УДК 343.2 Вестник СПбГУ. Право. 2022. Т. 13. Вып. 3

Уголовно-правовое регулирование противодействия киберпреступности в Китае: состояние, тенденции и недостатки*

Ван Гуанлун

Хэнаньский университет,
Китайская Народная Республика, 475001, Кайфун, ул. Минлунь, 85

Для цитирования: Ван Гуанлун. 2022. «Уголовно-правовое регулирование противодействия киберпреступности в Китае: состояние, тенденции и недостатки». *Вестник Санкт-Петербургского университета. Право* 3: 661–677. https://doi.org/10.21638/spbu14.2022.305

В современном Китае киберпреступность становится все более распространенной, что породило теоретическую необходимость переосмысления уголовного права на базовом теоретическом уровне. Китайские правоведы и практики характеризуют киберпреступность с четырех точек зрения: с точки зрения предмета преступления, инструмента преступления, места преступления и взаимных связей. Поддерживая данную позицию с учетом соответствующих положений уголовного законодательства Китая о киберпреступности, автор статьи считает, что под киберпрестпностью понимается любое преступление, совершаемое с помощью компьютерной системы или сети, в ее рамках либо против нее. При регулировании противодействия преступлениям в киберпространстве следует сместить акцент киберуголовного права с традиционного сетецентрического на ориентированное на данные и построить систему защиты правовых благ в виде ориентации на данные. Кроме того, расширение объективных составных элементов киберпреступлений должно быть умеренным. Определенные киберправонарушения нельзя квалифицировать как незаконное предпринимательство (ст. 225 Уголовного кодекса КНР), так как это противоречит принципу законности уголовного права. Содержание заведомости в качестве признака субъективной стороны преступления должно быть переосмыслено и расширено на вероятное представление о совершении преступлений без сговора с исполнителем в соучастии в преступлении. Теоретическая основа для идентификации соучастия в киберпреступлении должна быть скорректирована путем утверждения односторонней субъективной связи. Посредством систематической корректировки и переосмысления основной теории уголовного права в этой области осуществляется постепенное совершенствование уголовно-правовых норм по регулированию борьбы с киберпреступностью в эпоху информационных сетей.

Ключевые слова: киберуголовное право, киберпреступность, киберпространство, заведомость, незаконное приобретение данных, соучастие в киберпреступлении, соучастие с одной субъективной связью, регулирование киберпреступлений.

* Статья подготовлена в рамках проекта Национального комитета КНР по управлению фондом для обучения за границей (CSC) № 202110100004.

1. Введение

По состоянию на июнь 2021 г. число пользователей интернета в Китае составляло 1,011 млрд, что на 21,75 млн больше по сравнению с декабрем 2020 г., а уровень проникновения интернета достиг 71,6 %, увеличившись на 1,2 % по сравнению с декабрем 2020 г.[1] Однако пока люди используют множество удобств, созданных развитием интернета, киберпреступность также незаметно вторгается во все аспекты жизни человека. Известный американский ученый Р. Спинелло говорил о том, что интернет не только откроет новый мир создания и свободы, но и станет виртуальной площадкой для греха и разврата (Спинелло 2007, 2). В Китае доля киберпреступлений в настоящее время составляет почти треть от общего числа преступлений, и с каждым годом она увеличивается примерно на 30 % (Шан 2016). Уголовное законодательство не только не может закрывать глаза на такую безудержную киберпреступность, но и должно проявлять инициативу для принятия эффективных мер. Предпосылкой изучения уголовного законодательства выступает определение понятия «киберпреступление».

2. Основное исследование

2.1. Определение понятия «киберпреступление» в Китае

В китайском юридическом сообществе еще не сформировано единое понимание киберпреступления. Некоторые ученые даже утверждают, что это понятие «является наиболее расплывчатой и запутанной субкриминальной концепцией в области уголовного права» (Сюй 2017, 115). Другие ученые считают, что киберпреступность — это криминологическое понятие и не относится к разделению видов преступлений в уголовном праве (Юй 2003, 73).

В целом в кругу китайских ученых — специалистов в области уголовного права понятие киберпреступления характеризуется с четырех точек зрения:

— с точки зрения предмета преступления киберпреступление определяется как деяние, совершаемое против самой сети; также в эпоху Web 1.0 оно называлось компьютерным преступлением (Сюй 2002, 30); по мнению профессора Чжао Бинчжина, «компьютерные преступления относятся к совершаемым с помощью компьютерных операций преступным деяниям, которые ставят под угрозу безопасность компьютерных информационных систем (включая данные и программы памяти)» (Чжао 1998, 10);
— с точки зрения инструмента преступления киберпреступления определяются как преступные деяния, совершаемые с использованием интернета; эта точка зрения в основном была сформирована в Китае во время перехода от эпохи Web 1.0 к эпохе Web 2.0 и в начале формирования эпохи Web 2.0; ученые, придерживающиеся указанной позиции, определяют киберпреступления как «действия, совершаемые лицом с помощью ком-

[1] Приводится по: 中国上网人数调查2021年多少人?我国网民数量变化新数据公布 [Сколько человек будет онлайн в Китае в 2021 г.? Опубликованы новые данные об изменении числа пользователей сети в стране]. Дата обращения 2 ноября, 2021. https://www.ironge.com.cn/News/scroll/399341.html.

пьютеров, средств связи и других технических средств, направленные на нарушение или угрозу законным интересам» (Чжан 2003, 234);

— с точки зрения места преступления киберпреступления представляют собой преступные деяния, совершаемые в киберпространстве; эта точка зрения возникла из понятия «двухслойное общество», предложенного профессором Юй Чжиганом, полагающим, что человечество вступило в «двумерное пространство», в котором сосуществуют реальное общество и онлайн-общество; статус интернета в сфере преступности вырос от предмета преступления и инструмента преступления до места преступления — киберпространства (Юй 2014, 1045);

— с точки зрения взаимных связей киберпреступления включают в себя акты нападения на компьютер или сеть (т. е. компьютер и сеть рассматриваются как предмет нападения), акты с использованием компьютера или сети в качестве орудия преступления, а также акты, совершенные в киберпространстве (Сюй 2020, 32); эта позиция основана на положениях уголовного законодательства Китая о конкретных признаках определенных составов преступлений, связанных с компьютером или сетью, а именно на анализе шести составов преступлений, предусмотренных ст. 285–287 Уголовного кодекса КНР[2] (УК КНР); таким образом, понятие киберпреступления включает в себя такие элементы, как предмет преступления, инструмент преступления и пространство для совершения преступления.

Мы согласны с последней точкой зрения: даже в эпоху Web 3.0 не могут быть полностью исчерпаны передовые технологии предыдущих периодов, так как действия, которые разрушают компьютерные системы, функции или нарушают работу компьютеров без подключения к интернету, не исчезли, а потому соответствующие положения уголовного закона также не могут быть отменены. Существование этого явления не только неизбежный результат развития сетевых технологий, но и результат реакции уголовного законодательства на киберпреступность. Следовательно, термин «киберпреступность» включает в себя любое преступление, совершаемое с помощью компьютерной системы или сети, в ее рамках или против нее.

