M., Cheung, A., & Chan, K. (2019). Doxing: What adolescents look for and their intentions. International Journal of Environmental Research and Public Health, 16(2), 218.*

[2] *Hu, Q., Bernardo, A. B., Lam, S. W., & Cheang, P. K. (2016). Individualism-collectivism orientations and coping styles of cyberbullying victims in Chinese culture. Current Psychology, 37(1), 65-72.*

[3] *Chen, R., & Sharma, S. K. (2011). Human flesh search - facts and issues. Journal of Information Privacy and Security, 7(1), 50-71.*

[4] *Cai Jun. (2010). Rational Analysis of Legislation on Crimes Infringing Personal Information: Reflections and Prospects on the Legislation of this Crime. Modern Law Science, 32(4), 106.*

DOI: 10.54254/2753-7048/55/20240096

[5] *Cheng, X., Yang, Y., & Zhao, Y. (2022). Implicit media anomie of news entertainment oriented: A Social Media Content Study on jiang GE case. Proceedings of the 2022 3rd International Conference on Language, Art and Cultural Exchange.*

[6] *Tone, S. (2017, December 12). How a Chinese student's murder turned into a moral witch hunt. Retrieved from https://www.sixthtone.com/news/1001372.*

[7] *Weber, P. A., Zhang, N., & Wu, H. (2020). A comparative analysis of personal data protection regulations between the EU and China. Electronic Commerce Research, 20(3), 565-587.*

[8] *Hu, N. (2010). Understanding the Human Flesh Search Phenomenon in China (Master's thesis, University of Calgary). University of Calgary. Retrieved from file:///C:/Users/cvwle/Downloads/ucalgary_2010_hu_na_588996.pdf.*