ЗАРУБЕЖНЫЙ ОПЫТ

DOI: 10.17803/1994-1471.2022.138.5.196-206

А. С. Озерова*

Уголовно-правовая защита личной информации в Китае в условиях построения системы социального кредитования

Аннотация. В статье проводится анализ норм уголовного законодательства, в которых закреплена охрана личной информации в КНР. Исследуются тенденции правоприменительной практики по уголовным делам, предметом которых выступают личные данные. Повышенная уголовно-правовая охрана личной информации граждан Китая обусловлена появлением системы социального кредитования. В статье рассматриваются особенности функционирования системы социального кредитования, а также влияние указанной системы на права и свободы личности в условиях цифровизации. Интерес к рассматриваемой системе обусловлен значительным влиянием, которое оказывает КНР на формирование правовой культуры других стран. Автор приходит к выводу, что значительная степень вторжения государства в сферу частного пространства граждан коррелирует с эффективными мерами защиты личной информации. На примере Китая мы видим стремление государства защитить личные данные граждан, в том числе с помощью уголовно-правовых средств. При этом случаи правоприменения становятся все более распространенными, особенно в уголовном праве.

Ключевые слова: система социального кредитования; конфиденциальность; идентификация; личная информация; идентифицирующая информация; незаконная продажа личных данных; кража личных данных; частная жизнь; неприкосновенность частной жизни; социальный рейтинг; черный список.

Для цитирования: *Озерова А. С.* Уголовно-правовая защита личной информации в Китае в условиях построения системы социального кредитования // Актуальные проблемы российского права. — 2022. — Т. 17. — № 5. — С. 196–206. — DOI: 10.17803/1994-1471.2022.138.5.196-206.

* *Озерова Анна Сергеевна*, аспирант кафедры уголовного права и криминологии Московского государственного университета имени М.В.Ломоносова
Ленинские горы, д. 1, стр. 13 (4-й учебный корпус), г. Москва, Россия, 119991
annaozerova55@mail.ru

Criminal Law Protection of Personal Information in China in the context of Social Credit System Formation

Anna S. Ozerova, Postgraduate Student, Department of Criminal Law and Criminology, Lomonosov Moscow State University
Leninskie Gory, d. 1, str. 13 (4th uchebnyy korpus), Moscow, Russia, 119991
annaozerova55@mail.ru

Abstract. The paper analyzes the norms of criminal law, which enshrined the protection of personal information in the PRC. The tendencies of law enforcement practice in criminal cases, the subject of which are personal data, are being studied. Increased criminal law protection of personal information of Chinese citizens is due to the emergence of a social credit system. The paper discusses the features of the functioning of the social credit system, as well as the impact of this system on the rights and freedoms of the individual in the context of digitalization. Interest in the system under consideration is due to the significant influence exerted by the PRC on the formation of the legal culture of other countries. The author concludes that a significant degree of state intrusion into the private space of citizens correlates with effective measures to protect personal information. The Chinese case shows the desire of the state to protect the personal data of citizens, including through criminal law means. At the same time, cases of law enforcement are becoming more common, especially in criminal law.

Keywords: social credit system; confidentiality; identification; personal information; identifying information; illegal sale of personal data; identity theft; private life; privacy; social rating; black list.
Cite as: Ozerova AS. Ugolovno-pravovaya zashchita lichnoy informatsii v Kitae v usloviyakh postroeniya sistemy sotsialnogo kreditovaniya [Criminal Law Protection of Personal Information in China in the context of Social Credit System Formation]. *Aktual'nye problemy rossijskogo prava*. 2022;17(5):196-206. DOI: 10.17803/1994-1471.2022.138.5.196-206. (In Russ., abstract in Eng.).

Уголовный кодекс Китайской Народной Республики, принятый в 1997 г., изначально не предусматривал норм, в которых бы устанавливалась защита личных данных. В 2009 г. впервые в гл. 4 «Преступления против прав личности, демократических прав граждан» УК КНР был включен состав преступления «продажа или незаконное предоставление личных данных»[1]. Постоянный комитет Одиннадцатого Всекитайского собрания народных представителей принял седьмую поправку к Уголовному закону, предусмотрев ст. 253 (а) УК КНР. Указанная поправка стала наиболее широко используемым правовым инструментом для обеспечения защиты частной жизни в Китае[2].