2.2. Развитие уголовного законодательства Китая в области регулирования киберпреступлений

Уголовное законодательство Китая, касающееся системы составов преступлений, связанных с киберпреступностью, прошло три этапа развития.

[2] 中华人民共和国刑法 [Уголовный кодекс КНР]. 1997. Дата обращения 20 апреля, 2022. https://www.66law.cn/tiaoli/9.aspx. — К этим шести составам преступлений относятся: незаконное вторжение в компьютерные информационные системы (ч. 1 ст. 285); незаконное приобретение данных компьютерных информационных систем или незаконное управление компьютерными информационными системами (ч. 2 ст. 285); предоставление программ, приборов для вторжения в компьютерные информационные системы или незаконного управления ими (ч. 3 ст. 285); разрушение компьютерных информационных систем (ст. 286); отказ от выполнения обязательств по управлению безопасностью информационной сети (ст. 286.1); незаконное использование информационных сетей (ст. 287.1).

На первом этапе положения о киберпреступлениях были внесены в УК КНР 1997 г. С развитием компьютерных технологий, в целях защиты безопасности компьютерных информационных систем в УК КНР 1997 г. впервые были предусмотрены такие составы преступлений, как незаконное вторжение в компьютерные информационные системы (ст. 285) и разрушение компьютерных информационных систем (ст. 286)[3]. Нормы ст. 285 направлены на защиту прав доступа к компьютерным информационным системам в областях государственных дел, национальной обороны и передовых достижений науки и техники. Статья 286 предусматривает три вида действий, которые разрушают компьютерные информационные системы, в том числе удаление, изменение, добавление функций компьютерных информационных систем или вмешательство в них; удаление, изменение или добавление данных и прикладных программ, хранящихся, обрабатываемых или передаваемых в компьютерных информационных системах, а также преднамеренное создание или распространение разрушительных программ, таких как компьютерные вирусы.

Кроме того, в УК КНР 1997 г. была добавлена ст. 287 об использовании компьютеров для совершения преступлений. В соответствии с регламентацией указанной статьи те, кто с использованием компьютера совершил такие преступления, как финансовое мошенничество, кража, коррупционные действия, использование не по назначению общественных средств, хищение государственной тайны и т. д., должны быть квалифицированы и наказаны согласно соответствующим статьям УК КНР.

Вышеуказанные конкретные составы преступлений (ст. 285, 286) и общие положения (ст. 287) выступают основой системы составов киберпреступлений в Китае, которую ученые называют «двухточечной и одноинклюзивной» системой составов преступлений (Пи 2009, 50).

На этом этапе интернет был еще не популяризирован и киберпреступность оставалась новинкой, поэтому законодательные положения о ней были относительно просты, а основным носителем и средством совершения таких преступлений по-прежнему выступали компьютеры. Следовательно, в теории и практике того времени понятие «компьютерное преступление» использовалось чаще (Ян, Цинь 2000, 57).

На втором этапе Поправки № 7 к УК КНР от 28.02.2009[4] расширили круг киберпреступлений. После вступления в XXI в. с быстрым развитием информационных технологий в Китае уровень проникновения интернета быстро вырос и проблемы сетевой безопасности обострились. Например, согласно статистике Национального центра реагирования на компьютерные вирусы в чрезвычайных ситуациях, в 2007 г. в Китае около 91,47 % компьютеров, подключенных к интернету, были за-

[3] 全国人大常委会法制工作委员会刑法室编:《中华人民共和国刑法条文说明、立法理由及相关规定》, 北京：北京大学出版社，2009年版，第593页。 [Разъяснение, законодательные основания и соответствующие положения статей УК КНР, составленные Отделом уголовного права Комитета по правовым вопросам Постоянного комитета Всекитайского собрания народных представителей. 2009. Пекин: Издательство Пекинского университета].

[4] Поправки № 7 к УК КНР от 28.02.2009 были приняты и обнародованы на Седьмом заседании Постоянного комитета Одиннадцатого Всекитайского собрания народных Представителей Китайской Народной Республики, и вступили в силу с даты обнародования. (2009年2月28日，《中华人民共和国刑法修正案（七）》经中华人民共和国第十一届全国人民代表大会常务委员会第七次会议通过并公布，自公布之日起施行。) Дата обращения 20 апреля, 2022. http://www.gdxunfa.cn/article.asp?id=1136.

ражены вирусами и троянскими программами, а число компьютеров с более чем тремя вирусами и троянскими программами составляли 53,64 % (Хуан 2009, 16).

В контексте эпохи интернета сфера компьютерных информационных систем, о которых говорится в ст. 285 УК КНР, слишком узка, а такие системы, не относящиеся к сферам государственных дел, национальной обороны и передовой науки и техники, не защищаются уголовным законом; вместе с тем число случаев кражи данных и управления компьютерными информационными системами после вторжения в них быстро возросло, и такие деяния не могут быть охвачены диспозицией указанной статьи (Хуан 2015, 224). В связи с этим законодатель посредством добавления Поправками № 7 к УК КНР ч. 2 ст. 285 УК КНР «Незаконное приобретение данных компьютерной информационной системы, незаконное управление компьютерными информационными системами» криминализировал такие деяния, как вторжение в компьютерные информационные системы вне сферы государственных дел, национальной обороны и передовой науки и техники, приобретения данных с использованием других средств или незаконного управление компьютерными информационными системами.

Кроме того, одна из важных причин распространения незаконного вторжения в компьютерные информационные системы и кражи данных заключается в том, что некоторые люди специализируются на создании и продаже программ и устройств, используемых для совершения названных преступных деяний, что значительно уменьшает сложность совершения таких преступлений. Поэтому законодатель специально криминализировал указанные деяния — Поправками № 7 к УК КНР была добавлена ч. 3 ст. 285 «Незаконное предоставление программ и устройств для вторжения в компьютерные информационные системы и незаконного управления ими». В соответствии с рассматриваемой частью деяния, связанные с предоставлением программ, устройств, специально используемых для вторжения, незаконного управления компьютерными информационными системами, или предоставлением программ, устройств другим лицам, заведомо совершающим незаконные и преступные действия по вторжению или незаконному управлению указанными системами, квалифицируются как отдельный состав преступления. Законодательные органы считают, что поставщики вышеупомянутых программ, устройств чаще всего продают эту продукцию через несколько агентов, поэтому трудно определить связь между соучастниками (пособниками) и реальными исполнителями. Поэтому во избежание трудностей с выявлением соучастия в преступлении законодатель отдельно криминализировал деяния таких лиц (Хуан 2009, 18).

На данном этапе модель законодательства Китая о киберпреступности соответствовала международным стандартам, т. е. УК КНР охватывал несколько видов киберпреступности, распространенных во всем мире, и сфера защиты уголовного права была значительно расширена.

