УДК 34 **DOI: 10.34670/AR.2020.78.29.027**

Автоматизированная обработка персональных данных как особый институт охраны права на неприкосновенность частной жизни

Лазукина Владлена Андреевна

Аспирант кафедры уголовно-правовых дисциплин,
Московский городской педагогический университет,
129226, Российская Федерация, Москва, пр-д 2-й Сельскохозяйственный, 4;
e-mail: Lazukina@mail.ru

Аннотация

Масштабная цифровизация, несмотря на позитивные последствия ее развития, предполагает в том числе и отказ от частной жизни. В статье рассмотрены особенности правовой охраны персональных данных в информационном пространстве. Определена роль государства и субъекта персональных данных в защите права на неприкосновенность частной жизни. Указывается на то, что автоматизированная обработка персональных данных – это особый институт охраны права на неприкосновенность частной жизни. В настоящее время наблюдается переходное состояние экономики, характеризующееся взаимным сосуществованием классических и цифровых моделей и технологий организации жизнедеятельности. Растет объем цифрового присутствия, а следовательно, и объем цифровых следов, что может привести к переходу данных в руки третьих лиц. Для обеспечения охраны права на неприкосновенность частной жизни недостаточно принятия мер на государственном уровне. Делается вывод о том, что необходимо стремиться к тому, чтобы устранить противоречия между принципами развития цифровой экономики и концепций охраны частной жизни.

Для цитирования в научных исследованиях

Лазукина В.А. Автоматизированная обработка персональных данных как особый институт охраны права на неприкосновенность частной жизни // Вопросы российского и международного права. 2020. Том 10. № 10А. С. 241-248. DOI: 10.34670/AR.2020.78.29.027

Ключевые слова

Право на информацию, право на неприкосновенность частной жизни, конфиденциальность, цифровые технологии, цифровизация, персональные данные, автоматизированная обработка.

Введение

Информационное пространство сформировано в результате развития информационных систем и технологий, во многом способствующего увеличению потока информационного взаимодействия, позволяющего отражать все стороны общественной жизни в реальном времени. Этот факт остро ставит перед государством, в частности перед правоприменителями и законодателями, обязанность непрерывного обеспечения гарантии прав граждан на неприкосновенность частной жизни.

В Докладе Верховного комиссара ООН по правам человека от 3 августа 2018 г. отмечено, что развитие цифровых технологий, в том числе Big Data или искусственного интеллекта, обусловило увеличение объема используемых в них данных, касающихся экономической, социальной, политической и иных сфер жизни, в том числе данных о частной жизни [Доклад Верховного комиссара…, www]. Все это порождает угрозу формирования цифровой среды, которая предоставит государству и коммерческим предприятиям возможность отслеживать в широких масштабах данные о людях, проводить анализ и прогнозировать их поведение, предпринимать попытки манипулирования массами. В Доктрине информационной безопасности РФ также отмечается, что полная обработка данных с использованием информационно-телекоммуникационных систем приводит к росту числа преступлений в отношении конституционных прав граждан, связанных с неприкосновенностью частной жизни, личной и семейной тайной. Таким образом, масштабная цифровизация, несмотря на позитивные тенденции ее развития, предполагает в том числе и отказ от частной жизни, приводит к возникновению проблемы пределов и ограничений конституционного права граждан. Поток, в том числе трансграничный, персональных данных, подвергающихся автоматизированной обработке, увеличился и продолжает расти, что приводит к необходимости расширения гарантий прав физических лиц на неприкосновенность и уважение их частной жизни при реализации мирового принципа «свободы информации». Необходимо уточнить, что персональные данные рассматриваются нами как особо охраняемый объект частной жизни, объект организационно-правовой защиты, который представляет собой производную от права на неприкосновенность частной жизни [Макаров, Вологдина, 2019, 72].