В китайской правовой доктрине положительно оцениваются изменения уголовного законодательства 2009 г. о защите личной информации. В частности, указывается, что «седьмая поправка к Уголовному закону расширяет защиту личной информации в Китае. На данный момент — это единственный закон, предусматривающий защиту личной информации. В других законах обычно упоминается необходимость защиты частной жизни в очень общих чертах и попутно (одной фразой или одним предложением) или же они направлены на защиту определенных категорий данных»[3].

В редакции 2009 г. ст. 253 (а) УК КНР предусматривала уголовную ответственность за

[1] URL: http://www.gov.cn/flfg/2009-02/28/content_1246438.htm (дата обращения: 25.05.2021).

[2] *De Hert P.*, *Papakonstantinou V.* The Data Protection Regime in China. In-Depth Analysis // Brussels Privacy Hub Working Paper. 2015. Vol. 1, № 4. P. 15.

[3] *Wu Y*. Personal data protection in e-government: Globalization or glocalization? A comparative study of the United States, Germany and China, 2010 // URL: https://www-proquest-com.proxylibrary.hse.ru/dissertations-theses/personal-data-protection-e-government/docview/746090959/se-2?accountid=45451 (дата обращения: 25.05.2021).

незаконную продажу или незаконное предоставление личной информации граждан, полученной в ходе выполнения обязанностей или оказания услуг, государственными служащими или сотрудниками финансовых телекоммуникационных, транспортных, образовательных, медицинских и других учреждений, а также за кражу или иным способом незаконное получение вышеуказанной информации.

В связи с тем что законодательное определение категории «личная информация» было дано только в 2017 г. в Законе о кибербезопасности[4], это порождало множество доктринальных споров, а также практических вопросов относительно содержания указанной категории.

В частности, не существовало единого мнения о том, тождественно ли содержание понятий «личная информация» и «конфиденциальная информация». Профессор Чжао Бинчжи указывает[5], что личная общедоступная информация также может выступать объектом уголовно-правовой охраны в соответствии со ст. 253 (а) УК КНР. «Несмотря на то что некоторая личная информация может иметь общедоступный характер, она все равно должна подпадать под действие уголовного закона. Вред от утечки информации состоит в том, что виновное лицо, незаконно использующее личную информацию, может исключить потерпевшего из множества социальных отношений, “заблокировав” его. Уголовно-правовая защита личной информации — это не только защита частной жизни, но, что более важно, защита общественного порядка от возможного вреда из-за утечки информации»[6].

В 2016 г. в Шанхайском суде было проведено научно-практическое исследование, предметом которого стала личная информация. При анализе 125 уголовных дел о незаконном использовании личной информации были сделаны следующие выводы[7].

1. Суды, сложно и разнообразно определяя личную информацию граждан, охватывают почти все аспекты частной жизни. Так, в качестве личной информации суды расценивали следующие виды сведений: 1) идентификационная информация, в том числе имя, номер телефона, адрес, информация о членах семьи, информация о мобильной регистрации; 2) информация об имуществе, в том числе о банковских счетах, о транспортном средстве, недвижимости и финансовых транзакциях; 3) информация о местонахождении лица, в том числе о размещении в отеле, об авиаперелетах, о парковочном месте; 4) информация об образовании, 5) детализация звонков, 6) информация о сделках и иные виды информации.

2. Множество концепций личной информации, сложившихся в правовой доктрине Китая, можно представить в виде: а) теории ассоциации; б) теории конфиденциальности и в) теории идентификации.

Теория ассоциации рассматривает личную информацию в широком смысле – это любая информация, по какой-либо причине связанная с человеком. Указанная концепция охватывает все виды социальных отношений и включает наиболее широкий объем сведений в содержании понятия «личная информация». Например, информация об автомобиле или любом другом имуществе, принадлежащем лицу.

Теория конфиденциальности определяет личную информацию как сведения конфиденциального характера, которые лицо не желает распространять. Например, для большинства членов общества собственные биометрические

[4] Согласно ст. 76 указанного закона под термином «личная информация» понимается различная информация, записанная в электронном виде или другими способами, которая может идентифицировать личность физического лица отдельно или в сочетании с другими сведениями, включая, помимо прочего, имя физического лица, дату рождения, идентификационный номер, биометрическую информацию, адрес проживания, номер телефона и т.д. См.: URL: http://www.npc.gov.cn/wxzl/gongbao/2017-02/20/content_2007531.htm (дата обращения: 17.06.2021).

[5] URL: http://www.fxcxw.org.cn/dyna/content.php?id=6785 (дата обращения: 25.05.2021).

[6] URL: http://shfy.chinacourt.gov.cn/article/detail/2016/07/id/2001638.shtml (дата обращения: 17.06.2021).