На третьем этапе Поправки № 9 к УК КНР от 29.08.2015[5] еще больше расширили сферу криминализации правонарушений, связанных с интернетом. По состоянию

[5] Поправки № 9 к УК КНР от 29.08.2015 были приняты и обнародованы на Шестнадцатом заседании Постоянного комитета Двенадцатого Всекитайского собрания народных Представителей Китайской Народной Республики, и вступили в силу 1 ноября 2015 г. (2015年8月29日，第十二届全国人大常委会十六次会议表决通过刑法修正案（九），自2015年11月1日起开始施行。) Дата обращения 20 апреля, 2022. http://www.law-lib.com/law/law_view.asp?id=507352.

на июнь 2015 г. уровень проникновения интернета в Китае составил 48,8 %, число китайских пользователей интернета достигло 668 млн, из них число пользователей интернет-магазинов — 374 млн[6]. Однако киберпреступность продолжает развиваться. Общие ее масштабы и количество участников были беспрецедентны. В подобном социальном контексте в ответ на практические потребности законодатель еще раз расширил сферу криминализации поведения, связанного с кибернетикой.

Во-первых, была установлена прямая уголовная ответственность поставщика интернет-услуг, который в прошлом являлся субъектом косвенной ответственности, поскольку на практике некоторые лица часто не выполняли свои обязательства в соответствии с законами и административными регламентами, что приводило к серьезным последствиям. Поэтому неисполнение такими поставщиками обязательств по обеспечению информационной безопасности должно преследоваться по уголовному законодательству (Цан 2015, 190–191). Так, Поправками № 9 к УК КНР был введен отдельный состав преступления — отказ от выполнения обязательств по управлению безопасностью информационной сети (ст. 286.1 УК КНР). Если интернет-провайдер не выполняет свои обязательства по обеспечению безопасности информационной сети, предусмотренные законами и административными регламентами, и отказывается вносить исправления после того, как надзорный орган приказал принять меры, что приводит к одному из таких последствий, как крупномасштабное распространение незаконной информации, разглашение информации о пользователях, уничтожение доказательств по уголовным делам, то указанное деяние образует преступление.

Во-вторых, законодатель принял стратегию непосредственной криминализации подготовительного и вспомогательного деяний для совершения киберпреступления, т. е. рассматриваемые деяния были прямо предусмотрены в УК КНР в качестве отдельных составов преступлений.

Поскольку киберпреступность развивается, трудно реагировать на практические потребности путем борьбы только с нижестоящими звеньями преступной цепи. В связи с этим появилась новая превентивная уголовно-правовая теория о предварительном наказании, осуществлении раннего вмешательства и «ранней борьбе с малой преступностью» (Хэ 2017, 142). На практике возникают проблемы, касающиеся сбора доказательств, выявления фактов киберпреступлений и применения законов; межрегиональный, гибкий и децентрализованный характер подобных деяний затрудняет выявление всех участников преступления, поэтому законодатель дополнил УК КНР ст. 287.1 «Незаконное использование информационных сетей», в которой предусмотрены специальные положения для таких действий, как создание веб-сайтов и распространение информации, способствующей совершению преступлений (Цан 2015, 200–201). Это преступление может образовать любое из действий, совершенных с использованием информационной сети при отягчающих обстоятельствах. К таким деяниям относятся следующие: создание сайтов или связных групп, предназначенных для мошенничества, обучения способам преступления, изготовления или сбыта запрещенных или находящихся под контро-

[6] 中国互联网信息中心：《第36次中国互联网络发展状况统计报告》，2015年7月23日，第7, 29页。 [36-й статистический отчет о состоянии развития интернет-сети Китая, опубликованный Китайским информационным интернет-центром 23 июля 2015 г. С. 7, 29]. Дата обращения 20 апреля, 2022. http://www.cac.gov.cn/2015-07/23/c_1116018119.htm.

лем предметов; распространение информации об изготовлении, сбыте наркотиков, оружия, порнографических предметов и иных запрещенных или находящихся под контролем предметов или иной преступной информации; публикация информации для совершения мошенничества или иной преступной деятельности.

В то же время Поправками № 9 в УК КНР был добавлен еще отдельный состав преступления — содействие информационной киберпреступности (ст. 287.2):

> 1. Предоставление средства соединения с интернетом, сервера, хранения сети, передачи связи и иного технического обеспечения, предоставление рекламного продвижения, средств расчета или оказание иной помощи другим лицам, заведомо совершающим преступления с использованием информационных сетей, при отягчающих обстоятельствах — наказываются лишением свободы на срок до трех лет, арестом или надзором и дополнительно или в качестве самостоятельного наказания — штрафом.
>
> 2. Если те же деяния совершаются организацией, то в отношении организации применяется штраф, а несущие непосредственную ответственность руководители организации и другие непосредственно ответственные лица — наказываются в соответствии с ч. 1 первой настоящей статьи.
>
> 3. Те же деяния, содержащие состав другого преступления, — наказываются по санкции за более тяжкое из преступлений.

Кроме того, Поправками № 9 в УК КНР также дополнительно предусмотрена корпорация (юридическое лицо) в качестве субъекта следующих преступлений: незаконное вторжение в компьютерные информационные системы; незаконное приобретение данных компьютерных информационных систем или незаконное управление компьютерными информационными системами; предоставление программ, приборов для вторжения в компьютерные информационные системы или незаконного управления ими; разрушение компьютерных информационных систем.

2.3. Тенденции уголовно-правового регулирования киберпреступности в Китае

Проанализировав вышеупомянутые изменения в УК КНР о киберпреступности, можно выделить некоторые тенденции законодательства Китая в этой сфере:

— расширение системы составов преступлений в сфере киберпреступности, отвечающих на социальную реальность; выделенные ранее этапы развития уголовного законодательства Китая о киберпреступности показывают, что своевременное реагирование на реальность постепенного ухудшения ситуации и постоянное расширение системы составов преступлений в этой сфере являются одной из основных характеристик уголовно-правового регулирования в Китае;

— предварительное наказание с превентивным характером; по мере того как киберпреступность начала развиваться, законодатель создал превентивную стратегию предварительного наказания, чтобы более эффективно справиться с указанной ситуацией и преодолеть трудности, возникающие

при квалификации и назначении наказания за это деяние (Хэ 2017, 141); основываясь на идеях непосредственной криминализации подготовительных деяний и деяний соучастников, законодатель дополнительно предусмотрел в Поправках № 7 ч. 3 ст. 285 УК КНР, криминализирующую конкретные действия по оказанию технической помощи (т. е. предоставлению программ и устройств) при совершении преступлений, предусмотренных ч. 1 и 2 ст. 285, а также в Поправках № 9 добавил в УК КНР состав «незаконное использование информационных сетей» (ст. 287.1) и дополнительно ввел ст. 287.2 УК КНР для криминализации киберпреступности в широком смысле (т. е. всех преступлений, совершенных с использованием информационных сетей);

— тенденция открытого законодательства; содействие информационной киберпреступности, предусмотренное ст. 287.2, содержит характеристики обобщенного открытого законодательства: с одной стороны, в этой статье предусмотрено несколько видов соучастия, которые включают в себя почти все виды киберпреступности; с другой стороны, соучастие в этом составе преступления является достаточно широким: хотя в рассматриваемой статье четко перечислены конкретные действия по оказанию помощи, такие как «предоставление средства соединения с интернетом, сервера, хранения сети, передачи связи» и «предоставление рекламного продвижения, средств расчета», однако законодатель включил в эту статью такие обобщенные выражения, как «предоставление… иного технического обеспечения», «оказание иной помощи».

