

УДК 34

DOI: 10.34670/AR.2023.15.41.044

## Законодательный процесс, теоретическая практика и будущее направление развития киберпреступности в Китае

**Чжан Цян**

Докторант,  
Цзилиньский университет,  
Докторант, прошедший совместную подготовку в МГУ,  
130012, КНР, Чанчунь, Цяньцзинь, 2699;  
e-mail: qiangz20@ mails.jlu.edu.cn

**Лу Вэньчао**

Выпускник института русского языка  
Хэйлунцзянского университета,  
150080, КНР, Харбин, Сюэфу, 74;  
e-mail: zssluwenchao@163.com

### Аннотация

Цель настоящей статьи – разобраться в законодательном процессе по киберпреступности в Китае, проанализировать законодательную практику применения теорий Уголовного кодекса, связанных с киберпреступностью в Китае и заглянуть в будущее направления развития уголовного законодательства по киберпреступности в Китае с тем, чтобы предоставить опыт для российского законодательства по киберпреступности. В настоящее время киберпреступность стала наиболее многочисленным видом преступлений в Китае. Китай ввел основной состав киберпреступности в Уголовный кодекс 1997 года, расширил сферу борьбы с киберпреступностью в соответствии с Поправкой (VII) к Уголовному кодексу, Китай также ввел ряд новых составов киберпреступности в Поправку (IX) к Уголовному кодексу. Кроме того, в законодательной практике киберпреступности были применены такие теории, как криминализация приготовительных действий, криминализация помогающих действий и преступление с неисполнением обязанностей. С точки зрения будущего законодательства о киберпреступности китайские ученые в основном занимаются вопросами законодательной модели киберпреступности и установления уголовной порядочной системы преступлений, связанных с искусственным интеллектом. Киберпреступность имеет существенно иной образ действия и пространство действия по сравнению с традиционной преступностью. Поэтому в целях борьбы с растущим распространением киберпреступности в отношении особенностей киберпреступности необходимо своевременно принимать законодательство о киберпреступности и разрабатывать соответствующие теории Уголовного кодекса.

**Для цитирования в научных исследованиях**

Чжан Цян, Лу Вэньчао. Законодательный процесс, теоретическая практика и будущее направление развития киберпреступности в Китае // Вопросы российского и международного права. 2023. Том 13. № 8А. С. 371-379. DOI: 10.34670/AR.2023.15.41.044

**Ключевые слова**

Киберпреступность, уголовное законодательство, теоретическая инновация, китайская практика, Китай.

**Введение**

Развитие Интернета, с одной стороны, способствовало прогрессу человеческого общества, а с другой – породило киберпреступность. Китай, являясь мировой сверхдержавой по числу пользователей Интернета, отличается высоким уровнем киберпреступности. Согласно отчету, опубликованному Китайским исследовательским институтом судебных больших данных, в период с 2017 по 2021 год китайские суды всех уровней рассмотрели в первой инстанции в общей сложности более 282 тыс. дел о информационной киберпреступности, и количество таких дел растет из года в год. Для того чтобы справиться с постоянно меняющейся ситуацией с киберпреступностью, Китай способствует процессу уголовного законодательства в области киберпреступности, а также исследованию и инновации соответствующих уголовно-правовых теорий. Цель настоящей статьи – разобраться в законодательном процессе по киберпреступности в Китае, проанализировать законодательную практику применения теорий Уголовного кодекса, связанных с киберпреступностью в Китае и заглянуть в будущее направления развития уголовного законодательства по киберпреступности в Китае с тем, чтобы предоставить опыт для российского законодательства по киберпреступности.

**Основная часть***1. Обзор уголовного законодательного процесса по киберпреступности в Китае**1.1. УК1997 года: установление базового состава киберпреступности*

Уголовное законодательство Китая в области киберпреступности началось с принятия в 1997 году Уголовного кодекса КНР (далее – УК). Однако, поскольку Интернет в то время был недостаточно развит, соответствующие преступления, предусмотренные Уголовным кодексом 1997 года, в основном касались компьютерных информационных систем, включая преступление незаконного вторжения в компьютерную информационную систему (статья 285) и преступление нанесения ущерба компьютерной информационной системе (статья 286). Включение в УК 1997 года статьи о защите компьютерных информационных систем свидетельствует о том, что китайский законодательный орган стал придавать большое значение регулированию действий преступлений компьютерных и сетевых правонарушений, а также является одним из основных способов наказания за киберпреступность, что в определенной степени обеспечивает безопасность киберпространства Китая. Статья 285 УК в основном защищает права доступа к компьютерным информационным системам в области государственных дел, оборонного строительства, передовой науки и техники, а статья 286 УК предусматривает три вида действий по уничтожению компьютерных информационных систем, включая удаление, модификацию, дополнение и вмешательство в функции компьютерной