[7] URL: http://shfy.chinacourt.gov.cn/article/detail/2016/07/id/2001638.shtml (дата обращения: 17.06.2021).

данные, такие как рост или вес, не являются секретными сведениями. Однако некоторые люди стремятся сохранить указанную информацию в тайне.

В связи с тем, что некоторые люди считают определенную информацию конфиденциальной, а другие не возражают против ее раскрытия, критерий «конфиденциальность» не может лежать в основе определения личной информации.

Теория идентификации относит к личной информации граждан сведения, которые идентифицируют личность гражданина, такие как имя, род занятий и профессия, должность, возраст, семейное положение, образование и др. Следовательно, использование концепции идентификации отражает наиболее адекватный (с точки зрения уголовно-правовой защиты личной информации) объем указанной категории.

3. Личные данные, прямо или косвенно идентифицирующие лицо, различаются между собой по степени идентификации. В связи с этим не любая такая информация в отдельности (назовем это условно «единица информации», например, 10 фамилий граждан представляют собой 10 единиц личной информации; один домашний адрес лица — 1 единица информации) может выступать предметом уголовно-правовой охраны. Так, можно выделить следующие группы идентифицирующей информации:

а) информация, которая является уникальной для конкретного лица (например, идентификационный номер и биометрические данные). Посредством одной единицы такой информации возможна безошибочная идентификация физического лица. Очевидно, что указанный вид информации имеет наивысшую степень идентификации;

б) информация, принадлежащая конкретному лицу, однако имеющая свойство дублироваться и повторяться. Например, имя, номер телефона, сведения о транзакциях. Этот вид информации имеет высокую эффективность идентификации, но он не может безошибочно определить конкретное лицо из-за возможности повторения. Например, посредством имени и номера телефона можно идентифицировать лицо в пределах определенного района. Но когда диапазон поиска увеличивается, эффективность такой информации будет значительно снижена. Следовательно, отдельные единицы такой информации не подлежат уголовно-правовой охране, в связи с тем что отсутствует точная идентификация лица.

Судебная практика показывает, что сочетание имени и номера телефона является минимальным требованием для наделения информации статусом охраняемой законом личной информации;

в) информация, которая характеризует личность как члена тех или иных социальных групп. Например, возраст, род занятий, образование и т.д. Идентификационная эффективность указанного вида информации является самой низкой. Следовательно, даже если рассматриваемая категория информации объединяет множество сведений, сама по себе она не может соответствовать стандарту идентифицируемости.

Традиционно уголовно-правовая доктрина Китая основывается на теории четырехэлементного состава преступления[8]. В связи с этим представляется обоснованным рассмотрение объективных и субъективных признаков преступления против личной информации.

Глава 4 «Преступления против прав личности и демократических прав граждан» УК КНР, в которой установлен состав рассматриваемого преступления, указывает на то, что преступление против личной информации прежде всего наносит ущерб правам личности. Представляется верной позиция, согласно которой непосредственным объектом рассматриваемого преступления является право на безопасность личной информации отдельных граждан[9]. Указанное

[8] *Лун Ч.* Состав преступления в уголовно-правовой доктрине Китая // Lex russica (Русский закон). 2016. № 9. С. 129–135.

[9] URL: http://www.fxcxw.org.cn/dyna/content.php?id=6785 (дата обращения: 20.06.2021) ; http://shfy.chinacourt.gov.cn/article/detail/2016/07/id/2001638.shtml (дата обращения: 20.06.2021).

право выступает элементом права на неприкосновенность частной жизни. Согласно ст. 1034 Гражданского кодекса Китая[10] положения о праве на неприкосновенность частной жизни применяются в отношении личной информации. Несмотря на то что целью защиты личной информации выступает в том числе предотвращение дальнейших преступлений и нарушений прав граждан, вызванных утечкой информации, «личные интересы имеют приоритет над общественно-правовыми интересами в преступлениях против личной информации»[11].

Объективная сторона преступления, предусмотренного ст. 253 (а) УК КНР, характеризуется следующими альтернативными действиями: 1) продажа или незаконное предоставление личной информации, а также 2) кража или иные способы незаконного получения личной информации.

Согласно официальному судебному толкованию[12], к незаконному предоставлению личной информации относятся любые случаи ее распространения в отсутствие согласия субъекта данных. Кроме того, под предоставлением информации понимается распространение такой информации в сети Интернет.