Модель открытого законодательства стала стратегическим выбором для современного Китая. Она направлена на восполнение возможных упущений в уголовном законе, обеспечивает широкую нормативную базу для судебной системы, предоставляет бóльшие возможности для уголовно-правового регулирования новых видов киберпреступности, которые еще не сформировались в обществе, но вместе с тем оставляет много скрытых рисков.

2.4. Недостатки уголовно-правового регулирования киберпреступности в Китае

Действующее уголовное законодательство Китая имеет ряд недостатков в регулировании киберпреступности.

Во-первых, недостаточна системность норм о защите данных. Существующая в Китае система уголовного законодательства уделяет особое внимание защите сетей или компьютерных информационных систем, которые являются инфраструктурой киберпространства; в соответствии с этим установлены вышеупомянутые составы преступлений. Однако не так много внимания уделяется защите данных: в УК КНР имеется только один чистый состав преступления, связанный с данными, — незаконное приобретение данных компьютерной информационной системы (ч. 2 ст. 285).

Некоторые ученые отмечали, что сеть выступает необходимым условием и основой для обеспечения безопасности данных, а данные в сети представляют собой ядро и основу уголовно-правовой защиты (Ту 2019, 126). С развитием информа-

ционных технологий (особенно с широким использованием таких технологий, как большие данные) сбор и использование данных значительно влияют на все аспекты национальной безопасности, социальной деятельности и жизни людей. Поэтому следует содействовать инновациям и трансформации уголовно-правовой защиты благ в киберпространстве от традиционной сетевой ориентации к ориентации на данные. «Ориентация на данные» заключается не в том, чтобы абсолютно ослабить защиту сетевой инфраструктуры (например, компьютерных информационных систем), а в том, чтобы осуществить поэтапный сдвиг в относительной направленности защиты от традиционного сетецентрического к ориентированному на данные (Чэн 2019, 36–38).

По сравнению с традиционной защитой благ, система защиты правовых благ «ориентация на данные» имеет следующие основные характеристики: 1) юридические интересы, основанные на данных, следует рассматривать как самостоятельные блага уголовно-правовой защиты; кроме того, методы рассматриваемой защиты отличаются от способов защиты от традиционных имущественных преступлений; 2) данные нужно рассматривать как основной предмет уголовно-правовой защиты, которому должна быть предоставлена ключевая защита; 3) при проектировании системы должна быть создана комплесная система уголовно-правовой защиты данных в сфере их генерации, хранения, передачи, владения ими, их использования и передачи.

Во-вторых, возникают трудности в судебной практике, вызванные расширением объективной стороны киберпреступности. Сетевая трансформация правонарушений в первую очередь отражается на изменении объективных признаков преступного поведения. Одной из наиболее отличительных особенностей здесь является расширение признаков объективной стороны: количества предметов посягательства и расширительное толкование существующих составов преступлений.

Что касается первого, то в аспекте истории развития учения о преступлении сфера охвата предметов преступлений всегда увеличивается по мере прогресса науки и техники, повышения уровня знаний. В киберпространстве это особенно очевидно. Новыми формами киберпреступности выступают компьютерные информационные системы, данные и виртуальная собственность. Различия, основанные на понимании природы предмета преступления, приведут к очевидным различиям в судебных решениях и повлияют на единство уголовно-правовой оценки. Например, китайские суды имеют непоследовательное понимание правовой природы виртуальной собственности в киберпространстве[7], что привело к огромным различиям: акт кражи сетевой виртуальной собственности на практике квалифицировался по УК КНР как нарушение свободы переписки (ст. 252)[8], как кража

[7] Среди китайских ученых-юристов существуют совершенно различные мнения относительно правовой природы виртуальной собственности; она рассматривается как: 1) вещные права; 2) обязательственные права; 3) интеллектуальные достижения; 4) нематериальная собственность; 5) двойные атрибуты вещных и обязательственных прав (中国法学界对虚拟财产的法律属性仍然存在巨大的分歧，主要包括五种观点，分别是：物权说；债权说；智力成果说；无形财产说；物权债权双重属性说。).

[8] 参见广东省深圳市南山区人民法院(2006)深南法刑初字第56号刑事判决书。 [Приговор Народного суда района Наньшань г. Шэньчжэнь провинции Гуандун по уголовному делу № 56/2006]. Дата обращения 20 апреля, 2022. https://wenshu.lawtime.cn/pjxscpwsyishen/20110726104165.html.

(ст. 264)[9] или как незаконное приобретение данных компьютерных информационных систем (ч. 2 ст. 285)[10].

Вместе с тем на практике встречались случаи, когда аналогичное деяние рассматривалось как нарушение компьютерных информационных систем (ст. 286) или незаконное вторжение в компьютерные информационные системы (ч. 1 ст. 285). На самом деле рассматриваемая ситуация не ограничивается традиционными виртуальными активами, такими как игровые монеты, Q coin[11]. В судебной практике также существуют разные мнения о понимании виртуальных валют нового поколения, таких как биткоин. Например, в отношении одного и того же незаконного приобретения биткоинов содеянное квалифицировалось в качестве незаконного приобретения данных компьютерных информационных систем, как незаконное управление компьютерными информационными системами (ч. 2 ст. 285)[12] либо как кража (ст. 264). Полагаем, что различная квалификация одного и того же типа поведения коренится в различном понимании юридических атрибутов виртуальной онлайн-собственности (например, игровые монеты, Q coin и т. п.).

Что касается расширительного толкования существующих составов преступлений, то «киберизация» преступности приводит к появлению ряда нового типа общественно опасных деяний, и это вызывает споры и путаницу в применении уголовного закона, тем более что некоторые из этих новых деяний не относятся ни к одному из составов преступлений, предусмотренных УК КНР. Чтобы регулировать такие деяния, судебные органы часто расширяют сферу применения существующих составов преступлений. Например, при пролистывании онлайн-заказов лица используют фиктивные онлайн-транзакции для улучшения репутации онлайн-продавцов, чтобы привлечь других людей к покупке товаров. В приговоре, вынесенном судом района Юйхан города Ханчжоу провинции Чжэцзян, подобное поведение было квалифицировано как незаконное предпринимательство (ст. 225 УК КНР) (Фан 2017). Однако некоторые ученые отметили, что в действующем УК КНР нет уголовно-правовых норм, применимых к рассматриваемому деянию (Чжан 2014, 12), здесь неуместно применять и «карманную» норму п. 1 ст. 225 УК КНР («а также с *иными предметами*, в отношении торговли которыми имеются ограничения»). Их доводы заключаются в том, что рассматриваемые деяния не относятся к видам правонарушений, запрещенных Законом КНР о борьбе с недобро-

[9] 《上海市黄浦区人民检察院诉孟动、何立康网络盗窃案》，载《最高人民法院公报》(2006)年第0011期，第33–40页. [Народная прокуратура района Хуанпу г. Шанхая выдвинула против Мэн Дуна, Хэ Ликана обвинение в киберкраже. *Бюллетень Верховного народного суда* 11: 33–40].

