СРАВНИТЕЛЬНОЕ ПРАВО

УДК 34.05

Регулирование применения больших данных в Республике Корея и России

А. Э. Должикова[1], Б. Р. Сембекова[2], М. Ясин[3]

[1] Российский университет дружбы народов,
Российская Федерация, 117198, Москва, ул. Миклухо-Маклая, 6
[2] Евразийский национальный университет им. Л. Н. Гумилева,
Казахстан, 010000, Нур-Султан, ул. Сатбаева, 2
[3] Стамбульский университет,
Турецкая Республика, 34452, Стамбул, Беязыт

Для цитирования: Должикова, Анна Э., Бакиткул Р. Сембекова, Меликшах Ясин. 2022. «Регулирование применения больших данных в Республике Корея и России». *Вестник Санкт-Петербургского университета. Право* 1: 246–256. https://doi.org/10.21638/spbu14.2022.114

Современные инновации, обусловленные технологиями обработки больших данных, все чаще вступают в противоречие с международными принципами защиты персональных сведений и ставят под сомнение эффективность и адекватность имеющихся правовых механизмов защиты конфиденциальности личной информации. Актуальность исследуемой проблемы обусловлена недостаточной разработанностью теоретических и научно-методических аспектов правового регулирования больших данных в Российской Федерации и необходимостью имплементации положительного зарубежного опыта в ходе построения аналогичного отечественного механизма. Цель исследования заключается в изучении положительного опыта правового регулирования применения больших данных в Республике Корея с точки зрения его имплементации в российское законодательство. Ведущим методом исследования данной проблемы является сравнительно-правовой, позволяющий авторам сформулировать предложения по совершенствованию отечественного законодательства. Корейский опыт показывает необходимость расширения возможности обработки и использования персональных данных, что, в свою очередь, способствует более широкому применению больших данных. К основным направлениям совершенствования правового регулирования процессов использования больших данных относятся следующие области: право пользователей на доступ к своим данным и проверку деятельности компаний с ними; право на прекращение использования и дальнейшее удаление данных; право на изменение данных; право на перенос данных. Основываясь на зарубежном опыте, можно будет

создать эффективную российскую систему правового регулирования больших данных. Новизна и оригинальность исследования заключаются в том, что в нем впервые изучен опыт законодателя Республики Корея в области больших данных.

Ключевые слова: зарубежный опыт, правовое регулирование, большие данные, имплементация, персональные данные, автоматизированная обработка.

1. Введение

Большие данные сравнивают с галактикой, что призвано отразить необъятность этой новой цифровой реальности, влияющей на нашу жизнь, но, подобно многим космическим объектам, не видимой невооруженным глазом (Трофимова 2019). 4 января 2021 г. американская аналитическая компания Eurasia Group представила рейтинг главных рисков, с которыми может столкнуться мир в 2021 г., в частности, ключевыми рисками были названы проблемы с передачей конфиденциальных данных другим странам через интернет и возможность возникновения конфликта в киберпространстве[1].

Статья 24 Конституции РФ предусматривает, что сбор, хранение, использование и распространение информации о частной жизни лица без его согласия не допускаются. Органы государственной власти и органы местного самоуправления, их должностные лица обязаны обеспечить каждому возможность ознакомления с документами и материалами, непосредственно затрагивающими его права и свободы, если иное не предусмотрено законом. Считаем, что это положение напрямую относится и к персональным данным.

Следует согласиться с А. А. Карцхия в том, что «создание сложных объектов (искусственный интеллект, аналитические структуры на основе Big Data, самоуправляемые системы по типу Smart Everything и т. д.), построенных по принципу комплексных технологий, формирует запрос на расширение перечня охраноспособных объектов интеллектуальной собственности, изменение способов правовой охраны в цифровом пространстве, создание сегмента цифровых услуг как разновидности объектов интеллектуальной собственности, признание прав на виртуальные объекты цифровой экосистемы» (Карцхия 2017, 18).

А. С. Федосин рассматривает право на тайну частной жизни, защиту персональных данных и доступ к информации в качестве элементов комплексной структуры конституционного права на неприкосновенность частной жизни ввиду их тесного взаимного переплетения (Федосин 2009).

