Проблемы интеграции и интернационализации права и правовых систем в сфере цифровых технологий

Армен Жоресович СТЕПАНЯН,
доцент кафедры интеграционного и европейского права Университета имени О.Е. Кутафина (МГЮА), кандидат юридических наук
armen@stepanyan.com
125993, Россия, г. Москва, ул. Садовая-Кудринская, д. 9

РЕГУЛИРОВАНИЕ ЦИФРОВЫХ ТЕХНОЛОГИЙ: ЦИФРОВИЗАЦИЯ ИЛИ ГУМАНИЗАЦИЯ?[1]

Аннотация. *Рассматриваются аспекты применения цифровых технологий, в частности их влияние на права человека. Анализируется текущее содержание права цифровых технологий в части реальной возможности реализации прав и свобод человека и гражданина, в том числе в сложных информационных системах. Делается вывод о необходимости анализа применения технологии на предмет достижения баланса возможных благ для общества и потенциальных нарушений прав человека, а также принятии мер по регулированию такого применения, в частности документирования. Таким образом, создается возможность реальной реализации прав человека.*

Ключевые слова: *цифровые технологии, диджитализация, права человека.*

DOI: 10.17803/2311-5998.2020.68.4.114-120

A. G. STEPANIAN,
Associate Professor of Integrational and European Law Department of the Kutafin Moscow State Law University (MSAL), PhD in Law
armen@stepanyan.com
125993, Russia, Moscow, ul. Sadovaya-Kudrinskaya, 9

DIGITAL REGULATION: DIGITALIZATION OR HUMANIZATION?

Abstract. *Aspects of the application of digital technologies are examined, in particular, their impact on human rights. The current content of digital technology law is analyzed in terms of the real possibility of realizing the rights and freedoms of man and citizen, including in complex information systems. The conclusion is drawn on the need to analyze the application of technology with a view to achieving a balance of possible benefits for society and potential violations of human rights, as well as taking measures to regulate such use, in particular, documentation. Thus, it is possible to leave the possibility of real realization of human rights.*

Keywords: *digital technologies, digitalization, human rights.*

[1] Статья подготовлена в рамках проекта РФФИ № 18-29-16172.

Оборот персональных данных необратимо проник в нашу жизнь, а многочисленные сервисы и даже простые покупки все больше и больше направлены на персонализацию, использование личных предпочтений, особенностей, все больше используют категории того, что обычно люди называют личным пространством. Кто-то честно публикует условия, по сути, предлагая скидку или иное материальное благо в обмен на сами данные, ну а кто-то прячет мелкий текст в дебрях сайта, найти на котором информацию часто очень сложно или практически невозможно для среднего обывателя.

Все это обычно законно, т.е. соответствует положениям закона. При этом очевидно, что потребитель (гражданин) всегда является более слабой стороной, чем оператор персональных данных, ведь если у последнего есть ресурсы организовать обработку данных, то у гражданина контролировать такую обработку обычно нет возможностей. И если говорить о все том же обороте персональных данных, то перед анализом возможного будущего регулирования сто́ит рассмотреть вопрос о том, всегда ли возможно реализовывать те права, которые уже и так закреплены законодательством.

В частности, как указано в п. 7 ст. 5 Федерального закона «О персональных данных»[2], обрабатываемые персональные данные подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом. А в пункте 5 ст. 21 определено, что в случае отзыва гражданином согласия на обработку его персональных данных оператор обязан прекратить их обработку и, если сохранение персональных данных более не требуется для целей обработки персональных данных, уничтожить персональные данные или обеспечить их уничтожение, если иное не предусмотрено договором. Альтернативой является упомянутая в п. 6 ст. 21 Закона возможность блокирования таких данных в течение 6 месяцев и их уничтожение.

Однако автору несколько раз встречались в Интернете[3] вопросы работников тех или иных организаций (финансовых, интернет-магазинов) о том, как обеспечить реальное выполнение уничтожения данных, так как интерфейс информационной системы, обеспечивающей работоспособность организации, не позволял удалить данные самого клиента, а также его действия в системе или по отношению к организации. На запросы в технический отдел давались от не знакомых с требованиями законодательства специалистов ответы о невозможности совершения такого рода операции, так как при проектировании системы не было запроса на ее реализацию.