[10] 参见江苏省宿迁市中级人民法院(2014)宿中刑终字第0055号刑事判决书。[Приговор Промежуточного народного суда г. Суцянь провинции Цзянсу по уголовному делу № 0055/2014]. Дата обращения 20 апреля, 2022. https://cases.pkulaw.com/home.

[11] Q coin (именуемый QB) обычно конвертируется в 1Q coin = 1 юань. QB — это виртуальная валюта, запущенная Tencent, которую можно использовать для оплаты номеров QQ, услуг членства в QQ и других услуг. Tencent Q coin можно преобрести посредством покупки карты QQ, пополнения счета телефона, пополнения счета банковской карты, пополнения счета сети, карты пополнения счета мобильного телефона, карты пополнения всех карт и других способов получения. Номинальная стоимость карты QQ составляет 10, 15, 30, 60, 100 или 200 юаней. См. подробнее: Q币一种虚拟货币[Q coin — виртуальная валюта]. Дата обращения 11 июля, 2022. https://baike.baidu.com/item/Q%E5%B8%81/754182?fr=aladdin.

[12] 参见上海市普陀区人民法院(2014)普刑初字第1162号刑事判决书。[Приговор Народного суда района Путуо г. Шанхая по уголовному делу № 1162/2014]. Дата обращения 20 апреля, 2022. https://zhuanlan.zhihu.com/p/134062582.

совестной конкуренцией[13], и даже при подаче заявления соответствующий орган не имеет права выдать лицензию на ведение бизнеса, поэтому вообще не существует «лицензии на незаконное ведение бизнеса» (Чэнь 2017, 15; Чжоу 2019, 961) и аналогичные деяния не образуют незаконного предпринимательства, предусмотренного ст. 225 УК КНР[14].

Кроме того, существуют иные деяния, такие как платное удаление сообщений, массовая вредоносная регистрация торговых веб-сайтов и т. д., которые квалифицируются и наказываются в судебной практике Китая путем расширения существующих составов преступлений (Гао 2016), т. е. такие действия признаются незаконным предпринимательством (ст. 225 УК КНР). Тем не менее высказывается все больше мнений о том, что признание аналогичного поведения незаконным предпринимательством относится к толкованию по аналогии (Чжан 2016, 1066–1067; Оян 2017, 167, 170), что противоречит принципу законности уголовного права.

В-третьих, остается актуальной дилемма квалификации соучастия в преступлениях, совершенных в киберпространстве. Явление соучастия в преступлении в киберпространстве более сложное: существует соучастие в преступлении, перенесенное с традиционного физического пространства в киберпространство, а также соучастие в преступлении, сильно отличающееся от традиционных преступных форм из-за тесной интеграции информационных и сетевых технологий. Новый облик и характеристики соучастия в преступлении в киберпространстве проявляются в нескольких аспектах.

Первый из этих аспектов — наличие нетипичного характера субъективной связи между лицами. В киберпространстве формы и способы субъективной связи между субъектами нетипичны для субъективной связи традиционного соучастия в преступлении и даже претерпевают существенные изменения. Такие случаи довольно распространены в интернете. Например, если оператор онлайн-платформы, зная, что деяние лица, продающего запрещенные товары на предоставленной им онлайн-торговой платформе, образует преступление, допускает указанное поведение, то это может быть признано соучастием. В соответствии с п. 15 Замечаний по некоторым вопросам о применении законодательства при рассмотрении уголовных дел о нарушении прав интеллектуальной собственности, совместно опубликованным Верховным народным судом, Верховной народной прокуратурой, Министерством общественной безопасности и Министерством юстиции в 2011 г., «те, кто представляет другим лицам, *заведомо* совершающим преступления против прав интеллектуальной собственности, основное сырье для производства или изготовления контрафактной продукции… или предоставляет такие услуги, как до-

[13] Закон КНР о борьбе с недобросовестной конкуренцией принят 02.09.1993 на Третьем заседании Постоянного комитета Восьмого Всекитайского собрания народных представителей, пересмотрен 04.11.2017 на 30-м заседании Постоянного комитета 12-го Всекитайского собрания народных представителей (《反不正当竞争法》: 1993年9月2日第八届全国人民代表大会常务委员会第三次会议通过; 2017年11月4日第十二届全国人民代表大会常务委员会第三十次会议修订。). Дата обращения 8 ноября, 2021. http://www.npc.gov.cn/npc/c30834/201905/9a37c6ff150c4be6a549d526fd586122.shtml.

[14] Согласно ст. 225 УК КНР, «занятие одним из нижеперечисленных видов незаконной хозяйственной деятельности, дестабилизирующих рынок, при отягчающих обстоятельствах — наказывается <...>: 1) безлицензионная хозяйственная деятельность, связанная с товарами, в отношении которых законом и административными законоположениями установлена монополия, а также с иными товарами, в отношении торговли которыми имеются ограничения...».

ступ в интернет, хостинг серверов, сетевое хранилище, каналы связи и передачи, взимание сборов, расчеты и т. д., должны быть квалифицированы и наказаны как соучастники преступления в нарушении прав интеллектуальной собственности» (Пан и др. 2011).

«Заведомость» в приведенных выше положениях включает три различные ситуации: 1) наличие сговора с другими лицами для оказания помощи в совершении преступных деяний; 2) между лицом, оказывающим помощь, и исполнителем отсутствует сговор, но, зная, что конкретный исполнитель собирается совершать определенное преступное деяние, такое лицо предоставляет ему онлайн-поддержку и помощь; 3) поставщики онлайн-помощи не знают о виновнике и типе поведения преступных деяний, а также нет сговора с исполнителем преступных деяний, однако оказывается объективная помощь деянию виновника.

Второй аспект — размывание границ между пособничеством и исполнительством. В традиционном физическом пространстве нетрудно провести различие, но в киберпространстве, поскольку форма взаимодействия между лицами отличается от традиционного пространства, возникло явление размытых и неразличимых границ. Например, в сфере уголовного права остается весьма спорным вопрос о том, что деяние, нарушившее авторские права других лиц путем обеспечения глубоких нейронных сетей, по своей природе рассматривается как исполнительство в виде копирования, распространения работ других лиц либо как пособничество в виде оказания помощи другим лицам в нарушении авторских прав других лиц (Сунь 2015; Юй 2010a; Юй 2010b).

