Административное и муниципальное право
Правильная ссылка на статью:
Горян Э.В. — Безопасность персональных данных в КНР: тенденции совершенствования правового регулирования в финансово-банковском секторе // Административное и муниципальное право. – 2021. – № 5. DOI: 10.7256/2454-0595.2021.5.36237 URL: https://nbpublish.com/library_read_article.php?id=36237

Безопасность персональных данных в КНР: тенденции совершенствования правового регулирования в финансово-банковском секторе

Горян Элла Владимировна

ORCID: 0000-0002-5962-3929

кандидат юридических наук

доцент, Владивостокский государственный университет экономики и сервиса

690014, Россия, Приморский край, г. Владивосток, ул. Гоголя, 41, каб. 5502

ella-gorjan@yandex.ru

Статья из рубрики "Актуальный вопрос"

DOI:

10.7256/2454-0595.2021.5.36237

Дата направления статьи в редакцию:

06-08-2021

Дата публикации:

27-12-2021

Аннотация: В качестве объекта исследования выбраны правовые отношения в сфере регламентирования безопасности персональных данных в финансово-банковском секторе Китайской Народной Республики. Характеризуется новейшее законодательство Китайской Народной Республики (Гражданский кодекс, Закон о защите данных, Закон о кибербезопасности), действующие и разрабатываемые подзаконные нормативно-правовые акты в сфере обеспечения безопасности персональных данных. Уделяется внимание второй редакции проекта закона о защите личной информации и определяется институциональный механизм обеспечения безопасности персональных данных. Исследуются особенности регламентирования отношений по обеспечению безопасности персональных данных в финансово-банковской системе и характеризуется роль финансового регулятора в этом механизме. Процесс разработки механизма защиты персональных данных находится в стадии завершения – помимо принятия Гражданского кодекса КНР, заложившего основу регулирования, два из трех специальных законов уже приняты – о кибербезопасности и безопасности данных. К концу 2021 года ожидается принятие ключевого закона - о защите личной информации. В своей совокупности они охватывают все сферы информационной безопасности и

устанавливают жесткий режим защиты данных: определяют сферу регулирования, объекты и субъектный состав, ответственность и институциональный механизм контроля. Правовой режим охватывает такие аспекты отношений, как персональные данные умерших лиц, лиц с ограниченными возможностями (в силу возраста и здоровья), а также транснациональная передача данных. В финансово-банковском секторе уже действует ряд подзаконных нормативно-правовых актов, устанавливающих жесткие стандарты обеспечения безопасности личной информации. Ведущую роль в этом механизме играет финансовый регулятор - Народный банк КНР. Дальнейшего изучения требуют принятые им стандарты, что позволит сделать предложения по совершенствованию российской правовой системы.

Ключевые слова: персональные данные, личная информация, трансграничная передача данных, Китай, финансовый регулятор, правовой механизм, безопасность данных, большие данные, ответственность, оператор персональных данных

Актуальность темы исследования. Цифровизация экономики и проникновение информационных технологий во все сферы жизни человека и общества привели к уязвимости информации о личности, которая собирается в круглосуточном режиме, а субъектом персональных данных зачастую не осознается не только её сбор и обработка, но и цель таких действий. Государство выступает основным гарантом безопасности персональных данных, поэтому совершенствование правового механизма обеспечения безопасности персональных данных в современных условиях является постоянным процессом.

С 2019 года Китайская Народная Республика реализует масштабный план по регулированию Big Tech (крупные компании, способствующие значительным изменениям в обществе через собственное доминирование и роль в онлайн-деятельности): Alibaba Group, LinkDoc и DiDi уже получили предписания и запреты на размещение своих акций на зарубежных биржах. Озабоченность китайского государства состоянием защиты персональных данных наблюдается и в автомобильной отрасли – производители высокотехнологичных автомобилей обязаны соблюдать предписания по защите данных: под регулирование попадают практически все ситуации, в которых люди оказываются в машине или рядом с ней. В мае 2020 года Администрация киберпространства КНР (Cyberspace Administration of China) опубликовала проект Некоторых положений об администрировании безопасности автомобильных данных (Several Provisions on Administration of Automobile Data Security)[1], содержащий ряд предписаний по защите персональных данных. Эта мера вызвана в том числе недавним расследованием Администрации киберпространства КНР, Министерства общественной безопасности КНР, Министерства государственной безопасности КНР, Министерства природных ресурсов КНР, а также налоговых, транспортных и антимонопольных органов китайского государства в отношении одной из крупнейших компаний – DiDi Chuxing Technology Co. (ранее называвшейся Didi Dache и Didi Kuaidi, компании по аренде автомобилей с более чем 550 миллионами пользователей и десятками миллионов водителей). По предварительным данным, DiDi не в достаточной степени обеспечивают безопасность персональных данных своих клиентов [2].

В 2020 году были приняты Гражданский кодекс и пакет нормативно-правовых актов в сфере защиты данных. Особую роль в этом процессе играет Народный банк Китая [3, с. 97], продвигающий жесткий подход к регулированию деятельности FinTech-компаний -

применяя к ним такие же правила, как и к классическим финансовым компаниям: соблюдение правил об информационной безопасности персональных данных потребителей; улучшение корпоративного управления (повышение прозрачности), следование нормативам пруденциального надзора (направление отчетов финансовому регулятору для раннего выявления возможных проблем), недопущение незаконного кредитования, страхования и управления финансовыми активами [4]. Учитывая лидирующую роль КНР в цифровизации экономики и процессов государственного управления, опыт этого государства очень важен для совершенствования российской правовой системы. Всё вышесказанное и определяет актуальность исследования.

Цель и задачи исследования. Цель исследования – определить особенности правового регулирования института персональных данных в Китае в аспекте обеспечения информационной безопасности финансово-банковского сектора. Задачи исследования заключаются в характеристике нормативно-правовой основы регулирования; анализе основных положений как действующих нормативно-правовых актов, так и их проектов; определении особенностей регламентирования отношений в сфере защиты персональных данных и их влияния на обеспечение безопасности данных в финансово-банковском секторе.

Методология. С целью получения наиболее достоверных научных результатов были использованы системно-структурный, формально-логический и формально-юридический методы.

Предмет исследования, источниковая база исследования, противоречия в имеющихся исследованиях и авторская позиция. Предмет исследования составляет действующее законодательство КНР и проекты нормативно-правовых актов в сфере регулирования отношений по обеспечению безопасности персональных данных в том числе в финансово-банковском секторе.

Поиск в электронной библиотеке научных публикаций eLIBRARY.RU показал слабую изученность рассматриваемой темы. В 2020 году были опубликованы две работы о правовом регулировании защиты персональных данных в Китае [5; 6], однако они основываются на устаревшей нормативно-правовой базе и не включают в объект исследования финансово-банковский сектор, еще одна работа датируется 2016 годом [7] и исследование ввиду вышеуказанных причин уже не актуально. Такой недостаток научных публикаций доказывает необходимость исследования данной темы.

