

УДК 34

DOI 10.21661/r-130405

Т.В. Мавринская, А.В. Лошкарёв, Е.Н. Чуракова

ОБЕЗЛИЧИВАНИЕ ПЕРСОНАЛЬНЫХ ДАННЫХ И ТЕХНОЛОГИИ «БОЛЬШИХ ДАННЫХ» (BIGDATA)

***Аннотация:** вопрос об использовании персональных данных граждан очень важен, и решением данного вопроса должно послужить принятие законодательства, четко регулирующее деятельность операторов персональных данных. Авторами рассмотрен один из эффективных подходов к защите персональных данных – обезличивания, а также выявлены две абсолютно противоположные тенденции к принятию законов. Обезличивание данных не только является защитой интересов государства и, в первую очередь, граждан, но и механизмом, который позволит рекламным, страховым и иным компаниям улучшить качество своих продуктов и услуг.*

***Ключевые слова:** персональные данные, большие данные, bigdata, обезличивание данных, анонимизация, базы данных, операторы персональных данных, обезличивание, деобезличивание.*

T.V. Mavrinskaya, A.V. Loshkaryov, E.N. Churakova

DEPERSONALIZATION OF PERSONAL DATA AND «BIG DATA» TECHNOLOGY (BIGDATA)

***Abstract:** the question of the citizens' personal data processing is very important, and the solution for this problem should be the adoption of legislation expressly regulating the activities of personal data operators. The authors considered one of the most effective approaches to personal data protection – anonymization, as well as identified two developments to adoption of legislation. Anonymization not only protects the interests of the state and, first and foremost, the citizens, but it is also a mechanism that will allow advertising, insurance and other companies to improve the quality of their products and services.*

Keywords: *personal data, big data, bigdata, disclosure control, anonymization, database, operators of personal data, depersonalization.*

Современный мир вступил в эпоху высоких технологий, которая коренным образом изменила наше представление об информации, способах ее получения и обработки. Трансформируются такие понятия, как частная жизнь, личное пространство и тайна переписки. Всё больше социальных, и не только, процессов переходит из реального мира в виртуальный, и привычным стало использование онлайн сервисов для покупки вещей и информации, общения с друзьями, получения услуг. Удобство и широкий выбор технологий позволил современному человеку получать актуальную информацию практически обо всем. И используя различные информационные технологии, люди стали открывать про себя всё больше и больше личной информации, выкладывая в социальные сети фотографии мест отдыха и работы, свои предпочтения в музыке и литературе, родственные связи, состояние здоровья, информацию о финансовых операциях и прочее. Соответственно, эти данные собираются, хранятся и обрабатываются разными организациями и органами, которые используют полученную информацию в различных сферах деятельности: страховой, банковской, медицинской, электронной коммерции и т. д. [1]. И чем больше персональных данных (*персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому субъекту персональных данных*) человека содержится в информационном мире, тем больше возможно влияние на жизнь этого человека, и соответственно, величина риска нарушения его прав [2].

Вся персональная информация, хранящаяся и обрабатываемая в любых базах данных, должна быть защищена не только на физическом и программном уровне, но и главным образом на уровне законодательства.

Одним из способов использования персональные данные большого количества людей, при этом не нарушая их права, является «анонимизация данных», или согласно ст.3 Федерального закон от 27 июля 2006 г. №152-ФЗ «О персональных данных» «обезличивание персональных данных» – *действия, в результате которых становится невозможным без использования дополнительной*

информации определить принадлежность персональных данных конкретному субъекту персональных данных [2].

Обезличивание данных является важной социальной функцией, направленной на защиту граждан от риска причинения им вреда в случае утечки персональных данных и попадания этих данных в руки злоумышленников. В зависимости от целей и задач обработки персональных данных операторы связи используют разные методы обезличивания: введения идентификаторов; изменения состава или семантики; декомпозиции; перемешивания. Эти методы и требования к ним определены Приказом Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 5 сентября 2013 г. №996 «Об утверждении требований и методов по обезличиванию персональных данных» [4]. Еще одним способом обезличивания больших данных является применения криптографии. Криптографические преобразования, вопреки распространенному мнению, могут применяться не только для защиты информации, но и для других задач, в том числе и для обезличивания персональных данных [5].

Однако развитие информационных технологий происходит высокими темпами и уже на сегодняшний день «большие данные» (big data), которые объединяют и анализируют информацию из разных источников, могут с высокой вероятностью определить, к какому конкретно человеку относятся обезличенные данные. Базы данных объединяются, обмениваются информацией, и обезличив некий объем данных вчера, сегодня мы можем обнаружить, что «большие данные» их уже обратили. К тому же, сами методы обезличивания, согласно Приказу №996 от 5 сентября 2013 г. Роскомнадзора должны иметь свойство обратимости (возможность преобразования, обратного обезличиванию (деобезличивание), которое позволит привести обезличенные данные к исходному виду, позволяющему определить принадлежность персональных данных конкретному субъекту, устранить анонимность).

Профессор права Пол Ом (Paul Ohm) считает, что «данные могут быть либо полезными, либо анонимными, но никогда и теми, и другими одновременно». По

его мнению, существующие научные методы повторной идентификации (ре-идентификации) ставят под вопрос всю систему защиты персональных данных, убивая наше доверие к обезличиванию данных. Это важный вопрос, поскольку компании, обрабатывающие персональные данные, возлагают большое доверие на обезличивание, производя их обмен и постоянное хранение и заверяя своих пользователей, что они защищают неприкосновенность частной жизни. «Достижения в области деобезличивания выставляют эти обещания во многих случаях как иллюзорные» – заявил Пол Ом [6].