Конвенция о защите физических лиц при автоматизированной обработке персональных данных, заключенная в г. Страсбурге 28.01.1981[2], признает персональными данными любую информацию об определенном или поддающемся определению физическом лице (субъекте данных).

---

[1] «Рейтинг ключевых рисков для мира в 2021 году». *Eurasia Group.* 2021. Дата обращения 15 февраля, 2021. https://yandex.ru/turbo/regnum.ru/s/news/3157012.html?utm_source=yxnews&utm_medium=desktop.

[2] Здесь и далее все ссылки на российские и международные нормативно-правовые акты и судебную практику приводятся по СПС «КонсультантПлюс». Дата обращения 20 февраля, 2021. http://www.consultant.ru.

Статья 3 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» (далее — Закон № 152) признает таковыми любую информацию, относящуюся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

По мнению А. И. Савельева, с которым мы согласны, одна из наиболее часто звучащих в адрес существующего законодательства о персональных данных претензий связана с чрезмерно широким понятием персональных данных, что не позволяет операторам определить, какая именно информация относится к этой категории и в отношении чего следует применять особый правовой режим (Arkhipov, Naumov 2016; Дупан 2016). Как следствие, представители бизнес-сообщества нередко предлагают сузить данное понятие или вообще установить закрытый перечень персональных данных (Савельев 2018).

Проблема заключается в том, что в России до настоящего времени не выработано единого понимания и подхода к регулированию как больших данных, так и больших пользовательских данных, а последние являются исключительно новым предметом дискуссий (Савельев 2018; Есауленко 2017).

Понятие «большие данные» — технический термин, не имеющий на данный момент унифицированного юридического определения ни в отечественном, ни в международном законодательстве (Романова 2019).

В среде технических специалистов большие данные изначально понимались как большой объем информации, хранение которой не представлялось возможным в памяти одного компьютера ввиду его технических характеристик (Mayer-Schonberger, Cukier 2013). Для раскрытия сущностной характеристики понятия «большой объем данных» можно привести следующие определения: «Большие данные — данные, объем которых превосходит технические возможности конвенционных баз данных. Данные большого объема, характеризуемые высокой скоростью обработки, которые не могут быть помещены в архитектуру традиционных баз данных» (Wilder-James 2012); «Большие данные — это наборы данных, размер которых превышает возможности обычных инструментов баз данных для сбора, хранения, управления и анализа» (Manyika et al. 2011).

На сайте regulation.gov.ru опубликован законопроект о регулировании больших данных, который вносит поправки в Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и защите информации» (далее — Закон № 149), при этом под большими данными понимается «совокупность неперсонифицированных данных, классифицируемая по групповым признакам, в том числе информационные и статистические сообщения, сведения о местоположении движимых и недвижимых объектов, количественные и качественные характеристики видов деятельности, поведенческие аспекты движимых и недвижимых объектов, полученных от различных владельцев данных либо из различных структурированных или неструктурированных источников данных, посредством сбора с использованием технологий, методов обработки данных, технических средств, обеспечивающих объединение указанной совокупности данных, ее повторное использование, систематическое обновление, форма представления которых не предполагает их отнесение к конкретному физическому лицу» (Королев 2020).

А. И. Савельев определяет большие данные как динамически изменяющийся массив информации, который представляет собой ценность в силу своих больших

объемов и возможности эффективной и быстрой обработки автоматизированными средствами, что, в свою очередь, обеспечивает возможность его использования для аналитики, прогнозирования и автоматизации бизнес-процессов (Савельев 2018, 123).

Мы поддерживаем мнение А. Ю. Романовой (Романова 2019), полагающей, что это определение требует доработки и до принятия закона следует опираться на определение, данное рабочей группой по защите физических лиц при обработке персональных данных Европейской комиссии, в соответствии с которым большие данные определяются как совокупность цифровых досье, составляемых с помощью широкопрофильного компьютерного алгоритма и находящихся в распоряжении многочисленных компаний, корпораций и государственных органов[3].