Немного забегая вперед, отметим, что в 2015 г. девятая поправка к УК КНР исключила слово «незаконное» в отношении продажи или предоставления информации. Отмечается, что продажа или предоставление личной информации в отсутствие законного основания и (или) согласия субъекта данных незаконны по своей сути. Соответственно, термин «незаконное» не относится к способам или каким-либо иным обстоятельствам продажи личной информации[13].

Под иными способами (за исключением кражи) незаконного получения личной информации понимаются ее покупка, безвозмездное получение, обмен, а также сбор личной информации, например, в процессе оказания услуг.

Субъектом рассматриваемого преступного посягательства в редакции 2009 г. ст. 253 (а) УК КНР могли выступать отдельные физические лица; государственные служащие или сотрудники финансовых телекоммуникационных, транспортных, образовательных, медицинских и других учреждений, а также юридические лица, занятые в названных отраслях. Субъективная сторона рассматриваемого преступления характеризуется умышленной формой вины.

Первое уголовное дело[14] по ст. 253 (а) УК КНР было возбуждено в 2009 г. в отношении обвиняемого Х. из Чжухая, который незаконно приобрел журнал телефонных звонков должностных лиц местных органов власти, а затем продал его мошенникам. Последние, выдавая себя по телефону за должностных лиц, якобы попавших в «чрезвычайную ситуацию», получали денежные переводы от друзей или родственников потерпевших. Х. был приговорен к 18 месяцам тюремного заключения и оштрафован.

Содержание ст. 253 (а) УК КНР в редакции 2009 г. характеризовалось неопределенностью, которая стала причиной дальнейшего совершенствования нормы.

Во-первых, как уже было указано выше, на момент введения рассматриваемого состава преступления отсутствовало точное понимание объема охраны личной информации граждан.

Во-вторых, проблемы в правоприменительной практике вызывал открытый перечень сфер деятельности корпораций, которые могли подпадать под действие уголовного запрета («государственные, финансовые, телекоммуникационные, транспортные, образовательные и медицинские учреждения и т.д.»). Отсутствовало понимание того, должен ли этот

[10] URL: http://www.npc.gov.cn/npc/c30834/202006/75ba6483b8344591abd07917e1d25cc8.shtml (дата обращения: 25.05.2021).

[11] URL: https://www.spp.gov.cn/spp/ztk/dfld/202010/t20201026_486720.shtml (дата обращения: 25.05.2021).

[12] URL: http://www.court.gov.cn/fabu-xiangqing-43942.html (дата обращения: 20.06.2021).

[13] URL: https://www.spp.gov.cn/llyj/201607/t20160713_140194.shtml (дата обращения: 20.06.2021).

[14] *Greenleaf G.* Asian Data Privacy Laws — Trade and Human Rights Perspectives. Oxford University Press, 2014. P. 199.

перечень включать только перечисленные сферы деятельности юридических лиц или в него должны включаться и другие виды учреждений, предоставляющие услуги населению? Китайский правовед Чжоу Ханьхуа в связи с этим указывает[15], что в судебной практике различных регионов понимание исследуемого преступления было неоднородным. В некоторых регионах использовалось толкование, в соответствии с которым предмет ограничивался исключительно сферами деятельности, перечисленными в статье. Это, безусловно, ограничивало защиту личной информации. При этом в судебной практике встречался и противоположный подход[16], распространяющий сферу действия ст. 253 (а) УК КНР на прямо не поименованные в статье сферы деятельности компаний (например, экспресс-доставка).

Таким образом, несовершенство редакции ст. 253 (а) УК КНР порождало необходимость в ее уточнении. Неопределенность уголовно-правового запрета негативно влияла на единообразие судебной практики, а также создавала квалификационные проблемы.

В следующем деле проблема определения сфер деятельности компаний, подпадающих под действие уголовно-правового запрета, стала причиной неточной квалификации преступного деяния. Так, Питер Хамфри и его жена были осуждены по ст. 253 (а) УК КНР[17]. Питер возглавлял компанию ChinaWhys Co, которая специализировалась на предоставлении консультационных услуг. В июле 2013 г. полиция задержала супругов, а затем обвинила их в незаконном получении личной информации. Как утверждалось, супруги приобрели у маркетинговых компаний личную информацию, которая впоследствии была предоставлена их клиентам в виде подготовленных для них отчетов. Сведения включали 256 единиц личной информации (800–2 000 юаней за запись), включая информацию о хукоу (разрешение на проживание), перемещениях и местонахождении.

