Advances in Social Science, Education and Humanities Research, volume 615
Proceedings of the 2021 4th International Conference on Humanities Education and Social Sciences (ICHESS 2021)

Research on the Regulations of the Aiding Crime in China's Cybercrime Legislation
Taking Canadian Criminal Law as a Reference

Mengshihang Du[1, a, *]

[1]*Department of Political Science, McGill University, Montreal, Quebec, Canada*
[*]*Corresponding author. Email:[a] mengshihang.du@mail.mcgill.ca*

ABSTRACT
The Ninth Amendment to the Criminal Law of the People's Republic of China was a major step forward in advancing cybercrime regulations and punishment. While this change shed light on the Chinese legislature's determination to combat crimes committed via information networks through ways of refining the types of cybercrimes in the face of growing new criminal acts in cyberspace, limitations remain in the face of evolving new cybercrime cases. This article takes a deeper look at the similarities and differences in the cybercrime legislation of China and Canada. It draws attention to their legislative considerations, processes, and cybercrime patterns, both existing and predicted. On the whole, China's innovative addition of a "principalized" aiding cybercrime in the Criminal Law requires further reflection in its regulatory technologies, clearer definitions of certain terms in the articles, setting judging standards to cases, and limiting the scope of penalty for neutral acts of assistance.

Keywords: *Cybersecurity, Aiding Cybercrime, Principal Offender, Neutral Assistance.*

1. INTRODUCTION

On August 29th, 2015, the Ninth Amendment to the Criminal Law of the People's Republic of China (Amendment) was promulgated, once again filling the gaps in cybersecurity regulations and laws in China. The Amendment made modifications in seven aspects, in which additions of provisions on data privacy is deemed the most notable one. Through these additions, apart from directly committing cybercrime, providing help for criminals to perpetrate such crimes is to be punished, officially becoming a charge for facilitating cybercrimes in Chinese Criminal Law. This change shed light on the Chinese legislature's determination to combat crimes committed via information networks through refining the types of cybercrimes in the face of growing new criminal acts in cyberspace.

Apart from China, typical western countries have longer histories governing cybersecurity and engage in different approaches in legislation concerning security in cyberspace. As a leading developed country in the western world, Canada enacted its cybersecurity-related laws as early as 1985 (The Privacy Act). It established a legislative framework of a specific set of statutes and common law rules applicable to Canadian cybersecurity and data protection. Despite lacking an offence specifically for the assistance of cybercrime in Canadian law, the legislative structure is highly integrated and advanced. In a way, the classification of cybercrimes is even more comprehensive and mature, with more developed technologies put in place to tackle pertinent cybercrimes.

These two countries can both exert substantial leverage, and their law-making strategies on cybersecurity are thus influential in dealing with cyber incidents and regulating cyber behaviors domestically and worldwide.

Current studies on either country or comparing the countries in handling cybercrime legislation issues have been scarce. Literature in authoritative journals has identified problems regarding cybersecurity, but most of the articles rather focus on law enforcement in cyberspace and advice to internet users. For example, Fehr criticized the Canadian parliament's response in legislating cyber law to adjust to the surging crime rates in cyberspace but failed to recognize problems existing in the structure of cyber law legislation [1]. In his article that reflected on the latest developments and in criminal procedure law-making related to cybercrime in China [2],

Yong Pi revolved around digital evidence preservation and touched upon only a bit of the trend of international legislation on criminal procedure. As the criminalization of accessory offenders becomes the hot topic in Chinese cyber law-making, the need and the extent of criminalizing certain offenses of cybercrimes must be examined further.

China is currently obscure about whether helping in cybercrime is an act of perpetrating and how the division of responsibility is determined. Canadian criminal law studies have great reference significance for China. Carrying the prime goal of determining if the provider of assistance to the committing of cybercrime should be judged as a principal offender, this article will take a deeper look at the similarities and differences in the cybercrime legislation of China and Canada, also drawing attention to their legislative considerations, processes and cybercrime patterns existing and predicted.

2. COMPARISON OF CHINA AND CANADA'S LEGISLATION PATTERNS AGAINST CYBERCRIME

Over the years from the 2000s to 2015, the People's Republic of China had gradually established principles on the division of labor in Internet management, and relevant departments like the Ministry of Public Security, the Information Office of the State Council, have issued a series of laws and regulations on network and information security. Examples include the Electronic Signature Law, Regulation on the Protection of the Right to Communicate Works to the Public over Information Networks, Administrative Protection of Copyright on the Internet, all of which are administrative regulations. However, it was not until the enactment of the Ninth Amendment to the Criminal Law that the major breakthrough in Chinese cybercrime lawmaking took place. Article 287-2 of the Amendment reads, "clearly knowing that others are using information networks to perpetrate crimes, and providing them with technical support such as internet access, server hosting, web storage, or communications transfer, or providing help such as in advertising and promotions or paying bills, where circumstances are serious, is sentenced by up to three years imprisonment or short-term detention and/or a fine." [3] This official criminalization of accomplices in cybercrimes extended the scope of criminal liabilities in Chinese law. It embarked on key issues that the Chinese government had been facing since the rapid development of cyberspace.