Основная часть

Неприкосновенность частной жизни является одним из основных прав и свобод человека, которые не могут умаляться, неотчуждаемы и признаются в силу рождения. На уровне государства данное право закреплено в Конституции РФ, на международном уровне регламентировано ст. 12 Всеобщей декларации прав человека, ст. 17 Международного пакта о гражданских и политических правах, ст. 8 Конвенции о защите прав человека и основных свобод. Наступление века цифровых технологий наделяет особым значением конфиденциальность информации, в том числе информации о человеке и его жизни. В соответствии с пояснительной запиской к проекту Федерального закона № 262191-5 «О внесении изменения в статью 25 Федерального закона “О персональных данных”» (снят с рассмотрения Государственной Думы V созыва в связи с отзывом субъектом права законодательной инициативы) [Пояснительная записка…, www], информационные системы персональных данных в Российской Федерации начали создаваться юридическими лицами в начале 1990-х гг. При этом унификация законодательства в области защиты персональных

данных, в том числе подверженных автоматизированной обработке, была произведена посредством принятия Федерального закона от 27 июля 2006 г. № 152-ФЗ.

Автоматизированная обработка, согласно Конвенции о защите физических лиц при автоматизированной обработке персональных данных, представляет собой совокупность операций, осуществляемых полностью или частично с помощью автоматизированных средств: хранение данных, осуществление логических и/или арифметических операций с этими данными, их изменение, уничтожение, поиск или распространение. Согласно подготовленному Роскомнадзором докладу «Меры административного воздействия, принятые Роскомнадзором в первом полугодии 2019 года, в отношении операторов, чьи действия были обжалованы субъектами персональных данных», в первом полугодии поступило 25 768 жалоб от граждан по вопросам защиты персональных данных [Меры…, www]. По категориям операторов большинство заявлений поступили о нарушениях прав граждан на сайтах (26%), банками (17%), организациями ЖКХ (8%), коллекторами (4%). Предметом жалоб на сайты выступали обработка интернет-ресурсами персональных данных в отсутствие согласия граждан либо иных правовых оснований, отсутствие на сайте политики в отношении обработки персональных данных, создание «фейковых» аккаунтов. Подтвердились лишь 7,6% (1958) жалоб от общего количества. Количество жалоб, поданных в Роскомнадзор, несоизмеримо меньше общего количества случаев утечки данных, что отражает высокую латентность процесса обнаружения утечек и привлечения к ответственности виновных, говорит о недоверии граждан к эффективности мер, принимаемых уполномоченным органом по защите прав субъектов персональных данных. Для примера обратимся к подготовленной Risk Based Security статистике распространения киберугроз по количеству случаев утечки данных за 9 месяцев 2019 г., которое составило 7,9 млрд и выросло по сравнению с аналогичным периодом 2018 г. в два раза. Большинство утечек произошли из государственных и медицинских учреждений, организаций сферы розничной торговли [Что такое…, www]. Уязвимость данных в информационном пространстве может повлечь несоразмерные последствия как для определенных лиц, так или для группы лиц, для общества в целом, что усугубляет неравенство и дискриминацию.

Наличие у государства и компаний широкого доступа к личным данным физических лиц, а также отсутствие должного представления граждан о правовых гарантиях, о механизмах эффективного контроля за тем, кем и в каких целях используется информация об их личности и жизни, – основные причины задуматься о необходимости обеспечения мер, направленных на устранение допущенного дисбаланса для прав и свобод человека, на смягчение последствий вторжения в «privacy». Возвращаясь к Докладу Верховного комиссара ООН по правам человека, обозначим действия государства, которые не только не направлены на защиту конституционного права, но и приводят к достижению обозначенного дисбаланса.