В настоящий момент большие данные в Республике Корея используются как инструмент для решения различных проблем и для принятия стратегических решений по перспективным направлениям развития (Cichocki 2017).

С развитием технологий обработки больших данных делается акцент на комплексное изучение на основе анализа массивных данных, включая интеллектуальный анализ текста, анализ социальных сетей и инфометрию. Таким образом, данные, используемые для определения перспективных направлений развития, поступают не только из существующих статистических данных и документов, но также из широкого спектра источников больших данных, таких как социальные сети, общедоступные данные и данные веб-активности.

Большие данные задействованы в политике, науке, экономике, социальной сфере, защите окружающей среды и других сферах жизни общества. Конкретные проекты включают в себя меры, направленные:

— на прогнозирование социальных рисков с помощью анализа социальных сетей (в том числе для борьбы с суицидом среди несовершеннолетних и выявления его причин);
— определение перспективных технологий для решения потенциальных социальных проблем;
— мониторинг предпринимательского сектора с использованием социальных данных (в том числе для краткосрочного прогнозирования цен на продукты питания на основе анализа электронных торговых ресурсов);
— прогнозирование стихийных бедствий на основе комплексных метеорологических исследований с использованием научно-статистических методов, а также разработку прототипов для системы долгосрочного прогнозирования и анализа бедствий в будущем;
— обнаружение признаков надвигающегося социального или политического конфликта на основе изучения новостей, публикуемых в открытых источниках, а также отслеживание изменения настроения общественности в социальных сетях для выявления назревающих политических конфликтов;

[3] "Article 29 Data Protection Working Party Opinion 03/2013 on Purpose Limitation". *European Commission.* 2013. Дата обращения 15 февраля, 2020. https://ec.europa.eu/justice/article-29/documentation/opinionrecommendation/files/2013/wp203_en.pdf.

— создание системы мониторинга для раннего выявления и предотвращения эпидемий на основе анализа использования лекарственных средств населением и рецептов, выписываемых врачами;
— разработку системы прогнозирования автомобильных аварий по местоположению и времени суток на основе анализа записей об авариях и метеорологической информации.

Параллельно защита личной сферы граждан от вмешательства в нее новых технологий развивалась через толкование общего понятия права на неприкосновенность частной жизни. Гибкий подход к определению содержания этого права особенно ярко проявляется в практике Европейского суда по правам человека (далее — ЕСПЧ) (Савельев 2018). В качестве примеров использования новых технологий, признанных ЕСПЧ нарушением права на неприкосновенность частной жизни, можно привести ситуации, в которых осуществляется слежка за индивидом как посредством контроля за его коммуникациями и телефонными переговорами, в том числе с использованием системы тайного прослушивания вроде СОРМ (системы технических средств для обеспечения функций оперативно-разыскных мероприятий), так и посредством спутниковых систем навигации; другими примерами нарушения права на частную жизнь ЕСПЧ посчитал опубликование видеозаписей наблюдения в общественных местах, нерегламентированный контроль работодателя за использованием средств коммуникаций (служебного телефона, электронной почты, мессенджеров) работниками и ряд других[4].

2. Основное исследование

В январе 2020 г. Национальная ассамблея Кореи приняла ряд серьезных поправок в области регулирования использования баз данных, которые в значительной степени упростили применение псевдонимизированной информации (pseudonymised information), расширили возможности обработки и использования персональных данных, что, в свою очередь, способствует более широкому применению больших данных. Изменения коснулись, в частности, Закона о защите персональных данных[5] и Закона об использовании и защите кредитной информации[6].

Поправки закрепляют концепцию псевдонимизированной информации, которая трактуется аналогично определению, содержащемуся в Регламенте ЕС о защите персональных данных 2016 г.[7] Псевдонимизация понимается как обработка персональных данных таким образом, что они больше не могут быть отнесены к конкретному субъекту данных без использования дополнительной информации,

[4] См. Постановления ЕСПЧ по делам «Копланд (Copland) против Соединенного Королевства», 2007, жалоба № 62617/00; «Узун (Uzun) против Германии», 2010, жалоба № 35623/05; «Роман Захаров (Roman Zakharov) против Российской Федерации», 2015, жалоба № 47143/06.