First, cybercrime is not a new type of crime independent of traditional crime but a persistent disease of human society in the information age. According to Yu, technicality was one of the basic characteristics of the network, and network technology played a decisive role in the practice of behavior in cyberspace. In traditional crime, as one of the aiding behavior of a complex crime form, the behavior of providing help progressively became an essential part of cybercrime, and the combination of the network technical support and the direct infringement of cybersecurity law had become a norm of committing cybercrime in the information age [4]. Chinese legislators consider the "help behavior" in cyberspace to have thus a new outstanding presence in crime. They have put in enormous effort in evaluating this criminal behavior while accepting a comprehensive challenge brought to Chinese criminal law by the regeneration of criminal behavior in the information age.

Yu also explains that the reasons for the emphasis on the act of aiding were twofold [4]. Again, the technical nature of cyberspace was pivotal as early technologies were utilized by the specialized elite, which led to a natural, technological gap that prevented ordinary criminals from carrying out cybercrime. Therefore, the number of cybercrimes could be controlled as a whole, and the security in specific cyberspace can be guaranteed. However, with the development of the network, specialization of technology had become increasingly widespread. Many acts had appeared in cyberspace in providing technical support for the implementation of cybercrime, making it possible for the general public to commit cybercrime. It can be said that aiding crime has become a key factor in the vast majority of cybercrime. Secondly, the act of helping has helped achieve the "one to many" patterns of committing a crime due to the convenient transmission and infinite reproduction through the network, which, in real life, would be limited to "one to one" as assistance costs time and money. The helper simply publishes information about the methods, techniques, procedures of the crime to the Internet, and soon a wide range of potential criminals will have access to the information. In the meantime, it also crosses the technical threshold of cybercrime. The resulting danger and real-life damage to legal interests are beyond the reach of a single act of cybercrime. Hence, the harm of aiding goes beyond the danger of the act of the direct perpetrating, and it was deemed essential to create a criminal charge for this act in Chinese cybercrime laws and regulations.

Cybersecurity in Canada is governed by a more complex legal and regulatory framework, which, although lacking a specific charge for the assistance of cybercrime, contains various regulations relating to providing technical or advertising support under different statutes. To examine if this act is attached to as much importance as in the Chinese Criminal Law, it is thus essential to examine the overall cybersecurity framework in Canada.

First of all, it is acknowledged that cybersecurity laws in Canada are "supplemented by sector-based regulators, private corporations and organizations coordinating state and non-state actors and initiatives [5]." Regarding the regulatory and governance framework, the Office of the

Superintendent of Financial Institutions and the Canadian Securities Administration are two major regulators that provide guidance to address cybersecurity risks. In particular, the Cybersecurity Self-Assessment Guidance for Federally Regulated Financial Institutions was released by the OSFI to examine cyber risk management policies and practices. As principal regulatory guidance, they emphasize the necessity for issuers, registrants, and regulated entities to beware of cybercrime and take actions as needed to defend cybersecurity and safeguard their own interests.

Unlike China, the private sector in Canada indeed plays a significant role in setting out the basics. One of the most fundamental statutes within the private sector's control that concerns data protection is the Personal Information Protection and Electronic Documents Act. It is the Federal legislation enacted to protect employee's personal information by nation-wide organizations that are regulated federally, as well as the protection of personal information in commercial activities in all jurisdictions that do not have similar legislation [6]. The 2015 Amendment of the PIPEDA added a provision that requires organizations to keep records of breaches of cybersecurity rules. Those who knowingly fail to do so will be fined up to 100000 dollars, which will soon come into force in the future. With various kinds of security safeguards put in place, organizations are shown to be highly responsible for personal information under their control. With respect to governing personal information in the federal public sector, the Privacy Act is a legal framework that regulates the protection of personal information by the federal government. Canada's Anti-Spam Law is also a new law that contains provisions specifically aiming at combating spam communications in the course of commercial activities.

