Научная статья
УДК 343
DOI 10.17150/2500-4255.2022.16(1).122-134

УГОЛОВНО-ПРАВОВАЯ ЗАЩИТА ПЕРСОНАЛЬНОЙ ИНФОРМАЦИИ ГРАЖДАН В КИТАЕ: ДОКТРИНА, ЗАКОНОДАТЕЛЬНАЯ РЕГЛАМЕНТАЦИЯ, ПРАВОПРИМЕНЕНИЕ*

Пан Дунмэй[1], Фу Сянсян[2]
[1] Китайско-российский центр сравнительного правоведения Хэнаньского университета, г. Кайфун, Китай
[2] Институт по борьбе с преступностью и уголовной политике Хэнаньского университета, г. Кайфун, Китай

Информация о статье

Дата поступления
20 ноября 2021 г.

Дата принятия в печать
18 февраля 2022 г.

Дата онлайн-размещения
11 марта 2022 г.

Ключевые слова

Персональная информация граждан; уголовно-правовая защита; Уголовный кодекс Китая; эпоха цифровизации

Аннотация. В эпоху цифровизации китайское общество подвержено влиянию информационных технологий, так что сбор и анализ информации больше не являются случайными и непредсказуемыми процессами. Оцифрованная персональная информация граждан представляет огромный интерес, поэтому необходимо разобраться с взаимосвязью между современным социальным развитием и борьбой с преступлениями в сфере обращения персональной информации граждан. В данной статье представлен анализ норм китайского уголовного законодательства, регламентирующих уголовную ответственность за посягательства на охраняемую законом персональную информацию в Китае. Указанный анализ проводился с точки зрения доктрины уголовного права, уголовного законодательства и правоприменительной практики. В статье доктрина представлена разными подходами к пониманию природы персональной информации граждан, существующими в Китае, также обосновывается необходимость разработки концепции информационного уголовного права и построения иерархической системы уголовно-правовой защиты. С позиции законодательной регламентации, в действующем Уголовном кодексе КНР рассматриваемые посягательства включают в себя лишь три вида действия: незаконное приобретение, продажу и предоставление персональной информации. В то же время отсутствует норма по регулированию незаконного ее использования, которое на самом деле представляет собой общественно опасное деяние. Авторами обосновывается необходимость криминализации незаконного использования персональной информации граждан с целью выстраивания стратегии по ее уголовно-правовой защите. Что касается применения состава «Нарушения в сфере персональной информации граждан» (ст. 253.1 УК КНР), недостаточная аргументация и неполное установление обстоятельств посягательства нередко приводят к расхождениям в квалификации и назначении наказания по однотипным уголовным делам. Авторами указывается, что для преодоления возникающих проблем нужно четко определить элементы объективной стороны данного преступления. Предлагаются пути решения проблем правоприменительной практики, возникающих при квалификации посягательств на персональную информацию и определении наказания при постановке приговоров в суде.

Original article

CRIMINAL LAW PROTECTION OF PERSONAL INFORMATION OF CITIZENS IN CHINA: DOCTRINE, LEGISLATIVE REGULATION, ENFORCEMENT

Pan Dongmei[1], Fu Siansian[2]
[1] Chinese-Russian Center of Comparative Law, Henan University, Kaifeng, China
[2] Institute of Corruption Counteraction and Criminal Policy, Henan University, Kaifeng, China

Article info

Received
2021 November 20

Abstract. In the information era, the Chinese society lives under the influence of digital technologies, so the collection and analysis of information are no longer accidental and unpredictable. Digitalized private information poses a great interest, making it necessary to understand the interconnection between modern social development

* Русский текст представлен в научной редакции доктора юридических наук, профессора А.Л. Репецкой.
** The scientific editing of the Russian text was carried out by Doctor of Law, Professor A.L. Repetskaya.

ISSN 2500-4255

Accepted
2022 February 18
Available online
2022 March 11

Keywords

Personal information; criminal law protection; Criminal Code of China; era of digitization

and crime counteraction in the sphere of personal information of citizens. The authors analyze norms of the Chinese legislation that regulate criminal liability for infringements on personal information protected by the Chinese law. This analysis was conducted from the viewpoint of the doctrine of criminal law, criminal legislation and law enforcement practice. The doctrine is presented through different approaches to understanding the nature of personal information in China; the authors also show the necessity of developing a concept of information criminal law and building a hierarchical system of criminal law protection. In the sphere of legislative regulation, the analyzed infringements include only three types of actions in the current Criminal Code of the PRC: illegal purchase, sale and provision of personal information. At the same time, there is no norm regulating its illegal use which is, in fact, a publicly dangerous act. The authors show the necessity of criminalizing the use of personal information with the purpose of building a strategy of its criminal law protection. As for the enforcement of the norm «Violations in the sphere of personal information of citizens» (Art. 253.1 of the CC of the PRC), insufficient arguments and incomplete establishment of the circumstances of the infringement often result in differences in the qualification and sentencing for similar criminal cases. The authors show that, to overcome these problems, it is necessary to clearly determine the elements of the objective side of this crime. They present ways of solving the problems of law enforcement arising during the qualification of infringements on personal information and the determination of punishment when passing sentences in court.

Введение

Концепция BigData была впервые предложена В. Майером-Шенбергером. По его мнению, большие данные относятся к технологиям с функцией прогнозирования путем получения всех данных без использования сбора и анализа случайных выборок [1]. Использование BigData позволяет передавать персональную информацию граждан в киберпространстве. Такая информация, как правило, содержит сведения обо всех видах деятельности отдельных граждан, включая их личные, идентификационные и прочие данные. Персональная информация граждан, защищенная уголовным законом, должна обладать атрибутом правового блага в юридическом контексте. Это значит, что защита информации этого типа имеет не только уголовно-правовой характер, но и реальную срочность [2].

Лишь те деяния, которые действительно обладают общественной опасностью, могут быть регламентированы и наказуемы по уголовному закону [3, с. 6]. Защита персональной информации граждан китайским уголовным законодательством заключается главным образом в криминализации деяний, посягающих на данный объект, для достижения целей защиты прав граждан на личную и иную персональную информацию, наказания за посягательства на нее и поддержания общественного порядка. Пришла эра цифровизации (больших данных), и нам необходимо обратить внимание на проблему защиты персональной информации граждан средствами уголовного права.

Эволюция уголовно-правовой защиты личной информации граждан в Китае в эпоху цифровизации

В последние годы развитие сетевых информационных технологий Китая сделало систему цифровизации более совершенной. Однако время от времени происходят преступления, связанные с персональной информацией, что создает серьезную угрозу личной и имущественной безопасности граждан. Эффективная защита персональной информации граждан касается не только реализации прав членов общества, но и стратегической безопасности национальных данных и устойчивого прогресса социального порядка. Поэтому законодатели Китая продолжают искать эффективные пути уголовно-правовой защиты персональной информации граждан.