Третий аспект — утверждение теории односторонней субъективной связи. В случае если совместно совершаемое преступное деяние признается соучастием в преступлении, то и традиционные господствующие взгляды на соучастие в преступлении, и регламентация ч. 1 ст. 25 УК КНР[15] являются непреодолимыми препятствиями. Из общей позиции уголовного права, согласно которой между соучастниками преступления должна существовать субъективная связь, вытекает отрицание соучастия в преступлении с односторонней субъективной связью, поэтому может образоваться пробел (Чэнь 2015, 44). Ситуация вызвана объективным существованием одностороннего пособничества и подстрекательства и стала потенциальной опасностью в киберпространстве, угрожающей онлайн-порядку. Поэтому некоторые ученые полагают, что «субъективная связь в соучастии в преступлении включает не только двустороннюю, но и одностороннюю связь» (Пи 2004, 22).

В последние годы отдельные китайские ученые пытались расширить рамки соучастия в преступлении путем переосмысления положения ч. 1 ст. 25 УК КНР, с тем чтобы найти правовые и теоретические основания для наказания деяния с односторонней субъективной связью. По их мнению, «согласно ч. 1 ст. 25 УК КНР соучастием в преступлении признается совместное умышленное преступление, совершенное двумя и более лицами. Здесь “совместное” умышленное преступление не означает, что только при наличии совершенно одинакового содержания по умыслу и способу поведения содеянное образует соучастие в преступлении, поскольку поведение разных лиц, совершенное отчасти совместно, также признается “совместным” деянием» (Чжоу 2011, 209). Иными словами, соучастие в преступлении отно-

[15] Согласно ч. 1 ст. 25 УК КНР соучастием в преступлении признается «совместное умышленное соучастие в преступлении двух и более лиц».

сится не к преступлению, совершенному двумя и более лицами, а к умышленному преступлению (Чжан 2011, 349). Поэтому даже если между исполнителем и пособником, подстрекателем умышленного преступления отсутствует общая субъективная связь, это не повлияет на «совместность» совершенного деяния, что означает возможность существования односторонней субъективной связи.

3. Выводы

С развитием и изменением информационных технологий и компьютерных сетей киберпреступность приобрела новые характеристики и формы. В глобальном контексте, выходя за рамки географических и национальных границ, киберпреступность приводит к нарушению более широкого спектра защищаемых благ. С учетом особых атрибутов, присущих сети, информационные сети в различных видах преступлений выполняют разные роли в качестве предмета преступления, инструмента преступления или места совершения преступления — киберпространства. В условиях непрерывной эволюции форм киберпреступности многие страны продолжают изучать ее закономерности развития и эффективные меры для борьбы с ней. Когда традиционная теоретическая модель уголовного права сталкивается с этой новой проблемой, необходимо скорректировать или даже пересмотреть теорию, чтобы обеспечить надежную поддержку действующим правовым нормам и их судебному применению. Уголовное законодательство Китая в сфере борьбы с киберпреступностью пересматривалось несколько раз, но все еще существуют проблемы, которые необходимо решать, совершенствуя его.

Библиография

高艳东：《破坏生产经营罪包括妨害业务行为—批量恶意注册账号的处理》，载《预防青少年犯罪研究》2016年第2期，第14–24页。[Гао, Яньдун. 2016. «Состав преступления «незаконное предпринимательство» включает деяния, препятствующие ведению бизнеса, — квалификация деяний, связанных с массовой вредоносной регистрации онлайн-аккаунтов». *Исследование профилактики преступности несовершеннолетних* 2: 14–24].

逄锦温、刘福谦、王志广、丛媛：《关于办理侵犯知识产权刑事案件适用法律若干问题的意见》的理解与适用，载《人民检察》2011年第9期，第58–63页。[Пан, Цзиньвэнь, Лю Фуцянь, Ван Чжигуан, Цун Юань. 2011. «Понимание и применение "Замечаний по некоторым вопросам о применении законодательства при рассмотрении уголовных дел о нарушении прав интеллектуальной собственности"». *Народная прокуратура* 9: 58–63].

欧阳本祺：《论网络时代刑法解释的限度》，载《中国法学》2017年第3期，第164–183页。[Оян, Бенци. 2017. «Пределы толкования уголовного права в эпоху интернета». Китайское право 3: 164–183].

皮勇：《论网络"聚众"性犯罪及其刑事立法》，载《人民检察》2004年第2期，第20–22页。[Пи, Юн. 2004. «Уголовное законодательство в отношении киберпреступлений, совершаемых "группой"». *Народная прокуратура* 2: 20–22].

皮勇:《我国网络犯罪刑法立法研究》，载《河北法学》2009年第6期，第49–57页。[Пи, Юн. 2009. «Исследование уголовного законодательства о киберпреступности в нашей стране». *Хэбэйское право* 6: 49–57].

理查德·斯皮内洛：《铁笼，还是乌托邦—网络空间的道德与法律》，李伦译。北京：北京大学出版社，2007年版：导言。[Спинелло, Ричард. 2007. *Железная клетка или утопия — этика и закон в киберпространстве.* Пекин: Издательство Пекинского университета].

孙万怀：《慎终如始的民刑推演—网络服务提供行为的传播性质》，载《政法论丛》2015年第1期，第96–112页 [Сунь, Ваньхуай. 2015. «Вопросы о применении гражданского или уголовного

