

УДК 34

DOI 10.36511/2078-5356-2019-3-143-147

Пинкевич Татьяна Валентиновна
Tatyana V. Pinkevich

доктор юридических наук, профессор, профессор кафедры уголовной политики
Академия управления МВД России (125171, Москва, ул. Зои и Александра Космодемьянских, 8)
doctor of sciences (law), professor, professor of the department of criminal policy
Academy of management Ministry of internal affairs of Russia (8 Zoe and Alexander Kosmodemyan-
skih st., 125171)

E-mail: pinkevich@yandex.ru

Нестеренко Андрей Владимирович
Andrey V. Nesterenko

преподаватель кафедры криминалистики
Ставропольский филиал Краснодарского университета МВД России (355000, Ставрополь,
пр. Кулакова, 42)

lecturer of criminalistics department
Stavropol branch of the Krasnodar university of Ministry of internal affairs of Russia (42 Kulakova av.,
Stavropol, Russian Federation, 355000)

E-mail: nester-andrei2017@yandex.ru

Нарушение неприкосновенности частной жизни при использовании технологии «Больших данных»

Violation of privacy when using Big Data technologies

В статье рассмотрены проблемные вопросы, связанные с применением технологии «Больших данных», а также представлены положительные и отрицательные факторы влияния Big Data на личную жизнь граждан. Авторы приходят к выводу о том, что ввиду отсутствия закона о регулировании «больших данных» основным препятствием для злоупотребления частной информацией граждан является Закон о персональных данных, однако легитимное согласие на обработку персональных данных, их обезличивание, закрепленные в законе, не обеспечивают должной защиты личных сведений от использования третьими лицами, поэтому требуется серьезная проработка вопроса о введении уголовной ответственности за использование личной информации физических лиц с использованием технологии «Больших данных», повлекшее нарушение неприкосновенности частной жизни.

Ключевые слова: цифровые технологии, персональные данные, личная информация, «большие данные», Big Data, пользовательское соглашение, оператор, анонимность, обезличивание, деобезличивание.

The article deals with the problematic issues related to the use of Big Data technology, as well as the positive and negative factors of the Big Data influence on the personal life of citizens. The authors come to the conclusion that in the absence of the law on the regulation of Big Data, the main obstacle to the abuse of private information of citizens is the Law on personal data. However, legitimate consent to the processing of personal data, their depersonalization, enshrined in the law, do not provide adequate protection of personal data from use by third parties. Therefore, serious study is required on the introduction of criminal liability for the use of personal information of individuals, using the technology of Big Data, which led to the violation of privacy.

Keywords: digital technologies, information, personal information, personal information, Big Data, user agreement anonymity, operator, depersonalization, geometrician.

Развитие информационных технологий в современной России стремительно меняет при-

вычный образ экономических отношений и способствует построению системы цифровой

© Пинкевич Т.В., Нестеренко А.В., 2019

экономики как наиболее оптимальной среды применения электронных технологий [1, с. 374—380; 2, с. 94—99]. Одной из особенностей цифровой экономики и ее преимуществом является возможность получения, хранения и использования большого массива данных. Объемы личной информации, размещаемой и систематизируемой в сети «Интернет», возросли до беспрецедентных размеров, поскольку граждане стали добровольно предоставлять свои персональные данные, выкладывая их на сайтах в сети «Интернет». Как правило, такие сведения включают не только фамилию, имя и отчество, но и информацию о месте жительства, работе, учебе, семейном положении, номерах телефонов, банковской карты, в том числе биометрии и геолокации и т. д.

Аналитическое агентство WeAreSocial и крупнейшая SMM-платформа Hootsuite, проанализировав в текущем году российский цифровой рынок, установили, что объемы личной информации, размещаемой и систематизируемой в сети «Интернет» возросли за последние три года до беспрецедентных масштабов. С января 2017 года пользователей в сети «Интернет» стало больше на 5 млн и их прирост составил 4%, а социальными сетями теперь пользуются на 9 млн больше людей (+15%) чем в 2016 году. При этом, в социальных сетях зарегистрировано почти 56 млн человек, а мобильным интернетом активно пользуются 91,4 млн человек. Самые популярные мобильные приложения в России — WhatsApp, Viber, VK, Сбербанк Онлайн, Instagram [3].