информационной системы; удаление, модификацию и дополнение данных и прикладных программ, хранящихся, обрабатываемых или передаваемых в компьютерной информационной системе; также преднамеренную разработку и распространение компьютерных вирусов и иных разрушительных программ. Кроме того, в УК 1997 года была добавлена статья 287, согласно которой любое лицо, использующее компьютер для совершения соответствующего преступления, такого как финансовое мошенничество, кража, растрата, присвоение государственных средств, хищение государственной тайны или другие преступления, подлежит осуждению и наказанию в соответствии с соответствующими положениями УК. Перечисленные выше три преступления составляют основу состава киберпреступности в Китае. На этом этапе Интернет еще не был широко распространен, а киберпреступность была еще в новинку, поэтому законодательные нормы были относительно просты, а разработка таких преступлений была сосредоточена на компьютерных информационных системах, поэтому в теории и на практике в то время чаще использовалось понятие «компьютерное преступление».

### 1.2. Поправка (VII) к УК 2009 года: расширение сферы борьбы с киберпреступностью

После наступления нового тысячелетия, в связи с бурным развитием информационных технологий и сетевых приложений, ситуация с безопасностью компьютерных сетей в Китае стала очень серьезной. Во-первых, резко возросло число случаев заражения компьютерных систем вирусами, троян, бэкдорами и другими деструктивными программами, что представляет большую потенциальную опасность для сетевой безопасности. Во-вторых, преступники распространяются от профессионального технического персонала к народу. В-третьих, компьютерные вирусы объединяются с троянскими программами и другими вредоносными кодами, в данном случае количество случаев стремительно растет таких, как путем массового распространения компьютерных вирусов с троянскими программами и программами-шпионы незаконно получить номера чужих счетов и идентификационной информации, а затем вторгаться в чужие компьютерные информационные системы для кражи данных из компьютерных информационных систем или для удаленного управления компьютерными информационными системами. Исходя из этого, в 2009 году законодатель ввел второй пункт статьи 289 под названием «Незаконное получение данных компьютерной информационной системы, незаконное управление компьютерной информационной системой» в поправку (VII) к УК, согласно которой включаются такие действия в круг преступлений, как проникновение в компьютерную информационную систему, не относящуюся к сфере государственного управления, оборонного строительства, передовой науки и техники, или использование ее технических средств получить данные, или незаконное управление компьютерной информационной системой. Кроме того, еще добавлен третий пункт в статью 285 под названием «Преступление в виде незаконного предоставления программ или средств для вторжения в компьютерную информационную систему или незаконного контроля над этими программами и средствами». Согласно положениям данного пункта, предоставление программ или средств, специально предназначенных для вторжения в компьютерную информационную систему или незаконного контроля над ними, либо предоставление программ или средств другому лицу с осознанием того, что оно совершает преступление, связанное с вторжением в компьютерную информационную систему или незаконным контролем над ними, что образует отдельный состав преступления. На данном этапе расширены составы киберпреступности, а также увеличивается масштаб борьбы с киберпреступностью.

1.3. Поправка (IX) к УК 2015 года: установление новых видов преступлений, связанных с киберпреступностью

С дальнейшим распространением компьютеров и сетей киберпреступность развивается в направлении цепочки и индустриализации, причем на долю киберпреступности приходится почти треть от общего числа преступлений в Китае, что киберпреступность занимает первое место во всех видах преступности. В этих условиях законодатель, реагируя на потребности практики, приняли ряд идей уголовного наказания, отличающихся от прежних, в соответствии с поправкой (IX) к УК был установлен ряд новых видов преступлений в сфере киберпреступности. К ним относятся: отказ от выполнения обязанностей по управлению безопасностью информационных сетей (из ст. 286), незаконное использование информационных сетей и содействие преступной деятельности в информационных сетях (оба из ст. 287). Установление этих трех составов преступлений позволило усовершенствовать китайскую законодательную систему в области киберпреступности и решить проблему невозможности осуждения многих деяний, угрожающих кибербезопасности. Кроме того, в поправку (IX) к УК еще добавлены такие преступления, как незаконное вторжение в компьютерную информационную систему, незаконное получение данных из компьютерной информационной системы, незаконное управление компьютерной информационной системой, предоставление программ и инструментов для вторжения в компьютерную информационную систему или незаконного управления ними, а также корпоративное преступление, связанное с повреждением компьютерной информационной системы.