1) Расширение использования личных данных правительствами и компаниями, к которому относятся «усиление цифрового следа» за счет увеличения потока данных через компьютеры, смартфоны, иные аксессуары и устройства, содержащие в себе данные пользователя; «обмен и сведение данных» между государством и компаниями, размывающий границы определения конечного обладателя информацией; «сбор и использование биометрических данных», которые приводят к созданию централизованных баз данных хранения информации как в целях национальной безопасности, так и в иных целях, большинство из которых не ясны гражданам, при этом

остаются вопросы необходимости и соразмерности их сбора[1]. Еще одним пунктом является «укрепление аналитического потенциала»: используя методы анализа больших данных и искусственный интеллект, государство не только способно получать информацию о жизни людей, но также оценивать и делать выводы о физических и психоэмоциональных характеристиках человека, принимать автоматические решения на основе анализа, профилирования и оценки массива информации.

2) Государственное слежение и перехват сообщений носят массовый характер, осуществляются тайно, не позволяют оценить правомерность сбора на предмет соразмерности и необходимости, однако обосновываются государством как защищающие национальную безопасность. Несмотря на запрет такой практики на международном уровне, Верховный комиссар ООН упоминает об этом. Превентивные меры ООН хотя и носят императивный характер, зачастую не влияют на политику внутри государства. Страны продолжают идти на ущемление прав граждан, прикрываясь государственными интересами. Формальные цели в виде обеспечения национальной безопасности приводят к вовлечению коммерческих предприятий в предоставление государственным структурам прямого доступа к потоковым данным. В качестве примера выступают императивные требования государств к поставщикам телекоммуникационных услуг и услуг доступа в Интернет, что ограничивает возможности анонимного общения, приводит к злоупотреблениям, облегчает нелегитимное раскрытие информации третьим лицам. К угрозам безопасности и обеспечения конфиденциальности также приводят попытки государств ослабить технологии шифрования и ограничить анонимность в информационном пространстве, что напрямую влияет на нарушение права на неприкосновенность частной жизни.

Анализ способов посягательства государства на неприкосновенность частной жизни отражает политику двойных стандартов, при проведении которой, с одной стороны, необходимо защищать субъектов персональных данных от нарушения их конституционного права, с другой стороны, обходить собственно установленные правовые рамки для достижения стратегических целей и решения государственных задач. Там, где начинаются интересы общества и государства, заканчиваются права граждан относительно их персональных данных. Ограничения прав субъектов персональных данных в связи с обеспечением общественных интересов, безопасности государства и общественной безопасности установлены и российским законодательством.

Переходя от государства и организаций к иным лицам, которые могут завладеть информацией в противоправных целях, следует отметить, что они представляют собой наибольшую угрозу по сравнению с рассмотренными ранее. Извлечение финансовой выгоды, сбор информации, дестабилизация электронных систем с целью вызвать страх и панику – основные мотивы лиц, причастных к совершению киберпреступлений, кибератак и кибертерроризма. В качестве инструментов достижения результатов злоумышленниками используются вредоносное программное обеспечение, SQL-инъекции, фишинг, DoS-атаки, атаки Man-in-the-Middle. В данном случае обязанность государства принимать законодательные

[1] Подробнее см. Невьянцева В.А. Единый федеральный информационный регистр, содержащий сведения о населении: вопросы актуальности создания системы и обеспечения защиты персональных данных // Юридическая наука. 2020. № 10. С. 17-20.

и иные меры для введения в действие запрета и защиты от незаконного или произвольного вмешательства и вторжений государства, физических и юридических лиц, предусмотренная п. 1 ст. 2 Международного пакта о гражданских и политических правах, наиболее актуальна. Именно для исключения таких угроз государство должно предпринимать все без исключения меры, даже несмотря на то, что процедура может ограничивать права и свободы лиц, в данном случае подозреваемых в нарушении конституционных прав граждан, ущемлении интересов общества и государства. Это не может расцениваться как дискриминация, это защита прав большинства от преступных посягательств.