Происходящие процессы в цифровой среде способствовали появлению большого объема, или «больших данных» информации, которая, по сути, является, во-первых, неоднородной, во-вторых, она постоянно и быстрыми темпами пополняется и ее уже невозможно обработать традиционными инструментами [4]. Впервые названный термин был введен в 2008 году К. Линчем в статье журнала «Nature» [5].

В России понятие «большие данные» впервые определено Стратегией развития информационного общества в Российской Федерации на 2017—2030 годы как информация из различных источников в объемах, которые за разумное время вручную обработать невозможно. При этом такая информация может быть как структурированной, так и неструктурированной [6; 7].

Таким образом, технология «Больших данных» — это информационная система, включающая, прежде всего, обработку и использование сведений в цифровом виде колоссального объема и неоднородного содержания, которые непрерывно пополняются, обновляются и хра-

нятся в различных источниках. При этом информация носит универсальный характер и может использоваться во многих сферах жизнедеятельности общества (банковской, страховой, медицинской, правоохранительной сферах и т. д.) организациями, которые предоставляют такие данные, осуществляют их хранение, разрабатывают алгоритмы для их анализа [8]. Именно благодаря этой технологии, при ее использовании, у государства, юридических лиц открываются огромные перспективы развития, поскольку «кто сегодня владеет данными и средствами их аккумуляции, хранения и анализа — реально владеет миром» [9, с. 345].

«Большие данные» и «персональные данные» не являются синонимами и различаются по:

— субъектному составу (персональные данные имеют конкретного субъекта регулирования, а «большие данные» — это совокупность обезличенных данных);

— согласию на их использование (персональные данные собираются с согласия самого носителя персональных данных, который выражает волю на их обработку);

— субъекту обработки (обработкой персональных данных занимается определенный субъект — оператор данных, в то время как обрабатывать «большие данные» могут крупные компании, которые осуществляют свою деятельность в различных сферах) [10, с. 255].

На наш взгляд, это не совсем верно, так как указанные понятия соотносятся как общее с частным, поскольку персональные данные и иная личная информация является составной частью «больших данных». При этом личная информация физического лица на основании пользовательского соглашения выкладывается на сайтах юридических лиц в сети «Интернет», анализируется и обрабатывается оператором таким образом, что определить, к какому конкретно гражданину относятся обезличенные данные не составляет никакого труда. Соответственно, указанная информация может использоваться третьими лицами для оказания влияния на жизнь такого гражданина, что в свою очередь нарушит его права.

В 2018 году Президент Российской Федерации В.В. Путин заявил о том, что «Россия должна стать одним из мировых центров хранения, обработки, передачи и защиты информационных массивов — «больших данных» [11], однако Правительство Российской Федерации пока не знает, как проводить цифровое развитие страны, чтобы защитить личные данные граждан и дать возможность развиваться бизнесу в сфере

инновационных технологий [12]. Следовательно, необходимо создать организационно-правовые инструменты, позволяющие определить направления по использованию большого массива данных такого рода. В настоящее время актуальным остается вопрос, связанный с подготовкой и принятием закона о регулировании «больших данных», который предоставит возможность гражданам защитить свои права, запретить использование их личных данных операторам связи и другим компаниям; исключит факты использования персональных данных граждан в иных целях, вопреки подписанному ими пользовательскому соглашению. Физические лица должны иметь возможность влиять на судьбу тех данных, которые о нем получены [13].

Примером защиты личных данных пользователей может служить решение Девятого арбитражного апелляционного суда о частичном удовлетворении иска соцсети «ВКонтакте» к компании «Double», занимающейся анализом большого объема данных. Суть иска заключалась в том, что компания без разрешения соцсети и пользователей собирала сведения по персональным данным граждан и продавала их банкам, которые по ним оценивали кредитоспособность заемщиков. Согласно решению суда компании «Double» запрещен сбор и анализ сведений о пользователях сети «ВКонтакте» в рыночных целях [14].

Необходимо внесение изменений в законы Российской Федерации «Об информации, информационных технологиях и о защите информации», «О персональных данных», так как нормы, изложенные в них, устарели, не отвечают современным требованиям и в условиях развития цифрового общества и цифровых технологий, связанных с обработкой больших массивов информации о гражданах, выступают законодательным барьером.

Существует мнение, что возможности технологии «Больших данных» прямо противоречат принципам, закрепленным в указанном законе, так как частная жизнь и «большие данные» в современных реалиях не вполне совместимы [15, р. 70].