Супруги были признаны виновными в незаконном получении личной информации. Отсутствие в обвинении «незаконного предоставления или продажи» объясняется как раз неточностью закона. Так, маркетинговые компании выходили за рамки отраслей, охватываемых ст. 253 (а) в редакции 2009 г.

Питер Хамфри приговорен к двум с половиной годам лишения свободы и штрафу в размере 200 000 юаней (около 32 000 долл. США). Его жена Юй Инцзэн была приговорена к двум годам лишения свободы и штрафу в размере 150 000 юаней (24 000 долл. США).

1 ноября 2015 г. вступила в силу девятая поправка к УК КНР[18], усиливающая защиту личной информации. Во-первых, сфера действия уголовно-правового запрета была распространена на все сферы государственных и частных учреждений (как было указано выше, рассматриваемая статья в редакции 2009 г. определяла перечень сфер деятельности корпораций, в отношении которых устанавливалась уголовная ответственность). Во-вторых, поправка увеличила максимальное наказание до семи лет лишения свободы в случае, если обстоятельства совершения преступления являются «особо серьезными».

Так, ст. 253-1 УК КНР в редакции 2015 г. установила уголовную ответственность за незаконную продажу или предоставление третьим лицам личной информации граждан, полученную в процессе исполнения обязанностей или оказания услуг, и кражу или получение иным незаконным путем личной информации граждан.

Указанные выше деяния образуют состав преступления при наличии «серьезных обстоятельств» и наказываются лишением свободы на срок до 3 лет либо арестом, либо штрафом (в качестве дополнительного или основного

[15] URL: http://www.chinanews.com/gn/2015/08-31/7497951.shtml (дата обращения: 25.05.2021).

[16] *Livingston S.*, *Greenleaf G.* China Whys and Wherefores — Illegal Provision and Obtaining of Personal Information Under Chinese Law, 2014 // URL: https://ssrn.com/abstract=2541570 (дата обращения: 25.05.2021).

[17] *Livingston S.*, *Greenleaf G.* Op. cit. P. 1.

[18] URL: https://www.spp.gov.cn/spp/fl/201802/t20180205_364562.shtml (дата обращения: 25.05.2021).

наказания). При наличии «особо серьезных обстоятельств» наказание в виде лишения свободы может быть назначено на срок до 7 лет[19].

Согласно ст. 30 УК КНР, субъектом уголовной ответственности выступают корпорации[20]. В связи с этим если вышеуказанные преступления совершены корпорацией, то в качестве наказания назначается штраф, а физические лица, непосредственно ответственные за совершение деяний, наказываются самостоятельно в пределах санкции, установленной статьей.

Важным событием в сфере уголовно-правовой защиты личной информации стало обнародование 9 мая 2017 г. Верховным народным судом и Верховной народной прокуратурой Китая совместных разъяснений[21] по вопросам применения закона при рассмотрении уголовных дел, касающихся неправомерного использования личной информации граждан.

В статье 1 разъяснений указывается, что личная информация граждан – это сведения, представленные в электронном или ином формате, посредством которых физическое лицо может быть идентифицировано непосредственно или посредством которых лицо может быть идентифицировано в сочетании с иной информацией. В частности, имя, номер документа, удостоверяющего личность, контактная информация, адрес, пароль учетной записи, имущественное положение, местонахождение и т.д. Как видно из представленного определения, высшие государственные органы КНР избрали достаточно широкий подход к толкованию личных данных.

Под «серьезными обстоятельствами», при наличии которых имеется состав преступления, понимаются в том числе следующие[22]:

1) предоставление личной информации в целях осуществления преступной деятельности третьими лицами;
2) незаконное получение или предоставление более 50 единиц личной информации о местонахождении, кредитной информации или собственности потерпевшего;
3) незаконное получение или предоставление более 500 единиц личной информации (например, информация о месте проживания, состоянии здоровья, транзакциях и т.д.);
4) незаконное получение или предоставление более 5 000 единиц личной информации, которые не подпадают под указанные выше критерии;
5) незаконный доход от продажи или предоставления личной информации превышает 5 000 юаней;
6) продажа или предоставление личной информации, полученной при исполнении служебных обязанностей или оказании общественных услуг, количество единиц которой превышает половину верхнего предела, указанного в п. 2–4;
7) повторное в течение двух лет привлечение лица, подвергшегося административной ответственности или уголовному наказанию за нарушение правового режима личной информации граждан.