[5] *Personal Information Protection Act, PIPA. Act No. 16930. Assented to February 4, 2020*. Дата обращения 20 февраля, 2021. https://www.privacy.go.kr/eng/laws_view.do?nttId=8188&imgNo=3.

[6] *Credit Information Use and Protection Act, CIPA. Act No. 6360 Assented to January 16, 2001*. Дата обращения 20 февраля, 2021. https://www.privacy.go.kr/eng/laws_view.do?nttId=8188&imgNo=2.

[7] «Регламент от 27.04.2016 Европейского парламента и Совета (ЕС) 2016/679 "О защите физических лиц в отношении обработки персональных данных и о свободном перемещении таких данных и отмене Директивы 95/46/ЕС (Общие правила защиты данных)"». *General Data Protection Regulation (GDPR)*. 2016. Дата обращения 20 февраля, 2021. https://ogdpr.eu/ru/gdpr-2016-679.

при условии что такая дополнительная информация хранится отдельно и подлежит применению технических и организационных мер, гарантирующих, что персональные данные не отнесены к идентифицированному или идентифицируемому физическому лицу. Поправки в значительной степени облегчат государству сбор и использование такой информации.

Другие изменения ослабляют ограничения на использование и передачу клиентских данных без необходимости получения дополнительного согласия клиента. Личную информацию разрешено будет использовать без дополнительного согласия субъекта «в разумных пределах, в соответствии с целями ее первоначального сбора», при условии что это не наносит ущерб субъекту данных и в отношении такой информации приняты соответствующие меры безопасности.

Закон об использовании и защите кредитной информации с внесенными в него поправками также создает правовую основу для различных кредитных услуг и включает в себя положения о переносимости данных. Действие данного Закона распространяется на все организации, имеющие дело с кредитной информацией, т. е. практически на все финансовые учреждения. В упомянутом акте также дается определение псевдонимизированной личной кредитной информации, которая представляет собой кредитную информацию (включая банковские записи, кредитную историю и др.), псевдонимизированную таким образом, что она не может быть идентифицирована конкретному лицу без использования или объединения ее с дополнительной информацией для восстановления ее первоначального состояния. Практическое осуществление такой псевдонимизации с большой долей вероятности будет выполняться с использованием технологии распределенного реестра.

Согласно ст. 14.1 «Применение информационных технологий в целях идентификации граждан РФ» Закона № 149, государственные органы, банки и иные организации в случаях, определенных федеральными законами, после проведения идентификации при личном присутствии гражданина РФ с его согласия на безвозмездной основе размещают в электронной форме: 1) сведения, необходимые для регистрации гражданина РФ в единой системе идентификации и аутентификации, и иные сведения, если такие сведения предусмотрены федеральными законами, — в единой системе идентификации и аутентификации; 2) биометрические персональные данные гражданина РФ — в единой информационной системе персональных данных, обеспечивающей обработку, включая сбор и хранение биометрических персональных данных, их проверку и передачу информации о степени их соответствия предоставленным биометрическим персональным данным гражданина РФ.

Помимо этого, субъекты данных получат право требовать от финансовых учреждений передачи их персональных кредитных данных различным компаниям по управлению кредитными данными и другим финансовым учреждениям. Для передачи персональных кредитных данных третьим лицам, как правило, требуется получение согласия субъекта, однако в соответствии с предложенными поправками из этого правила будут установлены некоторые исключения. Так, согласие субъекта на передачу кредитных данных третьим лицам не понадобится, если будет иметься взаимосвязь между первоначальной целью сбора данных и целью их передачи, а также в зависимости от контекста первоначального сбора данных, соображений безопасности и некоторых других факторов. Корейские юристы признаю́т, что ука-

занные критерии носят общий характер, подчеркивая, что они с малой долей вероятности будут прояснены до вступления в силу закона (Tomar et al. 2017).

Псевдонимизированной информацией в понимании законодателя не является личная информация, которая, даже если не может быть идентифицирована сама по себе, способна «легко объединяться» с другой информацией таким образом, чтобы ее можно было идентифицировать конкретному лицу. При принятии решения о том, способна ли информация «легко объединяться», учитываются факторы «разумного рассмотрения», такие как способность получения другой информации, с которой объединится первоначальная, а также временные и иные ресурсы, требуемые для этого.