Личные данные уязвимы, подвержены несанкционированному разглашению, изменению и удалению. Надлежащие меры безопасности должны приниматься всеми лицами, вовлеченными в сбор, обработку и хранение данных, включая субъекта персональных данных, операторов и иных лиц, имеющих доступ к данным. На уровне субъекта персональных данных необходимо в том числе предпринимать меры для снижения рисков безопасности в условиях «транзитного мира» и эффективного перехода к цифровой эпохе. Роскомнадзор разработал и разместил в открытом доступе Методические рекомендации по организационной защите физическим лицом своих персональных данных, направленные на принятие физическими лицами всех зависящих от них мер, чтобы обеспечить себе контролируемое цифровое присутствие, минимизировать проявление вынужденного цифрового присутствия, осуществляемого без участия самого субъекта путем деятельности третьих лиц [Методические рекомендации…, www]. Субъектам, осуществляющим обработку данных, необходимо создать внутренний механизм надзора за возможными угрозами нарушения целостности данных и несанкционированного доступа, а также обеспечить принцип открытости в части уведомления о нарушении конфиденциальности данных всех лиц, чьи права оказались нарушены. Следует отметить, что существенное значение имеет не возмещение ущерба, уже причиненного посягательством, а недопущение нанесение ущерба, его смягчение, предотвращение возможности нарушения права на неприкосновенность частной жизни. Рассматривая роль государства в обеспечении охраны права на неприкосновенность частной жизни в Российской Федерации, необходимо создать более серьезную нормативно-правовую, организационную базу, предоставить независимость уполномоченному органу по защите прав субъектов персональных данных с целью наделения его достаточными правовыми полномочиями для выполнения возложенных функций, предоставления возможности привлекать к ответственности в соответствии с санкциями, соразмерными совершенным нарушениям, но не ограничивающимися санкциями административно-правовых норм.

Заключение

Автоматизированная обработка персональных данных – особый институт охраны права на неприкосновенность частной жизни. В настоящее время наблюдается переходное состояние экономики, характеризующееся взаимным сосуществованием классических и цифровых моделей и технологий организации жизнедеятельности. Растет объем цифрового присутствия, а следовательно, и объем цифровых следов, что может в случае непринятия превентивных мер привести к переходу данных в руки третьих лиц. Особое внимание заслуживает тот факт, что для обеспечения охраны права на неприкосновенность частной жизни недостаточно принятия мер на государственном уровне. К сожалению, большинство граждан не задумываются, какие персональные данные ими производятся, в каком объеме и каким субъектам они эти данные

передают, в том числе в информационном пространстве. Все это приводит к возникновению новых угроз для общества, а такое поведение является неэффективным в части использования ресурсов цифровой экономики. Для развития Big Data и искусственного интеллекта такая халатность, приводящая к бесконтрольному распространению персональных данных, только на руку. При этом необходимо стремиться к тому, чтобы устранить противоречия между принципами развития цифровой экономики и концепций охраны частной жизни.