Исследователь в области защиты данных Ян Фэн указывает, что примечательной особенностью защиты личной информации уголовным законодательством Китая являются низкие пороги криминализации неправомерного использования личных данных. Так, согласно судебному толкованию «серьезное обстоятельство», при котором выполняется состав преступления, представляет собой незаконное получение или предоставление более 50 единиц личной информации. Это данные о местонахождении, кредитной информации или собственности потерпевшего. Для менее важных данных, с

[19] *Lotus R.* Diminishing Rights: China's Data Laws and Regulations. Australian Strategic Policy Institute, 2018. P. 7–9.

[20] Согласно ст. 30 УК КНР компании, предприятия, организации, учреждения, коллективы, осуществляющие опасную для общества деятельность, исходя из положений, установленных УК КНР для преступлений, совершаемых организациями или учреждениями, должны нести уголовную ответственность.

[21] URL: http://www.court.gov.cn/fabu-xiangqing-43942.html (дата обращения: 25.05.2021).

[22] Необходимо отметить, что перечень таких обстоятельств является открытым и их определение оставляется на усмотрение суда.

точки зрения китайского законодателя, таких как сведения о месте проживания, состоянии здоровья и финансовых транзакциях, определен повышенный минимальный объем, необходимый для привлечения к уголовной ответственности, — 500 единиц. Для других личных данных минимальное количество определено в размере 5 000 единиц. Если правонарушитель является сотрудником государственного учреждения или предоставляет общественные услуги, порог еще ниже. Для них минимальный объем данных составляет половину указанного минимального количества[23].

Согласно разъяснениям, обстоятельства считаются «особо серьезными» в следующих случаях:

1) причинение тяжких последствий, таких как смерть, тяжкий вред здоровью, психическое расстройство или похищение жертвы;
2) причинение крупного имущественного ущерба или неблагоприятных социальных последствий;
3) количество единиц личной информации превышает более чем в десять раз значение любого из пороговых значений, предусмотренных для серьезных обстоятельств;
4) иные ситуации, когда обстоятельства особенно серьезны.

Согласно ст. 11 разъяснений, в случае незаконного получения, а затем продажи личных данных гражданина количество единиц такой информации не учитывается дважды. Однако если одна и та же личная информация продается различным корпорациям или физическим лицам, то количество единиц такой информации рассчитывается кумулятивно.

Суд назначает наказание с учетом размера ущерба, причиненного преступлением, размера незаконного дохода, полученного в результате совершения преступления, наличия судимости обвиняемого, наличия раскаяния и других обстоятельств.

Таким образом, можно заметить, что в настоящее время Китай предпринимает все больше усилий для защиты личной информации граждан, в том числе устанавливая достаточно строгие санкции за преступные посягательства на личную информацию.

Так, например, в 2016 г. Чжоу Биньчэн приобрел более 1,93 млн единиц личной информации студентов. Позже он продал указанную информацию за 65 400 юаней. Народный суд города Пинху, принимая во внимание явку с повинной, приговорил Чжоу Биньчэн к лишению свободы на один год и 11 месяцев, а также к штрафу в размере 40 000 юаней. Лица, которые покупали личные данные студентов, также были приговорены к лишению свободы и штрафу[24].

В другом деле Ся Фусяо[25] продал личные данные об онлайн-покупках, содержащие имена граждан, адреса доставки, номера мобильных телефонов и иные сведения. Виновный получил незаконную прибыль в размере около 50 000 юаней. Народный суд города Шаосин приговорил Ся Фусяо к лишению свободы на два года и штрафу в размере 2 000 юаней.

Согласно статистике Министерства общественной безопасности КНР, в 2020 г. было зарегистрировано более 3 100 уголовных дел о посягательстве на личную информацию граждан[26].

Исходя из анализа законодательства КНР и практики применения ст. 253-1 УК КНР, можно сделать вывод о сложившемся подходе к предоставлению уголовно-правовой охраны личной информации граждан. При этом представляется, что причины возникновения указанного подхода обусловлены появлением системы социального кредитования (далее — СКС), которая массово аккумулирует личные данные граждан. На основании полученных данных поведение граждан либо поощряется, либо порицается с применением ограничений. Официально заявлено о начале работы системы социального кредитования в 2014 г. в «Плане строительства

[23] *Feng Y.* The future of china's personal data protection law: Challenges and prospects // Asia Pacific Law Review. 2019. Vol. 27, № 1. P. 62–82.

[24] URL: http://www.court.gov.cn/zixun-xiangqing-43952.html (дата обращения: 25.05.2021).

[25] URL: https://www.chinacourt.org/article/detail/2017/05/id/2852398.shtml (дата обращения: 25.05.2021).