Основная часть. На материковом Китае термин «персональные данные» (personal data) используется в законодательстве редко. Термином, который используется для регулирования соответствующих отношений, выступает «личная информация» (personal information). В принятый в 2020 году Гражданский кодекс Китайской Народной Республики (далее – ГК КНР) была включена Книга четвертая, посвященная правам личности (Personality Rights) и содержащая главу VI «Право на личную жизнь и защита личной информации» (Rights to Privacy and Protection of Personal Information) [8].

Статья 1034 ГК КНР определяет личную информацию как информацию, записанную в электронном виде или другими способами, которая может использоваться сама по себе или в сочетании с другой информацией для идентификации физического лица. Закон непосредственно относит к таковым данным имя, дату рождения, идентификационный номер, биометрическую информацию, адрес проживания, номер телефона, адрес электронной почты, медицинскую информацию и местонахождение лица, оставляя этот список открытым. Особо отмечается, что к личной информации, являющейся тайной,

применяются соответствующие положения о праве на личную жизнь [9].

В настоящее время материковый Китай проводит полномасштабную работу по актуализации законодательства в сфере защиты персональных данных для снижения торговых барьеров. В частности, в 2017 году был принят Закон Китайской Народной Республики о кибербезопасности [10], а в следующем году - Закон об электронной торговле [11]. В 2018 году была проведена рабочая конференция Тринадцатого Постоянного комитета Всекитайского собрания народных представителей, где был утвержден пятилетний план реформирования законодательства КНР с включенным в него отдельным пунктом по персональным данным [12, с. 10].

Рост количества информационных сетей, а главное, объема и качества данных, передаваемых с их помощью приводит к пересмотру государственной политики в области работы с информацией. Китайские исследователи отмечают стремление законодателя совершенствовать правовые инструменты регулирования не только производства данных, но и их хранения и обработки, что позволит выйти в лидеры мирового рынка [13, с. 44]. Большие массивы данных (big data) собираются и обрабатываются как государственными органами, так и субъектами частного сектора, что повышает ценность такой информации и ее влияние на политические, социальные и экономические процессы, равно как и их регулирование. Между тем использование или обработка персональных данных при отсутствии юридических инструментов (регуляторов) также может привести к их компрометации (посягательству) и даже поставить под угрозу национальную безопасность. Поэтому рассмотрение механизма обеспечения безопасности персональных данных необходимо начать с характеристики нормативно-правовой и институционных основ.

Закон о законодательстве Китайской Народной Республики определяет Всекитайское собрание народных представителей и его Постоянный комитет в качестве законодательных органов китайского государства (ст. 7) [14]. Постоянный комитет Всекитайского собрания народных представителей уполномочен «принимать и изменять законы, кроме тех, которые должны быть приняты непосредственно Всекитайским собранием народных представителей» (ст. 67(2)) [15]. Эти законы и постановления, изданные Всекитайским собранием народных представителей и его Постоянным комитетом, имеют юридическую силу высшего уровня при формировании правовой системы в Китае. В июне 2021 года был издан Закон Китайской Народной Республики о безопасности данных [16], вступление в силу которого было определено довольно быстро – 1 сентября 2021 года. Принятие этого закона завершило напряженный период законотворчества и активного обсуждения представителями как государственного, так и частного сектора. В частности, исследователи отмечали некую децентрализацию в предлагаемой модели для защиты персональных данных [17, с. 30]. Это объясняется, прежде всего, особой правовой системой КНР, наделяющей подзаконные нормативные акты юридической силой, не сопоставимой с аналогичными документами, издаваемыми в других государствах. В результате нормативный механизм представлен рядом законов, постановлений и других правовых документов. Нормы касательно защиты персональных данных в материковом Китае содержатся в Конституции КНР и ряде законов в сфере гражданского, административного и уголовного права. Цифровизация экономики привела к появлению спроса на правовые инструменты применительно к ее специфичным объектам - телекоммуникациям, Интернету и электронной коммерции, поскольку они непосредственно связаны с персональными данными при производстве

или предоставлении продуктов и услуг. Рассмотрим нормативную базу подробнее.

Конституция Китайской Народной Республики[15] является основным законодательным актом правовой системы и устанавливает основные права и обязанности китайских граждан [12, с. 22], таких как право и обязанность работать (ст. 42) [15], свобода слова, печати, ассоциаций (ст. 35) [15], и некоторые другие основные права и обязанности. Согласно Конституции КНР все граждане Китая равны. Они могут пользоваться правами и выполнять обязанности, предусмотренные Конституцией КНР или другими законами (ст. 33) [15]. Конституция КНР прямо не упоминает защиту персональных данных, однако толкование некоторых ее статей позволяет говорить о включении этого института в сферу правового регулирования (нормы о человеческом достоинстве или частной жизни). В частности, статья 38 Конституции КНР гласит, что достоинство граждан защищается как одно из конституционных прав, а статья 40 регулирует свободу и конфиденциальность индивидуального общения. Очевидно, что персональные данные могут иметь тесную связь с человеческим достоинством и частной жизнью, особенно данные о здоровье, семейном положении, по своей природе они являются конфиденциальными. Всё это позволяет говорить о косвенном регулировании института персональных данных Конституцией КНР.

Нарушение режима персональных данных может нанести ущерб конфиденциальности лица, поэтому к таким отношениям применяются некоторые положения о конфиденциальности личной жизни (например, с целью предотвращения незаконного сбора или обработки персональных данных). Статья 2 Закона Китайской Народной Республики о деликтах [18] относила право на неприкосновенность личной жизни к субъективным гражданским правам и законным интересам лиц, а также подтверждает независимый статус права на неприкосновенность личной жизни. Это право обеспечивалось, в частности, в случае обращения в медицинские учреждения (ст. 62), от которых требовалось соблюдение конфиденциальности информации о пациентах (например данные истории болезни). Указанный закон квалифицировал нарушение режима персональных данных как вмешательство в личную жизнь.

Принятие в 2020 году первого кодифицированного закона в сфере гражданского права - Гражданского кодекса Китайской Народной Республики (далее – ГК КНР)[8] стало выдающимся событием в правовой жизни государства, исследователи нарекли этот закон энциклопедией жизни гражданского общества Китая [19, с. 18]. ГК КНР вступил в силу 1 января 2021 года и представлен семью книгами, посвященными общим положениям (General Part), вещным правам (Real Rights), договорам (Contracts), правам личности (Personality Rights), браку и семье (Marriage and Family), наследованию (Succession) и деликтной ответственности (Tort Liability).