На наш взгляд, обработка персональных данных должна осуществляться только с согласия субъекта персональных данных, однако согласие не требуется, когда предусматриваются мероприятия по защите гражданина и общества от терроризма, а также предупреждение преступлений при сохранности текстовой, голосовой, звуковой, видео, фото и иной информации в сети «Интернет» от 0 до 6 месяцев с момента окончания их приема, передачи, доставки и (или) обработки. Доступ к информации имеют органы, осуществ-

ляющие оперативно-разыскную деятельность и обеспечение безопасности, на основании судебного решения и при наличии у правоохранительных органов оперативных данных о лицах, совершивших или готовящих преступление [16].

Исходя из вышеизложенного, необходимо отметить, что «большие данные», как правило, собираются с той целью, чтобы посредством их объединения с иными базами извлечь новую информацию и применить ее. В настоящее время требования о том, что обработка персональных данных осуществляется с согласия субъекта персональных данных, являются неэффективными. Это обусловлено тем, что: а) оператор не в состоянии предоставить исчерпывающий объем сведений о целях и способах обработки персональных данных; б) у оператора, как правило, нет взаимодействия с другими организациями, которые осуществляют сбор и обработку персональных данных; в) не всегда субъект персональных данных правильно воспринимает информацию о политике конфиденциальности.

Сможет ли анонимность личных сведений (когда невозможно без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту) решить проблему применения злоумышленниками в своих целях личной информации граждан с помощью технологии «Больших данных»? Полагаем, что нет, поскольку для установления персональных данных реального субъекта анонимные данные должны иметь свойство обратимости и путем соответствующих методов они приводятся к изначальному виду [17].

Вопрос об использовании персональных данных граждан как составной части «больших данных» очень важен, но нельзя забывать, что и защита неприкосновенности частной жизни, личная и семейная тайна, гарантированные статьей 12 Всеобщей декларации прав человека [18], статьей 17 Международного пакта о гражданских и политических правах [19], а также частью 1 статьи 23 Конституции Российской Федерации [20], тоже необходимы. Ведь сведения о персональных данных лица, находясь в цифровом виде, могут стать достоянием преступников, использующих технологии «больших данных», и причинить вред гражданину и членам его семьи.

В то же время в Законе Российской Федерации «О персональных данных» в случаях их умышленного разглашения отсылочная норма, предусматривающая уголовную ответственность, отсутствует. При нарушении Закона Российской Федерации «Об информации, информационных технологиях и о защите информации»

наступает и уголовная ответственность (ст. 17) [21], однако, несмотря на множество изменений, внесенных в последнее время, ни в одном из указанных нормативных правовых актах не указывается о неправомерном использовании злоумышленниками личной информации граждан с применением технологии «Больших данных».

В этой связи решению данной проблемы должно послужить не только принятие закона о регулировании «больших данных» и внесение изменений в законы «О персональных данных» и «Об информации, информационных технологиях и о защите информации», но и введение квалифицирующего признака состава преступления, предусмотренного статьей 137 УК РФ «Нарушение неприкосновенности частной жизни». Предлагается часть 2 данной нормы изложить в следующей редакции:

«2. Те же деяния, совершенные:

а) лицом с использованием своего служебного положения;

б) путем незаконного собирания или распространения сведений о частной жизни лица, составляющих его личную или семейную тайну, без его согласия либо распространение этих сведений в публичном выступлении, публично демонстрирующемся произведении или средствах массовой информации, совершенные лицом с использованием результатов анализа обработки «больших данных» нейросетью (искусственным интеллектом) с применением виртуальных машин и технологии распределительного реестра, —».

Введение уголовной ответственности за незаконное собирание или распространение сведений о частной жизни лица, составляющих его личную или семейную тайну, без его согласия, с использованием технологии «Больших данных», станет барьером для лиц, применяющих цифровые технологии с целью эксплуатации персональных данных граждан в преступных целях.

Примечания

1. Пинкевич Т.В. Развитие цифровых технологий в России и их влияние на уровень криминологической безопасности // Актуальные проблемы противодействия коррупционным преступлениям и преступлениям в сфере экономики: сборник материалов Международной научно-практической конференции (31 октября 2017 г. Нижний Новгород). Н. Новгород, 2018. С. 374—380.

2. Пинкевич Т.В. Криминологические риски индустрии цифровых технологий в России // Криминальные реалии, реагирование на них и закон: сборник статей / под ред. А.И. Долговой. М., 2018. С. 94—99.

3. Интернет в России: главные цифры. URL: <http://security.mosmetod.ru/internet-zavisimosti/97-internet-v-rossii-2018-glavnye-tsifry> (дата обращения: 13.10.2018).