Библиография

1. Всеобщая декларация прав человека. URL: http://www.consultant.ru/document/cons_doc_LAW_120805/
2. Доклад Верховного комиссара ООН по правам человека «Право на неприкосновенность частной жизни в цифровой век». URL: https://undocs.org/pdf?symbol=ru/A/HRC/39/29
3. Конвенция о защите прав человека и основных свобод. URL: http://www.consultant.ru/document/cons_doc_LAW_29160/
4. Конвенция о защите физических лиц при автоматизированной обработке персональных данных. URL: http://www.consultant.ru/document/cons_doc_LAW_121499/
5. Конституция Российской Федерации: принята всенародным голосованием 12.12.1993. URL: http://www.consultant.ru/document/cons_doc_LAW_28399/
6. Макаров А.В., Вологдина Е.С. Персональные данные как объект преступных посягательств на неприкосновенность частной жизни: законодательный опыт в России и зарубежных странах // Российский следователь. 2019. № 5. С. 71-75.
7. Международный пакт о гражданских и политических правах. URL: http://base.garant.ru/2540295/
8. Меры административного воздействия, принятые Роскомнадзором в первом полугодии 2019 года, в отношении операторов, чьи действия были обжалованы субъектами персональных данных. URL: https://pd.rkn.gov.ru/docs/DOD_30.07.19.pdf
9. Методические рекомендации по организационной защите физическим лицом своих персональных данных. URL: https://pd.rkn.gov.ru/library/p195/
10. О персональных данных: федер. закон Рос. Федерации от 27.07.2006 № 152-ФЗ: принят Гос. Думой Федер. Собр. Рос. Федерации 08.07.2006: одобр. Советом Федерации Федер. Собр. Рос. Федерации 14.07.2006. URL: http://www.consultant.ru/document/cons_doc_LAW_61801/
11. Об утверждении Доктрины информационной безопасности Российской Федерации: указ Президента РФ от 05.12.2016 № 646. URL: http://www.consultant.ru/document/cons_doc_LAW_208191/
12. Пояснительная записка к проекту Федерального закона № 262191-5 «О внесении изменения в статью 25 Федерального закона “О персональных данных”». URL: https://sozd.duma.gov.ru/bill/262191-5
13. Ромашов П.А. К вопросу о праве на неприкосновенность частной жизни в цифровой век // Пермский юридический альманах. 2019. № 1. С. 103-118.
14. Что такое кибербезопасность? URL: https://www.kaspersky.ru/resource-center/definitions/what-is-cyber-security

Automated processing of personal data as a special institution protecting the right to privacy

Vladlena A. Lazukina

Postgraduate at the Department of criminal law disciplines,
Moscow City University,
129226, 4 2nd Selskokhozyaystvenny passage, Moscow, Russian Federation;
e-mail: Lazukina@mail.ru

Abstract

Large-scale digitalisation, despite the positive consequences of its development, also involves sacrificing private life. The article aims to discuss the features of the legal protection of personal

data in the information space. It makes an attempt to identify the role of the state and the subject of personal data in the protection of the right to privacy in the Russian Federation. The author of the article points out that automated processing of personal data is considered to be a special institution that protects the right to privacy. Currently, there is a transitional state of the economy, characterised by the mutual coexistence of classical and digital models and technologies of life organisation. The digital presence is growing, and therefore the volume of digital traces is also increasing, which can lead to the transfer of data to third parties. It is not enough to take measures at the state level in order to ensure the protection of the right to privacy. Having considered automated processing of personal data as a special institution protecting the right to privacy, the author concludes that it is necessary to strive to eliminate the contradictions between the principles of digital economy development and the concepts of privacy protection.

For citation

Lazukina V.A. (2020) Avtomatizirovannaya obrabotka personal'nykh dannykh kak osobyi institut okhrany prava na neprikosnovennost' chastnoi zhizni [Automated processing of personal data as a special institution protecting the right to privacy]. *Voprosy rossiiskogo i mezhdunarodnogo prava* [Matters of Russian and International Law], 10 (10A), pp. 241-248. DOI: 10.34670/AR.2020.78.29.027

Keywords

Right to information, right to privacy, confidentiality, digital technologies, digitalisation, personal data, automated processing.