Нормы о защите персональной информации включены в главу 6 «Право на неприкосновенность личной жизни и защиту личной информации» (Chapter VI Rights to Privacy and Protection of Personal Information) Книги четвертой «Права личности» (Book Four Personality Rights).

Статья 1034 ГК КНР определяет личную информацию как информацию, записанную в электронном виде или другими способами, которая может использоваться сама по себе или в сочетании с другой информацией для идентификации физического лица. Закон непосредственно относит к таковым данным имя, дату рождения, идентификационный номер, биометрическую информацию, адрес проживания, номер телефона, адрес электронной почты, медицинскую информацию и местонахождение лица, оставляя этот

список открытым.

Обработка личной информации должна осуществляться в соответствии с принципами законности, обоснованности и в необходимых пределах (не должна подвергаться чрезмерной обработке) и при соблюдении следующих условий (ст. 1035 ГК КНР): (1) получение согласия от физического лица или его опекуна, если иное не предусмотрено законами или административными постановлениями; (2) правила обработки информации должны быть опубликованы; (3) четкое указание цели, метода и объема обработки информации; (4) обработка не должна противоречить законам или административным постановлениям (согласию субъекта). Обработка личной информации включает сбор, хранение, использование, уточнение, передачу, предоставление, раскрытие и иные действия в отношении личной информации [12, с. 25].

До принятия ГК КНР законность обработки личной информации определялась Общими положениями гражданского законодательства Китайской Народной Республики, которые «регулируют личные отношения и имущественные отношения между физическими, юридическими лицами и организациями без юридического лица как равноправные стороны» [12, с. 25]: в статье 111 указывалось, что персональные данные физического лица должны защищаться законом; никакие организации или частные лица не могут незаконно собирать, использовать, обрабатывать, передавать, предоставлять, торговать или раскрывать персональные данные. Таким образом, по сравнению с Законом Китайской Народной Республики о деликтах и Общими положениями гражданского законодательства Китайской Народной Республики, ГК КНР усилил защиту персональных данных. В частности, кроме определения личной информации закрепляются принципы ее защиты, права субъектов, обязанности уполномоченных субъектов, а также обязательство государственных органов о соблюдении конфиденциальности. Отдельные положения посвящены специальным отношениям, в которых затрагивается личная информация (например, статья 1226 ГК КНР требует, чтобы медицинское учреждение и персонал сохраняли конфиденциальность данных о пациенте). Как отмечают исследователи, принятие ГК КНР является значительной вехой в развитии института личной информации в материковом Китае: в некоторой степени он отделяет защиту личной информации от защиты достоинства или конфиденциальности и признает, что защита личной информации может быть независимым объектом регулирования [12, с. 25].

На сегодняшний день в КНР действует два закона, касающиеся защиты данных и информации: Закон Китайской Народной Республики о кибербезопасности 2017 года[10] и Закон Китайской Народной Республики о безопасности данных[16]. На рассмотрении находится вторая редакция проекта закона о защите личной информации [20]. В случае его принятия можно будет говорить о создании всеобъемлющей правовой основы для регулирования режима защиты информации и данных в Китае.

Рассмотрим эти источники подробнее.

Закон Китайской Народной Республики о кибербезопасности 2017 года[10] разрабатывался два года – с 2014 по 2016 год. Его структура включает семь глав: (1) общие положения; (2) обеспечение и продвижение кибербезопасности; (3) безопасность работы сети, включающей два раздела: общие положения и безопасность операций на объектах критической информационной инфраструктуры; (4) безопасность информации в сети; (5) мониторинг, профилактика и реагирование на кибератаки; (6) юридическая ответственность; (7) дополнительные положения.

Глава IV Закона определяет режим защиты информации в киберпространстве, прежде всего - персональных данных. В соответствии с положениями этой главы на операторов сети возложены такие обязанности как (1) обеспечение конфиденциальности информации (ст. 40); (2) обеспечение критерия необходимости и достаточности персональных данных (ст. 41); (3) обезличивание информации (ст. 42); (4) удаление информации, полученной в нарушение закона или содержащей неверные сведения (ст. 43); (5) принятие немедленных мер по защите информации в случае неправомерности ее использования (ст. 47); (6) создание системы взаимодействия с клиентами, сотрудничество с уполномоченными органами (ст. 49); (7) прекращение передачи, обработки и других операций с информацией, применение необходимых технических мер по требованию уполномоченных органов (ст. 50).

Закон также устанавливает запрет на незаконное получение и распространение информации (ст. 44) и обязанность уполномоченных органов власти соблюдать требования конфиденциальности (ст. 45). Отдельно законом определен запрет на создание интернет-страниц или средств связи для осуществления противозаконной деятельности, в том числе распространения информации о способах такой деятельности и торговли запрещенными или ограниченными в обороте средствами (ст. 46). Запрещено также распространение вредоносных программ и запрещенной (ограниченной в пользовании) информацией (ст. 48).

Закон Китайской Народной Республики о безопасности данных[16] состоит из семи глав, охватывающих общие положения о безопасности (глава I), положения о безопасности и развитии данных (глава II) и системах защиты данных (глава III), обязательства по обеспечению безопасности данных (глава IV), положения о безопасности и открытости правительственных данных (глава V), а также юридической ответственности (глава VI) и дополнительных положениях (глава VII).

Закон был разработан с целью регулирования деятельности по обработке данных, обеспечения безопасности данных, содействия разработке и использованию данных, защиты законных прав и интересов физических лиц и организаций, обеспечения суверенитета, безопасности и интересов развития государства (ст. 1). Под термином «данные» понимаются записи информации с помощью электронных или иных средств (ст. 3), а термин «обработка данных» охватывает любую деятельность с ними, включая сбор, хранение, использование, обработку, передачу, предоставление, раскрытие и т.д.

Данный закон акцентирует внимание на роли государства в обеспечении безопасности данных, которое обязано принимать меры по эффективной защите и обеспечению состояния непрерывной безопасности путем следования общей концепции национальной безопасности, создания и совершенствования системы управления безопасностью данных (ст. 4).

В институциональный механизм обеспечения безопасности данных включатся органы государственной власти как общей (ст. 5), так и специальной компетенции (ст. 6): в сфере промышленности, телекоммуникаций, транспорта, финансов, природных ресурсов, здравоохранения, образования, науки и техники и соответствующих отраслях и областях. Ответственность за общую координацию работы по обеспечению безопасности сетевых данных и соответствующий надзора несет Государственный департамент сетевой информации.

Законом определяются принципы обеспечения безопасности данных: соответствие закону; соблюдение общественной морали и этики; соблюдение норм деловой и

профессиональной этики; честность и хорошая репутация операторов данных; соблюдение требований к обеспечению безопасности; отсутствие угрозы национальной безопасности и общественным интересам; не причинение вреда законным правам и интересам граждан и организаций (ст. 8).