With a number of statutes enacted to safeguard cybersecurity, the Criminal Code of Canada is believed to be the most definitive law, which sets out categorized criminal offenses in regard to cybercrime. In this sense, different from regulations and guidance, an act, a circumstance, and a consequence are laid out for the proportional punishment of committing cybercrime. As we all know, hacking is one of the criminal offenses under Section 184 of the Criminal Code of Canada, with a sentence of imprisonment of up to five years [7]. It is defined as willful interception of private communications. Section 342.1 of the Code "prohibits fraudulently obtaining any computer service or intercepting any function of a computer system" and "use of a computer system with the intent to commit such an offense and use or possession of a computer password to enable such an offense are also prohibited [7]." Regarding national security, the Criminal Code also punishes information activities that pose threats to national defense, economic interests, or international relations, with a possible sentence of up to 10 years in prison. It is also important to note that sentencing in Canada is determined case-by-case, and it must "be proportionate to the gravity of the offense and the degree of responsibility of the offender", also considering "the degree of planning involved in carrying out the offense and the duration and complexity of the offense." Financial consequences such as fraud involving $5000 or more result in a maximum sentence of 14 years imprisonment.

Other than the laws mentioned above, provinces in Canada have legislation that protects personal health information by certain types of custodians. Quebec has especially proposed crucial amendments to its privacy laws by introducing Bill 64 that is intended to "modernize the province's legislative framework with respect to the protection of PI in both the public and private sectors". The 10-principle Digital Charter exists as a guideline to represent Canadian citizens' rights in cyberspace, and export control laws like Canada's Export Control List also have cybersecurity implications.

3. LIMITATIONS OF CHINA'S CURRENT LEGISLATIVE PRACTICE ON THE AIDING CYBERCRIME

In recent years, no matter at the level of national criminal legislation or academic research, all parties in China have paid great attention and adopted corresponding specific measures in the face of the increasingly severe situation of cybercrime. On August 29, 2015, the Sixteenth Meeting of the Standing Committee of the Twelfth National People's Congress deliberated and passed the Criminal Law Amendment (9). Articles 27, 28, and 29 are specifically aimed at punishing crimes in cyberspace. The legislator's approach of "principalizing" the aiding cybercrime to cope with the alienation of cybercrime is rather contrary to China's traditional accomplice theory. It also reflects the legislator's tendency to break through the rule of law on this issue as the current internet age is full of subversion and challenges.

In the eyes of Chinese legal scholars, joint offense refers to a crime committed jointly by more than two persons. Formally, compared with a person committing a crime alone, joint crime is by no means a simple sum of a number of individual crimes but a combination of independent crime forms that produce greater social harm. The act of aiding is no longer limited to the subordination of the act. Still, it is embodied as an independent, single act of help, which means that if the principle of the attribute of accomplices is consistent, it will obviously lead to the imbalance of crime and the lack of fairness.

Nowadays, there are many legislative examples of helping to commit crimes in the Chinese criminal law, and heated debate in academia about the question of the legitimacy of the legislative model of " principalization "

goes on. The term "principalization", in many ways, refers to the decision of the Chinese legislators to turn "helpers" in committing cybercrimes equivalent to principal offenders. According to Zekai Zhang, the legislative model of the main offender and accomplices to divide the offense is not scientific. It weakens the guiding significance of the General Provisions of the Criminal Law. The difference between the social hazard of the main offenders and the accessories is prominent, which indicates that this kind of legislative model cannot be given extended application [8]. Thus, the decision to make someone a principal offender is against the greater benefit of society.

Scholar Liu Yanhong had brought up similar arguments regarding the "principalization" of accomplices' model [9]. She held that the problem brought about by the "principalization" of the "helpers" was to determine in what scope the criminal law, as a coercive means imposed by the state on the individual, should punish the criminals. Particularly on such a divergent and liberal platform as the Internet, further exploration is needed as to whether it is reasonable to "principalize", as we say, all acts of assistance criminally motivated and intentionally committed. Liu suggests that neutral assistance is one critical concept to introduce and that judging if the criminal activity of helping on the internet has the nature of neutrality is a complicated issue. One of the elements of establishing a crime of helping is the intention of the perpetrator to be helpful, and the definition of intention is twofold. To establish a help offender, the helper must, in addition to recognizing that the act being committed is a criminal act, recognize his or her act is an act of assistance that contributes to the realization of the offending act, which means the helper knowingly assists the true perpetrator for him to succeed in committing a crime. It can be seen that even if the perpetrator knows the criminal's plan but does not mean to promote the implementation of the crime, it may be possible to establish a neutral act of assistance that is not punishable. Therefore, according to Liu, it can be said that aiding behavior in conducting criminal acts is typical neutral assistance. There are many problems in the legislative means regarding aiding cybercrime in cybersecurity, and they blur the line between punishable and unpunishable behaviors. To a certain extent, the addition of the crime of helping information network criminal activities to the Chinese Criminal Law shows that the rigor of China's criminal law legislation still needs to be strengthened, and legislators are responsible for taking appropriate measures to address these problems raised by legal scholars.