Так, в 2009 г. китайский законодатель впервые обратил внимание на сферу регулирования, связанную с персональной информацией граждан. В результате в Поправки к УК КНР № 7 включили новый состав преступления, регламентированный ст. 253.1 УК КНР, которая предусматривает уголовную ответственность за посягательства на персональную информацию граждан. В указанной статье содержались три части:

1. «Работники государственных органов или сотрудники финансовых, телекоммуникационных, транспортных, образовательных, медицинских учреждений и иных организаций, в нарушение государственных установлений продавшие либо незаконно предоставившие другим лицам информацию о личности граждан, полученную

ими в процессе исполнения своих обязанностей или в ходе оказания услуги, при наличии отягчающих обстоятельств наказываются лишением свободы на срок до трех лет либо арестом, либо дополнительно или в качестве самостоятельного наказания штрафом» (ч. 1).

2. «Кража или приобретение иным незаконным путем такой информации при наличии отягчающих обстоятельств наказываются в соответствии с первой частью настоящей статьи» (ч. 2).

3. «Если преступления, упомянутые в частях первой и второй настоящей статьи, совершены организацией, то по отношению к организации применяется штраф, а непосредственно ответственные руководители и другие ответственные лица наказываются в соответствии с положениями частей первой или второй настоящей статьи» (ч. 3).

Таким образом, ч. 1 ст. 253.1 УК КНР был установлен состав преступления «Продажа, незаконное предоставление персональной информации граждан»; ч. 2 — «Незаконное приобретение персональной информации граждан»; ч. 3 предусмотрена уголовная ответственность за преступления, совершенные юридическими лицами.

Поскольку законы и другие нормативные акты Китая, регламентирующие сферу оборота персональной информации граждан, были еще не совершенны, санкция ст. 253.1 УК КНР содержала относительно легкое наказание (максимальное наказание — лишение свободы на срок трех лет). Кроме того, в рассматриваемой статье были указаны только «специальные субъекты»[1] и ограничительные условия — «нарушение государственных установлений» для указанных преступлений.

В 2015 г. преступность в Китае приобрела новые характеристики: большое количество преступных деяний было совершено с использованием компьютеров и других электронных устройств, и преступления становились все более кибернетизированными. Вопрос уголовно-правовой защиты персональных данных граждан вновь вернулся в поле зрения законодателей Китая.

В результате Поправки к УК КНР № 9, направленные на решение актуальных проблем социальных преобразований, еще больше усилили защиту персональной информации граждан. Так, указанная статья стала называться «Нарушение персональной информации граждан». Данными поправками была расширена сфера субъектов преступлений, предусмотренных ч. 1 ст. 253.1, с изменением специального субъекта на общий субъект; действия, связанные с нарушением государственных установлений, указанные в предыдущей регламентации в ч. 1, были выделены в самостоятельный состав, образовавший ч. 2. Соответственно, если лица совершили обозначенное преступление в ходе выполнения своих обязанностей или при предоставлении услуг, то содеянное должно квалифицироваться по ч. 2 ст. 253.1 УК КНР, и за него назначается более строгое наказание. В результате статья стала состоять из четырех частей, а максимальная санкция теперь предусматривает наказание в виде лишения свободы сроком от трех до семи лет со штрафом. Ужесточение наказания произошло также в ч. 2 и 3.

Таким образом, ст. 253.1 действующего УК КНР гласит: «В нарушение государственных установлений продажа или предоставление персональной информации граждан при наличии отягчающих обстоятельств наказывается лишением свободы на срок до трех лет или арестом, либо дополнительно или в качестве самостоятельного наказания штрафом; при наличии особо отягчающих обстоятельств наказывается лишением свободы на срок от трех до семи лет со штрафом.

В нарушение государственных установлений продажа или предоставление другим лицам личной информации граждан, полученной в процессе исполнения обязанностей или в ходе оказания услуги, наказываются более строго в пределах санкции части первой настоящей статьи.

Кража или незаконное приобретение личной информации граждан наказываются в соответствии с частью первой настоящей статьи.

Если преступления, упомянутые в частях первой, второй или третьей настоящей статьи, совершены организацией, то по отношению к организации применяется штраф, а непосредственно ответственные руководители и другие непосредственно ответственные лица наказываются в соответствии с положениями частей первой, второй или третьей настоящей статьи».

[1] То есть субъектами преступлений настоящей статьи могут быть только работники государственных органов или сотрудники финансовых, телекоммуникационных, транспортных, образовательных, медицинских учреждений и иных организаций и соответствующие организации.

Кроме того, юридическое толкование может в определенной степени помочь преодолеть неоднозначность законодательной регламентации и направить судебную практику. В 2011 и 2017 гг. Верховный народный суд и Верховная народная прокуратура Китая совместно опубликовали два юридических разъяснения, связанных с защитой персональной информации граждан в контексте цифровизации данных: «Разъяснения по вопросам, касающимся применения Законов при рассмотрении уголовных дел, о преступлениях, угрожающих безопасности компьютерных информационных систем»[2] (далее — Разъяснения по рассмотрению компьютерных уголовных дел), и «Разъяснения по вопросам, касающимся применения законов при рассмотрении уголовных дел о нарушении персональной информации граждан»[3] (далее — Разъяснения по рассмотрению уголовных дел в сфере персональной информации граждан). Так, Разъяснения по рассмотрению компьютерных уголовных дел определяют концепцию получения информации для идентификации личности граждан с точки зрения защиты интересов их личной собственности, для обеспечения ее безопасности в финансовых онлайн-сервисах; Разъяснения по рассмотрению уголовных дел о персональной информации граждан, расширяя объем защиты персональной информации граждан, восполняют недостатки уголовного законодательства в этой области. Однако в уголовном законодательстве и судебной практике Китая все-таки существуют некоторые проблемы, касающиеся защиты информации данного вида.

Анализ проблем, связанных с уголовно-правовой защитой персональной информации граждан

Как известно, у всего есть две стороны. Технология больших данных принесла неизмеримые выгоды для управления, а также обслуживания всего общества, но в эпоху цифровизации существует множество рисков, связанных с использованием персональных данных и информации о гражданах.

Так, «Вечеринка 15 марта»[4] в Китае в 2021 г. выявила ряд случаев, касающихся нарушений в сфере использования персональной информации граждан. В частности, поступившие личные резюме соискателей использовались на платформах по набору персонала для работы на черном рынке[5]. Кроме того, были внедрены вредоносные программы (APP) для незаконного получения информации из мобильных телефонов пожилых людей с целью дальнейшего манипулирования ими с применением мошеннических схем[6]. Это привело к нарушению личных прав и интересов отдельных граждан и потере их имущественных прав.