Стоит отметить систему общих гарантий, обеспечивающих безопасность данных и реализуемых непосредственно государством (ст. 9-12): 1) пропаганда и популяризация знаний о безопасности данных; 2) повышение осведомленности общества и уровня защиты данных на общественном уровне; 3) поощрение совместной деятельности соответствующих ведомств, отраслевых организаций, научно-исследовательских учреждений, предприятий и отдельных лиц по защите данных; 4) формирование благоприятных условий для совместного поддержания безопасности данных и содействия развитию всего общества; 5) разработка кодексов поведения операторами данных и повышение квалификации персонала; 6) международное сотрудничество в области управления безопасностью данных; 7) конфиденциальность рассмотрения заявлений и жалоб.

В отношении личной информации заслуживают более пристального рассмотрения следующие положения закона.

Во-первых, это требования к трансграничной передаче данных, закрепленные в статьях 31 и 36. Согласно статье 31 трансграничная передача важных данных, собираемых и генерируемых операторами критической информационной инфраструктуры в Китае, регулируется Законом о кибербезопасности, устанавливающим требование хранения на территории КНР данных, собранных и генерируемых операторами критической информационной инфраструктуры. При необходимости передачи таких данных за границу осуществляется оценка безопасности.

К слову, новеллой закона о защите данных является введение термина «важные данные», определяемого как данные, связанные с национальной безопасностью, состоянием национальной экономики, жизнедеятельностью важных государственных лиц и общественными интересами. В отношении таких данных внедряется более жесткая система управления.

Для трансграничной передачи важных данных, собираемых и производимых в процессе работы операторами данных на территории КНР, статья 31 предусматривает, что меры по проверке безопасности должны быть согласованы Администрацией киберпространства КНР с соответствующими ведомствами при Государственном совете. На данный момент отсутствуют конкретные правила в отношении оценки безопасности важных данных при передаче их за границу. Операторы данных, которые нарушают вышеуказанную статью и незаконно передают важные данные за границу, получат предписание от уполномоченного государственного органа с требованием исправить нарушение и могут быть оштрафованы на сумму от 100 тыс. до 1 млн юаней (ст. 45). Если обстоятельства нарушения серьезны, то размер штрафа составит от 1 до 10 млн юаней с последующим приостановлением деятельности и отзывом лицензий и разрешений. Непосредственно ответственное лицо и другие лица, несущие прямую ответственность за нарушение, будут оштрафованы на сумму от 100 тыс. до 1 млн юаней (ст. 46).

Статья 36 закона устанавливает порядок предоставления данных по запросам судебных или правоохранительных органов зарубежных государств: любые организации и частные лица в Китае должны получить разрешение компетентного органа при работе с запросами на передачу данных за границу, сделанными иностранными судебными или

правоохранительными органами. Компетентный орган должен рассматривать такие запросы в соответствии с соответствующими законами, международными договорами и соглашениями, заключенными Китайской Народной Республикой, или на основе принципа равенства и взаимной выгоды.

Нарушение порядка предоставления данных иностранным судебным или правоохранительным органам без разрешения компетентных органов Китая влечет за собой штраф до 100 тыс. до 5 млн юаней с одновременным изданием предписания о приостановлении деятельности компании до устранения нарушений и отзывом лицензий и разрешений. Непосредственно ответственное лицо и другие лица, несущие прямую ответственность за нарушение, будут оштрафованы на сумму от 50 до 500 тыс. юаней (ст. 48).

Следует отметить, что сам закон не регламентирует процедуру получения подобного разрешения, равно как и не устанавливает уполномоченный орган (систему органов). Смеем предположить, что будет издан соответствующий подзаконный нормативный акт.

Во-вторых, это требования соответствия к поставщикам посреднических услуг (data intermediary services provider), количество которых в последние годы неуклонно растет (Tianyuan Data, Jingdong Cloud, Guiyang Big Data Exchange, Shanghai Data Exchange Center). Фактически такие компании предоставляют торговую платформу для осуществления трансакций между поставщиками и покупателями (потребителями), объектом которых являются данные. До принятия указанного закона не существовало специальных положений, регламентирующих мониторинг и контроль процессов торговли данными, равно как и стандарты деятельности поставщиков посреднических услуг, что негативно сказывалось на интересах сторон, участвующих в сделках с данными.

Этот пробел был заполнен положениями статьи 33 закона о защите данных. Она выдвигает формальные требования к процессу обмена данными, а именно к субъектам, оказывающим посреднические услуги по продаже данных: (1) обязанность требовать от поставщика данных объяснения источника данных. Данные не должны иметь дефектов собственности, что означает, что данные не были получены путем кражи или других незаконных средств, и данные не относятся к числу запрещенных китайскими законами и постановлениями; (2) обязанность проверять правовой статус обеих сторон сделки: они должны быть юридическими или физическими лицами. Для определенных операций по торговле данными, которые требуют от соответствующих сторон получения определенных лицензий для совершения сделок, посредник должен проверить, есть ли у сторон необходимые лицензии; (3) обязанность хранить записи об исследованиях и сделках.

Поставщики посреднических услуг, нарушающие вышеуказанные положения, могут быть подвергнуты многочисленным штрафам. Незаконно полученная прибыль будет конфискована и будет наложен штраф максимум в десятикратном размере незаконно полученной прибыли. В случае отсутствия таковой или если ее размер составляет менее 100 тыс. юаней, то субъект будет оштрафован на сумму от 100 тыс. до 1 млн юаней. Кроме того, возможно приостановление деятельности субъекта и отзыв разрешений и лицензий. Непосредственно ответственное лицо и другие лица, несущие прямую ответственность за нарушение, будут оштрафованы на сумму от 10 тыс. до 100 тыс. юаней.

Как и в предыдущем случае, закон не регламентирует процедуру проверки деятельности поставщиков посреднических услуг, равно как и не устанавливает уполномоченный орган (систему органов). Ожидается принятие соответствующего подзаконного

нормативного акта.

В-третьих, это защита интересов особых групп населения. Речь идет о лицах с ограниченными возможностями в силу возраста (пожилые) и здоровья (инвалиды). Как отмечают исследователи, на практике было много случаев, когда продавцы или поставщики услуг отказывались принимать наличные, в то время как пожилые люди не знали, как использовать Alipay или WeChat Pay. Кроме того, после вспышки COVID-19 сообщалось, что в некоторых городах людям было отказано в доступе к общественному транспорту или услугам из-за того, что они не получили цифровой код здоровья, что было реализовано в рамках мер по предотвращению эпидемии [21]. Для защиты прав этих групп и обеспечения принципа равенства статья 15 закона устанавливает обязанность любого субъекта в полной мере учитывать потребности пожилых людей и инвалидов при разработке мобильных приложений для общественных услуг. С одной стороны, пожилых людей и инвалидов нельзя заставить использовать так называемые интеллектуальные продукты. Например, помимо заказа еды путем сканирования QR-кода и оплаты счета цифровыми платежами, рестораны должны предоставлять в качестве альтернативы традиционные методы заказа и оплаты. С другой стороны, учет их потребностей при разработке соответствующих продуктов осуществляется путем подключения дополнительных технологических функций в интерфейс (крупный шрифт, голосовой помощник и т.д.).