Надзор за защитой персональных данных осуществляют Министерство внутренних дел и безопасности Кореи (Ministry of Interior & Safety) и Комиссия по связи (Korea Communications Commission, KCC). В соответствии с Законом о защите персональных данных, выработка политики и другие регуляторные функции в рассматриваемой области переданы Комиссии по защите личной информации (Personal Information Protection Commission, PIPC), вновь создаваемому органу из девяти членов, подотчетному премьер-министру, членами которого являются правительственные чиновники и эксперты по вопросам политики и права. В полномочия Комиссии входят мониторинг и контроль за соблюдением конфиденциальности данных, а также издание принципов и рекомендаций в рассматриваемой сфере (Ryoo et al. 2020). Создание такого независимого надзорного органа также содержится в требованиях Регламента ЕС о защите персональных данных, на который регулярно ссылаются корейские юристы и, очевидно, опирается корейский законодатель.

В 2019 г. вступила в силу новая редакция Закона о содействии использованию информационно-коммуникационных сетей и защите данных[8], которая ввела для операторов крупных онлайн-сервисов новые требования в отношении защиты данных. Эти поправки распространяются на компании, которые получают доход от информационных технологий (ИТ) более 8 млн долларов США за предыдущий год или имеют ежедневно не менее 1 млн корейских пользователей (посетителей), зарегистрированных в сервисе, либо чьи персональные данные сохранены иным образом. Так называемые провайдеры ИТ-услуг, в том числе социальные сети, различного рода агрегаторы, онлайн-сервисы и приложения, подходящие под указанные выше критерии, должны назначить местного представителя по конфиденциальности данных (при неимении делового присутствия в Корее), выполняющего исключительно эту роль, и страховать свою ответственность (или иметь финансовый резерв) на случай неблагоприятных инцидентов с персональными данными пользователей. За нарушение указанных требований установлен административный штраф в размере до 18 тыс. долларов США (Yang Minwoon et al. 2020).

По мнению Н. И. Касперской, часто говорят о том, что большие пользовательские данные (далее — БПД) должны регулироваться Законом № 152, согласно которому владельцем персональных данных является лицо, эти данные предоставившее. Однако в случае БПД это невозможно, так как «пользователь не предоставля-

[8] *Act on Promotion of Information and Communications Network Utilisation and Data Protection*. Дата обращения 20 февраля, 2021. https://en.wikisource.org/wiki/Act_on_Promotion_of_Information_and_Communication_Network_Utilization_and_Information_Protection.

ет эти данные по собственному желанию (например, он прошел по улице, попал в зону действия видеокамеры — лицо его зафиксировано, но он же не давал разрешение на фиксацию своего лица). Таким образом, как только пользователь что-то сделал в интернете, действие и его последствия пользователю уже не принадлежат, поскольку он не может контролировать их дальнейшее распространение, не влияет на их дальнейшее существование, не может отозвать или запретить их использование нежелательным ему способом» (Касперская 2016).

Говоря о российской практике, А. И. Савельев предлагает при нарушении прав субъекта персональных данных вместо возмещения убытков и/или компенсации морального вреда требовать от нарушителя выплаты компенсации в пользу указанного субъекта. Компенсация подлежит взысканию при доказанности факта нарушения, совершенного оператором. При этом субъект персональных данных, обратившийся за защитой права, освобождается от доказывания размера причиненных ему убытков и/или размера морального вреда. Размер компенсации варьируется от 10 тыс. до 5 млн руб. и определяется по усмотрению суда исходя из характера нарушения и иных обстоятельств дела, с учетом требований разумности и справедливости (Савельев 2018, 142).

А. П. Сергеев и Т. А. Терещенко отмечают, что в доктрине и тем более в правоприменительной практике пока нет готовых и продуманных подходов к решению существующих проблем, а конкретные вопросы находятся в стадии осмысления (Сергеев, Терещенко 2018, 120).