4. Мир Big Data в 8 терминах. URL: <https://rb.ru/howto/big-data-in-8-terms/> (дата обращения: 14.10.2018).

5. Черняк Л. Большие Данные — новая теория и практика // Открытые системы. СУБД. 2011. № 10. URL: <https://www.osp.ru/os/2011/10/13012252/> ISSN1028-7493 (дата обращения: 14.10.2018).

6. О Стратегии развития информационного общества в Российской Федерации на 2017—2030 годы: указ Президента Российской Федерации от 9 мая 2017 г. № 203. URL: http://www.consultant.ru/document/cons_doc_LAW_10699/ (дата обращения: 17.10.2018).

7. Об утверждении программы «Цифровая экономика Российской Федерации»: распоряжение Правительства Российской Федерации от 28 июля 2017 г. № 1632-р. URL: http://www.consultant.ru/document/cons_doc_LAW_221756/2369d7266adb33244e178738f67f181600cac9f2/ (дата обращения: 14.10.2018).

8. Боева Н. У новых стартапов в области bigdata неплохие шансы на успех // Коммерсантъ.ru. Интернет-газета. URL: <https://www.kommersant.ru/doc/3083474> (дата обращения: 14.10.2018).

9. Ларина Е.С., Овчинский В.С. Криминал будущего уже здесь. М.: Книжный мир, 2018.

10. Мамонтова М.Ю. Настоящее и будущее больших пользовательских данных: материалы межвузовской научно-практической конференции с международным участием. М., 2017.

11. Путин призвал сделать Россию одним из мировых центров «больших данных». URL: <https://www.rbc.ru/rbcfreenews/5a97d1bd9a79476b19eab85c> (дата обращения: 14.10.2018).

12. Законопроект о регулировании больших данных внесут до конца года. URL: <https://pravo.ru/news/205919/> (дата обращения: 14.10.2018).

13. Закон о Big Data позволит россиянам запретить сбор данных о себе. URL: https://www.rbc.ru/technology_and_media/27/03/2017/58d551429a794719618a4245 (дата обращения: 14.10.2018).

14. Суд осложнил жизнь bigdata в России. URL: <http://expert.ru/2018/01/30/sud-oslozhnil-zhizn-big-data-v-rossii/> (дата обращения: 14.10.2018).

15. Lane J., Stodden V., Bender S., Nissenbaum H. Privacy, Big Data, and the Public Good: Framework for engagement. Cambridge. Cambridge University Press. 2014.

16. Кто будет хранить данные пользователей услуг связи с 1 июля? URL: <http://duma.gov.ru/news/27433/> (дата обращения: 16.10.2018).

17. Об утверждении требований и методов по обезличиванию персональных данных: приказ Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от

5 сентября 2013 г. № 996. URL: <http://www.garant.ru/products/ipo/prime/doc/70351476/> (дата обращения: 17.10.2018).

18. Всеобщая декларация прав человека (принята Генеральной Ассамблеей ООН 10.12.1948). URL: http://www.consultant.ru/document/cons_doc_LAW_120805/ (дата обращения: 17.10.2018).

19. Международный пакт о гражданских и политических правах (Нью-Йорк, 16 декабря 1966 г.). URL: <http://base.garant.ru/2540295/> (дата обращения: 17.10.2018).

20. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993) (с учетом поправок, внесенных законами РФ о поправках к Конституции РФ от 30.12.2008 № 6-ФКЗ, от 30.12.2008 № 7-ФКЗ, от 05.02.2014 № 2-ФКЗ, от 21.07.2014 № 11-ФКЗ). URL: http://www.consultant.ru/document/cons_doc_LAW_28399/ (дата обращения: 17.10.2018).

21. О персональных данных: федеральный закон от 27 июля 2006 г. № 152-ФЗ (ред. от 31.12.2017). URL: http://www.consultant.ru/document/cons_doc_LAW_61801/ (дата обращения: 13.10.2018).

Reference

1. Pinkevich T.V. Development of digital technologies in Russia and their impact on the level of criminological security. *Actual problems of combating corruption crimes and crimes in the sphere of economy: collection of materials International scientific and practical conference (31 October 2017, Nizhny Novgorod)*. Nizhny Novgorod, 2018. P. 374—380. (In Russ.)