И наконец, в отношении персональных данных необходимо придерживаться норм социальной морали и этики. В частности, статья 28 устанавливает, что любые операторы данных и разработчики новых технологий обработки данных «должны способствовать экономическому и социальному развитию, повышению благосостояния людей и соблюдению норм социальной морали и этики». Эта норма свидетельствует об уточнении требований законодателя к безопасности личной информации: если до принятия этого закона упор делался на правовые аспекты обработки данных, то сейчас этот вопрос рассматривается в моральном контексте. Поэтому все субъекты отношений в сфере личной информации при обработке данных, разработке программного обеспечения и другой сопутствующей деятельности должны проводить анализ соответствия деятельности и разрабатываемых продуктов нормам социальной морали и этики.

Проект закона о защите личной информации (Personal Information Protection Law of the People's Republic of China, далее - PIPL)[20] обсуждается с октября 2020 года. Он состоит из 8 глав: 1) общие положения; 2) правила обращения с личной информацией; 3) правила трансграничного предоставления личной информации; 4) права физических лиц при работе с личной информацией; 5) обязанности обработчиков личной информации; 6) подразделения, выполняющие обязанности по защите личной информации; 7) юридическая ответственность; 8) дополнительные положения.

В апреле 2021 года была опубликована его вторая редакция, анализ которой позволяет сделать предварительные прогнозы относительно модели защиты персональных данных, к которой склоняется законодатель. В целом законодательство Китая о конфиденциальности информации разрабатывается на основе «согласие-ориентированного» подхода, при котором согласие вместе с ограниченным перечнем исключений является законным основанием для обработки личной информации. Как и в большинстве других юрисдикций Азиатско-Тихоокеанского региона сфера имплементируемых положений Общего регламента ЕС по защите данных (General Data Protection Regulation, GDPR), как правило, не охватывает обработку в рамках «законных интересов» ("legitimate interests" processing), то есть оператор имеет право

обрабатывать личную информацию, находящуюся в публичном доступе, без получения предварительного согласия лица, при условии соблюдения надлежащего баланса своих деловых интересов с интересами конфиденциальности субъектов данных и обеспечения справедливой обработки. Этот более узкий подход был реализован в первой редакции проекта закона о защите личной информации, вторая редакция вводит дополнительную правовую основу для обработчиков личной информации (лиц, осуществляющих обработку персональной информации, термин, аналогичный «контроллеру данных» в соответствии с GDPR и «оператору данных» в России), которая позволяет обрабатывать общедоступную личную информацию «в разумных пределах» (ст. 13). Законопроект не содержит положений, раскрывающих содержание термина «разумные пределы», кроме оговорки о том, что цель обработки общедоступной личной информации не должна существенно отклоняться от основной цели публикации информации.

PIPL устанавливает более высокие стандарты обработки личной информации несовершеннолетних (ст. 15). Независимо от того, знает ли обработчик данных или должен знать, что он обрабатывает личную информацию лица младше 14 лет, он должен получить согласие родителей несовершеннолетнего или другого опекуна.

Законопроект предусматривает возможность отзыва согласия на обработку личной информации (ст. 16): обработчик данных должен предоставить субъектам данных удобный способ отзыва согласия. Это не повлияет на какие-либо действия по обработке, которые имели место до того, как согласие было отозвано.

Отдельно определен порядок обработки данных третьими лицами (ст. 22): если соглашение с третьими лицами об обработке данных не вступает в силу или недействительно, отменяется или прекращается, третьи лица не должны хранить личную информацию, а должны вернуть ее обработчику данных или удалить.

В 2019 году был опубликован проект Мер по оценке безопасности трансграничной передачи личной информации (Measures on Security Assessment of Cross-Border Transfers of Personal Information), куда был включен список требований к стандартным условиям договора (standard contractual clauses, SCC) для трансграничной передачи личной информации. Этот акт так и не был принят. SCC снова упоминаются во второй редакции проекта PIPL (ст. 38), что еще больше увеличивает шансы того, что Администрация киберпространства КНР после принятия PIPL примет отдельный нормативный акт с перечнем стандартных условий договора при трансграничной передаче личной информации. На данном этапе неизвестно, какие положения будут включены в SCC, но ясно, что некоторые из условий, предложенных в проекте Мер по оценке безопасности трансграничной передачи личной информации, будут сложными для согласования со сторонами, включая право на компенсацию субъектам данных и требование о расторжении контракта, если его выполнение становится затруднительным из-за изменений в законах в юрисдикции получателя [22].

Вторая редакция проекта PIPL расширяет обязанности обработчиков личной информации, управляющими «базовыми» службами интернет-платформ (basic internet platform services) для обслуживания «массового» (massive) числа пользователей (без указания порогового числа) и имеют «сложные» (complex) типы бизнеса (ст. 57). Такие обязанности включают: (i) создание руководящего комитета, независимого от обработчика, для надзора за действиями по обработке личной информации; (ii) приостановление предоставления услуг поставщикам продуктов или услуг, работающих на платформе обработчика личной информации, если они серьезно нарушают законы о защите данных; и (iii) выпуск регулярных отчетов о социальной ответственности в

отношении обработки личной информации. Исследователи отмечают, что исполнение обязанностей таких субъектов связано с рядом сложностей, таких как 1) неопределенность терминологии («базовая» интернет-платформа, «массовое» количеством пользователей, «сложные» типы бизнеса); 2) неопределенность основания приостановления услуг поставщикам продуктов или услуг, работающих на платформе обработчика личной информации; 3) неопределенность в содержании отчетов о социальности ответственности [22].

Новеллой законопроекта являются положения о защите прав умерших лиц: родственники умерших лиц могут осуществлять права в отношении личной информации от их имени (ст. 49). Права умерших на личную информацию не упоминались ни в предыдущей редакции проекта, ни в любом другом нормативно-правовом акте о защите данных. Однако в проекте не раскрыты такие аспекты реализации права, как 1) порядок определения уполномоченного родственника умершего и 2) механизм его реализации обработчиком личной информации, включая порядок подтверждения личности родственников и факта смерти лица.

Заслуживает внимания такая новелла второй редакции законопроекта, как определение презумпции вины: в соответствии со ст. 65 в случаях причинения вреда интересам, связанным с личными данными, если обработчик данных не смог доказать отсутствие своей вины, он несет гражданско-правовую ответственность за деликт.