Согласно п. 10 ст. 14.1 Закона № 149, контроль и надзор за выполнением организационных и технических мер по обеспечению безопасности персональных данных, установленных в соответствии со ст. 19 Закона № 152, при обработке персональных данных в единой биометрической системе, за исключением контроля и надзора за выполнением банками организационных и технических мер по обеспечению безопасности персональных данных при использовании единой биометрической системы, осуществляются федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности, и федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации, в пределах их полномочий, установленных законодательством РФ о персональных данных. Контроль и надзор за выполнением банками организационных и технических мер по обеспечению безопасности персональных данных при использовании единой биометрической системы осуществляются Центральным банком РФ.

Мы согласны с мнением А. Ю. Романовой (Романова 2019, 22): основная проблема применения технологии больших данных состоит в том, что ее функциональные возможности находятся в серьезном противоречии с международными основами охраны и защиты персональных данных, информированным согласием и принципом ограничения обработки персональных данных заранее определенной и конкретной целью (data minimization principle)[9].

[9] См., напр.: “Regulation 679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)”. *European Union*. 2016. Дата обращения 15 февраля, 2020. https://eur-lex.europa.eu/eli/reg/2016/679/oj.

3. Выводы

С учетом норм зарубежных законов, в частности законодательства Республики Кореи, целесообразно принять в России специальный закон о больших данных и регламентировать следующие права в области больших данных: право пользователей на доступ к своим данным и проверку компаний, право на удаление данных, право на изменение данных, право на перенос данных.

Библиография

Дупан, Анна С. 2016. *Новая парадигма защиты и управления персональными данными в Российской Федерации и зарубежных странах в условиях развития систем обработки данных в сети.* М.: Издательский дом Высшей школы экономики.

Есауленко, Алексей О. 2017. «Регулирование больших данных не за горами». *Директор информационной службы* 4: 46–48.

Карцхия, Александр А. 2017. «Цифровой императив: новые технологии создают новую реальность». *Интеллектуальная собственность. Авторское право и смежные права* 8: 17–26.

Касперская, Наталья И. 2016. «Большие пользовательские данные должны являться собственностью нации». Дата обращения 20 февраля, 2021. https://www.facebook.com/natalya.kaspersky/posts/1795341197420340*.

Королев, Игорь А. 2020. «Власти начинают регулировать большие данные. Вести реестр будет Роскомнадзор». *CNews*. Дата обращения 20 февраля, 2021. https://www.cnews.ru/news/top/2020-02-17_vlasti_nachinayut_regulirovat.

Романова, Алена Ю. 2019. «К вопросу о правовом режиме больших данных». *Конституционное и муниципальное право* 8: 20–25.

Савельев, Александр И. 2018. «Направления регулирования Больших данных и защита неприкосновенности частной жизни в новых экономических реалиях». *Закон* 5: 122–144.

Сергеев, Александр П., Татьяна А. Терещенко. 2018. «Большие данные: в поисках места в системе гражданского права». *Закон* 11: 106–123.

Трофимова, Елена В. 2019. «Информация о субъектах предпринимательства в единых государственных реестрах — черная дыра в галактике больших данных?» *Предпринимательское право* 3: 44–49.

Федосин, Алексей С. 2009. «Защита конституционного права человека и гражданина на неприкосновенность частной жизни при автоматизированной обработке персональных данных в Российской Федерации». Дис. … канд. юрид. наук, Саратовский государственный университет им. Н. Г. Чернышевского.

Arkhipov, Vladislav V., Viktor B. Naumov. 2016. "The legal definition of personal data in the regulatory environment of the Russian Federation: Between formal certainty and technological development". *Computer Law and Security Review* 32 (6): 868–887.

Cichocki, Andrzej. 2017. "A new approach to future strategy in the era of Big Data". *National Information Society Agency* 2: 1–30.

Manyika, James, Michael Chui, Brad Brown, Jacques Bughin, Richard Dobbs, Charles Roxburgh, Angela Hung Byers. 2011. "Big data: The next frontier for innovation, competition, and productivity". *McKinsey Global Institute*. Дата обращения 20 февраля, 2021. https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/big-data-the-next-frontier-for-innovation.