References

1. *Chto takoe kiberbezopasnost'?* [What is cybersecurity?] Available at: https://www.kaspersky.ru/resource-center/definitions/what-is-cyber-security [Accessed 25/08/20].
2. *Doklad Verkhovnogo komissara OON po pravam cheloveka "Pravo na neprikosnovennost' chastnoi zhizni v tsifrovoi vek"* [The report of the United Nations High Commissioner for Human Rights "The right to privacy in the digital age"]. Available at: https://undocs.org/pdf?symbol=ru/A/HRC/39/29 [Accessed 25/08/20].
3. *Konstitutsiya Rossiiskoi Federatsii: prinyata vsenarodnym golosovaniem 12.12.1993* [Constitution of the Russian Federation: adopted by popular vote on December 12, 1993]. Available at: http://www.consultant.ru/document/cons_doc_LAW_28399/ [Accessed 25/08/20].
4. *Konventsiya o zashchite fizicheskikh lits pri avtomatizirovannoi obrabotke personal'nykh dannykh* [Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data]. Available at: http://www.consultant.ru/document/cons_doc_LAW_121499/ [Accessed 25/08/20].
5. *Konventsiya o zashchite prav cheloveka i osnovnykh svobod* [Convention for the Protection of Human Rights and Fundamental Freedoms]. Available at: http://www.consultant.ru/document/cons_doc_LAW_29160/ [Accessed 25/08/20].
6. Makarov A.V., Vologdina E.S. (2019) Personal'nye dannye kak ob"ekt prestupnykh posyagatel'stv na neprikosnovennost' chastnoi zhizni: zakonodatel'nyi opyt v Rossii i zarubezhnykh stranakh [Personal data as an object of criminal attacks on privacy: legislative experience in Russia and foreign countries]. *Rossiiskii sledovatel'* [Russian investigator], 5, pp. 71-75.
7. *Mery administrativnogo vozdeistviya, prinyatye Roskomnadzorom v pervom polugodii 2019 goda, v otnoshenii operatorov, ch'i deistviya byli obzhalovany sub"ektami personal'nykh dannykh* [Administrative measures taken by Federal the Service for Supervision of Communications, Information Technology and Mass Media in the first half of 2019 against operators whose actions were appealed by personal data subjects]. Available at: https://pd.rkn.gov.ru/docs/DOD_30.07.19.pdf [Accessed 25/08/20].
8. *Metodicheskie rekomendatsii po organizatsionnoi zashchite fizicheskim litsom svoikh personal'nykh dannykh* [Guidelines for the organisational protection of personal data by an individual]. Available at: https://pd.rkn.gov.ru/library/p195/ [Accessed 25/08/20].
9. *Mezhdunarodnyi pakt o grazhdanskikh i politicheskikh pravakh* [International Covenant on Civil and Political Rights].

Available at: http://base.garant.ru/2540295/ [Accessed 25/08/20].
10. *O personal'nykh dannykh: feder. zakon Ros. Federatsii ot 27.07.2006 № 152-FZ: prinyat Gos. Dumoi Feder. Sobr. Ros. Federatsii 08.07.2006: odobr. Sovetom Federatsii Feder. Sobr. Ros. Federatsii 14.07.2006* [On personal data: Federal Law of the Russian Federation No. 152-FZ of July 27, 2006]. Available at: http://www.consultant.ru/document/cons_doc_LAW_61801/ [Accessed 25/08/20].
11. *Ob utverzhdenii Doktriny informatsionnoi bezopasnosti Rossiiskoi Federatsii: ukaz Prezidenta RF ot 05.12.2016 № 646* [On approving the Information Security Doctrine of the Russian Federation: Decree of the President of the Russian Federation No. 646 of December 5, 2016]. Available at: http://www.consultant.ru/document/cons_doc_LAW_208191/ [Accessed 25/08/20].
12. *Poyasnitel'naya zapiska k proektu Federal'nogo zakona № 262191-5 "O vnesenii izmeneniya v stat'yu 25 Federal'nogo zakona "O personal'nykh dannykh""* [The explanatory note on Draft Federal Law No. 262191-5 "On amending Article 25 of the Federal Law "On personal data""]. Available at: https://sozd.duma.gov.ru/bill/262191-5 [Accessed 25/08/20].
13. Romashov P.A. (2019) K voprosu o prave na neprikosnovennost' chastnoi zhizni v tsifrovoi vek [On the right to privacy in the digital age]. *Permskii yuridicheskii al'manakh* [Perm legal almanac], 1, pp. 103-118.
14. *Vseobshchaya deklaratsiya prav cheloveka* [Universal Declaration of Human Rights]. Available at: http://www.consultant.ru/document/cons_doc_LAW_120805/ [Accessed 25/08/20].