Нынешняя ситуация с «утечкой» персональной информации граждан отражает недостатки ее уголовно-правовой защиты в Китае. Эти недостатки характеризуются несколькими аспектами.

1. В доктрине уголовного права по-разному понимается персональная информация. Принцип защиты правовых благ (Rechtsgutschutz) как одного из важных начал уголовного права заключается в защите интересов, которые признает уголовный закон: «Если целью уголовного закона не является защита правовых благ, то предусмотренные в нем составы преступлений являются незаконными или неконституционными» [4, с. 18].

Так как существует фактическое пересечение между правовыми благами, связанными с персональной информацией граждан, и содержанием прав других, связанных с ними закон-

[2] 最高人民法院网 [Верховный народный суд Китайской Народной Республики]. URL: http://www.court.gov.cn/fabu-xiangqing-3085.html.

[3] 最高人民检察院网 [Верховная народная прокуратура]. URL: https://www.spp.gov.cn/xwfbh/wsfbt/201705/t20170509_190088.shtml.

[4] «Вечеринка 15 марта» — это благотворительная вечеринка, организованная правительственными ведомствами и транслируемая в прямом эфире Центральным управлением радио и телевидения Китая с целью защиты прав и интересов потребителей вечером 15 марта каждого года.

[5] Например, подозреваемый в совершении такого преступления заплатил всего 7 юаней за резюме соискателей на онлайн-платформе по подбору персонала в онлайн-группе информационных транзакций. Резюме содержит имя заявителя, пол, возраст, фотографию, контактную информацию, опыт работы, образование и др. (Центральное телевидение Китая. URL: http://315.cctv.com).

[6] Некоторые малые программы (APP) для мобильных телефонов, которые якобы ими управляют, на самом деле помогают получить большой объем информации из памяти телефонов об их владельцах. Затем украденные данные, как правило у пожилых людей, которые «легко вводятся в заблуждение», используются для объединения их в группы. Через рекламные объявления им навязываются некачественные или несуществующие товары и услуги (Центральное телевидение Китая. URL: http://315.cctv.com).

ных интересов, при этом границы определения указанных благ и интересов размыты, возникают различия в их понимании. Если иные законные интересы охватывают сами правовые блага о персональных данных граждан, то нечеткое субъективное их понимание не будет способствовать правильному применению уголовного законодательства. Исходя из этого, первое, что нужно сделать, — это уточнить границы между различными благами и интересами. В основном здесь речь идет о границе между личной информацией граждан, персональными данными граждан и неприкосновенностью частной жизни. Что касается различия между личной информацией и персональными данными граждан, одни считают, что «личная информация — это четкая информация, которая может определить личность конкретного человека. Она более контролируема, чем персональные данные. Персональные данные — это информационная база данных, сформированная после компьютерного поиска личной информации» [5, с. 19]. Другие полагают, что эти два понятия в основном относятся к разным областям: «личная информация фокусируется в правовом поле, в то время как персональные данные находятся в технической области» [6]. Третьи утверждают, что эти два понятия согласуются: «Личная информация граждан и персональные данные граждан: первое — это содержание, а второе — форма» [7].

Обсуждение взаимосвязи между личной информацией граждан и их персональными данными показывает, что в эпоху цифровизации персональные данные стали представлением личной информации граждан, а последняя передается с использованием данных в качестве носителя, т.е. персональные данные граждан являются отображением их личной информации в киберпространстве. В результате были ослаблены идентифицируемые характеристики личной информации граждан, что снизило степень различия в правовых благах между личной информацией и персональными данными граждан, и они постепенно стали тождественными под влиянием BigData. Традиционный механизм согласия граждан на обработку их персональных данных не может эффективно справляться с юридическими рисками, с которыми сталкиваются персональные данные граждан. Особенности усвоения личной информации граждан, обрабатываемой с помощью больших данных, являются одним из ключевых моментов, на которые следует обратить внимание в современных исследованиях теории уголовно-правовой защиты в Китае.

Что касается правовой границы между правами граждан на личную информацию и на неприкосновенность частной жизни, то в Гражданском кодексе Китая параллельно закреплены права на неприкосновенность частной жизни и права на личную информацию граждан, а также в отношении личной тайной информации установлены правила применения норм, обеспечивающих неприкосновенность частной жизни. Данный факт в определенной степени создает иллюзию взаимосвязи между этими двумя видами прав. Это привело к тому, что граница между правами граждан на личную информацию и правами граждан на неприкосновенность частной жизни в субъективном понимании размывается. По мнению некоторых ученых, «личная информация граждан является объективной, то есть лишь те личные данные, которые могут помочь идентифицировать личность отдельного гражданина, входят в сферу регулирования уголовного закона, а неприкосновенность частной жизни характеризуется субъективной оценкой, и ее уголовно-правовая защита требует определенных субъективных суждений» [8]. Иными словами, уголовное законодательство Китая активно защищает личную информацию граждан, а в отношении неприкосновенности частной жизни рассматриваемая защита имеет пассивный характер. С углублением цифровизации общественной жизни восприятие людьми динамичных изменений значительно влияет на концепцию защиты правовых благ: возникает «противоречие между спросом и предложением» — между своевременным вмешательством уголовного правосудия и спросом на защиту средствами уголовного закона.

Определение правовых благ не только влияет на то, могут ли индивидуальные права граждан быть защищены уголовным законом, но также и на суждение об объекте отдельного преступления в уголовном законе. В УК КНР преступления, посягающие на персональную информацию граждан, находятся среди преступлений против личных прав граждан и демократических прав. Это показывает, что китайское законодательство рассматривает указанное преступление как преступление против личных прав, свобод и интересов отдельных граждан. Некоторые ученые отмечают, что «правовые блага, на которые посягают преступления, связанные с нарушениями в сфере персональной

информации граждан, заключаются в индивидуальных правах граждан, а не в общественном порядке или социальных интересах» [5]. Иными словами, по их мнению, правовые блага как объект указанного преступления являются лишь личными интересами граждан.

Другие ученые подчеркивают, что незаконное предоставление персональной информации нарушает «право граждан на самоопределение в правовых благах» в отношении их личной информации [9]. Основой такого самоопределения является право субъектов информации на информированное согласие [10]. Информированное согласие означает, что сторона, получающая информацию, обязана уведомить сторону, предоставляющую информацию, о том, что эта информация будет обработана, и получить согласие на ее сбор и обработку.