*2. Анализ законодательной практики применения уголовно-правовых теорий, связанных с киберпреступностью в Китае*

#### 2.1. Законодательная практика теории криминализации приготовительных действий

Если в традиционной преступности преступное деяние может быть направлено только на один объект преступления, то развитие интернета совсем изменило традиционную схему «один на один». Иными словами, приготовительное действие, являющееся частью преступного процесса в традиционной преступности, в киберпреступности часто оно становится ключевым этапом в киберпространстве. Этим оно отличается от приготовительного действия в традиционной преступности, которое незаметно меняет весь преступный процесс и ключевые узлы, становясь одной из типичных форм преступности в информационную эпоху. Например, если преступник использует интернет для публикации мошеннического сообщения, то получателями этого сообщения могут быть тысячи людей. Если преступник, разместивший в сети мошенническую информацию, будет осужден и наказан в соответствии с составом преступления мошенничества, то его деяние будет признано как приготовление к преступлению мошенничества, поэтому если оно будет признано только приготовлением к преступлению мошенничества, то трудно будет отразить серьезную общественную опасность и совершенные новые характеристики самостоятельности деяния этого вида преступного действия, отличающегося от традиционного приготовительного действия. Поэтому в соответствии с поправкой (IX) к УК был создан состав преступления как «незаконное использование информационных сетей», который выделяет приготовительные действия к совершению преступлений с использованием информационных сетей как отдельный новый состав преступления. Данный состав преступления предусматривает, что «лицо, использующее информационную сеть для совершения одного из следующих деяний, при наличии серьезных обстоятельств, наказывается лишением свободы на определенный срок не более трех лет или уголовным арестом и наказывается штрафом дополнительно или только штрафом: (а) создание веб-сайта или коммуникационной группы с целью совершения незаконных и преступных действий, таких как мошенничество, обучение методам совершения преступлений,

изготовление или продажа запрещенных или контролируемых предметов; (б) публикация информации об изготовлении или продаже наркотиков, огнестрельного оружия, непристойных предметов и других запрещенных предметов, контролируемых предметов, или публикация другой незаконной и преступной информации; (в) публикация информации с целью совершения мошенничества и другой незаконной преступной деятельности». Криминализация приговорительных действий также отвечает диффузности киберпреступности и создает правовую основу для эффективного наказания за кибермошенничество и другие преступления.

## 2.2. Законодательная практика теории криминализации помогающих действий

Организационная структура киберпреступности изменилась от пирамидальной формы традиционной преступности к сетеподобной и цепной структуре в киберпространстве. Такая структура преступного действия делает отношения между субъектами совместной преступной деятельности более децентрализованными, а связь между помогающим действием в киберпреступности и выполняющим действием становится более отдаленной. По сравнению с традиционным помогающим действием, помогающее действие в киберпреступности играет все более решающую роль в завершении преступления. Поэтому необходимо выделить помогающее действие в киберпреступлениях как отдельный состав преступления, то есть криминализация помогающих действий. Криминализация действия соучастия (помогающих действий) – это законодательное явление, которое ограничивает сферу соучастия и расширяет сферу криминализации, основываясь на разграничении отдельного преступника и соучастника, с точки зрения законодательства предусматривать действие соучастия в качестве отдельного преступления. Законодательным примером криминализации помогающих действий является преступление содействия преступной деятельности в информационной сети, предусмотренное поправкой (IX) к УК, в которой, в частности, говорится: «Зная, что другое лицо использует информационную сеть для совершения преступления, оно обеспечивает техническую поддержку, таких как доступ в интернет, вэб-хостинг, сетевое хранение, передачу сообщений и т.д., или оказывает содействие в рекламе и продвижении, оплате и расчетах и др., при наличии серьезных обстоятельств, наказывается лишением свободы на срок не более трех лет или уголовным арестом, наказывается штрафом дополнительно или только штрафом». Благодаря установлению вышеуказанного состава преступления большое количество деяний по содействию преступлениям, совершаемым с использованием интернета, может быть признано отдельными преступлениями, что позволит бороться с сетеподобной и цепной структуре соответствующих преступлений.

