

## Adequacy of criminal legislation concerning the money laundering for cybercrimes in Mainland China

 Yu Chenghao<sup>1\*</sup>,  Mohd Zamre Mohd Zahir<sup>2</sup>,  Ramalinggam Rajamanickam<sup>3</sup>

<sup>1,2,3</sup>Faculty of Law, Universiti Kebangsaan Malaysia (UKM), Malaysia; p136222@siswa.ukm.edu.my (Y.C.).

zamre@ukm.edu.my (M.Z.M.Z.) rama@ukm.edu.my (R.R.).

**Abstract:** This article examines the rising trend of cybercrime-related money laundering in Mainland China since 2020, focusing on challenges posed by legal ambiguities in enforcement. By comparing Mainland China's legal framework with Taiwan's recent legislative reforms, the study aims to provide recommendations for improving Mainland China's criminal legislation to ensure consistent legal application and strengthen anti-money laundering efforts. Utilizing a qualitative methodology, this research combines analytical and comparative legal approaches. It analyzes relevant criminal laws, judicial interpretations, and enforcement practices in Mainland China and Taiwan, with a particular focus on legislative amendments made by Taiwan in 2023 and 2024. The study reveals that ambiguous legal definitions in Mainland China's Criminal Law and judicial interpretations have led to inconsistent enforcement and difficulties in effectively combating money laundering related to cybercrimes. In contrast, Taiwan's proactive amendments demonstrate the benefits of precise legal provisions and comprehensive regulations. To enhance legal certainty, Mainland China should revise its laws to include explicit provisions on cybercrime-related money laundering and align enforcement mechanisms with international best practices. These recommendations can improve Mainland China's legal framework, ensuring more effective prosecution of cybercrime-related money laundering and fostering greater judicial consistency.

**Keywords:** Criminal law, Cybercrime, Judicial interpretation, Mainland China, Money laundering, Taiwan.

### 1. Introduction

The global economic loss resulting from cybercrime has already reached \$8 trillion by 2023 [1]. Since 2017, economic crimes such as casino operations and fraud have emerged as the predominant forms of cybercrime in Mainland China [2]. Correspondingly, money laundering, an ancillary offence intricately linked to economic crime, has permeated the realm of cybercrime as well. In 2015, the Criminal Code of the People's Republic of China (hereafter the "Criminal Code") introduced Article 287b (hereafter "Article 287b"), encompassing the provision of payment and settlement assistance for cybercrimes as a criminal behaviour under the article.

However, despite a steady increase in the total number of cybercrimes in Mainland China following the introduction of Article 287b, its inherent ambiguity has made it difficult for judges to apply in judicial practice [3]. As a result, between 2017 and 2019, the application of Article 287b for convicting cybercrime cases reached its peak in 2019, yet it remained low at only 5.78% of all cybercrime cases [2]. Moreover, absolute case numbers remained remarkably low, prior to 2018, fewer than 100 nationwide cases invoked Article 287b for conviction. By 2019, the number of cases processed by procuratorates involving this provision still did not exceed 500 [4]. In October 2019, the Supreme People's Court and the Supreme People's Procuratorate of Mainland China issued the Interpretation on Several Issues Concerning the Application of Criminal Law to Cases Involving Illegal Use of Information Networks and Assistance in Information Network Criminal Activities (hereafter the "Judicial Interpretation

2019”), Article 12 of the Judicial Interpretation 2019 (hereafter Article 12) provides a detailed explanation of the term ‘circumstances are serious’ as mentioned in Article 287b, aiming to address the ambiguity surrounding Article 287b. Moreover, in October 2020, Mainland China initiated a specialized campaign to combat emerging illicit activities in the telecommunications network, aiming to lawfully eradicate fraudulent bank cards, phone cards and associated online accounts [5]. Consequently, there was a remarkable 34.6-fold increase in the number of convictions under Article 287b in 2020, followed by an additional 17.16-fold increase in 2021 based on the previous year’s figures [2]. By 2023, the cases falling under Article 287b have constituted 8 percent of all criminal cases in Mainland China, representing the third largest proportion. Within this substantial caseload, approximately 80 percent pertains to the provision of financial accounts for cybercrimes [6].

This atypical exponential surge in case numbers unveils the issue of law abuse [5]. There are two significant factors contributing to the abuse of law. First, the unresolved ambiguity concerning mens rea in Article 287b has led to an unwarranted reduction in the standard of proof required to establish the perpetrator’s mens rea [7]. Consequently, this particular provision is perceived as a “Catch-all Clause” pertaining to cybercrimes within judicial practice [8]. For instance, in the Shanyin County v. Zeng Zhongping and Chen Mingwei case, as Internet cafe operators, were convicted under Article 287b solely based on their continued provision of Internet services despite being aware of others may engaging in cyber-fraud at their establishment [9]. Second, the violation of the principle of legality in Article 12 expanding the scope of punishment outlined in Article 287b to acts that were initially considered only as administrative illegality. While Article 12 should be applied as an exceptional circumstance, it effectively relieves the prosecution from proving that behaviour be assisted by perpetrator constitutes a crime in numerous cases within judicial practice [7] thereby it gives rise to tensions with the principle of legality. The above tensions exacerbate concerns regarding the misuse of Article 287b and raise apprehensions about potential encroachments on civil liberties and societal implications.

This article aims to address the inconsistent and inadequacy surrounding Article 12 and the Article 287b in relation to money laundering in cybercrime. By adopting pure doctrinal legal research, using qualitative method encompassing analytical legal research and comparative legal research, this article critically examines the application of laws and judicial interpretations pertaining to cybercrime-related money laundering within China and Taiwan jurisdictions. The primary sources for this article were derived from cases in Mainland China. These precedents were obtained from authoritative database such as China Judgements Online. Secondary sources utilizing in this article derived from journal articles, statutes, text books, research reports in Mainland China and Taiwan. In order to ensure the accuracy of legal texts, this article will gather laws and judicial interpretations from official government databases in Mainland China and and Taiwan.

Comparative legal research method can enhance the scope of legal analysis and criticism, enabling a more profound examination of the shortcomings within one’s own legal system and facilitating the formulation of suggestions to address legal issues based on a comprehensive understanding of other legal systems [10]. Taiwan and Mainland China share remarkable similarities in terms of culture, language and economy. Furthermore, both Mainland China and Taiwan are confronted with significant issues of cybercrime-related money laundering. Cases involving providing financial accounts accounted for 51.12 percent of all online fraud cases in Taiwan in 2019, progressively increasing to a peak of 72.02 percent in 2022 [11]. To combat the aforementioned money laundering offences effectively, Mainland China introduced Article 287b and Article 12. Taiwan amended the Money Laundering Control Act in 2023 and 2024. The aforementioned judicial interpretation and criminal laws of Mainland China and Taiwan both primarily focus on money laundering associated with cybercrimes, thereby forming the foundation for a comparative analysis of these criminal laws and judicial interpretations in this article.

## 2. Literature Review

As previously mentioned, since the enactment of Article 287b in 2015, with a focus on the year 2020 as a pivotal point, the implementation of this legislation in judicial practice has encountered two

contrasting issues: legal inefficiency and abuse. Consequently, academic research on this law in China mainland exhibits two distinct characteristics. Prior to 2020, the primary research content revolved around debates concerning the autonomy of Article 287b, specifically whether it can be established independently from Predicate Crime. However, following widespread misuse of Article 287b in numerous cases after 2020, research perspectives shifted towards limiting its application from various angles.

Among these perspectives are three noteworthy approaches. Focusing on the perspective of subjective imputation, a considerable body of research has revealed that a substantial number of judicial cases have employed the negligence standard to ascertain the subjective constitutive element of Article 287b, namely “knowing that others use information networks to commit crimes.” [12-14]. Consequently, their findings suggest that establishing at least a reasonable possibility for perpetrators to comprehend cybercrimes committed by others in specific cases [4, 12, 14] or employing high probability criteria [13] should serve as the basis for determining the subjective components of this offence. Some other studies have focused on the discourse surrounding the principle of complicity subordination [15-17]. Professor Zhang Mingkai advocates for adherence to the principle of complicity subordination in judicial practice when applying Article 287b, suggesting that conviction under Article 287 should only occur if the actions assisted by the perpetrator constitute a criminal offence [17] the viewpoint of Professor Zhang Mingkai is corroborated by TieCheng [16] Contrary to the viewpoint of Professor Zhang Mingkai, Professor Zhang Wei argues that Article 287 constitutes a distinct offence, thereby obviating the necessity to scrutinize whether the perpetrator’s assistance in committing an act amounts to a criminal act. However, akin to Prof Zhang Mingkai, Prof Zhang Wei also concurs that accomplices involved in other offences take precedence over Article 287b [15]. The legal interest theory serves as the fundamental framework for criminal law in China mainland, and numerous studies have applied this theory to analyze Article 287b [18, 19]. According to the research conducted by Professor Li Minglu and Professor Pi Yong, the legal interest protected by this legislation pertains to the emerging legal interest of maintaining public order within information networks [18] thereby supporting Professor Zhang Wei’s perspective indirectly. However, criticisms were raised against Li Minglu’s viewpoint by Professor Feng Weiguo and Chen Benzhen. Their research underscores the ambiguity surrounding the safeguarded legal interests under Article 287b and advocates for a more restrictive application of this law, emphasizing its utilization solely when absolutely necessary [19]. This stance aligns with Professor Zhang Mingkai’s suggestion to remove Article 287b [17]. The aforementioned studies collectively identify the inconsistency and ambiguity present in Article 287b, while endeavoring to propose solutions from diverse perspectives. However, these studies approach Article 287b holistically and overlook the differentiation among the three categories of criminal conduct delineated within Article 287b.