В эпоху цифровизации безопасность согласия граждан на обработку персональной информации была поставлена под сомнение, поскольку создается иллюзия осуществления личного права граждан на информированное согласие. В современном обществе согласие на обработку персональных данных в большей части случаев является необходимым условием социализации граждан, и некоторые лица, предоставляющие персональную информацию, недостаточно осведомлены о рисках, связанных с информационным обменом. Незаконное использование персональной информации граждан еще не криминализировано в Китае, поэтому для граждан возникают скрытые опасности в сфере защиты их личных данных.

2. Недостаточная регламентация УК КНР способов нарушения персональной информации граждан. Способы посягательств под влиянием цифровизации быстро совершенствуются, тем не менее в положениях УК КНР, касающихся персональной информации граждан, их регламентация не изменилась. Как уже указывалось, в настоящее время в УК КНР предусмотрены только три вида деяний, которые могут быть совершены либо в результате незаконного приобретения, либо продажи, либо незаконного предоставления персональных данных граждан. Между тем в действующем УК КНР не регламентировано незаконное использование персональной информации граждан, а в реальной жизни такие случаи часто происходят. Так, в качестве примеров, можно привести уголовное дело об изменении заявления на вступительный экзамен в вуз[7]; дело Ло Цайся (о присвоении имени)[8]; дело о самоубийстве врача из Дэяна[9]. Поскольку уголовное законодательство Китая еще не предусмотрело уголовную ответственность за незаконное использование личной информации граждан, упомянутые деяния либо были квалифицированы по иным составам преступлений, либо лица, допустившие такие действия, были оправданы. Следовательно, в уголовном законодательстве Китая существуют пробелы в плане привлечения к уголовной ответственности за совершение преступлений в сфере персональной информации граждан.

Деяния, связанные с незаконным использованием персональной информации граждан, постепенно стали распространенными, а отсутствие их регламентации в уголовно-правовых нормах не позволяет осуществлять уголовно-правовую защиту интересов пострадавших лиц. Если незаконное использование персональной информации граждан будет криминализировано, и за такой вид посягательства будет предусмотрена уголовная ответственность, то, соответственно, будет лучше осуществляться уголовно-правовая защита прав граждан [11]. Поскольку в настоящее время незаконное использование персональной информации граждан не криминализировано законодателем

[7] Чэнь Зоцзя, бывший ученик средней школы в уезде Шаньсянь провинции Шаньдун, взломал компьютерную систему и исправил заявления четырех одноклассников на вступительный экзамен в вуз. Суд обвинил его в преступлении «Взлом компьютерных информационных систем» (ст. 286). Однако реальными жертвами в этом деле были несколько абитуриентов вуза. Предметом преступления в этом случае была информация о заявлениях на вступительные экзамены в вуз, хранящаяся в компьютерной информационной системе (Дело о фальсификации вступительных экзаменов в колледж Шаньсянь // Новости Народного суда. URL: https://www.chinacourt.org/article/detail/2017/01/id/2509078.shtml).

[8] Ван Цзяцзюнь из провинции Хунань незаконно присвоил идентификационные данные одноклассника Ло Цайся и поступил в университет под вымышленным именем. Ван Цзяцзюнь не был привлечен к уголовной ответственности (CCTV. URL: http://news.cntv.cn/special/lanse/weiquan).

[9] Женщина-врач в Дэяне, провинция Сычуань, поссорилась с двумя гражданками во время купания. После того как ее обвинили в конфликте, обыскали и раскрыли ее личную информацию, она решила покончить с собой. Суд признал двух гражданок виновными в оскорблении (Инцидент самоубийства женщины-врача в Дэян // Baidu. URL: https://baike.baidu.com/item/8·25德阳女医生自杀事件/22842202?fr=aladdin).

Китая, деяния, посягающие на нее указанным способом, квалифицируются по другим составам преступлений. Так, судебные органы используют для квалификации подобных действий такие составы, как «Незаконное использование информационных сетей» (ст. 287.1 УК КНР), «Взлом компьютерных информационных систем» (ст. 286 УК КНР), «Оскорбление» (ст. 246 УК КНР) и др.

Данный подход в определенной степени косвенно позволяет осуществлять защиту прав и интересов граждан в области личной информации. Однако такие приговоры не являются эквивалентными совершенным деяниям, поскольку, во-первых, упомянутые составы преступлений предусмотрены в разных главах УК КНР, а значит, предусматривают посягательства на другой объект; во-вторых, эти составы с точки зрения законодательной цели не были установлены для защиты персональной информации граждан.

3. Другой причиной слабости уголовно-правовой защиты в указанной сфере являются недостатки при определении квалифицирующих обстоятельств. Примечание к ст. 13 УК КНР[10] разъясняет, что квалификация преступлений в Китае представляет собой сочетание качественного и количественного анализа, который влияет на окончательную оценку уголовного правосудия. Обстоятельства, содержащиеся в диспозиции ст. 253.1 УК КНР «Нарушение персональной информации граждан», подразделяются на два вида: отягчающие обстоятельства и особо отягчающие обстоятельства. Виновный, допустивший нарушение персональной информации граждан при наличии отягчающих обстоятельств, будет приговорен к лишению свободы на срок до трех лет или к аресту, или к штрафу; при наличии особо отягчающих обстоятельств ему будет назначено наказание в виде лишения свободы на срок от трех до семи лет со штрафом.

В судебном толковании, опубликованном совместно Верховным народным судом Китая и Верховной народной прокуратурой Китая, дополнительно уточняются упомянутые два вида обстоятельств в ст. 253.1 УК КНР. В частности, ст. 5 и 6 Разъяснений по рассмотрению уголовных дел о нарушениях персональной информации граждан были подробно установлены количественные критерии для определения отягчающих обстоятельств и особо отягчающих обстоятельств. Разъяснения разделяют указанные обстоятельства на несколько видов, таких как объем (тип) информации, размер незаконного дохода, функция информации, личности субъектов, степень вины [12].

В п. 3–5 ст. 5 Разъяснений по рассмотрению уголовных дел о нарушениях персональной информации граждан были установлены критерии для определения количества и типа информации, подвергшейся посягательству, размера незаконного дохода, которые позволяют разделять при квалификации основной и квалифицированные составы рассматриваемых преступлений. Согласно этим разъяснениям, по типу информация делится на несколько категорий. Кроме того, необходимо зафиксировать определенное число нарушений, касающихся информации конкретного типа.

Для первых четырех категорий информации (местонахождение конкретных граждан, содержание сообщений, кредитная отчетность, имущество), минимальным порогом для признания совершенных действий при отягчающих обстоятельствах является 50 нарушений. В отношении других категорий информации (записи с различных средств связи, здоровье и физиология, транзакции) требуется большее количество нарушений — не менее 500, или незаконный доход свыше 5 тыс. юаней, чтобы квалифицировать данное деяние как совершенное при отягчающих обстоятельствах. Если нарушений было не менее 5 тыс., то такие действия квалифицируются как совершенные при особо отягчающих обстоятельствах.