В финансово-банковском секторе личная информация является едва ли не самым важным активом как инвесторов, так и финансовых учреждений. Они требуют от клиентов предоставления подробных персональных данных (включая конфиденциальные) для предоставления финансовых услуг. Неправильная обработка этих персональных данных может привести к угрозам личной безопасности или сохранности имущества клиентов. Как в Законе Китайской Народной Республики о Народном банке Китайской Народной Республики [23], так и в законах о коммерческих банках [24] и страховании [25] есть нормы, касающиеся защиты личных финансовых данных. Например, закон о коммерческих банках возлагает на них обязанность соблюдать конфиденциальность перед вкладчиками (ст. 29) [24]. В 2017 году Народный банк КНР издал Меры по защите финансовых прав и интересов клиентов [26], в которых указывается, что сбор личных финансовых данных должен осуществляться в соответствии с принципами законности, рациональности и необходимости. В апреле 2019 года был принят Рабочий план Народного банка Китая по разработке нормативных актов на 2019 год (People's Bank of China's 2019 Regulations Development Work Plan), который включает план по разработке Мер по защите личных финансовых данных (Measures for the Protection of Personal Financial Data) [27].

Тем временем Государственная администрация регулирования рынков (State Administration of Market Regulation, SAMR) в лице своего специального подразделения - Администрации стандартизации Китая (Standardisation Administration of China) разработала ряд руководств, призванных регулировать отношения в сфере защиты личной информации в финансово-банковском секторе. 6 марта 2020 года был издан документ Изменения в спецификации безопасности личной информации (Personal Information Security Specification Revisions) [28], установивший особые требования по усилению защиты личной информации. Руководство по оценке воздействия на безопасность личной информации (Guidance for Personal Information Security Impact Assessment) [29] вступило в силу 1 июня 2021 года с целью детализаций положений

статьи 54 проекта закона о защите личной информации. В отношении мобильных приложений Национальный технический комитет по стандартизации информационной безопасности (National Information Security Standardization Technical Committee (TC260)) и Администрация киберпространства КНР издали серию руководств и стандартов по обработке данных операторами мобильных приложений, включая самооценку, использование SDK (software development kits) и минимальный объем личной информации, необходимой для работы.

Следует отметить роль финансового регулятора (Народного банка Китая) в установлении стандартов защиты персональных данных. В частности, в 2020 году были приняты три стандарта:

(1) Техническая спецификация защиты личной финансовой информации (Personal Financial Information Protection Technical Specification)[30] – определяет уровни (3 уровня) и категории (7 категорий) личной финансовой информации. В частности по уровню чувствительности разграничивают идентификационную информацию пользователя (C3), информацию, которая может идентифицировать личность и финансовый статус (C2), а также внутренние информационные активы (C1). Категоризация определяется в зависимости от вида информации: 1) информация об учетной записи; 2) идентификационная информация; 3) информация о финансовых транзакциях; 4) личная идентификационная информация; 5) информация об имуществе; 6) информация о займе; 7) другая информация, отражающая определенные ситуации с конкретным субъектом финансовой информации;

(2) Руководство по классификации безопасности данных (Guidelines for Data Security Classification) [31] требует разграничения уровней безопасности от высокого до низкого с учетом воздействия на национальную безопасность, общедоступность. интересы, неприкосновенность частной жизни и юридические права предприятия, а также степень воздействия ущерба для безопасности данных финансовых учреждений (всего 4 уровня).

(3) Меры по защите прав и интересов потребителей финансовых услуг (Measures on the PBOC on the Protection of Financial Consumers' Rights and Interests)[32]. По сравнению с редакцией 2017 года новый документ ужесточает требования к финансовым операторам. Во-первых, теперь этот акт имеют бóльшую юридическую силу - нарушение новых правил квалифицируется ка уголовное преступление (ст. 64). Во-вторых, особое внимание уделяется таким правам потребителей финансовых услуг как право на имущественную безопасность, право на уважение, право на информацию, право на справедливые условия сделки, право на усиленную информационную безопасность (ст. 14–21). В-третьих, это стандартизация прямого маркетинга с упором на право на получение информации (ст. 30). И наконец, это усиление санкции за нарушение законов и постановлений до 500 тыс. юаней (ст. 60).

Выводы. В результате проведенного исследования мы пришли к следующим выводам. Законодательство Китая о персональных данных разрабатывается на основе «согласие-ориентированного» подхода, при котором согласие вместе с ограниченным перечнем исключений является законным основанием для обработки личной информации. Процесс разработки механизма защиты персональных данных находится в стадии завершения – помимо принятия Гражданского кодекса КНР, заложившего основу регулирования, два из трех специальных законов уже приняты – о кибербезопасности и безопасности данных. К концу 2021 года ожидается принятие ключевого закона - о защите личной

информации. В своей совокупности они охватывают все сферы информационной безопасности и устанавливают жесткий режим защиты данных: определяют сферу регулирования, объекты и субъектный состав, ответственность и институциональный механизм контроля. Правовой режим охватывает такие аспекты отношений, как персональные данные умерших лиц, лиц с ограниченными возможностями (в силу возраста и здоровья), а также транснациональная передача данных. В финансово-банковском секторе уже действует ряд подзаконных нормативно-правовых актов, устанавливающих жесткие стандарты обеспечения безопасности личной информации. Ведущую роль в этом механизме играет финансовый регулятор - Народный банк КНР. Дальнейшего изучения требуют принятые им стандарты, что позволит сделать предложения по совершенствованию российской правовой системы.

Исследование выполнено при финансовой поддержке РФФИ в рамках научного проекта 20-011-00454 «Обеспечение прав инвесторов в банковском и финансовом секторах в условиях цифровизации экономики в РФ и ведущих финансовых центрах Восточной Азии: сравнительно-правовой аспект».