Research in China mainland on the types of payment and settlement assistance provided in Article 287b is still in its early stages. These studies primarily focus on differentiating between the three closely related offences of money laundering (Article 191 of the Criminal Code of the People’s Republic of China, hereafter Article 191 ), the concealment of criminal proceeds and illicit gains (Article 312 of the Criminal Code of the People’s Republic of China, hereafter Article 312), and providing payment and settlement assistance as outlined in Article 287b, aiming to address the ambiguity surrounding their application in judicial practice [5, 20-23]. Zhou [20] examine the relationship between the type of payment settlement assistance outlined in Article 287b and Article 312. Zhou Xiaotian proposes that this relationship can be categorized as general law versus special law, suggesting a preferential application of Article 312 while applying Article 287b only if the perpetrator’s behaviour does not impede judicial authorities from identifying and recovering criminal proceeds [20]. Professor Zhang highlights that the distinction between Article 312 and Article 287b lies in their respective temporal stages of involvement in predicate offenses: the conduct penalized under Article 287b involves intervening before a predicate offence acquires illicit gains, whereas Article 312 addresses intervention after such proceeds have been obtained [22]. Xie’s research underscores the imperative of establishing

complementary legal measures across various legal domains, beyond solely focusing on criminal law [5]. Chen Jialing and Wu Ke conducted a study on the behaviour of providing fund accounts as stipulated in Article 191, emphasizing that the essence of this behaviour lies in concealing the origin and nature of criminal proceeds. They further propose that determining whether money laundering has occurred should be based on the effectiveness of achieving such concealment [21]. The aforementioned studies are confined to the domestic legislation of China mainland, with a research gap of comparative legal research encompassing other jurisdictions.

Following the amendment in 2023 and 2024, Money Laundering Control Act has garnered significant attention from scholars and experts in Taiwan who specializing in criminal justice, several of these studies have specifically examined the act's novel provision regarding the unauthorized provision of financial accounts [11, 24–27]. One of Tsai's studies underscores the practical challenges associated with implementing financial account crime prevention, as evidenced by interviews conducted with judicial practitioners [11]. Another study conducted by Tsai [11] examines the criteria used to determine the constitutive elements of providing financial accounts and offers suggestions for mitigating such criminal activities [27]. One study conducted by Professor Chen Junwei offers valuable recommendations for determining the subjective elements of the offence of providing financial accounts [24]. Another study by Professor Chen Junwei raises concerns regarding the potential expansion of this crime and advocates for strengthening regulatory measures beyond criminal law [25]. Lin [28] research examines the legal advantages associated with the offence of providing financial accounts, conducting a comparative analysis between domestic legislation and Japanese law to provide a comprehensive understanding from a comparative legal perspective [28].

Although Article 287b cases in practice primarily revolve around payment and settlement assistance provided in the Article, there is a dearth of studies focusing on this specific behaviour within mainland China. Particularly, there exists a research gap in comparative law research pertaining to this field. While, the research conducted by scholars from Taiwan on the offence of providing financial accounts under the Money Laundering Control Act lacks comparative legal analysis with Mainland China. The aforementioned studies hold significant implications for further comparative analysis between China mainland's and Taiwan's criminal legislation concerning cybercrime-related money laundering. This article presents a comparative analysis of the criminal legal systems governing cybercrime-related money laundering in Taiwan and Mainland China, aiming to address the existing research gap. Given the extensive economic exchanges, particularly the inherent cross-border nature of cybercrime-related money laundering, this study not only contributes to addressing above legal deficiencies within Article 287b but also enhances judicial cooperation in combating such illicit financial activities between Mainland China and Taiwan.

### 3. Analysis and Discussion

#### 3.1. Criminal Legal System on Money Laundering in Mainland China

The crime of money laundering in Mainland China is defined under Article 191, Article 312, and Article 349 of the Criminal Code of the People's Republic of China (hereafter Article 349). The provisions of criminal law concerning money laundering have significantly influenced how subsequent legislation addresses money laundering associated with cybercrimes. Consequently, an analysis of criminal legislations related to the offence of money laundering is essential for gaining a comprehensive understanding of Article 287b and Article 12. It is noteworthy that the offence referred to as “the crime of money laundering” is stated in Article 191 [29] while offence under Article 312 referred to as “the crime of concealment of criminal proceeds and illicit gains” [29] and offence under Article 349 referred to as “the crime of harboring, transferring or concealing drugs and drug proceeds” [29]. However, it is imperative to underscore that the assertion of Mainland China's criminal law against money laundering being limited to only 191 articles is an incomplete perspective. Mainland China amended Article 312 twice in 2006 and 2009 to align with the Financial Action Task Force (hereafter FATF) requirements,

thereby incorporating Article 312 and Article 349 into a comprehensive anti-money laundering (hereafter AML) legal system as clarified in legislative documents [30].

Therefore, the aforementioned three legal provisions collectively establish a criminal legal system for money laundering offences corresponding to various types of predicate crimes [31-34]. Paragraph 1 of Article 191, delineates seven distinct categories of criminal offences that serve as the predicate offence, and also delineates five modes of money laundering, encompassing the provision of funds accounts for money laundering. Moreover, the provisions of Article 191 do not exclude the subject of predicate offences from being considered as a potential criminal subject of money laundering. In contrast to Article 191, Article 312 does not impose restrictions on the types of predicate offences, thereby encompassing proceeds and gains from any criminal activity as potential objects of money laundering. Moreover, Article 312 delineates five methods through which this offence can be committed, the terms “transferring,” “purchasing,” and “acting as an intermediary for sale” cover both financial and non-financial modalities. Therefore, even when applying the principle of *eiusdem generis*, it is unreasonable to interpret Article 312 as limiting money laundering exclusively to non-financial methods. Additionally, self-laundering by perpetrators of predicate offences is not subject to punishment under Article 312.

### *3.2. Internal Relation between Article 191 and Article 312*

In the context of the Mainland China's criminal legal system for AML, academic debates have arisen regarding the applicability and interrelationships between Article 191 and Article 312 due to similarities in the constitutive elements of crimes and the legal interests they protect. In this field, two prevailing theories exist. The first theory, proposed by Professor Zhang Mingkai, posits that Article 191 primarily aims to protect the financial order, it does not cover the legal interests related to the efficiency of judicial authorities in identifying and recovering criminal proceeds as Article 312. Therefore, the relationship between these two provisions should be one of coincidence of offences [35]. Professor Zhang's perspective is partially corroborated by other scholars. For instance, Wu [36] argues that the modes of criminal conduct under Article 191 and Article 312 differ fundamentally in terms of whether they confer a legitimate appearance on criminal proceeds and benefits. Consequently, these two provisions should not be considered to be overlap of laws [36]. Wang Yonghao also opposes the inclusion of judicial order as a legal interest protected by Article 191, thereby emphasizing the an coincidence of offences between these two provisions in his research [37]. Professor Wang Gang maintains that Article 191 safeguards dual legal interests: both financial order and the legal interests violated by predicate offenses, while explicitly excluding judicial authorities' recovery claims from its protective scope [38].

In contrast, another theory directly challenges the aforementioned view, asserting that the relationship between Article 191 and Article 312 constitutes a overlapping of laws. Represented by Professor Wang Xin, his perspective critiques Professor Zhang Mingkai's viewpoint, arguing that the claim that the legal interests protected by Article 191 differ from those under Article 312 reflects a partial interpretation of Article 312. It overlooks the fact that Article 312 has effectively been expanded to encompass general money laundering offences, including those involving financial means. Moreover, whether based on judicial interpretations or guiding cases, the relationship between these two provisions should be recognized as a overlapping of laws [33]. Numerous scholars have also espoused similar perspectives as Professor Wang. Professor He Ronggong argues that judicial interpretations have effectively expanded the scope of Article 191 beyond financial means, thereby broadening the protection of legal interests from solely financial order to encompass judicial order as well. This expansion establishes a relationship between Article 191 and Article 312, where the former serves as a special law while the latter acts as a general law, primarily differing in terms of predicate offences He [31]. Zhao [34] argues that there exists a similarity in the legal interests protected by Article 191 and Article 312, accompanied by an overlap in the constituent elements of the crime. Consequently, the

relationship between these two provisions can be characterized as a “cross-relational overlapping of laws.” [35].

Regarding the academic debates in this field, this article identifies three key focal questions. First, and serving as the foundation for these discussions, what is the legal interest protected by Article 191? Second, does Article 191 extend to encompass non-financial means? Finally, what is the relationship between Article 191 and Article 312? “...the rule of recognition exists only as a complex, but normally concordant, practice of the courts, officials, and private persons in identifying the law by reference to certain criteria” [39]. In Professor Hart’s theory of the rule of recognition, legal validity does not stem from an ultimate sovereign who promulgates the law, but rather from the identification of law by diverse subjects engaged in legal practice. Consequently, when identifying, interpreting, and applying the law, we should be guided by genuine societal needs instead of being solely bound to legislative intent.