Такой дифференцированный подход позволяет квалифицировать рассматриваемые деяния в зависимости от количества нарушений, типа информации, на которую посягает виновный, и размера ущерба, причиняемого в результате этих посягательств. Если нарушений было меньше установленного разъяснениями количества, то действия виновного могут признать непреступными. Само же количество на-

[10] Статья 13 УК КНР гласит: «Все деяния, наносящие вред государственному суверенитету, территориальной целостности и безопасности государства, направленные на раскол государства, подрывающие власть народно-демократической диктатуры, свергающие социалистический строй, нарушающие общественный и экономический порядок, посягающие на государственную или коллективную собственность трудящихся масс, на личную собственность граждан, их личные, демократические и прочие права, а также другие наносящие вред обществу деяния, за которые в законе предусмотрено уголовное наказание, являются преступлениями. *Однако явно малозначительное деяние небольшой опасности не признается преступлением*» (оговорка — выделяется курсивом авторами).

рушений и размер ущерба влияют на назначение вида и размера наказания по конкретному уголовному делу.

Анализ статистических данных, проведенный авторами[11], показал, что за исследуемый период было вынесено 7 857 приговоров за преступления, связанные с персональной информацией граждан. Из общего количества преступлений 4 411 (56 %) были квалифицированы, как совершенные с отягчающими обстоятельствами, а 3 365 (42 %) — с особо отягчающими обстоятельствами (рис. 1). Таким образом, доля преступлений, имеющих высокую общественную опасность в сфере посягательств на персональные данные граждан, является значительной.

Структуру уголовных дел исследуемой категории можно разделить на преступления с однотипными обстоятельствами и преступления, совершенные с различными типами обстоятельств. Согласно проведенному анализу, доля уголовных дел, в которых присутствуют несколько типов обстоятельств при нарушении персональной информации граждан, составила 84 % (рис. 2). Как правило, в таких случаях

[11] Были изучены данные, опубликованные с 28 февраля 2009 г. (даты вступления в силу Поправок к УК КНР № 7) по 1 августа 2021 г., взятые из Сети судейских документов Китая (China Judgements Online). 中国裁判文书 [Сеть судейских документов Китая]. URL: https://wenshu.court.gov.cn.

Рис. 1. Структура приговоров по тяжести обстоятельств, вынесенных судами Китая в отношении преступлений в сфере персональной информации граждан за 2009–2021 гг., %

Fig. 1. Structure of sentences depending on aggravating circumstances imposed by Chinese courts for crimes in the sphere of personal information of citizens in 2009–2021, %

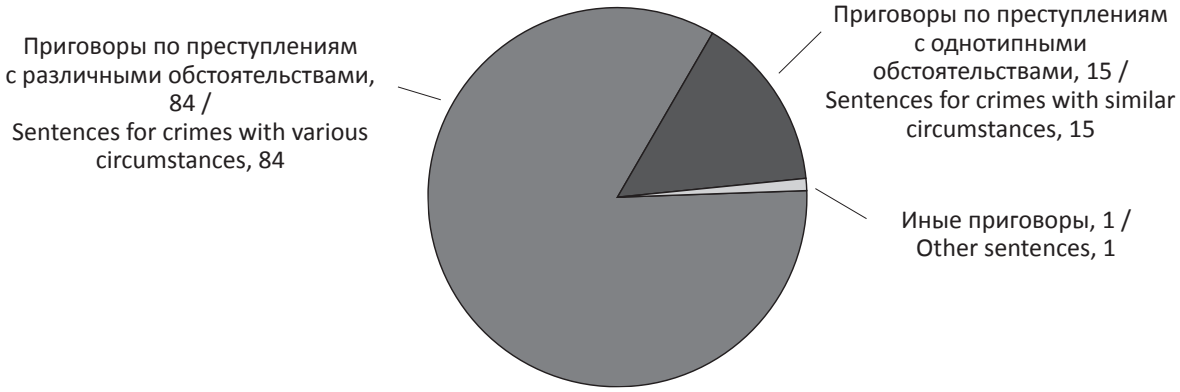

Рис. 2. Структура приговоров по типам обстоятельств, вынесенных судами Китая в отношении преступлений в сфере персональной информации граждан за 2009–2021 гг., %

Fig. 2. Structure of sentences depending on type of circumstances imposed by Chinese courts for crimes in the sphere of personal information of citizens in 2009–2021, %

китайским судебным органам необходимо при рассмотрении конкретных дел учитывать важность выявленных обстоятельств, чтобы выбрать наиболее значимые для вынесения приговора, либо комплексно определить значение различных обстоятельств в целях вынесения конечного решения.

В преступлениях с однотипными обстоятельствами количественный критерий нарушений в сфере персональной информации или размер незаконного дохода четко определен, так что судебные органы могут подробно обосновать решения по таким делам в судебных документах. Однако в судебной практике Китая все чаще встречаются преступления, посягающие на персональную информацию граждан, предметом которых выступают различные виды (типы) информации. В этих случаях не любой судья может путем комплексного анализа значимости определенных видов информации и количественных критериев ее нарушения вынести обоснованный приговор. В основном судьи выносят приговоры, выбирая одно, на их взгляд, главное квалифицирующее обстоятельство (или тип информации), при этом полная аргументация в судебных документах как правило отсутствует. Представляется, что такой судейский подход влечет существенные расхождения при принятии решения по однотипным делам и назначении по ним наказания.

Перспективы уголовно-правовой защиты персональной информации граждан в эпоху цифровизации в Китае

Представленный анализ позволяет предложить несколько направлений по совершенствованию уголовно-правовой защиты граждан.

1. Рекомендации по совершенствованию доктрины указанного уголовно-правового института.

По мнению большинства авторов, основной целью уголовного закона выступает защита правовых благ. Поэтому определение объектов преступлений, посягающих на персональную информацию граждан, а также четкое понимание предмета данных преступлений не только поможет их правильной квалификации, но и уточнит сферу криминализации подобных деяний.

Учитывая взаимосвязь между персональной информацией граждан и их личными данными, авторы считают, что следует обратить внимание на их структурный статус в области BigData и сформулировать концепцию иерархического соотношения между ними [13]. Иными словами, необходимо построить систему уголовно-правовой защиты по уровням: «уголовно-правовая защита любых онлайн-данных — уголовно-правовая защита персональных данных — уголовно-правовая защита личной информации граждан».