## 2.3. Законодательная практика теории преступления с неисполнением обязанностей

Теория преступления с неисполнением обязанностей – это концепция, предложенная немецким криминалистом профессором Клаусом Роксаном. Обязанности при преступлении с неисполнением обязанностей – это требования, предъявляемые непосредственно к правонарушителю извне, без каких-либо предпосылок со стороны какого-либо лица, дела или предмета, в данном случае обязанность действия является позитивной обязанностью, специальной обязанностью, исключительной для конкретного юридического интереса в результате вступления в определенный режим. Смысл этого заключается в том, что даже если результат возник не в результате его действия, он все равно должен нести за него ответственность. Отказ от исполнения обязанности по управлению безопасностью информационной сети, предусмотренное поправкой к УК, является типичным преступлением с неисполнением обязанностей. Закон гласит: Если поставщик сетевых услуг не выполняет обязанности по управлению безопасностью информационной сети, предусмотренные законами

и административными регламентами, и отказывается принять меры по исправлению ситуации по предписанию надзорного ведомства, и если такой отказ приводит к определенным серьезным последствиям, он наказывается лишением свободы на срок до трех лет, уголовным арестом или контролем, наказывается штрафом дополнительно или только штрафом. Обязанность управления безопасностью информационной сети является уголовной порядочной обязанностью поставщиков сетевых услуг, а невыполнение такой уголовной порядочной обязанности представляет собой преступление. Благодаря законодательной практике, основанной на теории преступления с неисполнением обязанностей, бездействие поставщиков сетевых услуг эффективно регулируется.

### *3. Направление развития уголовного законодательства о киберпреступности в Китае*

#### 3.1. Обсуждение будущих законодательных моделей киберпреступности

В настоящее время в отношении законодательной модели киберпреступности в Китае существуют различные мнения, среди которых можно выделить следующие три основных типа. Первый тип взглядов заключается в том, что уголовное законодательство о киберпреступности должно по-прежнему поправиться в рамках УК. Второй тип взглядов считает, что киберпреступность должна быть независимой от УК и составлять отдельный Уголовный кодекс. Третий тип взглядов считает, что киберпреступность должна регулироваться Законом о кибербезопасности, Законом о безопасности данных, Законом о защите персональной информации и т.д., т.е. моделью субсидиарного уголовного права. По мнению автора, соответствующее содержание УК о киберпреступности должно быть системно пересмотрено на основе соблюдения законодательной модели единого УК. Во-первых, киберпреступность может быть выделена в отдельную главу по примеру Уголовного кодекса Российской Федерации. Во-вторых, следует систематически пересматривать составы преступлений, связанных с киберпреступностью, придавая им более научный характер. И наконец, необходимо поправить дополнительные составы преступлений, связанных с киберпреступностью, чтобы ужесточить правовую сетку киберпреступности.

#### 3.2. Обсуждение направления развития законодательства о преступлениях, связанных с искусственным интеллектом (ИИ)

В связи с непрерывным развитием технологий искусственного интеллекта обсуждение преступлений, совершаемых искусственным интеллектом, постепенно расширяется, и основным вопросом дискуссии является уголовная ответственность ИИ. Спорным является вопрос о том, несет ли уголовную ответственность за преступления, совершенные ИИ, сам ИИ или его создатель или пользователь. Согласно современным китайским теориям, ИИ подразделяется на два типа: слабый и сильный. Считается также, что современный ИИ все еще находится на стадии слабого ИИ, и в центре внимания слабого ИИ должен стоять правовой интерес алгоритмической безопасности, а разработчики или пользователи слабого ИИ должны быть наказаны, и законодательство также должно быть построено вокруг этого правового интереса. Некоторые ученые считают, что преступление разработки, производства, продажи и использования продуктов ИИ, не соответствующих стандартам алгоритмической безопасности, преступление незаконной разработки, производства, владения, торговли, транспортировки и использования оружия ИИ, преступление несанкционированного изменения алгоритма и использования продуктов ИИ, преступление неправомерного использования ИИ, нарушение правил дорожного движения, связанное с ИИ и другие преступления против алгоритмической безопасности, они должны быть добавлены к второй Главе особенной части УК о преступлении против общественной безопасности. Что касается сильного ИИ, по мнению некоторых ученых,