Adopting this approach to legal interpretation, logical answers can be provided to the disputes surrounding aforementioned three questions. Concerning the legal interest protected under Article 191, it is crucial to emphasize that the interpretation of any individual legal provision should not be isolated from the broader legal framework [40]. Failing to do so may result in inaccurate conclusions. Consequently, the interpretation of the legal interest safeguarded by Article 191 should be grounded in the overarching goals of the AML legal system and judicial practices. According to the “Money Laundering and Confiscation” section of the FATF Recommendations, countries are encouraged not only to broaden the scope of predicate offences for money laundering but also to prioritize the recovery of criminal assets as the primary objective of AML measures [41]. The wording of Article 191 indicates that the core of the money laundering is the concealment and disguise of the origin and nature of the proceeds from predicate offences. In other words, although Articles 191 and 312 focus on different aspects, they both ultimately contribute to the broader aim of the AML legal system: disrupting the flow of funds associated with money laundering and recovering criminal assets. Therefore, the legal interest safeguarded by Article 191 must necessarily encompass judicial order.

Professor Zhang Mingkai deconstructs the legal interest of money laundering offences into a “blocking layer” and a “underlying layer” [35]. He argues that, the former pertains to the regulatory framework that prevents the financial system from legitimizing the proceeds and benefits of criminal activities, while the latter addresses public confidence in the financial system and financial security. The relationship between these two layers is one of means to an end. Although this article critiques Professor Zhang’s emphasis on financial security as potentially overshadowing the core aspects of money laundering crimes, his method of analysing the structure of the legal interest under Article 191 remains valuable for reference. Since Articles 191 and 312 are located in different chapters of the Criminal Code and exhibit significant disparities in their penalty ranges, this highlights the distinct legal interests they aim to protect. Article 191, which falls under the chapter on crimes disrupting the financial order, suggests that the “blocking layer” of the legal interest it protects pertains to the financial order, particularly the regulatory framework that prevents the financial system from legitimizing the proceeds and benefits of crime, as Professor Zhang has noted. However, given that this financial regulatory framework serves as a means, its primary objective is to facilitate the effective implementation of legal measures by judicial authorities to identify, trace, freeze, and recover criminal proceeds and benefits. In essence, the “underlying layer” of the legal interest protected by Article 191 is the judicial order that ensures the proper recovery of criminal proceeds and benefits.

It is crucial to acknowledge that the remaining two questions are explicitly addressed in Articles 5 and 6 of the 2024 judicial interpretation [42]. However, just as legal provisions do not preclude academic debate and critique, judicial interpretations, despite their quasi-legislative authority in Mainland China [43] also permit scholarly exploration. Scholarly discussions on whether Article 191 encompasses non-financial means, ultimately revolve around the legislative intent behind the provision. Nevertheless, even if we assume that legislative intent can be definitively determined, the law is never solely an embodiment of such intent. Otherwise, given that the legislative intent underlying the

forementioned judicial interpretation is unequivocal, it is unnecessary to delve further into subsequent issues. According to the Mutual Evaluation Report of China 2019 issued by FATF, the report highlights some issues within Mainland China's AML legal system. Prison sanctions for money laundering were low compared to the penalties for some of the main predicate offences [44]. Given the complexity and cost associated with legislative procedures, the objective of a reasonable interpretation, of the current AML criminal legal system should be "enhanced penalization." Specifically, Article 191 prescribes more severe imprisonment terms compared to Article 312, thus justifying a broader application of Article 191. If we redirect the focus of academic discussion to the practical needs of legal practice, the pertinent questions are no longer about the legal interest the legislature aims to protect under Article 191 or why self-laundering is explicitly limited to this article. Instead, the central issue is whether applying the more severe penalties under Article 191, compared to Article 312, for money laundering using non-financial methods aligns with the principle of proportionality between crime and punishment.

The predicate offences for money laundering under Article 191 are characterized by at least one of the following features, or both: they constitute serious crimes, or the proceeds and gains from these crimes significantly exceed those of ordinary offences. These predicate offences, including major drug offences, corruption and bribery, and financial crimes, are inherently complex and challenging to investigate [36]. Particularly in group crimes, perpetrators can swiftly destroy evidence, and the flow of criminal funds is often obscured, making it particularly difficult to trace [31]. Moreover, the proceeds from these predicate offences frequently play a critical role in facilitating subsequent recidivism of predicate offences [35]. Therefore, money laundering associated with these serious offences, regardless of whether financial methods are employed, poses a more substantial threat to the judicial system compared to money laundering linked to ordinary crimes. It is clear that incorporating non-financial methods under Article 191 does not violate the principle of proportionality between crime and punishment. On the contrary, applying the relatively lighter penalties under Article 312 solely because financial instruments were not used would amount to unjustified leniency. Such an approach not only contradicts the FATF's Recommendations but also falls short in effectively addressing the need to combat these serious predicate offences.

Regarding the final question, the relationship between Article 191 and Article 312, it is evident from the preceding analysis that the money laundering offences under these Articles exhibit complete overlap in terms of both the mode of criminal behaviour and the legal interests implicated. The sole distinction lies in the scope of predicate offences, with Article 191 encompassing a narrower range compared to Article 312. Therefore, the relationship between the two articles can be characterized as overlap of laws. The conclusion of the above analysis is as follows: the money laundering offence under Article 191 encompasses both financial and non-financial methods. Given the overlap of laws between Article 191 and Article 312, Article 191, as a special provision, should take precedence over Article 312, which serves as a general provision.

### *3.3. The Anti-Money Laundering Law in Mainland China*

The Anti-Money Laundering Law of the People's Republic of China (hereinafter referred to as the "AML Law") constitutes the cornerstone of the administrative regulatory framework and complements the AML criminal legal system. The AML Law and the criminal legal system, discussed in Sections 3.1 and 3.2, are not merely parallel or isolated systems. Adhering to the principle of ultima ratio, criminal law should be invoked only as a last resort when administrative, civil, and other preliminary legal measures prove insufficient to curb harmful behaviours. The precise demarcation of jurisdictional competences and institutionalized coordination mechanisms between financial institutions and supervisory authorities represent a fundamental prerequisite for establishing an effective legal framework to combat money laundering. Ideally, the administrative legal framework and the criminal penalty system should function synergistically to form a comprehensive AML legal system [45].



Therefore, analysing the AML Law is essential for a comprehensive understanding of the entire AML legal system.

The AML Law can be structured into four main components based on its content. Chapter 1 outlines general principles and foundational provisions related to AML. Chapters 2 and 4 focus on the establishment, powers, and investigative procedures of AML supervisory and regulatory agencies. Chapters 3 and 6 elaborate on the AML obligations of financial institutions and the corresponding legal consequences, while Chapter 5 addresses international cooperation in combating money laundering [46]. As a precursor to the AML criminal legal system, the AML Law complementarity with criminal law. For instances, the AML Law imposes specific obligations on financial institutions, empowering them to prevent and combat money laundering activities in accordance with the stipulations of the AML Law. For instance, Article 29 and Article 38 grant financial institutions due diligence responsibilities over clients, while Article 30 authorizes financial institutions to impose transaction restrictions on high-risk money laundering activities. These provisions collectively constitute the core administrative legal framework for AML.

However, there are also challenges in integrating the two legal systems. Article 2 of the AML Law encompasses all crimes as predicate offences for money laundering and defines money laundering as any act of concealing or disguising the origin or nature of criminal proceeds and their gains through any means. Some scholars argue that this definition diverges from that in the AML criminal legal system, thereby hindering the connection between criminal law and administrative law [46]. Moreover, this combined framework exhibits notable deficiencies. While Chapter 6 of the AML Law prescribes penalties for financial institutions that fail to fulfill their AML obligations, the administrative sanctions are inadequate considering the severe harm caused by such failures. However, in Mainland China's AML criminal law system, there is no criminal legislation concerning the negligence of financial institutions in supervision [46]. Additionally, the malfeasance crimes outlined in Chapter 9 of the Criminal Law are limited to state officials as offenders, thereby creating a legal gap in addressing AML negligence by other entities. This deficiency was also highlighted in the FATF's 2021 Second Enhanced Follow-Up Report and Technical Compliance Re-Rating for the People's Republic of China, which noted: "There were concerns that the sanctions applicable to the financial sector were not effective, dissuasive, and proportionate given their low scale and cap compared to the size and composition of the financial sector in China." [46] Furthermore, although Mainland China's AML criminal legal system delineates three distinct money laundering offences, it lacks specific administrative penalties for money laundering activities [46]. Consequently, it is evident that Mainland China's AML legal system exhibits certain inadequacies in imposing administrative sanctions for money laundering activities.

### *3.4. An Analysis of Cybercrime-related Money Laundering within the AML Criminal Legal System in Mainland China*

In Mainland China, cybercrime is legally characterized as a by-product accompanying the development of the digital economy. The financial sector has been identified as one of the primary risk domains for such crimes, where criminal activities have already reached a substantial scale. Consequently, legislators have adopted a multi-layered criminal law approach to suppress these illicit financial flows. This systematic legal intervention has consequently rendered money laundering associated with cybercrimes subject to particularly intricate provisions within the AML regulatory framework. This complexity arises from two main factors: the inherent intricacies of cybercrimes and the overlapping provisions within the AML system. Establishing a money laundering offence requires that the funds involved originate from predicate offences and that the perpetrator has clear knowledge that the property or funds constitute criminal proceeds or profits [47]. Based on this requirement, under the current AML criminal legal system in Mainland China, if the perpetrator possesses clear knowledge that the laundered funds originate from cybercrimes that qualify as predicate offences under Article 191, then Article 191 takes precedence over Article 312. Conversely, if cybercrimes do not qualify as predicate offences under Article 191, Article 312 applies as the general provision. At this



point, Article 287b appears unrelated to cybercrime-related money laundering. However, this apparent lack of connection actually highlights inadequacies within Mainland China's AML criminal legal system, particularly concerning the prerequisites for constituting money laundering offences.