Mayer-Schonberger, Viktor, Kenneth Cukier. 2013. *Big Data: A revolution that will transform how we live, work, and think.* John Murray Publ.

Ryoo, Kwang Hyun, Juho Yoon, Tae Uk Kang, Jeong Eun Park. 2020. "Korea's data privacy laws amended, paving way for Big Data services". Дата обращения 15 февраля, 2020. https://www.lexology.com/library/detail.aspx?g=0b7bb83a-0b93-4f64-b3d0-552aedbf3c07#:~:text=The%20amendments%20to%20PIPA%20and,as%20well%20as%20other%20sectors.

* Meta включена в реестр НКО, выполняющих функции иностранного агента.

Tomar, Louisa, William Guicheney, Hope Kyarisiima, Tinashe Zimani. 2017. "How Big Data can be used in the public sector". *National Information Society Agency* 8: 1–52.
Wilder-James, Edd. 2012. "What is Big Data?" *O'Reilly Radar* 4: 1–12.
Yang Minwoon, Susan Park, Juho Yoon, Kwang Hyun Ryoo. 2020. "Data protection & privacy 2020". Дата обращения 15 февраля, 2020. https://www.bkl.co.kr/law/field/fieldView.do?fieldNo=18&lang=ko. (In Korean)

Статья поступила в редакцию 24 февраля 2021 г.;
рекомендована к печати 10 декабря 2021 г.

Контактная информация:

Должикова Анна Эдуардовна — аспирант; l_a_buka@mail.ru
Сембекова Бакиткул Рактаевна — д-р юрид. наук, проф.; b.sembekova@yandex.ru
Ясин Меликшах — д-р юрид. наук, проф.; meliksah.yasin@istanbul.edu.tr

Regulation of the use of big data in the Republic of Korea and Russia

A. E. Dolzhikova[1], B. R. Sembekova[2], M. Yasin[3]

[1] Peoples' Friendship University of Russia (RUDN University),
6, ul. Miklukho-Maklaya, Moscow, 117198, Russian Federation
[2] Eurasian National University named after L. N. Gumilyov,
2, ul. Satbaeva, Nur-Sultan, 010000, Kazakhstan
[3] Istanbul University,
Beyazıt, Istanbul, 34452, Republic of Turkey

For citation: Dolzhikova, Anna E., Bakitkul R. Sembekova, Melikşah Yasin. 2022. "Regulation of the use of big data in the Republic of Korea and Russia". *Vestnik of Saint Petersburg University. Law* 1: 246–256. https://doi.org/10.21638/spbu14.2022.114 (In Russian)

Modern innovations driven by big data processing technologies are increasingly in conflict with international principles for protecting personal information and call into question the effectiveness and adequacy of existing legal mechanisms for protecting confidentiality of personal information. The relevance of the problem under study is due to the insufficient development of theoretical and methodological aspects of legal regulation of big data in the Russian Federation and the need to implement positive foreign experiences for building a mechanism for legal regulation of this institution. The purpose of the essay is to study the positive experience of legal regulation of the use of big data in the Republic of Korea for its implementation in Russian legislation. The leading method for studying this problem is a comparative legal one, which allows the authors to formulate proposals for improving domestic legislation. The study led to the following conclusion. The main area for improvement the legal regulation of the processes of using big data are: the right of users to access their data and check the activities of companies with them, the right to stop using and further delete data, the right to change data, the right to data portability. The study revealed that the Korean experience shows the need to expand the processing and use of personal data, which in turn contributes to the wider use of big data. The study will allow, based on foreign experience, to create an effective Russian system of legal regulation of big data. The novelty and originality of the study lies in the fact that it was the first to study the experience of the legislator of the Republic of Korea in this area.

Keywords: foreign experience, legal regulation, big data, implementation, personal data, automated processing.

References

Arkhipov, Vladislav V., Viktor B. Naumov. 2016. "The legal definition of personal data in the regulatory environment of the Russian Federation: Between formal certainty and technological development". *Computer Law and Security Review* 32 (6): 868–887.

Cichocki, Andrzej. 2017. "A new approach to future strategy in the era of Big Data". *National Information Society Agency* 2: 1–30.