Технический писатель, основатель проекта Open Heat Map и консультант Нью-Йорк Таймс Пит Уорден (Pete Warden), заявил, что «анонимизация – это иллюзия» [6]. Он так же указывает на существование очень большого количества различных государственных наборов данных и возможность их сопоставления, что с большой долей вероятности идентифицирует человека.

Вопрос об использовании персональных данных граждан очень важен, и решением данного вопроса должно послужить принятие законодательства, четко регулирующее деятельность операторов персональных данных. Можно отметить две противоположных тенденции в принимаемых законах разных стран:

1. Разрабатываемое законодательство Европейского союза о защите персональных данных – «Общие правила защиты персональных данных» (General Data Protection Regulation, GDPR), которое установит более высокие требования при получении согласий, необходимых операторам персональных данных для того, чтобы легально обрабатывать данные других лиц. Операторы персональных данных будут обязаны обеспечить *«четкие и более детализированные методы дачи согласия, хорошее документирование согласий и простые, легкодоступные способы, позволяющие людям отзываться своё согласие»*, а в противном случае они будут признаны нарушителями. В Российской Федерации также разрабатывается законопроект, регулирующий работу с «большими пользовательскими данными». Помощник президента и руководитель рабочей группы по вопросам развития интернета при администрации президента Игорь Щеголев отмечает, что в

разрабатываемом законе о «больших пользовательских данных» появится возможность для пользователей запретить использование данных о себе операторам персональных данных. Помощник президента отметил, что с развитием промышленного интернета и интернета вещей объем данных, по которым можно будет однозначно вычислить человека, с которыми эти данные связаны, будет увеличиваться. В соответствии с законами, которые действуют на данный момент, эти данные не всегда могут быть определены напрямую как персональные, но часть из них «находится на грани, в серой зоне», которая на данный момент никак не отрегулирована [7].

2. Сенат США 23 марта 2017 года проголосовал за отмену правил конфиденциальности, обязывающих американских операторов запрашивать у клиентов разрешение на использование, обмен или продажу конфиденциальной информации, включая историю просмотров веб-страниц, компаниям, занимающимся в сфере рекламы и других сферах, прибыль которых напрямую зависит от объема обрабатываемых персональных данных граждан. Джонатан Швантс, старший юрисконсульт Союза потребителей США, заявил, что отмена правил конфиденциальности *«представляет собой огромный шаг в неправильном направлении и полностью игнорирует потребности и интересы потребителей»* [8].

Таким образом, разные подходы к принимаемым законам подтверждают тот факт, что персональные данные граждан являются важнейшим аспектом построения отношений между самими гражданами, государством и операторами связи. Обезличивание же данных должно не только являться защитой интересов государства и, в первую очередь, граждан, но и механизмом, который позволит рекламным, страховым и иным компаниям улучшать качество своих продуктов и услуг. И законодательная база должна стать тем барьером, который не позволит сдвинуть баланс реальной власти в пользу крупных корпораций, использующих огромные базы персональных данных граждан без их согласия, но и позволит улучшить корпорациям свои услуги путем обезличенных больших данных.

Список литературы

1. Савельев А.И. Проблемы применения законодательства о персональных данных в эпоху «Больших данных» (Big Data) // Журнал Высшей школы экономики. – 2015. – №1. – С. 45–47.
2. Федеральный закон «О персональных данных» от 27.07.2006 №152-ФЗ // СПС «Консультант плюс».
3. Конвенция о защите физических лиц при автоматизированной обработке персональных данных (Заключена в г. Страсбурге 28.01.1981).
4. Приказ Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор) от 5 сентября 2013 г. №996 г. Москва «Об утверждении требований и методов по обезличиванию персональных данных», Федеральный выпуск «Российская газета» №6184 (208) от 18 сентября 2013 г.
5. Лукацкий А. Применение криптографии для обезличивания персональных данных [Электронный ресурс]. – Режим доступа: <https://www.slideshare.net/lukatsky/ss-73558883>
6. Paul Ohm. Broken promises of privacy: responding to the surprising failure of anonymization [Электронный ресурс]. – Режим доступа: <http://www.uclalawreview.org/pdf/57-6-3.pdf>
7. Игорь Щеголев, интервью информационному агентству «РБК» от 27.03.2017 [Электронный ресурс]. – Режим доступа: www.rbc.ru/technology_and_media/27/03/2017/58d551429a794719618a4245
8. Шепардсон Д. Сенат США проголосует за отмену правил конфиденциальности // Агентство Новостей «Reuters» 23.03.2017 [Электронный ресурс]. – Режим доступа: <http://www.reuters.com/article/us-usa-internet-idUSKBN16U2ER>

Мавринская Татьяна Владимировна – студентка Института права ФГБОУ ВО «Самарский государственный экономический университет», Россия, Самара.

Mavrinskaya Tatyana Vladimirovna – student at the Institute of Law FSBEI of HE “Samara State University of Economics”, Russia, Samara.

Лошкарёв Андрей Викторович – канд. юрид. наук, доцент кафедры гражданского и арбитражного процесса Института права ФГБОУ ВО «Самарский государственный экономический университет», Россия, Самара.

Loshkaryov Andrey Viktorovich – candidate of juridical sciences, associate professor of the Department of Civil and Arbitration Process at the Institute of Law FSBEI of HE “Samara State University of Economics”, Russia, Samara.

Чуракова Екатерина Николаевна – канд. юрид. наук, доцент кафедры гражданского и арбитражного процесса Института права ФГБОУ ВО «Самарский государственный экономический университет», Россия, Самара.

Churakova Ekaterina Nikolaevna – candidate of juridical sciences, associate professor of the Department of Civil and Arbitration Process at the Institute of Law FSBEI of HE “Samara State University of Economics”, Russia, Samara.