Библиография

1. Duan K. Brief Comments on Draft Automobile Data Security Provisions / K. Duan, T. Wang, K. Cai // Hankunlaw.com, URL: https://www.hankunlaw.com/downloadfile/newsAndInsights/8c9f977eb01519c5f6f342e5a0ace6da.pdf.
2. China Weighs Unprecedented Penalty for Didi After U.S. IPO // Bloomberg News, URL: https://www.bloomberg.com/news/articles/2021-07-22/china-is-said-to-weigh-unprecedented-penalty-for-didi-after-ipo.
3. Горян Э.В. Роль финансового регулятора в обеспечении информационной безопасности России и Китая: сравнительно-правовой аспект / Э.В. Горян // Территория новых возможностей. Вестник Владивостокского государственного университета экономики и сервиса. 2020. Т. 12. № 2. С. 88–102.
4. 中国人民银行副行长潘功胜就金融管理部门再次约谈蚂蚁集团情况答记者问 // People's Bank of China, URL: http://www.pbc.gov.cn/goutongjiaoliu/113456/113469/4229432/index.html.
5. Линь Д. Правовое регулирование защиты персональных данных и их контроль со стороны государства в Китае / Д. Линь // Политика и общество. 2020. № 2. С. 1-9.
6. Цзя Ш. Административно-правовая защита персональных данных в Китае: проблемы и пути решения / Ш. Цзя // Административное право и процесс. 2020. № 12. С. 64-68.
7. Евсеева А.А. Сравнительный анализ российского и китайского законодательства в области обработки и защиты персональных данных // А.А. Евсеева, И.В. Калуцкий, А.Г. Спеваков // Известия Юго-Западного государственного университета. Серия: Управление, вычислительная техника, информатика. Медицинское приборостроение. 2016. № 3 (20). С. 78-84.
8. Civil Code of the People's Republic of China // The State Council of The People's Republic Of China, URL: http://english.www.gov.cn/archive/lawsregulations/202012/31/content_WS5fedad98c6d0f72576943005.html.
9. Гражданский кодекс Китайской Народной Республики / отв. ред. П. В. Трощинский.- М.: Синосфера, 2020. – 448 с.
10. Cybersecurity Law of the People's Republic of China // PKULaw.com, URL:

https://pkulaw.com/en_law/4dce14765f4265f1bdfb.html.

11. E-Commerce Law of the People's Republic of China // IPkey.eu, URL: https://ipkey.eu/sites/default/files/documents/resources/PRC_E-Commerce_Law.pdf.
12. Wu X. Research on Personal Data Protection in the Guangdong-Hong Kong-Macao Greater Bay Area – Macau: University of Macau, 2020. – 155 p.
13. Ning J. Actively Promoting The Development of the Big Data Industry and Promoting China's Transition from a Big Data Country To A Strong Data Country // World Telecommunications. 2014. Iss. 1. P. 44.
14. Legislation Law of the People's Republic of China (2015 Amendment) // Chinalawtranslate.com, URL: https://www.chinalawtranslate.com/en/2015lawlaw/.
15. Constitution of People's Republic of China (2018 Amendment) // The National People's Congress of the People's Republic of China, URL: http://www.npc.gov.cn/englishnpc/constitution2019/constitution.shtml.
16. Data Security Law of the People's Republic of China // NPCobserver.com, URL: https://npcobserver.com/legislation/data-security-law/.
17. Zhou M. On Personal Data Protection Via Right to be Forgotten / M. Zhou // Journal of Guangxi Administrative Cadre Institute of Politics and Law. 2017. Iss. 2. P. 28
18. Tort Liability Law of the People's Republic of China // The National People's Congress of the People's Republic of China, URL: http://www.npc.gov.cn/zgrdw/englishnpc/Law/2011-02/16/content_1620761.htm.
19. Wang Q. Civil Code: The Guarantee of Civil Rights and the Encyclopedia of Social Life-A New Milestone and Synthesizer of Civil Legislation in China / Q. Wang, L. Li // Contemporary China History Studies. 2020. Iss. 4. P. 18.
20. Personal Information Protection Law of the People's Republic of China (Draft) (Second Review Draft) // digichina.stanford.edu, URL: https://digichina.stanford.edu/news/translation-personal-information-protection-law-peoples-republic-china-draft-second-review.
21. Chen A. A Close Reading of China's Data Security Law, in Effect Sept. 1, 2021 // China Briefing by Dezan Shira & Associates, URL: https://www.china-briefing.com/news/a-close-reading-of-chinas-data-security-law-in-effect-sept-1-2021/
22. Parsons M. China's first personal information protection law in the home stretch / M. Parsons, S. Gong, J. Xie, L. Xu // JD Supra, URL: https://www.jdsupra.com/legalnews/china-s-first-personal-information-1211024/
23. Law of the People's Republic of China on The People's Bank of China // People's Bank of China, URL: http://www.pbc.gov.cn/english/130733/2941519/2015082610501049304.pdf.
24. Law of the People's Republic of China on Commercial Banks // China.org.cn, URL: http://www.china.org.cn/english/DAT/214824.htm.
25. Insurance Law of the People's Republic of China // The National People's Congress of the People's Republic of China, URL: http://www.npc.gov.cn/zgrdw/englishnpc/Law/2011-02/15/content_1620648.htm.
26. Implementation Measures for the Protection of Financial Rights and Interests of Customers // Lawinfochina.com, URL: http://lawinfochina.com/display.aspx?id=34143&lib=law.
27. Chen J. China unveils fintech development plan / J. Chen // Chinadaily.com.cn, URL: http://www.chinadaily.com.cn/a/201908/22/WS5d5e5ed7a310cf3e35567595.html.
28. Personal Information Security Specification Revisions (GB/T 35273-2020) //

Max.book118.com, URL: https://max.book118.com/html/2020/0317/8112141116002102.shtm.
29. Guidance for Personal Information Security Impact Assessment (GB/T 39335-2020) // Max.book118.com, URL: https://max.book118.com/html/2020/1218/7000125131003032.shtm.
30. Personal Financial Information Protection Technical Specification (JR/T 0171-2020) // Chinesestandard.net, URL: https://www.chinesestandard.net/PDF/English.aspx/JRT0171-2020.
31. Guidelines for Data Security Classification (JR/T 0197-2020) // Chinesestandard.net, URL: https://www.chinesestandard.net/PDF.aspx/JRT0197-2020.
32. Measures on the PBOC on the Protection of Financial Consumers' Rights and Interests // People's Bank of China, URL: http://www.pbc.gov.cn/tiaofasi/144941/144957/4099060/index.html.

Результаты процедуры рецензирования статьи

В связи с политикой двойного слепого рецензирования личность рецензента не раскрывается.
Со списком рецензентов издательства можно ознакомиться здесь.