сам сильный ИИ уже может стать субъектом преступления в УК, поэтому преступления, совершаемые им в соответствии с особенной частью УК, должны подлежать уголовному наказанию, только меры наказания за них должны быть добавлены к общим положениям УК. Некоторые ученые предлагают ввести дополнительные наказания, такие как удаление данных, модификация программ, необратимое уничтожение и т.д., которые могут быть применены к интеллектуальным роботам, а когда созреют условия, добавить такие уголовные наказания, как имущественные или правовые, которые могут быть применены к интеллектуальным роботам.

### Заключение

Киберпреступность имеет существенно иной образ действия и пространство действия по сравнению с традиционной преступностью. Поэтому в целях борьбы с растущим распространением киберпреступности в отношении особенностей киберпреступности необходимо своевременно принимать законодательство о киберпреступности и разрабатывать соответствующие теории Уголовного кодекса.

### Библиография

1. Ван Хуавэй. Систематическая оценка и рефлексия китайского законодательства о киберпреступности // Журнал права. 2019. № 1. С. 130.
2. Вэй Дун. Взгляд на преступность в сфере алгоритмической безопасности искусственного интеллекта и его нормативное расширение в уголовной науке // Записки политики и права. 2020. № 3.
3. Ли Сянся. Об информатизации организованной преступности и организации киберпреступности // Социальная наука Хэнань. 2016. № 11.
4. Лю Сяньцюань. Внутреннее беспокойство, внешнее осложнение и уголовная ответственность в эпоху искусственного интеллекта // Восточное право. 2018. № 1. С. 184.
5. Лю Сяньцюань. Юриспруденческие основы реконструкции уголовной системы Китая в эпоху искусственного интеллекта // Юридическая наука. 2018. № 4. С. 47.
6. Сунь Даоцзуй. Трансформация знаний о киберуголовном праве и ответы законодательства // Современное право. 2017. № 1. С. 117-131.
7. Хуан Тайюнь. Толкование поправки (VII) к УК // Народная прокуратура. 2009. № 6. С. 16.
8. Хэ Цинжэнь. Исследование о преступлении с неисполнением обязанностей. Издательство Китайского народного университета, 2010. С. 257.
9. Цзан Тивэй. Толкование Поправки к УК Китайской Народной Республики (IX). Китайское юридическое издательство, 2015. С. 206.
10. Чжан Минкэй. Уголовное законодательство в эпоху сетей // Юридическая наука. 2017. № 3. С. 69-82.
11. Чу Хуайши, Сюэ Мэйцинь. Размышления об уголовном законодательстве в эпоху сетей // Народная прокуратура. 2018. № 9. С. 15.
12. Чэнь Синьян. Криминализация действия соучастия: с точки зрения содействия информационной киберпреступности // Журнал сравнительно-правового исследования. 2022. № 2. С. 44.
13. Чэнь Синьян. Уголовно-правовые ответы на киберпреступность // Обзор законодательства Китая. 2020. № 1. С. 93.
14. Юй Чжиган. Идея санкций и совершенствование системы преступного подготовительного действия в киберпространстве // Законовед. 2017. № 6. С. 58.
15. Юй Чонг. Законодательное совершенствование и идеи развития системы составов киберпреступности – от УК 1997 года до Проекта поправок (IX) к УК // Вестник Китайского университета политических наук и права. 2015. № 4. С. 40.
16. Ян Чуньчжу, Цинь Сючунь. Представление концепции компьютерных преступлений в УК // Юридический форум. 2000. № 3. С. 57.