In practice, cybercrime offenders frequently collaborate with intermediaries who gather financial accounts. These intermediaries then contact individual financial account providers. The providers only supply the financial accounts without engaging in activities such as transferring, cashing out, or withdrawing funds—actions that are explicitly classified as money laundering behaviours under China's AML criminal system. Moreover, the account providers typically have only a general awareness that their accounts might be used for illicit activities, lacking specific knowledge of the predicate offences or the criminal nature of the funds involved [20]. Therefore, the essential prerequisites for establishing money laundering offences are not fulfilled, thereby preventing the application of Articles 191, 312, or 349. This underscores the deficiencies within the Mainland China's AML criminal legal system. In the subsequent section, this article will examine the connection between these deficiencies and the misuse of Article 287b.

### *3.4.1. An Analysis of Article 287b under the Principle of Complicity*

Numerous academic studies on Article 287b, are based on the interpretation that Article 287b pertains to conduct constituting aiding in cybercrimes [16, 17, 48]. This viewpoint arises from a logical inference derived from the structural and linguistic elements of the offence outlined in Article 287b. Furthermore, irrespective of whether the offence under Article 287b is considered as the transformation of an accomplice into a principal offender, the requisite *mens rea* demands that the perpetrator have a high degree of certainty of the cybercrime committed by the principal offender [13]. This perspective is also evident in judicial interpretations. Specifically, as illustrated by Paragraph 1 in Article 12, which states “knowingly providing assistance to others in committing crimes through information networks” and “providing assistance to more than three entities.” These provisions are all framed within the context of joint criminal activities [49]. Thus, the interpretation of Article 287b as an accessory offence in joint cybercrimes has become a persuasive view in both judicial practice and academic research. However, this consensus not only gives rise to multiple challenges in judicial application but also constrains academic inquiry to a single perspective.

In judicial practice, one of the most challenging issues is the inconsistent criteria for determining the *mens rea* element, especially the “knowledge” requirement for offences under Article 287b [14]. For example, in the case of *Xiao Mouli v. Tangshan City* [50] the defendant lent his bank card after inquiring about its intended use. The individual who borrowed the bank card asserted that it was for legitimate purposes. Although the bank account was subsequently used to launder proceeds from online fraud, there is no evidence that the defendant had knowledge of the predicate offence at any point during the provision of payment settlement services. In both the first and second-instance rulings, the court's reasoning for attributing “knowledge” to the defendant was based on the bank's routine warning against lending accounts when the account was opened. However, a general warning regarding the prohibition on account lending does not equate to specific knowledge of the intention to commit cybercrime.

In the case of *Wang Moulin v. Ganzhou City* [51] the defendant, while applying for a loan on an online platform, was instructed by customer service to provide a bank account to fabricate fund flows in order to meet loan requirements. The defendant's account was subsequently used for laundering proceeds from online fraud. In this case, the defendant had no awareness of assisting others in committing any crime and thus lacked the *mens rea* necessary to be considered an accomplice to cybercrimes. Nonetheless, both the first and second-instance rulings inferred the defendant's “knowledge” based on the assumption that lending a bank card could potentially facilitate cybercrimes. This presumption regarding the defendant's subjective state can only be described as judicial conjecture and clearly violates the principle of legality.

The lack of a consistent judicial standard for proving “knowledge” under Article 287b, coupled with the Supreme People's Court's shifting interpretations of this critical element, has resulted in widespread

inconsistency in the provision's application [4]. However, criticism of judicial arbitrariness alone is insufficient, as this erroneous judicial tendency stems from inherent ambiguity of the Article 287b. Since Article 287b specifies a distinct offence separate from the accessories in cybercrime, while the actus reus outlined in Article 287b does not sufficiently differentiate it from the accessories in cybercrime, consequently, this distinction must be achieved through the mens rea element. Accessories in cybercrime have explicit knowledge of the principal offenders' criminal activities, consequently, to achieve the aforementioned distinction, the mens rea under Article 287b has been interpreted as a "generalized" awareness of the cybercrime. As Professor Zhang Mingkai notes, crimes under Article 287b are essentially accessories to predicate offences but lack the specific intent required for joint crime [22]. The ambiguous standard for determining this "generalized" knowledge leaves room for potential misuse of Article 287b in judicial practice. As Professor Yan Erpeng has noted, "since the evidentiary standard for proving intent in aiding predicate offences is higher than that required under Article 287b, adjudicators might opt for the latter to secure a conviction due to judicial inertia." [48]. Thus, as long as Article 287b continues to be interpreted within the framework of joint criminal liability, such abuses in judicial practice will persist.

Furthermore, interpreting Article 287b from the perspective of an accessory triggers a tension with the principle of legality while pursuing legal effectiveness. As discussed in introduction Section, prior to 2020, the application of Article 287b was exceptionally rare. This rarity can be attributed not only to the inherent ambiguity of the provision but also to the principle of derivative liability in joint criminal conduct. In civil law jurisdictions, this principle stipulates that an accessory's liability is secondary and contingent upon the principal offender's criminal responsibility [47]. Specifically, without a crime committed by the principal offender, the accessory's liability cannot be established. Therefore, under this principle, if offence prescribed under Article 287b are interpreted as aiding cybercrimes, the necessary precondition for applying this provision would be the substantiation of the principal cybercrime through sufficient evidence. However, due to the concealed, anonymous, and transnational nature of cybercrimes, as well as the increasingly tenuous connection between the criminal acts and the aiding acts in the cyber context, substantiating cybercrimes becomes significantly more challenging.

Although some scholars advocate interpreting Article 287b through the theory of independent accessory liability in an attempt to circumvent this predicament and enable its application independently of the upstream cybercrime [16, 18] such an approach faces significant theoretical challenges. As Professor Zhang Mingkai has noted, the specific wording of Article 287b and the prescribed modes of conduct do not align with the conditions required by the independent accessory liability theory [17]. Therefore, the synergistic impact of ambiguity and the constraints imposed by principle of derivative liability has rendered Article 287b ineffective in practical application, before 2020.

To address this legal ineffectiveness, second paragraph of Article 12 allows for the application of Article 287b under certain conditions even in the absence of a predicate offence. While Article 12 effectively resolves the issue of legal ineffectiveness, it simultaneously gives rise to a new issue for legal abuse. The crux of this issue lies in the fact that Article 12 contravenes the principle of derivative liability, thereby undermining the more fundamental principle of legality. Consequently, Article 287b has become entangled in a tension between legal effectiveness and the principle of legality. Given that the principle of legality permits no compromise, this paradox appears irresolvable. This is the rationale behind Professor Zhang Mingkai's assertion that, from a legislative perspective, abolishing the crime of aiding information network criminal activities may potentially be a viable solution [17].

Moreover, confining academic discourse on Article 287b within the principle of complicity has led to an underemphasis on the practical requirements of judicial practice. As outlined in Section 1.2, current research predominantly centers on applying principle of complicity to limit the scope of Article 287b. In practice, however, legislative bodies prioritize fulfilling their mandates, particularly in criminal legislation where the timely and effective response to crime is paramount. Consequently, legislative bodies often emphasize utilitarian objectives in their efforts to combat crime [52]. While legal

utilitarianism may not be entirely justifiable, academic research that overlooks the practical demands of judicial practice risks losing its relevance and credibility.

In light of judicial practice, widespread application of law often indicates its relevance to addressing specific issues encountered in the judicial practice. If concerns about potential misuse of the law overshadow more fundamental issues in judicial practice, these unresolved issues are likely to resurface in alternative forms. In the context of Article 287b, its extensive application in cases involving the provision of financial accounts for cybercrime strongly suggests that Mainland China's criminal legal system indeed requires a legal provision capable of criminalizing the act of providing financial accounts even in the absence of proof of a predicate offence. The subsequent section will deconstruct the types of conduct addressed under Article 287b, with particular emphasis on independently examining and analyzing the conduct of "providing assistance for payment and settlement" as prescribed under this provision. The objective is to determine whether this conduct should be classified as aiding cybercrime or as a form of money laundering.

### *3.4.2. An Analysis of the Nature of Payment Settlement Assistance under Article 287b*

Article 287b delineates three categories of criminal activities in its first paragraph: providing technical support for cybercrimes, offering advertising and promotional services, and assisting with payment and settlement operations. According to Xie Yangqiang's quantitative study of 15,249 judgements rendered under Article 287b up to and including 2023, 91.08% of cases involving assistance with payment and settlement pertained to the provision of financial accounts equipped with payment and settlement functionalities to facilitate cybercrimes [5]. Applying Hart's theory of the rule of recognition to evaluate the practical function of Article 287b reveals that, its primary role in judicial practice is to combat acts of concealing or disguising proceeds and benefits derived from cybercrimes, essentially addressing cybercrime-related money laundering. If the provisions in Article 287b concerning payment and settlement assistance are interpreted as an AML criminal provision, it is essential to distinguish Article 287b from Article 312 and Article 191. As discussed in Section 3.2, Article 312 and 191 already covers cybercrime-related money laundering. This raises the question: why is it still necessary to apply Article 287b to address cybercrime-related money laundering?