законодательства — характер распространения предоставления онлайн-услуг». *Библиотека политики и права* 1: 96–112].
许秀中：《网络犯罪概念及类型研究》，载《江淮论坛》，2002年第6期，第29-35页。[Сюй, Сючжун. 2002. *Исследование понятия и видов киберпреступности*. Форум Цзянхуай 6: 29–35].
徐剑锋：《互联网时代刑法参与观的基本思考》，载《法律科学》，2017年第3期，第115–122页。[Сюй, Цзяньфэн. 2017. «Основное мышление о концепции участия уголовного права в эпоху интернета». *Юридическая наука* 3: 115–122].
徐翕明：《网络时代刑事立法：理念转型与规范调整》，载《新疆大学学报》，2020年第1期，第31–38页。[Сюй, Шимин. 2020. «Уголовное законодательство в эпоху интернета: концептуальная трансформация и нормативное регулирование». *Журнал Синьцзянского университета* 1: 31–38].
涂龙科：网络时代经济刑法变革的系统阐释，载《法学评论》， 2019年第6期，第125–134页。[Ту, Лунке. 2019. «Систематическое толкование экономического уголовного права в эпоху интернета». *Правовые комментарии* 6: 125–134].
范跃红：《全国首例组织刷单炒信刑事案件宣判》，载《检察日报》2017年。[Фан, Юэхун. 2017. «Вынесение приговора по первому уголовному делу о пролистывании онлайн-заказов». *Прокурорская ежедневная газета.* Дата обращения 20 апреля, 2022. https://www.spp.gov.cn/spp/zdgz/201706/t20170621_193604.shtml].
黄太云:《＜刑法修正案(七)＞解读》，载《人民检察》2009年第6期，第5–21页。[Хуан, Тайюнь. 2009. «Разъяснение Поправок № 7 к УК КНР». *Народная прокуратура* 6: 5–21].
黄太云:《刑法修正案解读全编—根据＜刑法修正案(九)＞全新阐释》，北京：人民法院出版社2015年版。[Хуан, Тайюнь. 2015. *Сборник разъяснений Поправок к УК КНР — новое толкование, основанное на Поправках № 9 к УК КНР.* Пекин: Издательство Народного суда].
何荣功:《预防刑法的扩张及其限度》，载《法学研究》2017年第4期，第138–154页。[Хэ, Жунгун. 2017. «Расширение превентивного уголовного права и его пределы». *Прововое исследование* 4: 138–154].
臧铁伟主编:《中华人民共和国刑法修正案(九)解读》，中国法制出版社2015年版。[Цан, Тевэй. 2015. *Разъяснение к Поправкам № 9 к УК КНР.* Издательство Китайской законности].
张明楷：《刑法学》，北京：法律出版社2011年版。[Чжан, Минкай. 2011. *Уголовное право.* Пекин: Юридическое издательство].
张明楷：《网络时代的刑法理念》，载《人民检察》2014年第5期，第6–12页。[Чжан, Минкай. 2014. «Концепция уголовного права в эпоху интернета». *Народная прокуратура* 5: 6–12].
张明楷:《刑法学》，法律出版社2016年版第 [Чжан, Минкай. 2016. *Уголовное право.* Пекин: Юридическое издательство].
张楚：《网络法学》，北京：高等教育出版社，2003年版。[Чжан, Чу. 2003. *Интернет-право.* Пекин: Издательство высшего образования].
赵秉志，于志刚：《论计算机犯罪的定义》，载《现代法学》，1998年第5期，第7–10页。[Чжао, Бинчжин, Чжиган Юй. 1998. «Определение понятия компьютерной преступности». *Современное право* 5: 7–10].
周光权：《刑法总论》（第 2 版），北京：中国人民大学出版社2011年版。[Чжоу, Гуанцюнь. 2011. *Уголовное право. Общая часть.* 2-е изд. Пекин: Издательство Китайского народного университета].
周光权：《刑法软性解释的限制与增设妨害业务罪》，载《中外法学》2019年第4期，第951–966页。[Чжоу, Гуанцюань. 2019. «Ограничения на мягкое толкование уголовного законодательства и добавление состава преступления «Препятствие ведению бизнеса». *Китайское и зарубежное право* 4: 951–966].
程燕：《网络犯罪防治中大数据安全管理对策研究》，载《犯罪研究》2019年第5期，第33–38页。[Чэн, Янь. 2019. «Исследование контрмер для обеспечения безопасности больших данных в предотвращении киберпреступности». *Исследование преступности* 5: 33–38].
陈兴良：《刑法阶层理论：三阶层与四要件的对比性考察》，载《清华法学》2017年第5期，第6–19页 [Чэнь, Синлян. 2017. «Теория слойной структуры в уголовном праве: сравнительное исследование трехслойной и четырехчленной структуры состава преступления». *Чинхуаское право* 5: 6–19].

陈洪兵：《“二人以上共同故意犯罪”的再解释—全面检讨关于共同犯罪成立条件之通说》，载《当代法学》2015年第4期，第32–44页。[Чэнь, Хунбин. 2015. «Новое толкование “совместного умышленного преступления, совершенного двумя и более лицами” — всесторонний обзор общего учения об условиях для установления соучастия в преступлении». *Современное право* 4: 32–44].

商西：《网络犯罪成我国第一大犯罪类型》，载《南方都市报》2016 年A08 版。[Шан, Си. 2016. «Киберпреступность стала видом преступности номер один в нашей стране». *Южная городская газета* A08]. Дата обращения 20 апреля, 2022. http://www.chinapeace.gov.cn/chinapeace/c54224/2016-10/15/content_11813443.shtml.

于志刚：《虚拟空间中的刑法理论》，北京：中国方正出版社，2003年版。[Юй, Чжиган. 2003. *Теория уголовного права в виртуальном пространстве*. Пекин: Китайское издательство Фанчжэн].

于志刚：《网络犯罪与中国刑法应对》，载《中国社会科学》2010年第3期，第109–126页。[Юй, Чжиган. 2010a. «Киберпреступность и ответные меры уголовного законодательства Китая». *Китайская общественная наука* 3: 109–126].

于志刚：《搜索引擎恶意链接行为的刑法评价》，载《人民检察》2010年第12期，第6–10页。[Юй, Чжиган. 2010b. «Уголовно-правовая оценка поведения вредоносных ссылок в поисковых системах». *Народная прокуратура* 12: 6–10].

于志刚：《网络思维的演变与网络犯罪的制裁思路》，载《中外法学》，2014年第4期，第1045–1058页。[Юй, Чжиган. 2014. «Эволюция сетевого мышления и мысли о санкциях за киберпреступность». *Китайское и зарубежное право* 4: 1045–1058].

杨春洗、秦秀春：《刑法上计算机犯罪概念之提出》，载《法学论坛》2000年第3期，第57–63页。[Ян, Чуньси, Сючунь Цинь. 2000. «Определение понятия компьютерной преступности в уголовном праве». *Правовой форум* 3: 57–63].

Статья поступила в редакцию 13 декабря 2021 г.;
рекомендована к печати 27 мая 2022 г.

Контактная информация:

Ван Гуанлун — науч. сотр.; guanglong95@163.com

Criminal law regulation of countering cybercrime in China: State, trends and shortcomings*

Wang Guanglong

Henan University,
85, Minglun Street, Kaifong, 475001, People's Republic of China

For citation: Wang Guanglong. 2022. “Criminal law regulation of countering cybercrime in China: State, trends and shortcomings”. *Vestnik of Saint Petersburg University. Law* 3: 661–677. https://doi.org/10.21638/spbu14.2022.305 (In Russian)

In modern China, cybercrime is becoming more widespread, which has given rise to the need to rethink criminal law at the basic theoretical level. It seems that when countering crimes in cyberspace, it is necessary to shift the focus of cyber-criminal law from the traditional “network-centric” to “data-oriented” and to build a system for the protecting legal benefits of “data centralism”. In addition, the expansion of the objective components of cybercrime should be moderate: certain cyber-violations cannot be qualified as “illegal entrepreneurship”, as this contradicts the principle of legality of criminal law. The content of “knowingness” as a sign of the subjective side of the crime should be rethought: it should include such different

* This article was prepared as part of the China Scholarship Council (CSC) (No. 202110100004).

forms as: a) the presence of collusion with other persons to assist in the commission of criminal acts; b) lack of collusion between the person providing assistance and the perpetrator, but the previous one, knowing that a particular perpetrator he is going to commit a certain criminal act, provides online support and assistance to the latter; c) online help providers who only have a probable idea of the existence of criminal acts, but do not have a clear idea of the culprit and the type of behavior of criminal acts, and as such there can be no collusion with the perpetrator of criminal acts, only objectively assists the culprit's act. The theoretical basis for identifying complicity in cybercrime should be adjusted by approving "one-sided" subjective connection. Ultimately, through systematic adjustment and rethinking of the basic theory of criminal law in this area, the gradual improvement of criminal law norms to regulate the fight against cybercrime in the era of information networks is being carried out.