Предмет исследования довольно интересный и посвящен тенденциям совершенствования правового регулирования в финансово-банковском секторе безопасности «…персональных данных в КНР». Методология исследования – ряд методов, правильно используемых автором: «системно-структурный, формально-логический и формально-юридический методы», как представляется еще и исторический, сравнительно-правовой, анализ и синтез. Актуальность обоснована автором во введении к статье и выражается в следующем: «Государство выступает основным гарантом безопасности персональных данных, поэтому совершенствование правового механизма обеспечения безопасности персональных данных в современных условиях является постоянным процессом», «Учитывая лидирующую роль КНР в цифровизации экономики и процессов государственного управления, опыт этого государства очень важен для совершенствования российской правовой системы». Научная новизна хорошо обоснована в исследовании автора. Стиль, структура, содержание заслуживают особого внимания. Стиль работы хороший, она легко читается и носит исследовательский характер. Содержание отражает существо статьи. Исследование имеет все необходимые структурные элементы: актуальность, постановка проблемы, цели и задачи, предмет, научная новизна, методология и выводы. Автор логично подводит читателя к существующей проблеме. Он акцентирует внимание читателя на предмете статьи. Он показывает, опираясь на исследования оппонентов, что «…С 2019 года Китайская Народная Республика реализует масштабный план по регулированию Big Tech» и перечисляет основные направления регулирования, среди которых автомобильная отрасль, «Alibaba Group, LinkDoc и DiDi уже получили предписания и запреты на размещение своих акций на зарубежных биржах», «Особую роль в этом процессе играет Народный банк Китая [3, с. 97], продвигающий жесткий подход к регулированию деятельности FinTech-компаний…». Автор отмечает, что предметом исследования является «…действующее законодательство КНР и проекты нормативно-правовых актов в сфере регулирования отношений по обеспечению безопасности персональных данных в том числе в финансово-банковском секторе». Далее автор переходит к анализу темы, используя ссылки на исследования оппонентов и документы, отмечая при этом, что «…недостаток научных публикаций доказывает необходимость исследования данной темы», «Термином, который используется для

регулирования соответствующих отношений, выступает «личная информация» (personal information) …». Озаботившись проблемами автор отмечает, что в 2020г. принят «… Гражданский кодекс Китайской Народной Республики» в который «была включена Книга четвертая, посвященная правам личности (Personality Rights) и содержащая главу VI «Право на личную жизнь и защита личной информации» (Rights to Privacy and Protection of Personal Information) [8]», а именно «ГК КНР определяет личную информацию …» и делает вывод «Китай проводит полномасштабную работу по актуализации законодательства в сфере защиты персональных данных для снижения торговых барьеров …», «…был утвержден пятилетний план реформирования законодательства КНР с включенным в него отдельным пунктом по персональным данным [12, с. 10]», «В июне 2021 года был издан Закон Китайской Народной Республики о безопасности данных [16], вступление в силу которого было определено довольно быстро – 1 сентября 2021 года». Переходя к анализу вопросов, исследуемых в статье, автор правильно показывает, что необходимо подробнее рассмотреть нормативную базу: «…Конституция КНР прямо не упоминает защиту персональных данных, однако толкование некоторых ее статей позволяет говорить о включении этого института в сферу правового регулирования», «ГК КНР вступил в силу 1 января 2021 года и представлен семью книгами, посвященными общим положениям (General Part), вещным правам (Real Rights), договорам (Contracts), правам личности (Personality Rights), браку и семье (Marriage and Family), наследованию (Succession) и деликтной ответственности (Tort Liability)», «Нормы о защите персональной информации включены в главу 6 «Право на неприкосновенность личной жизни и защиту личной информации» (Chapter VI Rights to Privacy and Protection of Personal Information) Книги четвертой «Права личности» (Book Four Personality Rights)», «На сегодняшний день в КНР действует два закона, касающиеся защиты данных и информации: … о кибербезопасности 2017 года [10] и … о безопасности данных [16]. На рассмотрении находится вторая редакция проекта закона о защите личной информации [20]». При этом автор подробно останавливается на положениях этих законов и отмечает, среди прочего, «…новеллой закона о защите данных является введение термина «важные данные», определяемого как данные, связанные с национальной безопасностью, состоянием национальной экономики, жизнедеятельностью важных государственных лиц и общественными интересами», «в отношении персональных данных необходимо придерживаться норм социальной морали и этики…», «Для трансграничной передачи важных данных, собираемых и производимых в процессе работы операторами данных на территории КНР, статья 31 предусматривает, что меры по проверке безопасности должны быть согласованы Администрацией киберпространства КНР с соответствующими ведомствами при Государственном совете», делает вывод: «Нарушение порядка предоставления данных иностранным судебным или правоохранительным органам без разрешения компетентных органов Китая влечет за собой штраф… с одновременным изданием предписания о приостановлении деятельности компании до устранения нарушений и отзывом лицензий и разрешений». Автор замечает: законопроект «PIPL устанавливает более высокие стандарты обработки личной информации несовершеннолетних …» и делает правильный вывод: «…если обработчик данных не смог доказать отсутствие своей вины, он несет гражданско-правовую ответственность за деликт». Примеры подкрепляются ссылками на источники и осуществляется переход к основной теме исследования: «В финансово-банковском секторе личная информация является едва ли не самым важным активом как инвесторов, так и финансовых учреждений», «…в Законе Китайской Народной Республики о Народном банке Китайской Народной Республики [23], так и в законах о коммерческих банках [24] и страховании [25] есть нормы, касающиеся защиты личных финансовых данных» и автор подробно их анализирует. В качестве примера автор

приводит «…Государственная администрация регулирования рынков (State Administration of Market Regulation, SAMR) в лице своего специального подразделения - Администрации стандартизации Китая (Standardisation Administration of China) разработала ряд руководств, призванных регулировать отношения в сфере защиты личной информации в финансово-банковском секторе…», «…роль финансового регулятора (Народного банка Китая) в установлении стандартов защиты персональных данных». В заключение автор подводит итог: «Законодательство Китая о персональных данных разрабатывается на основе «согласие-ориентированного» подхода, при котором согласие вместе с ограниченным перечнем исключений является законным основанием для обработки личной информации» и приводит свои доводы, вытекающие из исследования, в частности «Процесс разработки механизма защиты персональных данных находится в стадии завершения …» и «…К концу 2021 года ожидается принятие ключевого закона - о защите личной информации …», «В финансово-банковском секторе уже действует ряд подзаконных нормативно-правовых актов, устанавливающих жесткие стандарты обеспечения безопасности личной информации. Ведущую роль в этом механизме играет финансовый регулятор - Народный банк КНР». Как нам кажется, приведены конкретные, однозначные и дающие для практики и теории выводы. Необходимо констатировать, что журнал, в который представлена статья является научным, и автор направил в издательство статью, соответствующую требованиям, предъявляемым к научным публикациям, в частности для научной полемики он обращается к текстам научных работ российских и зарубежных (китайских) исследователей. Библиография достаточная и содержит определенное количество как современных научных исследований, так и ссылки на НПА и другие документы, к которым автор обращается. Это позволяет автору правильно определить проблемы и поставить их на обсуждение. Он, исследовав их, раскрывает предмет статьи. К замечаниям можно отнести некоторое отступление от заявленной темы (скорее ее расширение за счет подробного анализа всей сферы безопасности «…персональных данных в КНР). Апелляция к оппонентам в связи с вышесказанным присутствует. Автором используется материал других исследователей. Выводы – работа заслуживает опубликования, интерес читательской аудитории будет присутствовать.