As discussed in Section 3.4.1, the extensive application of Article 287b provisions concerning payment and settlement assistance in judicial practice arises from the significant challenges in proving cybercrimes as predicate offences in money laundering cases. Both Articles 191 and 312 mandate the establishment of a predicate offence as a prerequisite for application. Moreover, to apply Articles 191 and 312, it must be demonstrated that the perpetrator providing a financial account has specific intent to commit money laundering, which is particularly difficult to prove when the perpetrator's actions are limited to merely providing a financial account. Understanding this practical challenge clarifies why the widespread application of Article 287b occurred once Article 12 alleviated the burden of proving the predicate offence. This phenomenon exemplifies a "functional compensation" by Article 287b, addressing the legal gap in Mainland China's AML legal system concerning money laundering offences where the predicate offence cannot be proven. Indeed, an influential perspective has sought to interpret the provisions related to payment settlement assistance under Article 287b in conjunction with Article 312 as the relationship between a special law and a general law [20]. This interpretation indirectly underscores the money laundering nature of the provisions concerning payment settlement assistance under Article 287b.

From another perspective, in the Criminal Code, whether a law qualifies as AML provision should not be determined by the name of the offence but rather by whether the prohibited behaviour constitutes money laundering. This criterion has been clearly reflected in legislative interpretations issued by the legislative body [30]. Indeed, numerous scholars have utilized this standard to identify and analyse Mainland China's AML legal system [31, 36, 37]. Without this criterion, justifying the inclusion of Articles 312 and 349 within the AML criminal legal system would be considerably more challenging.

Conversely, if one maintain the position that payment and settlement assistance under Article 287b constitutes aiding cybercrimes, this perspective appears ambiguous or even demonstrates a lack of comprehension regarding a fundamental premise: what is cybercrime? As highlighted by Wall [53] there is no universal consensus on the definition of cybercrime [53]. According to the Article 2 in issued by the Supreme People's Procuratorate of the People's Republic of China, cybercrime is defined as crimes targeting information networks, crimes committed through the use of information networks, and other upstream and downstream related crimes [54]. Even under this definition, cybercrime constitutes a complex criminal system encompassing various offences, each characterized by distinct elements of *actus reus*, *mens rea*, causation, and harm. Consequently, the detrimental impact resulting from aiding these diverse crimes also varies significantly. Therefore, classifying these aiding crimes, under a single legal provision and subjecting them to an identical sentencing range inevitably violates the principle of proportionality between crime and punishment.

Therefore, if it is necessary to treat payment and settlement assistance under Article 287b as a single offence with a uniform penalty range, it becomes imperative to identify a fundamental commonality other than cybercrime. This commonality stems from the fact that providing payment and settlement assistance for cybercrime is, in essence, an act of money laundering—concealing or disguising the proceeds and gains derived from such activities. Unlike offering technical support or advertising promotion for cybercrime, which require specific technical expertise, money laundering through payment facilitation does not necessitate specialized skills and poses a fundamentally different level of harm. Consequently, these three distinct types of acts should not be subject to the same sentencing range [20].

Moreover, it is crucial to emphasize that Article 12, Paragraph 1 specifies that administrative penalties constitute one of the prerequisites for establishing a crime under Article 287b. However, there are no corresponding administrative penalties for Article 287b under the Public Security Administration Punishments Law of the People's Republic of China. This discrepancy results in two significant issues. First, if an individual engages in behaviour specified under Article 287b but does not meet the threshold for criminal liability, such behaviour, while not constituting a crime under Article 287b, may still pose substantial harm. In these cases, administrative penalties are necessary, yet a legal gap exists regarding administrative measures to address such behaviour [55]. Second, this legal inconsistency renders the relevant provisions in Article 12, Paragraph 1 ineffective. In other words, the misalignment between criminal law and administrative law leads to the partial invalidity of the legal provisions in Article 12, Paragraph 1.

Based on the foregoing analysis, it has been established that the payment and settlement assistance under Article 287b possesses a money laundering nature. Additionally, we have identified a legal gap within Mainland China's AML criminal legal system as well as inconsistencies between Mainland China's AML criminal legal system and its administrative legal system. Building on this foundation, the subsequent section will critically analyse and evaluate Taiwan's AML legal system to facilitate a more comprehensive comparison with Mainland China's AML legal system.

### 3.5. Money Laundering Control Act in Taiwan

Similar to Mainland China, Taiwan has faced the challenge of cybercrime-related money laundering in recent years. According to a 2023 report on cybercrime statistics released by the National Police Agency of Taiwan, cyberfraud cases accounted for the largest proportion among all categories of cybercrime in Taiwan from 2018 to 2022 [56]. Within the realm of cyberfraud activities, the provision of financial accounts plays a crucial role in facilitating money laundering. A significant proportion of individuals involved in this process, commonly referred to as “money mules,” are primarily engaged in supplying these accounts [11]. Moreover, Furthermore, in 2019, the percentage of money laundering crimes linked to cyberfraud reached 96.1%, accounting for the vast majority of all money laundering offences [27].

Consequently, Taiwan has faced challenges similar to those in Mainland China in proving the intent behind money laundering activities by individuals who provide financial accounts and the difficulty of establishing predicate offences. To address these issues, Taiwan amended its Money Laundering Control Act (hereinafter referred to as the “MLC Act”) in 2023, introducing Article 15-1 and Article 15-2. In 2024, Taiwan further revised the MLC Act, renumbering Article 15-1 to Article 21 and Article 15-2 to Article 22. The primary objectives of these amendments are to prevent financial accounts from being used as tools for money laundering and to reduce the prosecutorial burden of proving intent in cases involving the mere collection and provision of financial accounts, thereby easing investigative pressures [57].

The MLC Act in Taiwan constitutes the cornerstone of the criminal legal framework designed to combat money laundering. As stipulated in Article 2 of the MLC Act [58] any acts involving the transfer, conversion, or concealment of specific criminal proceeds with the intent to obscure their illicit origins are classified as money laundering. It is crucial to emphasize that this legislation does not limit money laundering activities to those conducted on behalf of others. Instead, self-money laundering falls within the scope of money laundering offences as defined in this Article. Furthermore, Article 3 of the MLC Act specifies that these offences include all crimes carrying a minimum sentence of six months or more, thereby encompassing a broad spectrum of criminal activities [58].

In the MLC Act, money laundering offences are categorized into two types: general money laundering offences as outlined in Article 19, and specific money laundering offences detailed in Articles 20, 21, and 22. Article 19 specifically prohibits both self-laundering and facilitating money laundering for others [58]. To apply Article 19, it is essential to establish both the perpetrator's intent to launder money and that the funds are derived from predicate offences. Should either the perpetrator's intent or the origin of the funds fail to be substantiated, the perpetrator may still face charges under one of the specific money laundering offences detailed in Articles 20, 21, and 22.

Specifically, Article 20 prohibits the act of circumventing AML checks by financial institutions through illegal means to obtain financial accounts [58]. Article 21 addresses the criminal liability for the unlawful retention of another individual's financial account [58]. Moreover, Article 22 prohibits the provision of financial accounts to others without justifiable reasons, it is important to note that, in contrast to Article 21, Article 22 encompasses both criminal and administrative sanctions [58]. The distinction between these two Articles arises from the different roles that their targeted criminal behaviour play in money laundering crimes. Article 21 specifies preparatory conduct, which constitutes the principal offence in money laundering, whereas Article 22 addresses accomplice acts [28]. According to the principle of accessory liability in joint crime, an accomplice's behaviour is deemed less harmful than that of the principal offender. Consequently, the crime under Article 22 is subject to stricter constraints for establishment compared to the crime under Article 21. It also carries a lighter penalty and establishes a progressive system of punishment that integrates both administrative and criminal penalties.

Focusing on Article 22, considering the practical reality that the transfer or provision of financial accounts occurs for diverse reasons with varying degrees of culpability, Article 22 adopts a balanced approach, integrating leniency and strictness in penalties [25]. Paragraph 2 of Article 22 stipulates that individuals violating Paragraph 1 “shall be reprimanded by the police authorities.” The legislative explanation further clarifies that the “reprimand” mentioned in Paragraph 2 is aligned with relevant provisions of Taiwan's Administrative Penalty Law to ensure its effective enforcement [58]. Additionally, Paragraph 3 establishes the “reprimand” under Paragraph 2 as a prerequisite for determining recidivism within five years. This model of criminal determination endows the “reprimand” with a significant crime prevention function, extending beyond its role as a mere warning or educational measure. Considering the distinct legal nature of criminal penalties versus administrative sanctions, Paragraph 4 of Article 22 mandates concurrent imposition of administrative sanctions and criminal penalties. This stipulation enhances the crime prevention effect of the “reprimand” by extending its impact to perpetrators already deemed to have committed a money laundering crime under Article 22.

Furthermore, recognizing that providing accounts to others without justifiable reasons poses a significant risk of facilitating money laundering offences, Paragraphs 5 and 6 introduce supplementary administrative measures. These measures include restrictions or closures on both existing and newly applied financial accounts of the offender. Such post-incident measures targeting high-risk accounts effectively mitigate the risk of recidivism. In practice, organized crime often exploits the financial hardships of individuals to induce them to provide financial accounts [58]. Merely penalizing these individuals without addressing their economic challenges may exacerbate their risk of recidivism. To this end, Paragraph 7 establishes a mechanism for information exchange and coordination between law enforcement authorities and social welfare agencies. This auxiliary legal measure enhances the provision of effective social relief to offenders, thereby reducing their likelihood of recidivism.