Keywords: cyber criminal law, cybercrime, cyberspace, knowingness; complicity in cybercrime, one-sided accomplice.

References

Chen, Hongbing. 2015. "A new interpretation of the 'joint intentional crime committed by two or more persons' — A comprehensive review of the general teaching on the conditions for establishing complicity in a crime". *Dangdai Faxue* 4: 32–44. (In Chinese)

Chen, Xingliang. 2017. "The theory of the layered structure in criminal law: a comparative study of the three-layered and four-membered structure of the corpus delicti". *Qinghua Faxue* 5: 6–19. (In Chinese)

Cheng, Yan. 2019. "Research of countermeasures to ensure the security of big data in the prevention of cybercrime". *Fanzui Yanjiu* 5: 33–38. (In Chinese)

Fan, Yuehong. 2017. "Sentencing in the first criminal case of flipping through online orders". *Jiancha Ribao.* Accessed April 20, 2022. https://www.spp.gov.cn/spp/zdgz/201706/t20170621_193604.shtml. (In Chinese)

Gao, Yandong. 2016. "The composition of the crime of Illegal entrepreneurship includes acts that hinder the conduct of business — the qualification of acts related to the mass malicious registration of online accounts". *Yufang Qingshaonianfanzui Yanjiu* 2: 14–24. (In Chinese)

He, Ronggong. 2017. "Expansion of preventive criminal law and its limits". *Faxue Yanjiu* 4: 138–154. (In Chinese)

Huang, Taiyun. 2009. "Explanation of Amendments No. 7 to the Criminal Code of the People's Republic of China". *Renmin Jiancha* 6: 5–21. (In Chinese)

Huang, Taiyun. 2015. *Collection of clarifications of amendments to the Criminal Code of the People's Republic of China — A new interpretation based on Amendments No. 9 to the Criminal Code of the People's Republic of China.* Beijing, Rénmín fǎyuàn chūbǎn shè Publ. (In Chinese)

Pang, Jinwen, Liu Fuqian, Wang Zhiguang, Cong Yuan. 2011. "Understanding and application of 'Comments on some issues on the application of legislation in the consideration of criminal cases of violation of intellectual property rights'". *Renmin Jiancha* 9: 58–63. (In Chinese)

Ouyang, Benqi. 2017. "Limits of interpretation of criminal law in the Internet age". *Zhongguo Faxue* 3: 164–183. (In Chinese)

Pi, Yong. 2004. "Criminal legislation regarding cyber crimes committed by a 'group'". *Renmin Jiancha* 2: 20–22. (In Chinese)

Pi, Yong. 2009. "Investigation of criminal legislation on cybercrime in our country". *Hebei Faxue* 6: 49–57. (In Chinese)

Shang, Xi. 2016. "Cybercrime has become the number one type of crime in our country". *Nanfang Dushibao* A08. Accessed April 20, 2022. http://www.chinapeace.gov.cn/chinapeace/c54224/2016-10/15/content_11813443.shtml. (In Chinese)

Spinello, Richard. 2007. *The iron cage, or Utopia-morality and law in cyberspace.* Chinese Ed. Beijing, Běijīng dàxué chūbǎn shè Publ. (In Chinese)

Sun, Wanhuai. 2015. "Questions about the application of civil or criminal legislation — The nature of the distribution of online services". *Zhengfa Luncong* 1: 96–112. (In Chinese)

Tu, Longke. 2019. "Systematic interpretation of economic criminal law in the Internet age". *Faxue Pinglun* 6: 125–134. (In Chinese)
Xu, Jianfeng. 2017. "Basic thinking about the concept of criminal law participation in the Internet age". *Falu Kexue* 3: 115–122. (In Chinese)
Xu, Shiming. 2020. "Criminal legislation in the Internet age: Conceptual transformation and regulatory regulation". *Xinjiangdaxue Xuebao* 1: 31–38. (In Chinese)
Xu, Xiuzhong. 2002. "Research of the concept and types of cybercrime". *Jianghuai Luntan* 6: 29–35. (In Chinese)
Yang, Chunxi, Qin Xiuchun. 2000. "Definition of the concept of computer crime in criminal law". *Faxue Luntan* 3: 57–63. (In Chinese)
Yu, Zhigang. 2003. *Theory of criminal law in the virtual space.* Beijing: Fangzheng Publ. (In Chinese)
Yu, Zhigang. 2010a. "Cybercrime and China's Criminal Law response". *Zhongguo Shehuikexue* 3: 109–126. (In Chinese)
Yu, Zhigang. 2010b. "Criminal legal assessment of the behavior of malicious links in search engines". *Renmin Jiancha* 12: 6–10. (In Chinese)
Yu, Zhigang. 2014. "The evolution of network thinking and the thought of sanctions for cybercrime". *Zhongwan Faxue* 4: 1045–1058. (In Chinese)
Zang, Tiewei. 2015. *Explanation of Amendments No. 9 to the Criminal Code of the People's Republic of China*. Beijing, Zhōngguó fǎzhì chūbǎn shè Publ. (In Chinese)
Zhang, Chu. 2003. *Internet law.* Beijing, Gāoděng jiàoyù chūbǎn shè Publ. (In Chinese)
Zhang, Mingkai. 2011. *Criminal law*. Beijing, Fǎlǜ chūbǎn shè Publ. (In Chinese)
Zhang, Mingkai. 2014. "The concept of criminal law in the Internet age". *Renmin Jiancha* 5: 6–12. (In Chinese)
Zhang, Mingkai. 2016. *Criminal law*. Beijing, Fǎlǜ chūbǎn shè Publ. (In Chinese)
Zhao, Bingzhi, Yu Zhigang. 1998. "Definition of the concept of computer crime". *Xiandai Faxue* 5: 7–10. (In Chinese)
Zhou, Guangquan. 2011. *Criminal law. The general part.* 2nd ed. Beijing, Zhōngguó rénmín dàxué chūbǎn shè Publ. (In Chinese)
Zhou, Guangquan. 2019. "Restrictions on the soft interpretation of criminal legislation and the addition of the corpus delicti 'Obstruction of business'". *Zhongwai Faxue* 4: 951–966. (In Chinese)

Received: December 13, 2021
Accepted: May 27, 2022

Author's information:

Wang Guanglong — Research Fellow; guanglong95@163.com