С учетом прав на личную информацию граждан и на неприкосновенность частной жизни, исходя из их различных характеристик, на основе узнаваемости личной информации граждан и конфиденциальности личной жизни граждан необходимо точно определить содержание и объем соответствующих правовых благ, а также отразить генерацию и передачу личной информации граждан в эпоху цифровизации.

Напомним, что основной целью состава преступления, регламентирующего нарушение персональной информации граждан, является защита личных прав и интересов граждан. Вместе с тем в эпоху цифровизации персональная информация граждан постоянно используется (в экономической, финансовой, социальной и других сферах), в результате чего могут появиться определенные социально-экономические ценности. Уголовное законодательство Китая считает приоритетом защиту персональных правовых благ, но в этом контексте указанные блага нельзя понимать просто как личные законные интересы, а следует учитывать содержащиеся в них трансперсональные правовые интересы. Иными словами, при уголовно-правовой защите персональной информации нельзя игнорировать общественные интересы, которые появляются при ее использовании в эпоху BigData. Безусловно, в отношении трансперсональных правовых интересов необходимо уделять внимание уголовной концепции предотвращения рисков, осуществлять многоуровневое и постепенное уголовно-правовое регулирование для того, чтобы избежать необоснованного ущемления права граждан на самоопределение в отношении личной информации из-за чрезмерного стремления к защите трансперсональных правовых интересов.

Информация создает ценности при ее использовании. В контексте характеристик значительного объема хранения больших данных персональная информация граждан постоянно обрабатывается и передается. Это приводит к тому, что традиционная модель согласия граждан на обработку персональной информации не всегда обеспечивает ее достаточную защиту.

Традиционные правила такого согласия[12] плохо работают в эпоху цифровизации. Сегодня следует переосмыслить эти правила, и модель динамического согласия на обработку персональных данных[13] можно рассматривать как рецепт решения возникающих дилемм. Эта модель позволяет гражданам в процессе раскрытия персональной информации преодолеть дилемму одноразового согласия и его формализации. Механизм динамичного согласия на обработку персональных данных характеризуется гибкостью, эффективностью и своевременностью, что как раз соответствует постоянно меняющейся сфере BigData.

2. Рекомендации по совершенствованию уголовного законодательства Китая.

Продажа, предоставление, незаконное приобретение данных, предусмотренные в диспозиции ст. 253.1 УК КНР, отражают способы посягательства на персональную информацию граждан. Между тем все чаще посягательства на персональную информацию граждан происходят в виде ее незаконного использования. Такие нарушения представляют серьезную общественную опасность, но еще не урегулированы уголовным законодательством [14]. Криминализация незаконного использования личной информации граждан не только будет способствовать решению проблем действующего уголовного законодательства Китая, но также позволит снизить затраты на борьбу с преступностью и сформировать комплексную систему уголовно-правовой защиты персональной информации граждан.

Что касается конкретного пути криминализации незаконного использования персональной информации граждан, то в настоящее время в Китае существует два способа криминализации деяний, которые наносят серьезный вред обществу. Один из них заключается во внесении изменений в действующее уголовное законодательство путем принятия Поправок к УК КНР, а другой — в расширении толкования уже имеющихся деяний путем опубликования разъяснений к существующим в УК КНР положениям уполномоченными на это органами. По мнению авторов, для криминализации незаконного использования персональной информации граждан следует принять Поправки к УК КНР. Основные доводы такой криминализации заключаются в следующем: с одной стороны, инкриминирование незаконного использования личной информации граждан в качестве самостоятельного деяния превысило надлежащую сферу юридического толкования; с другой стороны, законодательный метод внесения поправок соответствует основному принципу законности, поскольку он реализуется субъектом, обладающим высшей законодательной властью, а процедуры внесения поправок таковы, что не могут вызвать нестабильность в уголовном законодательстве. Криминализация незаконного использования персональной информации граждан, несомненно, сыграет положительную роль в судебной практике Китая.

3. Рекомендации по совершенствованию судебной практики в данной сфере.

При рассмотрении уголовных дел о нарушениях персональной информации граждан для всесторонней оценки элементов состава преступления и квалифицирующих эти составы обстоятельств, основное внимание должно уделяться количественным показателям. В процессе постановки и вынесения приговора количественные и качественные показатели необходимо оценивать совместно и единообразно, чтобы достичь судебной цели: вынесения равноценного приговора по однотипным преступлениям.

С учетом соответствующих положений Руководящих заключений Верховного народного суда и Верховной народной прокуратуры о вынесении приговоров за общеуголовные преступления[14], введенных в действие с 1 июля 2021 г., предлагаются следующие шаги для совершенствования судебной практики по делам о нарушениях персональной информации граждан:

1. В делах с однотипным предметом посягательства на персональную информацию граж-

[12] Суть правила информированного согласия заключается в уважении воли субъекта информации и реализации его намерения в практике обработки персональных данных [15, с. 76].

[13] Модель динамического согласия пропагандирует использование современных методов сетевых информационных технологий для создания платформы обмена между субъектами информации и ее обработчиками, что делает информированное согласие непрерывным, динамичным и открытым процессом. С помощью этой технологической платформы субъекты информации могут в любое время быть в курсе обработки их персональных данных и принимать решение о присоединении или выходе, а также могут персонализировать свои предпочтения в отношении информированного согласия, включая объем, тип информации и т.д. При этом настройки могут быть изменены в любое время [16].

[14] Верховный народный суд. URL: https://m.thepaper.cn/baijiahao_13435809.

дан количество нарушений должно использоваться в качестве основной оценки наличия квалифицирующих или особо квалифицирующих обстоятельств. Если при совершении такого преступления была получена незаконная прибыль, при квалификации деяния и назначении наказания следует учитывать сумму незаконного дохода.

2. Дела о посягательствах с несколькими видами квалифицирующих обстоятельств можно разделить на две группы в зависимости от количества людей, права которых нарушены: деяния, посягающие на персональную информацию большого числа граждан, и деяния, посягающие на аналогичную информацию отдельных граждан.

В случаях, когда нарушаются права большого числа граждан, при этом наличествуют различные квалифицирующие обстоятельства, судебное решение должно быть вынесено на основе количества и типов допущенных нарушений, а также с учетом критерия комплексной оценки обстоятельств количественного и неколичественного характера.

Иначе говоря, во-первых, следует определить, образует ли содеянное состав преступления. Если ответ положительный, необходимо установить базовую точку назначения наказания за совершенное преступление. Далее на основе количества и типа допущенных нарушений следует установить соответствие содеянного квалифицируемому составу преступления и определить базовую точку назначения наказания в пределах установленного законом диапазона наказаний. Если есть обстоятельства, квалификация которых затруднена, то приоритет оценки должен отдаваться сумме незаконного дохода, полученного от преступления, которая заменяет предыдущий количественный критерий. Во-вторых, судебное решение (приговор) должно быть вынесено на основе анализа всех установленных законом обстоятельств, таких как сумма незаконного дохода, функция, которую сыграла использованная информация, личность субъектов, степень вины. В результате суд использует метод комплексной оценки для обеспечения вынесения справедливого судебного решения по делам о преступлениях, связанных с нарушениями персональной информации граждан.