Under the MLC Act, cybercrime-related money laundering is governed by multiple legal provisions. The determination of applicable laws hinges not on the classification of predicate offences but rather on the specific behaviours of the perpetrator. Firstly, if the perpetrator provides financial accounts for money laundering in the context of cybercrime, two scenarios arise: If the perpetrator knowingly provides their account for use in cybercrime-related money laundering, they are considered an accomplice to general money laundering under Article 19. If the perpetrator lacks intent to facilitate money laundering, their conduct constitutes a specific money laundering offence under Article 22 [24]. Secondly, if the perpetrator evades AML supervision by financial institutions through methods prohibited under Article 20, their actions constitute a specialized money laundering offence under this article. Thirdly, if the perpetrator unjustifiably collects others accounts, they are liable for a specific money laundering offence under Article 21. This legal framework ensuring tailored legal accountability based on the nature of the perpetrator's actions and intent, which aligns closely with the principle of proportionality between crime and punishment.

However, several scholars have raised concerns regarding this legislation. Specifically, criticisms have arisen regarding the inadequacies in Paragraph 3 of Article 22. Paragraph 3 stipulates that for recidivism to be applicable, the perpetrator must have been reprimanded by the police within five years for providing financial accounts to others. Nevertheless, considering the challenges related to enforcement efficiency and inter-departmental differences in law enforcement, there may be instances where an perpetrator repeatedly provides financial accounts within a five-year period without being reprimanded by the police. Additionally, there are cases where the offence is directly merged into another case, resulting in prosecution and conviction without prior police reprimand. Both scenarios fail to satisfy the criminal liability requirements under Paragraph 3 of Article 22 [46]. Furthermore, there is an ongoing debate regarding the authority of prosecutors and courts to review the legality of police-imposed reprimands during the prosecution or trial process [28]. Despite the issues highlighted by scholars, it is undeniable that, from a crime prevention perspective, providing financial accounts remains a primary method in facilitating money laundering [11]. It is evident that Article 22 effectively addresses the challenges inherent in money laundering cases involving the provision of accounts.

### *3.6. Comparative Analysis of Legislation on Cybercrime-related Money Laundering in Mainland China and Taiwan.*

This section will first provide a comparative analysis of the overarching AML legal system in Taiwan and Mainland China, followed by an in-depth examination of the specific legal norms addressing cybercrime-related money laundering in both jurisdictions. The objective is to evaluate and contrast the roles of relevant criminal laws concerning cybercrime-related money laundering within their respective legal systems from a broader perspective. First and foremost, a significant distinction exists in the legislative structures of AML criminal law in the two jurisdictions. Mainland China employs a unitary legislative model for criminal law, wherein all provisions related to money laundering offences are codified within the Criminal Code [59] operating independently from any administrative law. Conversely, Taiwan adopts a dual legislative model, enacting the MLC Act as a specialized criminal law

distinct from its Criminal Code. Moreover, the MLC Act integrates both criminal and administrative AML measures, ensuring consistent coordination between these two legal dimensions.

As discussed in Section 3.3, the misalignment between Mainland China's AML criminal and administrative legal systems undermines their collective efficacy in combating money laundering. This discrepancy partly arises from Mainland China's unitary legislative model under the Criminal Code. Although this model ensures conciseness and clarity in criminal legislation, it restricts flexibility and often neglects the necessary coordination with other branches of law [59]. Although, this does not imply that Mainland China must adopt a dual legislative model or enact a specialized AML criminal law akin to the MLC Act. But, it underscores the necessity of addressing and rectifying the inconsistencies and inadequacies within its Mainland China's AML legal system.

Despite the global recognition of money laundering as a criminal activity, its definition and scope differ significantly across countries and regions [60]. In Taiwan and Mainland China, there are notable distinctions in the legal definitions of money laundering. This article analyses these differences by examining Mainland China's AML legal framework outlined in Sections 3.1 to 3.4, as well as the MLC Act discussed in Section 3.5, it is evident that the definition of money laundering under the MLC Act is both consistent and comprehensive. Specifically, Article 2 of the MLC Act explicitly includes self-laundering, while Article 3 expands the scope of predicate offences to encompass a wide range of criminal activities. In Mainland China, the definition of money laundering varies across different legal provisions. Article 191 criminalizes self-laundering but limits predicate offences to seven specific categories. In contrast, Articles 312 and 349 do not recognize self-laundering as an offence; Article 349 restricts predicate offences to drug-related crimes. This comparison highlights that although Mainland China defines a broader range of predicate offences for money laundering, its treatment of self-laundering is significantly constrained by the nature of the predicate offences. Conversely, in Taiwan, the scope of predicate offences is identical for both self-laundering and third-party laundering crimes. Furthermore, Mainland China's AML criminal legal system does not criminalize certain money laundering-related acts, such as evading financial institutions' AML scrutiny, unjustifiably collecting others' financial accounts, and unjustifiably providing financial accounts to others. This inadequacy in the AML criminal law systematically amplifies financial risks associated with money laundering.

The differences are also evident in the context of cybercrime-related money laundering. In Mainland China's AML criminal legal system, the absence of provisions addressing the illegal acquisition and unjustified collection or provision of financial accounts, coupled with the difficulty in proving money laundering intent. Consequently, Articles 191 and 312 can only be invoked to secure a conviction if the perpetrators have already utilized the acquired financial accounts for money laundering activities related to cybercrime. This post facto severe criminal sanction is aligned with traditional criminal law theories that emphasize retribution and deterrence. However, in the context of money laundering offences, such an approach fails to effectively serve the preventive function of criminal law [61]. Focusing on the act of providing financial accounts for cybercrimes, Mainland China addresses this behaviour under Article 287b by treating it as an accessory to cybercrime. In contrast, Taiwan's MLC Act criminalizes the unjustified provision of financial accounts as a money laundering offence under Article 22. As discussed in Sections 3.4, Mainland China's approach do not fully capture the money laundering aspects of providing financial accounts for cybercrimes. This approach also poses challenges in meeting the practical needs of judicial practice, in cases where the perpetrator's awareness of the predicate offences cannot be established. The discrepancy between the legal provisions and practical requirements leads to confusion in judicial practice regarding the determination of criminal intent under Article 287b and creates tensions with the principle of legality. Furthermore, by not classifying the provision of financial accounts as a money laundering offence, Mainland China's approach exempts such activities from the legal measures stipulated under the AML Law. This exemption means that financial institutions are not empowered to lawfully conduct account investigations, issue alerts, freeze accounts, suspend transactions, or impose administrative penalties for these activities in



accordance with the AML Law. As a result, this significantly undermines the practical effectiveness of Article 287b in combating money laundering crimes.

In contrast, Taiwan views the provision of financial accounts as a “preparatory act” for money laundering offences [28]. This approach, grounded in the preventive objectives of AML efforts, facilitates early criminal law intervention and punishment. By recognizing the provision of financial accounts as an independent money laundering offence, separate from predicate crime, this approach enables Article 22 to eliminate the need to prove the perpetrator’s subjective awareness of predicate crimes or the existence of such crimes as constitutive elements, while remaining consistent with the principle of legality. Furthermore, by treating the provision of financial accounts as a money laundering act, AML preventive and supervisory measures under the administrative and social legal system can be applied to this behaviour. This comprehensive legal strategy effectively mitigates the risk of financial accounts being exploited for money laundering crimes. Table 1 summarizes the above comparisons.

**Table 1.**  
Comparison of Legal System for Cybercrime-related Money Laundering in Mainland China and Taiwan.

Money laundering behaviour	Mainland China	Taiwan	Similarities	Differences
The perpetrator engages in money laundering involving the proceeds and profits of another individual’s cybercrime.	Criminal Code Article 191 Article 312	MLC Act Article 19	Both Mainland China and Taiwan have criminalized third-party money laundering related to cybercrime.	Mainland China has established different penalty ranges for various types of predicate offences, while Taiwan’s money laundering laws differentiate penalties based solely on the amount of funds involved.
The perpetrator engages in money laundering involving the proceeds and profits of their own cybercrime.	Criminal Code Article 191	MLC Act Article 19	Both Mainland China and Taiwan have criminalized certain types of cybercrime-related self-money laundering.	In Taiwan, the scope of self-money laundering is consistent with that of third-party money laundering. In contrast, in Mainland China, self-money laundering is limited to the seven categories of predicate offences specified under Article 191.
The perpetrator evades financial institution supervision to illegally obtain financial accounts.	None	MLC Act Article 20	/	Mainland China fails to classify fraudulent applications for fund account establishment as a distinct money laundering offence under its Criminal Code, despite such conduct recognized high-risk status in global AML frameworks. By contrast, Taiwan criminalizes such conduct as a special money laundering offence.
The perpetrator collects another person’s financial accounts without legitimate reason in cybercrime-related money laundering	None	MLC Act Article 21	/	The unauthorized collection of others’ financial accounts, while typically merely treated as preparatory conduct for money laundering in Mainland China, is expressly criminalized as a distinct money laundering offence under MLC Act. This

				statutory classification enables Taiwan authorities to intervene at earlier stages against such high-risk financial behaviours.
The perpetrator provides a financial account to another person in cybercrime-related money laundering	Criminal Code Article 287b	MLC Act Article 22	Both Mainland China and Taiwan criminalize the provision of financial accounts for cybercrime.	In Mainland China, this behaviour is classified as an accomplice to cybercrime, while Taiwan treats it as a money laundering offence. Taiwan has established administrative penalties and social relief legal measures for this behaviour, whereas Mainland China lacks supplementary legal measures beyond the criminal law.