[26] URL: http://www.gov.cn/xinwen/2020-12/30/content_5575322.htm (дата обращения: 25.05.2021).

Системы социального кредитования на 2014–2020 годы»[27].

СКС имеет некоторое сходство с кредитными рейтингами, существующими в других странах, но позволяет получить информацию, касающуюся практически всех сфер жизни китайских граждан. «Система направлена на оценку “надежности” в соблюдении правовых и моральных норм, профессиональных и этических стандартов»[28].

В отсутствие единого законодательного определения термина «социальный кредит»[29] существует множество доктринальных подходов к его толкованию. Гу Минканг, правовед из Сянтаньского университета, указывает[30], что в широком смысле социальный кредит означает объективную способность и субъективную готовность гражданина выполнять социальные обязательства.

В рамках СКС органы государственной власти и частные компании обмениваются кредитной информацией о нарушителях. Механизм такого взаимодействия, а также ряд последствий за нарушения (ограничение на выезд из страны, покупку недвижимости, проезд на высокоскоростных поездах, проживание в отеле выше стандартного класса) установлен в 2016 г. Государственным советом КНР в постановлении «О совместной дисциплинарной системе»[31] (так называемый механизм совместного наказания).

Сущность механизма совместного наказания заключается в том, что гражданам, нарушившим доверие в сфере деятельности одного ведомства и занесенным в соответствующий черный список, отказывают в услугах другие органы или компании. Результатом такого партнерства, например, стало то, что к началу 2017 г. 6,15 млн граждан были лишены возможности покупать авиабилеты. В результате занесения в черный список у нарушителей не только отменялись деловые сделки, но и распадались браки вследствие разрушения репутации[32].

Не давая оценки складывающейся в Китае системе социального кредитования, подчеркнем, что личные данные граждан являются объектом пристального внимания общественности и государства. Решение о включении

---

[27] URL: http://www.gov.cn/zhengce/content/2014-06/27/content_8913.htm (дата обращения: 25.05.2021). 14 июня 2014 г. Госсовет выпустил «Уведомление Госсовета о выпуске Плана строительства системы социального кредитования (2014–2020 гг.)». По сравнению с документом Госсовета 2007 г. документ 2014 г. дает более детальную картину построения единой системы социального кредитования. Необходимо отметить, что до 2014 г. пилотные программы социального кредитования реализовывались в Китае на региональном уровне. Например, в 2010 г. был проведен эксперимент «массового кредитования», который измерял и оценивал индивидуальное поведение. Первоначально гражданам было выдано 1 000 кредитных баллов, которые могли быть списаны за нарушение определенных правовых, административных и моральных норм. Например, вождение в нетрезвом виде стоило 50 баллов, рождение ребенка без разрешения на планирование семьи стоило 35 баллов, а невозврат ссуды — от 30 до 50 баллов. Утраченные баллы могли быть восстановлены по прошествии времени: от двух до пяти лет, в зависимости от нарушенного правила и серьезности нарушения. На основе полученных баллов граждане были разделены на категории от A до D. См. подробнее: *Creemers R.* China’s Social Credit System: An Evolving Practice of Control. P. 10. URL: https://ssrn.com/abstract=3175792 (дата обращения: 25.05.2021).

[28] *Chen Y.*, *Cheung A.* The Transparent Self Under Big Data Profiling: Privacy and Chinese Legislation on the Social Credit System // The Journal of Comparative Law. 2017. Vol. 12, № 2. P. 356.

[29] *Drinhausen K.*, *Brussee V.* China’s Social Credit System in 2021: From fragmentation towards integration, 2021 // URL: https://merics.org/en/report/chinas-social-credit-system-2021-fragmentation-towards-integration (дата обращения: 25.05.2021).

[30] URL: https://www.creditchina.gov.cn/home/lfyj/202012/t20201208_219709.html (дата обращения: 25.05.2021).

[31] URL: http://www.gov.cn/zhengce/content/2016-06/12/content_5081222.htm (дата обращения: 25.05.2021).

[32] *Chen Y.*, *Cheung A.* The Transparent Self Under Big Data Profiling: Privacy and Chinese Legislation on the Social Credit System // The Journal of Comparative Law. 2017. Vol. 12, No 2. P. 366–367.

гражданина в черный список принимается государственными органами на основании личной информации, что влечет за собой ряд негативных ограничений. Представляется, что именно эти тенденции побудили законодателя уделить повышенное внимание защите личных данных, в том числе уголовно-правовыми средствами.