2. Pinkevich T.V. Criminological risks of the industry of digital technology in Russia. *Criminal realities, respond tion and law (Moscow, 23—24 January 2018) / under the editorship of A.I. Dolgova*. Moscow, 2018. P. 94—99. (In Russ.)

3. Internet in Russia: the main figures. URL: <http://security.mosmetod.ru/internet-zavisimosti/97-internet-v-rossii-2018-glavnye-tsifry> (accessed 13.10.2018). (In Russ.)

4. Big Data world in 8 terms. URL: <https://rb.ru/howto/big-data-in-8-terms/> (accessed 14.10.2018). (In Russ.)

5. Chernyak L. big Data — new theory and practice. *Open systems. DBMS*, 2011, no. 10. URL: https://www.osp.ru/os/2011/10/13012252/ISSN_1028-7493 (accessed 14.10.2018). (In Russ.)

6. On the Strategy of development of the information society in the Russian Federation for 2017—2030: decree of the President of the Russian Federation of 09.05.2017 no. 203. URL: http://www.consultant.ru/document/cons_doc_LAW_216363/e91cc5f89aac60e19c6554fc03432f4ee971/ (accessed 14.10.2018). (In Russ.)

7. On approval of programme “Digital economy of the Russian Federatsii”: the government of the Russian Federation from 28.07.2017 no. 1632-p. URL: http://www.consultant.ru/document/cons_doc_LAW_221756/2369d7266adb33244e178738f67f181600cac9f2/ (accessed 14.10.2018). (In Russ.)

8. Boyeva N. New startups in the field of Big Data have good chances of success. *Kommersant*. The Internet newspaper. URL: <https://www.kommersant.doc/3083474> (accessed 14.10.2018). (In Russ.)

9. Larina E.S., Ovchinsky V.S. Crime of the future is already here. Moscow: Book world Publ., 2018. (In Russ.)

10. Mamontova M.Y. Present and future of large user data. Materials of the interuniversity scientific-practical conference with international participation. Moscow, 2017. (In Russ.)

11. Putin urged to make Russia one of the world centers of Big Data. URL: <https://www.rbc.ru/rbcfreenews/5a97d1bd9a79476b19eab85c> (accessed 14.10.2018). (In Russ.)

12. The draft law on the regulation of Big Data will contribute to the end of the year. URL: <https://pravo.ru/news/205919/> (accessed 14.10.2018). (In Russ.)

13. The law on Big Data will allow Russians to prohibit the collection of data about themselves. URL: https://www.rbc.ru/technology_and_media/27/03/2017/58d551429a794719618a4245 (accessed 14.10.2018). (In Russ.)

14. The court complicated the life of Big Data in Russia. URL: <http://expert.ru/2018/01/30/sud-oslozhnil-zhizn-big-data-v-rossii/> (accessed 14.10.2018). (In Russ.)

15. Lane J., Stodden V., Bender S., Nissenbaum H. Privacy, Big Data, and the public Good: Framework for engagement. Cambridge. Cambridge University Press. 2014. (In Russ.)

16. Who will store the data of users of communication services from July 1? URL: <http://duma.gov.ru/news/27433/> (accessed 16.10.2018). (In Russ.)

17. On approval of requirements and methods for depersonalization of personal data: order of the Federal service for supervision of communications, information technology and mass communications of 05.09.2013 no. 996. URL: <http://www.garant.ru/products/ipo/prime/doc/70351476/> (accessed 17.10.2018). (In Russ.)

18. Universal Declaration of human rights (adopted by the UN General Assembly on 10.12.1948). URL: http://www.consultant.ru/document/cons_doc_LAW_120805/ (accessed 17.10.2018). (In Russ.)

20. The Constitution of the Russian Federation (adopted by popular vote 12.12.1993) (subject to amendments made by the Laws of the Russian Federation on amendments to the Constitution of 30.12.2008 no. 6-FKZ, from 30.12.2008 no. 7-FKZ, from 05.02.2014 no. 2-FKZ, from 21.07.2014 no. 11-FKZ). URL: http://www.consultant.ru/document/cons_doc_LAW_28399/ (accessed 17.10.2018). (In Russ.)

19. International Covenant on civil and political rights (new York, 16 December 1966). URL: <http://base.garant.ru/2540295/> (accessed 17.10.2018). (In Russ.)

21. On personal data: federal law no. 152-FZ of 27.07.2006 (as amended on 31.12.2017). URL: http://www.consultant.ru/document/cons_doc_LAW_61801/ (accessed 13.10.2018). (In Russ.)