#### 4. Conclusion and Recommendation

Based on the foregoing analysis, this article proposes the following legislative amendments. First, inspired by Article 22 of Taiwan's MLC Act, it is recommended to revise Article 287b, Paragraph 1, by removing the phrase 'or payment and settlement.' Additionally, in Article 12, Paragraph 1, the clause 'where the payment and settlement amount exceeds RMB 200,000' should be deleted. Second, a new Article 312b should be introduced under Article 312 to criminalise the provision of financial accounts without legitimate reasons. Concurrently, administrative penalties for such actions should be incorporated into the AML Law, along with social relief measures for those involved. Article 312b serves as a general provision addressing money laundering crimes involving the use of financial accounts when an individual provides such accounts without legitimate justification but lacks knowledge of predicate offences. When an individual has clear knowledge that the funds constitute criminal proceeds and profits, thereby demonstrating intent to commit money laundering, the applicable law—Article 191 or Article 312—should be determined based on the type of the predicate offence. Meanwhile, given the necessity to combat account collectors commonly associated with cybercrime and to prevent cybercriminals from illicitly obtaining accounts, it is imperative to criminalize acts such as evading financial institutions' AML supervision and unjustifiably collecting others' financial accounts, by drawing on the provisions of Articles 20 and 21 of the MLC Act. These measures would more comprehensively mitigate the risk of financial accounts being exploited for cybercrime-related money laundering.

The proposed amendments to the law and judicial interpretations can yield several significant positive effects: Firstly, they will clearly differentiate between providing financial accounts for cybercrimes and acting as an accomplice in cybercrime. This distinction will further prevent disputes regarding the nature of payment and settlement assistance under Article 287b within the framework of accessory liability theory. Consequently, this could help mitigate the tension between Article 287b and the principle of legality. Secondly, incorporating the provision of financial accounts into AML criminal law will harmonize it with administrative penalties, AML risk prevention measures, supervision, and other legal frameworks, thereby establishing a comprehensive and well-structured AML legal system. This would address the lack of coordination between Article 287b and administrative law, enhancing the effectiveness of combating and preventing money laundering. Thirdly, these amendments will provide a robust legal foundation that meets the needs of judicial practice in addressing money laundering related to cybercrimes, thus preventing potential misinterpretation and abuse of Article 287b in judicial proceedings. Finally, as discussed in Section 3.4.2, punishing money laundering alongside cybercrime-related technical support and advertising under the same sentencing range creates tension with the

principle of proportionality between crime and punishment. By separating the provision of financial accounts without legitimate reasons from Article 287b, this tension can be mitigated.

This article examines and analyses the provisions related to payment and settlement in Article 287b within the framework of the AML legal system in Mainland China, with the aim of reviewing the true function of these provisions from the perspective of judicial practice. Existing literature has predominantly concentrated on the issues within Article 287b, while neglecting the fact that the fundamental cause of the problem does not lie within Articles 287b and 12, but rather in the “misplaced” legal rule concerning payment and settlement provisions. As the Chinese proverb states, “One man’s candy is another man’s poison.” Rely on legislators to fully understand the practical needs in combating money laundering within the judicial practice and incorporate provisions concerning the provision of financial accounts without legitimate reasons into the AML criminal legal framework. In that case, they can effectively mitigate the misuse of Article 287b and alleviate tensions between this article and the principle of legality and proportionality between crime and punishment.

### Transparency:

The authors confirm that the manuscript is an honest, accurate, and transparent account of the study; that no vital features of the study have been omitted; and that any discrepancies from the study as planned have been explained. This study followed all ethical practices during writing.

### Acknowledgement:

Acknowledgment to the Ministry of Higher Education (MOHE), Malaysia for grant Skim Geran Penyelidikan Fundamental (FRGS) under grant code: FRGS/1/2023/SSI12/UKM/02/2; Universiti Kebangsaan Malaysia (UKM) for providing a grant named Geran Universiti Penyelidikan (GUP) under grant code: GUP-2023-082; and to the members of the research group.

### Copyright:

© 2025 by the authors. This open-access article is distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

### References

- [1] A. O. Felix, O. J. Olabode, and J. K. Ayeni, "The criminalization of the internet and cybercrime in general: A comprehensive study," *Scientific and Practical Cyber Security Journal*, vol. 7, no. 3, pp. 1-25, 2023.
- [2] C. I. O. J. B. Data, "Characteristics and trends of cybercrimes (2017.1-2021.12) judicial big data special report," Retrieved: <https://www.chinacourt.org/article/detail/2022/08/id/6826831.shtml>, 2022.
- [3] X. Huang, "Research on the application of the crime of helping cybercrime. Tianfu New Idea," *Tianfu New Idea*, vol. 1, p. 9, 2021. <https://doi.org/10.3969/j.issn.1004-0633.2021.01.015>
- [4] W. Hongqi, "A normative examination and generalized correction of the 'knowledge' determination rule in the crime of aiding information network criminal activities," *Legal Forum*, vol. 40, no. 2, pp. 11-20, 2025.
- [5] Y. Xie, "Practical inspection and integrated governance of the crime of providing payment and settlement aid for criminal activities in relation to information network," *Journal of Hunan Agricultural University(Social Sciences)*, vol. 2, p. 9, 2024. [https://doi.org/10.13331/j.cnki.jhau\(ss\).2024.02.010](https://doi.org/10.13331/j.cnki.jhau(ss).2024.02.010)
- [6] The Third Criminal Division of the Supreme People's Court, "Research report on judicial governance of the crime of helping cybercrime," Retrieved: <https://www.chinacourt.org/article/detail/2023/08/id/7489185.shtml>, 2023.
- [7] H. Wang, "Judicial misconceptions and theoretical corrections concerning the crime of assisting cybercrime activities," *Law and Economy*, vol. 5, p. 14, 2024. <https://doi.org/10.16823/j.cnki.10-1281/d.2024.05.002>
- [8] H. Chen, "Pocketization" corrections of crimes of helping cybercrime," *Journal of Hunan University (Social Sciences)*, vol. 36, no. 2, p. 9, 2022. <https://doi.org/10.16339/j.cnki.hdxbskb.2022.02.017>
- [9] Shanyin County v. Zeng Zhongping and Chen Mingwei, *People's Court of Shanyin County*. China: Shanxi Province People's Court Press, 2020.
- [10] P. I. Bhat, *Idea and methods of legal research*. India: Oxford University Press, 2019.
- [11] I.-C. Tsai, "2022 crime situations and analyses—Types and prevention of dummy accounts' providers," *Criminal Policies and Crime Prevention*, vol. 37, p. 112, 2023. [https://doi.org/10.6460/cpcp.202404\\_\(37\).0004](https://doi.org/10.6460/cpcp.202404_(37).0004)
- [12] X. Liu, "An academic study on the intermediate path for determining 'knowledge' in the crime of assisting cybercrimes," *Journal of Law Application*, vol. 6, pp. 13-18, 2024.