Dupan, Anna S. 2016. *A new paradigm for the protection and management of personal data in the Russian Federation and foreign countries in the context of the development of data processing systems in the network*. Moscow, Vysshaia shkola ekonomiki Publ. (In Russian)

Esaulenko, Aleksei O. 2017. "Big Data regulation is around the corner". *Direktor informatsionnoi sluzhby* 4: 46–48. (In Russian)

Fedosin, Aleksei S. 2009. "Protection of the constitutional right of a person and a citizen to privacy during automated processing of personal data in the Russian Federation". PhD diss., Saratovskii gosudarstvennyi universitet im. N. G. Chernyshevskogo. (In Russian)

Kartskhiia, Aleksandr A. 2017. "The digital imperative: New technologies create a new reality". *Intellektual'naia sobstvennost'. Avtorskoe pravo i smezhnye prava* 8: 17–26. (In Russian)

Kasperskaia, Natal'ia I. 2016. "Big user data must be the property of the nation". Accessed February 20, 2021. https://www.facebook.com/natalya.kaspersky/posts/1795341197420340*. (In Russian)

Korolev, Igor' A. 2020. "Authorities are starting to regulate big data. The register will be maintained by Roskomnadzor". *CNews*. Accessed February 20, 2021. https://www.cnews.ru/news/top/2020-02-17_vlasti_nachinayut_regulirovat. (In Russian)

Manyika, James, Michael Chui, Brad Brown, Jacques Bughin, Richard Dobbs, Charles Roxburgh, Angela Hung Byers. 2011. "Big data: The next frontier for innovation, competition, and productivity". *McKinsey Global Institute*. Accessed February 20, 2021. https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/big-data-the-next-frontier-for-innovation/

Mayer-Schonberger, Viktor, Kenneth Cukier. 2013. *Big Data: A revolution that will transform how we live, work, and think*. John Murray Publ.

Romanova, Alena Iu. 2019. "On the issue of the legal regime of Big Data". *Konstitutsionnoe i munitsipal'noe pravo* 8: 20–25. (In Russian)

Ryoo, Kwang Hyun, Juho Yoon, Tae Uk Kang, Jeong Eun Park. 2020. "Korea's data privacy laws amended, paving way for Big Data services". Дата обращения 15 февраля, 2020. https://www.lexology.com/library/detail.aspx?g=0b7bb83a-0b93-4f64-b3d0-552aedbf3c07#:~:text=The%20amendments%20to%20PIPA%20and,as%20well%20as%20other%20sectors.

Savel'ev, Aleksandr I. 2018. "Big Data regulations and privacy in new economic realities". *Zakon* 5: 122–144. (In Russian)

Sergeev, Aleksandr P., Tat'iana A. Tereshchenko. 2018. "Big Data: Seeking a place in the civil law system". *Zakon* 11: 106–123. (In Russian)

Tomar, Louisa, William Guicheney, Hope Kyarisiima, Tinashe Zimani. 2017. "How Big Data can be used in the public sector". *National Information Society Agency* 8: 1–52.

Trofimova, Elena V. 2019. "Information about business entities in unified state registries — a black hole in the big data galaxy?" *Predprinimatel'skoe pravo* 3: 44–49. (In Russian)

Wilder-James, Edd. 2012. "What is Big Data?" *O'Reilly Radar* 4: 1–12.

Yang Minwoon, Susan Park, Juho Yoon, Kwang Hyun Ryoo. 2020. "Data protection & privacy 2020". Accessed February 15, 2020. https://www.bkl.co.kr/law/field/fieldView.do?fieldNo=18&lang=ko. (In Korean)

Received: February 24, 2021
Accepted: December 10, 2021

Authors' information:

Anna E. Dolzhikova — Postgraduate Student; l_a_buka@mail.ru
Bakitkul R. Sembekova — Dr. Sci. in Law, Professor; b.sembekova@yandex.ru
Melikşah Yasin — Dr. Sci. in Law, Professor; meliksah.yasin@istanbul.edu.tr

* Meta включена в реестр НКО, выполняющих функции иностранного агента.