## Legislative process, theoretical practice and future direction of cybercrime in China

**Zhang Qiang**

PhD student of the School of Law, Jilin University,  
130012, 2699, Qianjin ave., Changchun, China;  
e-mail: qiangz20@ mails.jlu.edu.cn

**Lu Wenchao**

Graduate of the Institute of Russian Language,  
Heilongjiang University,  
150080, 74, Xuefu Road, Harbin, China;  
e-mail: zsslwenchao@163.com

### Abstract

The purpose of this article is to understand the legislative process on cybercrime in China, analyze the legislative practice of applying the theories of the Criminal Code related to cybercrime in China, and look into the future direction of development of criminal legislation on cybercrime in China in order to provide experience for Russian legislation on cybercrime. Currently, cybercrime has become the most numerous types of crime in China. China introduced the basic offenses of cybercrime in the Criminal Code of 1997, expanded the scope of combating cybercrime in accordance with Amendment (VII) of the Criminal Code, and China also introduced a number of new offenses of cybercrime in Amendment (IX) of the Criminal Code. In addition, in the legislative practice of cybercrime, theories such as the criminalization of preparatory actions, the criminalization of assisting actions and the crime of dereliction of duty have been applied. From the perspective of future cybercrime legislation, Chinese scholars mainly focus on the legislative model of cybercrime and the establishment of a criminal justice system for crimes related to artificial intelligence. Cybercrime has a significantly different *modus operandi* and operating space compared to traditional crime. Therefore, in order to combat the growing prevalence of cybercrime, regarding the characteristics of cybercrime, it is necessary to timely enact cybercrime legislation and develop relevant Penal Code theories.

### For citation

Zhang Qiang, Lu Wenchao (2023) *Zakonodatel'nyi protsess, teoreticheskaya praktika i budushchee napravlenie razvitiya kiberprestupnosti v Kitae* [Legislative process, theoretical practice and future direction of cybercrime in China]. *Voprosy rossiiskogo i mezhdunarodnogo prava* [Matters of Russian and International Law], 13 (8A), pp. 371-379. DOI: 10.34670/AR.2023.15.41.044

### Keywords

Cybercrime, criminal legislation, theoretical innovation, Chinese practice, China.

---

## References

1. Chen Xinliang (2020) Criminal legal responses to cybercrime. *Review of Chinese legislation*, 1, p. 93.
2. Chen Xinliang (2022) Criminalization of the act of complicity: from the point of view of promoting information cybercrime. *Journal of Comparative Legal Research*, 2, p. 44.
3. Chu Huaishi, Xue Meiqin (2018) Reflections on criminal legislation in the era of networks. *People's Prosecutor's Office*, 9, p. 15.
4. He Qingren (2010) *A study on the crime of dereliction of duty*. Chinese People's University Press.
5. Huang Taiyun (2009) Interpretation of Amendment (VII) to the Criminal Code. *People's Prosecutor's Office*, 6, p. 16.
6. Li Xiangxia (2016) On the informatization of organized crime and the organization of cybercrime. *Social Science of Henan*, 11.
7. Liu Xianquan (2018) Internal anxiety, external complication and criminal liability in the era of artificial intelligence. *Eastern law*, 1, p. 184.
8. Liu Xianquan (2018) Legal basis for the reconstruction of the Chinese criminal system in the era of artificial intelligence. *Legal science*, 4, p. 47.
9. Sun Daozui (2017) Transformation of knowledge about cyber criminal law and legislative responses. *Modern law*, 1, pp. 117-131.
10. Wang Huawei (2019) Systematic assessment and reflection of Chinese legislation on cybercrime. *Journal of Law*, 1, p. 130.
11. Wei Dong (2020) A look at crime in the field of algorithmic security of artificial intelligence and its normative expansion in criminal science. *Notes on politics and law*, 3.
12. Yang Chunzhu, Qin Xiuchun (2000) Presentation of the concept of computer crimes in the Criminal Code. *Legal Forum*, 3, p. 57.
13. Yu Chong (2015) Legislative improvement and ideas for developing the system of cybercrime offenses – from the 1997 Criminal Code to the Draft Amendments (IX) to the Criminal Code. *Bulletin of the Chinese University of Political Science and Law*, 4, p. 40.
14. Yu Zhigang (2017) The idea of sanctions and improving the system of criminal preparatory action in cyberspace. *Lawyer*, 6, p. 58.
15. Zang Tiwei (2015) *Interpretation of Amendments to the Criminal Code of the People's Republic of China (IX)*. Chinese Legal Publishing House.
16. Zhang Mingkei (2017) Criminal legislation in the era of networks. *Legal science*, 3, pp. 69-82.