В случаях, когда установлены нарушения персональной информации отдельных граждан, следует выяснить, повлекло ли это конкретное деяние серьезные последствия, такие как смерть, тяжелые травмы, психическое расстройство или похищение жертвы, и есть ли в результате таких нарушений крупные экономические потери или неблагоприятные социальные последствия. Если в деле имеются перечисленные обстоятельства, то в соответствии с ч. 2 ст. 5 Разъяснений по рассмотрению уголовных дел о персональной информации граждан указанное преступление признается совершенным с особо отягчающими обстоятельствами.

Таким образом, в судебной практике Китая при рассмотрении уголовных дел, связанных с нарушениями персональной информации граждан, следует в соответствии с фактической ситуацией по делу определить модель комплексной оценки обстоятельств. Судебным органам при рассмотрении конкретного дела следует учитывать общественную опасность как самого подсудимого, так и совершенного им деяния, чтобы реализовать «принцип соответствия наказания преступлению» и осуществить цель наказания и предупреждения преступности.

Заключение

Уголовный закон — это палка о двух концах: при верном использовании выиграют как отдельные люди, так и общество, а при неправильном применении пострадают и отдельные люди, и общество [17, с. 10]. BigData подобны дамоклову мечу, висящему над персональной информацией граждан, а новый вид преступления — это всего лишь симбионт, созданный цифровизацией. Уголовное законодательство должно, придерживаясь нулевой терпимости к таким преступлениям, принимать контрмеры в случае нарушения правовых благ в отношении персональных данных граждан. Однако для защиты такой информации уголовный закон не является ни единственным, ни первоначальным средством. Уголовное законодательство может быть использовано только после того, как будут исчерпаны гражданские, экономические, административные и другие неуголовные меры.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1. Mayer-Schönberger V. Big Data: A Revolution That Will Transform How We Live, Work, and Think / V. Mayer-Schönberger, K. Cukier. — London : HarperCollins, 2013. — 272 p.

2. 黄祖帅：《中国个人信息的刑法保护研究》，载《首都师范大学学报(社会科学版)》2015年第5期，第65页。[Хуан Цзушуай. Исследование уголовно-правовой защиты личной информации в Китае / Хуан Цзушуай // Журнал Столичного педагогического университета. Общественная наука. — 2015. — № 5. — С. 65].

3. 陈兴良：《刑法哲学》，北京：中国政法大学出版社2004年版，第6页。[Чэнь Синлян. Философия уголовного права / Чэнь Синлян. — Пекин : Изд-во Кит. полит.-юрид. ун-та, 2004].

4. 山口厚：《刑法总论》，北京：中国人民大学出版社2011年版，第18页。[Ацуси Ямагучи. Уголовное право. Общая часть / Ацуси Ямагучи. — Пекин : Изд-во Кит. нар. ун-та, 2018].

5. 于冲：《侵犯公民个人信息罪中"公民个人信息"的法益属性与入罪边界》，载《政治与法律》2018年第4期，第19页。[Юй Чун. Атрибуты правовых благ личной информации граждан и граница квалификации в преступлении против личной информации граждан / Юй Чун // Политика и право. — 2018. — № 4. — С. 19].

6. 史卫民：《大数据时代个人信息保护的现实困境与路径选择》，载《情报杂志》2013年第12期32卷，第157页。[Ши Вэйминь. Реалистичная дилемма и выбор пути по защите личной информации в эпоху больших данных / Ши Вэйминь // Журнал разведки. — 2013. — № 12. — С. 157].

7. 杨惟钦：《价值维度中的个人信息权属模式考察—以利益属性分析切入》，载《法学评论》2016年第4期34卷，第69页。[Ян Вэйцинь. Исследование модели атрибутов прав на личную информацию в ценностном измерении — с точки зрения анализа атрибутов интересов / Ян Вэйцинь // Правовые комментарии. — 2016. — № 4. — С. 69].

8. 凌萍萍，焦冶：《侵犯公民个人信息罪的刑法法益重析》，载《苏州大学学报(哲学社会科学版)》2017年第6期，第68页。[Лин Пинпин. Повторный анализ уголовно-правовых благ в преступлении посягательства на личную информацию граждан / Лин Пинпин, Цзяо Е // Журнал Сучжоуского университета. Философия и общественная наука. — 2017. — № 6. — С. 68].

9. 冀洋：《法益自决权与侵犯公民个人信息罪的司法边界》，载《中国法学》2019年第4期，第73页。[Цзи Ян. Судебная граница между правом на самоопределение правовых благ и преступлением посягательства на личную информацию граждан / Цзи Ян // Китайская юридическая наука. — 2019. — № 4. — С. 73].

10. 张勇：《APP个人信息的刑法保护：以知情同意为视角》，载《法学》2020年第8期，第117页。[Чжан Юн. Уголовно-правовая защита личной информации App: с точки зрения информированного согласия / Чжан Юн // Юридическая наука. — 2020. — № 8. — С. 117].

11. 刘仁文：《论非法使用公民个人信息行为的入罪》，载《法学论坛》2019年第6期34卷，第119页。[Лю Женвен. Криминализация незаконного использования персональных данных граждан / Лю Женвен // Юридический форум. — 2019. — Т. 34, № 6. — С. 119].

12. 喻海松：《最高人民法院、最高人民检察院侵犯公民个人信息罪司法解释理解与适用》，北京：中国法制出版社2018年版，第37–46页。[Юй Хайсун. Понимание и применение судебных разъяснений, опубликованных Верховным народным судом, Верховной народной прокуратурой / Юй Хайсун. — Пекин : Изд-во кит. правовой системы, 2018].

13. 李源粒：《网络数据安全与公民个人信息保护的刑法完善》，载《中国政法大学学报》2015年第4期第78页。[Ли Юаньли. Совершенствование уголовного законодательства о безопасности сетевых данных и защите личной информации граждан / Ли Юаньли // Журнал Китайского политико-юридического университета. — 2015. — № 4. — С. 78].

14. 皮勇，王肃之：《大数据环境下侵犯个人信息犯罪的法益和危害行为问题》，载《海南大学学报(人文社会科学版)》2017年第5期35卷，第123页。[Пи Ен. Правовые блага и опасные деяния в преступлениях, связанных с нарушением личной информации граждан в среде больших данных / Пи Ен, Ван Сучжи // Журнал Хайнаньского университета. Гуманитарная и общественная наука. — 2017. — № 5. — С. 123].