4. OPTIMIZING REGULATIONS OF THE AIDING CRIME IN CHINA'S CRIMINAL LAW

The original concept in Chinese legislation, "principalization" of aiding cybercrime, remains a controversial issue both in legislation and legal academia. To start with, the legislative operability is not strong enough. This means that the provisions regarding aiding cybercrime cannot expose social development challenges, and Chinese legislation is at a disadvantage to adapt to and combat sophisticated high-tech cybercrimes. On this front, the Canadian Anti-Fraud Centre, operated by the Royal Canadian Mounted Police, the Ontario Provincial Police, and the Competition Bureau, is one good source to learn from regarding closely monitoring and regulating frauds. Canada has also developed a number of programs and tools, such as Assemblyline, to contribute to its cyber defense. The addition of aiding cybercrime could use additional technologies in like manner to further China's improvement of the regulations of cybercrimes.

There also exist problems with the implementation and application of the law. For one, boundaries for "clearly knowing" from article 287 are not yet set. What behaviors would demonstrate that the helper clearly knows the true intentions of the criminal? How can legislators observe the patterns? Without defining the behaviors, it is difficult to recognize if one "clearly knows" the potential happening of the perpetration of cybercrime before helping the criminal achieve it. For two, article 287-2 of the Criminal Law of China treats "serious circumstances" as a condition for establishment, providing a legal basis for limiting the scope of punishment for neutral acts of assistance. Again, the standard in determining "serious circumstances" is not detailed enough. The damage could be a certain amount of money loss or a loss of national confidential information.

Furthermore, the inductive mode in China's cybercrime legislation is not conducive to implementing specific regulations and rules. This indicates that the wording in the new provision, "technical support such as," needs to be refined. Without doing, it is confusing for the judiciary to identify the severity of the cybercrime cases. In fact, China has only legislative content with no operational standards, no standards for identifying specific behaviors, and no standards for identifying the terms in the provisions. In this regard, Canada's Case Law traditions are of help for Chinese legislators to refer to, where standards are determined for cybercrime cases, especially the aiding cybercrime, and judgments of following cases would adhere to the set standards. Once legal precedents are there to supplement judicial interpretations and the aiding behaviors are categorized, the legislation of aiding cybercrime will truly have a substantive effect on regulating cybercrimes overall.

Finally, the scope of the penalty for neutral assistance must be severely limited, which is undeniable, difficult to set. Chinese legislators should further learn from the advantage of the case law tradition by specifying the neutrality and underlining both the absolutely neutral helping behaviors and the absolutely non-neutral helping behaviors. When going to court, judges would therefore readily avoid punishing the absolutely non-neutral helping behaviors to rectify the cyber legislative problem of being "too harsh".

5. CONCLUSION

As aforementioned, the legislative bodies in China and Canada take vastly distinct approaches to regulating cybersecurity and combating cybercrimes. Compared to Canada, China's legislative process concerning cybercrimes has been very recent and is still developing. This article uses the comparative method to find an optimization path for cybercrime regulation, particularly in consideration of the "principalization" of the act of assistance. The flaws of legislation in China are the inconsistency between legislative reforms and practical needs, and understanding this feature is of great significance for further optimization of the laws and regulations. We hope that the supposed suggestions with regard to the optimization of cybercrime regulations be of the value of reference. At the same time, we await research advances in academia on improving the legislative structure of cybersecurity beyond the sole examination of aiding cybercrime.

REFERENCES

[1] Fehr, C. (2019). Criminal Law and Digital Technologies: An Institutional Approach to Rule Creation in a Rapidly Advancing and Complex Setting. McGill Law Journal, 65(1), 67-113. https://doi.org/10.7202/1074418ar.

[2] Pi Yong (2012). The New Development of Criminal Procedure Legislation Related to Cybercrime in China after the Implementation of the New Criminal Procedure Law, Law Review, 30(6), 116-122.

[3] Criminal Law of the People's Republic of China, 2021.

[4] Yu Zhigang (2016), On the Method of Improving Criminal Sanctions against Cybercrime Assisting Behaviours, China Legal Science, vol.02,15-20.

[5] Rosati, N. (2019). Canadian National Security in Cyberspace The Legal Implications of the Communications Security Establishment's Current And Future Role As Canada's Lead Technical Cybersecurity And Cyber Intelligence Agency. Manitoba Law Journal, 42(4), 189-206.

[6] Ng, K. (2005). Span legislation in Canada: Federalism, freedom of Expression and the Regulation of the Internet. University of Ottawa Law & Technology Journal, 2(2), 447-492.

[7] The Criminal Code of Canada, 2005.

[8] Zhang Zekai (2017), The Criminal Regulation Of Assisting Behaviour about Network Joint Crime: Concurrent Research on Assisting Criminal Activity in Network, Master's Database of Yunnan University, 42-50.

[9] Liu Yanhong (2016), Criticism on the Principalization of Cybercrime Helping Behaviour, Studies in Law and Business, 33(3), 18-22.