Таким образом, можно сделать вывод, что повышенная уголовно-правовая охрана личной информации граждан Китая обусловлена появлением системы социального кредитования. Указанная система предполагает аккумулирование из государственного и частного секторов информации, касающейся всех сфер жизни китайских граждан. Значительная степень вторжения государства в частное пространство граждан коррелирует с эффективными мерами защиты личной информации. На примере Китая мы видим стремление государства защитить личные данные граждан, в том числе с помощью уголовно-правовых средств.

БИБЛИОГРАФИЯ

1. *Лун Ч.* Состав преступления в уголовно-правовой доктрине Китая // Lex russica (Русский закон). — 2016. — № 9. — С. 129–135.
2. *Chen Y.*, *Cheung A.* The Transparent Self Under Big Data Profiling: Privacy and Chinese Legislation on the Social Credit System // The Journal of Comparative Law. — 2017. — Vol. 12. — № 2. — P. 356–378.
3. *De Hert P.*, *Papakonstantinou V.* The Data Protection Regime in China. In-Depth Analysis // Brussels Privacy Hub Working Paper. — 2015. — Vol. 1. — № 4.
4. *Drinhausen K.*, *Brussee V.* China's Social Credit System in 2021: From fragmentation towards integration — 2021 // URL: https://merics.org/en/report/chinas-social-credit-system-2021-fragmentation-towards-integration (дата обращения: 25.05.2021).
5. *Feng Y.* The future of china's personal data protection law: Challenges and prospects // Asia Pacific Law Abstract. — 2019. — Vol. 27. — № 1. — P. 62–82.
6. *Greenleaf G.* Asian Data Privacy Laws — Trade and Human Rights Perspectives. — Oxford University Press, 2014. — 624 p.
7. *Livingston S.*, *Greenleaf G.* China Whys and Wherefores — Illegal Provision and Obtaining of Personal Information Under Chinese Law // URL: https://ssrn.com/abstract=2541570 (дата обращения: 25.05.2021).
8. *Lotus R.* Diminishing Rights: China's Data Laws and Regulations. — Australian Strategic Policy Institute, 2018. — 20 p.
9. *Sithigh D. M.*, *Siems M.* The Chinese social credit system: a model for other countries? // Modern Law Abstract. — 2019. — Vol. 82. — № 6. — P. 1034–1071.
10. *Wu Y.* Personal data protection in e-government: Globalization or localization? A comparative study of the United States, Germany and China. — 2010. — 216 p.

Материал поступил в редакцию 7 сентября 2021 г.

REFERENCES (TRANSLITERATION)

1. Lun Ch. Sostav prestupleniya v ugolovno-pravovoj doktrine Kitaya // Lex russica (Russkij zakon). — 2016. — № 9. — S. 129–135.
2. Chen Y., Cheung A. The Transparent Self Under Big Data Profiling: Privacy and Chinese Legislation on the Social Credit System // The Journal of Comparative Law. — 2017. — Vol. 12. — № 2. — P. 356–378.
3. De Hert P., Papakonstantinou V. The Data Protection Regime in China. In-Depth Analysis // Brussels Privacy Hub Working Paper. — 2015. — Vol. 1. — № 4.

4. Drinhausen K., Brussee V. China's Social Credit System in 2021: From fragmentation towards integration — 2021 // URL: https://merics.org/en/report/chinas-social-credit-system-2021-fragmentation-towards-integration (data obrashcheniya: 25.05.2021).
5. Feng Y. The future of china's personal data protection law: Challenges and prospects // Asia Pacific Law Abstract. — 2019. — Vol. 27. — № 1. — P. 62–82.
6. Greenleaf G. Asian Data Privacy Laws — Trade and Human Rights Perspectives. — Oxford University Press, 2014. — 624 p.
7. Livingston S., Greenleaf G. China Whys and Wherefores — Illegal Provision and Obtaining of Personal Information Under Chinese Law // URL: https://ssrn.com/abstract=2541570 (data obrashcheniya: 25.05.2021).
8. Lotus R. Diminishing Rights: China's Data Laws and Regulations. — Australian Strategic Policy Institute, 2018. — 20 p.
9. Sithigh D. M., Siems M. The Chinese social credit system: a model for other countries? // Modern Law Abstract. — 2019. — Vol. 82. — № 6. — P. 1034–1071.
10. Wu Y. Personal data protection in e-government: Globalization or localization? A comparative study of the United States, Germany and China. — 2010. — 216 p.