15. 齐爱民：《信息法原论—信息法的产生与体系化》，武汉大学出版社 2010 年版，第 76 页。 [Ци Айминь. Оригинальная теория информационного права: Генерация и систематизация информационного права / Ци Айминь. — Ухань : Изд-во Ухан. ун-та, 2010].

16. 马新彦、张传才：知情同意规则的现实困境与对策检视，[J].上海政法学院学报,2021,(05):103. [Ма Синьян. Практическая дилемма Правил информированного согласия и ее контрмеры / Ма Синьян, Чжан Чуаньцай // Журнал Шанхайского политико-юридического института. — 2021. — № 5. — С. 103].

17. 陈兴良：刑法的价值构造，北京：中国人民大学出版社1998年版，第10页。[Чэнь Синлян. Ценностная структура уголовного права / Чэнь Синлян. — Пекин : Изд-во Кит. нар. ун-та, 1998].

REFERENCES

1. Mayer-Schönberger V., Cukier K. *Big Data: A Revolution That Will Transform How We Live, Work, and Think*. London, Harper Collins, 2013. 272 p.

2. Huang Zushuai. The Research of Criminal Law Legislation of Personal Information in China. *Shǒudū shīfàn dàxué xuébào (shèhuì kēxué bǎn) = Journal of Capital Normal University (Social Sciences Edition)*, 2015, no. 5, pp. 65. (In Chinese).

3. Chen Xingliang. *Philosophy of Criminal Law*. Beijing, China University of Political Science and Law Publ., 2004.

4. Atsushi Yamaguchi. *General Theory of Criminal Law*. Beijing, Renmin University of China Publ., 2018.

5. Yu Chong. The Nature of Legal Interest of «Citizens' Personal Information» and the Criminalizing Boundary in the Crime of Infringing Citizens' Personal Information. *Zhèngzhì yǔ fǎlǜ = Politics and Law*, 2018, no. 4, pp. 19. (In Chinese).

6. Shi Weimin. Personal Information Protection in Big Data Era: Predicament and Path Selection. *Qíngbào zázhì = Journal of Intelligence*, 2013, no. 12, pp. 157. (In Chinese).

7. Yang Weiqin. Study on the Ownership Model of Personal Information in Value Dimension: From the Perspective of Benefit Attribute Analysis. *Fǎxué pínglùn = Law Review*, 2016, no. 4, pp. 69. (In Chinese).

8. Ling Pingping, Jiao Ye. Reanalysis on the Legal Interests of Criminal Law for the Crime of Infringing Citizens' Personal Information. *Sūzhōu dàxué xuébào (zhéxué shèhuì kēxué bǎn) = Journal of Soochow University (Philosophy and Social Sciences Edition)*, 2017, no. 6, pp. 68. (In Chinese).

9. Ji Yang. Legal Interest Self-Determination Right and the Judicial Boundary of the Crime of Infringing on Citizens' Personal Information. *Zhōngguó fǎxué = China Legal Science*, 2019, no. 4, pp. 73. (In Chinese).

10. Zhang Yong. Criminal Law Protection of APP Personal Information: From the Perspective of Informed Consent. *Fǎxué = Law Science*, 2020, no. 8, pp. 117. (In Chinese).

11. Liu Renwen. On the Criminalization of Illegal Use of Citizens' Personal Information. *Fǎxué lùntán = Legal Forum*, 2019, vol. 34, no. 6, pp. 119. (In Chinese).

12. Yu Haisong. *Understanding and Application of Judicial Interpretation of the Crime of Infringing upon Citizens' Personal Information by the Supreme People's Court and the Supreme People's Procuratorate*. Beijing, Zhōngguó fǎzhì chūbǎn shè Publ., 2018.

13. Li Yuanli. Criminal Law Perfection for Cyber Security and Personal Information Protection. *Zhōngguó zhèngfǎ dàxué xuébào = Journal of China University of Political Science and Law*, 2015, no. 4, pp. 78. (In Chinese).

14. Pi Yong, Wang Suzhi. Legal Interests and Dangerous Acts in the Crime of Infringing Personal Information in a Big Data Environment. *Hǎinán dàxué xuébào (rénwén shèhuì kēxué bǎn) = Humanities & Social Sciences Journal of Hainan University*, 2017, no. 5, pp. 123. (In Chinese).

15. Qi Aimin. *The original Theory of Information Law: Generation and Systematization of Information Law*. Wuhan University Press, 2010.

16. Ma Xinyan, Zhang Chuancai. The Practical Dilemma of Informed Consent Rules and Its Countermeasures. *Shànghǎi zhèngfǎ xuéyuàn xuébào = Journal of Shanghai University of Political Science and Law*, 2021, no. 5, pp. 103. (In Chinese).

17. Chen Xingliang. *The Value Structure of Criminal Law*. Beijing, Renmin University of China Publ., 1998.

ИНФОРМАЦИЯ ОБ АВТОРАХ

Пан Дунмэй — заведующий Китайско-российским центром сравнительного правоведения Хэнаньского университета, доктор юридических наук, профессор, г. Кайфун, Китай; e-mail: pangdongmei71@163.com.

Фу Сянсян — научный сотрудник Института по борьбе с преступностью и уголовной политике Хэнаньского университета, кандидат юридических наук, г. Кайфун, Китай; e-mail: fxyfxx@henu.edu.cn.

ДЛЯ ЦИТИРОВАНИЯ

Пан Дунмэй. Уголовно-правовая защита персональной информации граждан в Китае: доктрина, законодательная регламентация, правоприменение / Пан Дунмэй, Фу Сянсян. — DOI 10.17150/2500-4255.2022.16(1).122-134 // Всероссийский криминологический журнал. — 2021. — Т. 16, № 1. — С. 122–134.

INFORMATION ABOUT THE AUTHORS

Pan Dongmei — Head, Chinese-Russian Center of Comparative Law, Henan University, Doctor of Law, Professor, Kaifeng, People's Republic of China; e-mail: pangdongmei71@163.com.

Fu Siansian — Researcher, Institute of Corruption Counteraction and Criminal Policy, Henan University, Ph.D. in Law, Kaifeng, People's Republic of China; e-mail: fxyfxx@henu.edu.cn.

FOR CITATION

Pan Dongmei, Fu Siansian. Criminal law protection of personal information of citizens in China: doctrine, legislative regulation, enforcement. *Vserossiiskii kriminologicheskii zhurnal = Russian Journal of Criminology*, 2022, vol. 16, no. 1, pp. 122–134. (In Russian). DOI: 10.17150/2500-4255.2022.16(1).122-134.