- [13] Z. Long and J. Hu, "The determination of 'knowledge' in the crime of assisting cybercrimes," *Journal of Southwest University for Nationalities (Humanities and Social Science Edition)*, vol. 1, pp. 45-58, 2024.
- [14] X. Wang and X. Cui, "Identification of 'knowing' in the crime of assisting in information network criminal activities," *Journal of Beijing University of Posts and Telecommunications (Social Sciences Edition)*, vol. 25, no. 6, pp. 50-58, 2023. <https://doi.org/10.19722/j.cnki.1008-7729.2023.0110>
- [15] Z. Wei, "The dogmatic study of the crimes of providing assistance in the web-based criminal activities," *Journal of Comparative Law*, vol. 1, pp. 97-111, 2023.
- [16] X. TieCheng, "Explanation approach of the crime of helping cybercrime: Accomplice theory and non-accomplice theory," *Shandong Social Sciences*, vol. 10, pp. 175-184, 2023. <https://doi.org/10.14112/j.cnki.37-1053/c.2023.10.023>
- [17] M. Zhang, "A comprehensive analysis of the crime of helping cybercrime," *Studies in Law and Business*, vol. 41, no. 1, pp. 21-30, 2024. <https://doi.org/10.16390/j.cnki.issn1672-0393.2024.01.005>
- [18] M. Li and P. Yong, "Research into the legal interests of public order in cyberspace crimes: From the perspective of the independence of the crime of helping information network criminal activities," *Journal of Hainan University (Humanities and Social Sciences)*, vol. 41, no. 5, p. 13, 2023. <https://doi.org/10.15886/j.cnki.hnus.202210.0334>
- [19] W. Feng and B. Chen, "The correction and reconstruction of the double layered discrimination system for the recognition of assistance in cybercrime," *Academic Journal of Zhongzhou*, vol. 7, pp. 9-15, 2024.
- [20] X. Zhou, "The distinction and application criteria between payment settlement-type 'assisting information network crime' and 'concealing or hiding criminal proceeds,'" *Law Science*, vol. 516, no. 11, pp. 75-92, 2024.
- [21] J. Chen and K. Wu, "The normative interpretation and judicial application of money laundering crime of 'providing fund account type,'" *Journal of Henan University of Economics and Law*, vol. 5, pp. 12-17, 2023.
- [22] M. Zhang, "The interrelation between the crime of concealment or disguise of criminal proceeds and associated crimes," *Criminal Science*, vol. 4, pp. 20-29, 2024. <https://doi.org/10.19430/j.cnki.3891.20240903.001>
- [23] Y. Liu, "Research on judicial application issues of money-laundering-type assistance in cybercrime", Master's Thesis) Nanjing University of Information Science and Technology, 2024.
- [24] C. Junwei, "On the intentional provision of accounts to facilitate fraud or money laundering," *Formosan Jurist*, vol. 26, pp. 26-30, 2023.
- [25] C. Junwei, "Interpretation of the offense of providing accounts without justifiable grounds as stipulated in the money laundering control act of 2023," *Formosan Jurist*, vol. 28, pp. 19-22, 2023.
- [26] C. Li, "On the duality of money laundering crime in China," *Journal of Beijing Normal University (Social Sciences Edition)*, vol. 1, pp. 9-12, 2023.
- [27] I.-C. Tsai, "Is the behavior of providing accounts identified as a sin? Analyzing the consideration of accessory of money laundering and the trend of becoming a principal offender," *Legal Aid And Society Review*, vol. 10, p. 47, 2023. [https://doi.org/10.7003/LASR.202303\\_\(10\).0002](https://doi.org/10.7003/LASR.202303_(10).0002)
- [28] Z. Lin, "On the crime of special delivery account under Item 3 of Article 15-2 of the Money Laundering Control Act," *Taiwan Prosecutor Review*, vol. 33, pp. 52-61, 2024.
- [29] Standing Committee of National People's Congress of the People's Republic of China, "Criminal code of the people's Republic of China," Retrieved: <http://www.npc.gov.cn/englishnpc/c23934/>. [Accessed 1997].
- [30] J. An, "Explanation on the amendment to the criminal law of the people's republic of China (VI)(Draft) - delivered at the 19th session of the standing committee of the tenth national people's Congress on December 24, 2005 - An Jian," presented at the Gazette of the Standing Committee of the National People's Congress, 4, 2005, 426.
- [31] R. He, "Discussions, and reflections on the judicial application of the crime of money laundering," *Law Review*, no. 3, p. 9, 2023. <https://doi.org/10.13415/j.cnki.fxpl.2023.03.013>
- [32] J. Lu and X. Wang, "The imbalance and improvement of the anti-money laundering offense system," *Journal of People's Public Security University of China Social Sciences Edition*, vol. 6, pp. 7-12, 2022.
- [33] X. Wang, "An analysis of fundamental issues in the crime of money laundering: A discussion with Professor Zhang Mingkai," *Law Review*, vol. 3, p. 8, 2023. <https://doi.org/10.13415/j.cnki.fxpl.2023.03.011>
- [34] Y. Zhao, "The legal interests protected by the crime of money laundering and its normative application," *Law Science*, vol. 511, no. 6, pp. 18-27, 2024.
- [35] M. Zhang, "The legal interest protected by the crime of money laundering," *Law Science*, vol. 486, no. 5, pp. 15-24, 2022.
- [36] B. Wu, "The judicial application dilemmas and solutions of money laundering crimes," *Law Science*, vol. 479, no. 10, pp. 15-25, 2021.
- [37] Y. Wang, "On the coordinated application of money laundering crime and booty crime," *Journal of Henan Administrative Institute of Politics and Law*, vol. 2, pp. 12-20, 2024.
- [38] W. Gang, "Systematic interpretation of money laundering crimes," *Journal of Comparative Law*, vol. 3, pp. 18-29, 2025.
- [39] H. L. A. Hart and L. Green, *The concept of law*, 3rd ed. London: Oxford University Press, 2012.
- [40] M. Z. M. Zahir, T. N. A. T. Zainudin, R. Raja-Manickam, and Z. Abd Rahman, "Do not resuscitate (DNR) orders in the health sector from a legal perspective," *Akademika*, vol. 89, pp. 143-154, 2019.
- [41] The Financial Action Task Force, *The FATF recommendations*. Paris: The Financial Action Task Force, 2023.

- [42] The Supreme People's Procuratorate, "Interpretation of the supreme people's court and the supreme people's procuratorate on several issues concerning the application of law in handling criminal cases of money laundering," Retrieved: [https://www.spp.gov.cn/xwfbh/wsfbt/202408/t20240819\\_663652.shtml#2](https://www.spp.gov.cn/xwfbh/wsfbt/202408/t20240819_663652.shtml#2), 2024.
- [43] M. Chen, M. R. A. Rahman, and M. Z. M. Zahir, "Market value appraisal of virtual property from a Chinese legal perspective," *Pakistan Journal of Life and Social Sciences*, vol. 23, no. 1, pp. 93-99, 2025. <https://doi.org/10.57239/pjlss-2025-23.1.0093>
- [44] The Financial Action Task Force, *Mutual evaluation Report of China - 2019*. Paris: The Financial Action Task Force, 2019.
- [45] S. Z. Zulkhafri, H. M. Ali, M. Z. M. Zahir, and M. S. Hassan, "Enforcement against Ponzi scheme, the fraudulent method to generate easy money in Malaysia," *Malaysian Journal of Law & Society*, 2023.
- [46] Z. Pan, "Anti-money laundering legislation from the connection of criminal law and administrative law in the background of the digital economy," *Local Legislation Journal*, vol. 8, no. 4, pp. 17-22, 2023.
- [47] M. Zhang, *Criminal jurisprudence*, 6nd ed. Beijing: Acomplete Publishing, 2021.
- [48] E. Yan, "Help information network crime activity crime legislative interpretation and judicial correction," *Science of Law (Journal of Northwest University of Political Science and Law)*, vol. 5, p. 12, 2024. <https://doi.org/10.16290/j.cnki.1674-5205.2024.05.008>
- [49] Supreme People's Court Supreme People's Procuratorate, "Interpretation of the Supreme People's Court and the Supreme People's Procuratorate on Several Issues concerning the application of the Law in handling criminal Cases such as illegal Use of information networks and assistance in information network criminal Activities, Article 12 ", Retrieved: [https://www.spp.gov.cn/spp/xwfbh/wsfbh/201910/t20191025\\_436138.shtml](https://www.spp.gov.cn/spp/xwfbh/wsfbh/201910/t20191025_436138.shtml), 2019.
- [50] Xiao Mouli v. Tangshan City, *Tangshan Intermediate People's Court of Hebei Province*. China: Hebei Province People's Court Press, 2024.
- [51] Wang Moulin v. Ganzhou City, "Ganzhou Intermediate People's Court of Jiangxi Province," Retrieved: <https://wenshu.court.gov.cn/website/wenshu/181107ANFZOBOXSK4/index.html?docId=Np7NlKPz418ml64jBMoiUCINPYWw/aCBxU1zrDQ55vcYyDF4mgipO3qNaLMqsJBhwZJmAr2cYuEdOSn8nYFzqxkK2+Owb9odrVaNM4h8EKYT/ej84qdo4h6ESK9Z54OAht9CN6bcZdg2DYCJhCOJlvegCdTob>, 2024.
- [52] X. Chen, "Turning the accomplice into the perpetrator: Perspective from the crime of providing assistance in cybercriminal activities," *Journal of Comparative Law*, vol. 2, pp. 15-20, 2022.
- [53] D. S. Wall, *Cybercrime: The transformation of crime in the information*, 2nd ed. Cambridge, UK: Polity Press, 2024.
- [54] S. P. S. Procuratorate, "Regulations on handling cybercrime cases," Retrieved: Retrieved from [https://www.spp.gov.cn/spp/xwfbh/wsfbh/202101/t20210125\\_507446.shtml](https://www.spp.gov.cn/spp/xwfbh/wsfbh/202101/t20210125_507446.shtml), 2021.
- [55] H. Zhang, "A brief analysis of administrative penalty for non-prosecution of minor crimes in the crime of aiding information network crime," 2023.
- [56] National Police Agency of the Republic of China (Taiwan), *Overview of cybercrime from January to May 2023*. Taipei: National Police Agency of the Republic of China, 2023.
- [57] Ministry of Justice of Taiwan, "Legislative explanation of the money laundering control act," Retrieved: <https://www.moj.gov.tw/media/25371/%E4%B8%89%E8%AE%80%E9%80%9A%E9%81%E7%89%88-%E6%B4%97%E9%8C%A2%E9%98%B2%E5%88%B6%E6%B3%95%E7%AC%AC%E5%8D%81%E4%BA%94%E6%A2%9D%E4%B9%8B%E4%B8%80-%E7%AC%AC%E5%8D%81%E4%BA%94%E6%A2%9D%E4%B9%8B%E4%BA%8C%E5%8F%8A%E7%AC%AC%E5%8D%81%E5%85%AD%E6%A2%9D%E4%BF%AE%E6%AD%A3%E6%A2%9D%E6%96%87%E5%B0%8D%E7%85%A7%E8%A1%A8.pdf?mediaDL=true>. [Accessed 2023].
- [58] Money Laundering Control Act, "Legislative Council of Taiwan," Retrieved: <https://mojlaw.moj.gov.tw/LawContent.aspx?LSID=FL006664#lawmenu>, 1996.
- [59] M. Zhang, "Regarding the amendments to the criminal law and the codification of the criminal law," *Tribune of Political Science and Law*, vol. 39, no. 4, pp. 15-25, 2021.
- [60] D. P. Ramada, "Prevention of money laundering: Various models, problems, and challenges," *Journal of Law and Legal Reform*, vol. 3, no. 1, pp. 67-84, 2022. 10.15294/jllr.v3i1.54837
- [61] T. Li, M. Z. Mohd Zahir, and H. Mohd Ali, "A legal perspective of corporate compliance governance to collusive bidding in China," *Journal of Money Laundering Control*, vol. 27, no. 2, pp. 300-313, 2023. <https://doi.org/10.1108/jmlc-02-2023-0044>