В действительности такое удаление возможно провести, однако оно, в зависимости от реализации информационной системы и структуры базы данных, использующейся в этой системе, вероятно, будет трудозатратным. Возможно даже, что техническими специалистами, не понимающими положений закона, такое

[2] Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» // Российская газета. 29.07.2006. № 165.

[3] См.: URL: https://www.sql.ru/forum/796094/udalenie-personalnyh-dannyh ; URL: https://www.sql.ru/forum/827801/polnoe-udalenie-dannyh-iz-bazy-postgresql (дата обращения: 20.01.2020).

уничтожение фактически не будет выполнено, а может быть, будет выполнено путем анонимизации или замены данных субъекта данными другого субъекта, в том числе вымышленного.

Налицо нарушение законодательства. Следует поставить вопрос: кто виноват — заказчики системы, не давшие задание реализовать возможность блокирования и (или) удаления данных, или разработчики, не знающие законодательства? Ответ на него не так очевиден. Конечно, программисты не должны проектировать действие самих информационных систем, однако можно сказать, что непосредственно с самими данными они должны проектировать и возможности как их заведения, так и их удаления.

Принятый в 2016 г. и вступивший в силу в 2018 г. Общий регламент по охране персональных данных[4] (GDPR) сделал ситуацию для подобных организаций более сложной. Так, в ст. 25 GDPR указано, что, «принимая во внимание состояние развития науки и техники, расходы на внедрение, характер, объем, особенности и цели обработки, а также вероятностное возникновение рисков и опасности для прав и свобод физических лиц в результате обработки, контролер должен как во время определения средств обработки, так и во время самой обработки внедрить соответствующие технические и организационные меры, например, псевдонимизацию, которые предназначены для эффективной реализации принципов защиты данных, например минимизации данных, и для интегрирования необходимых гарантий в обработку в целях выполнения требований настоящего Регламента и защиты прав субъектов данных».

Как видно, установлены требования организационных мер, в том числе не только простых с логической точки зрения (архитектуры информационной системы), таких как уничтожение, но и достаточно непростых — таких как псевдонимизация и минимизация (которые, в свою очередь, прямо поименованы, т.е., по сути, внесены в обязательный список).

Так, GDPR установил и большие штрафы за несоответствие этому регламенту: ст. 83 говорит о максимальных 20 млн евро, или 4 % общемирового оборота за последний год. И практика — тому подтверждение: штрафы за нарушение в том числе ст. 25 за 2019 г. колеблются от 1 300 евро до 14,5 млн евро[5]. Самый большой штраф за год (более 70 % от максимальной суммы) был получен риэлторской компанией Deutsche Wohnen SE из Берлина из-за невозможности удалять уже ненужные данные[6] (хранился весь архив их клиентов — арендаторов недвижимости). При этом хранились все сведения, полученные от клиентов, включая данные

---

[4] Regulation (EU) 2016/679 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) (Text with EEA relevance) // OJ L. 119. 04.05.2016. C. 1—88.

[5] Данные штрафов по GDPR можно отследить на сайте URL: https://enforcementtracker.com/ (дата обращения: 20.01.2020).

[6] Пресс-релиз Berliner Datenschutzbeauftragteverhängt Bußgeldgegen Immobiliengesellschaft надзорного органа Берлинавсфере персональных данных // URL: https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/pressemitteilungen/2019/20191105-PM-Bussgeld_DW.pdf (дата обращения: 20.01.2020).

о личном и финансовом положении арендаторов, о заработной плате, налогах, медицинском страховании, социальном обеспечении, банковских счетах, а также выписки к ним, самостоятельно заявленные данные и т.д. Как видно, такой объем данных был действительно не нужен, однако хранился. Стóит отметить, что в отношении этой же компании орган выписал еще 15 штрафов от 6 до 17 тыс. евро каждый за конкретные случаи недолжного хранения данных клиентов.

Как видно, принципы обработки данных должны быть рассмотрены еще при проектировании информационной системы, при выстраивании ее архитектуры и дизайна (конечно, не графического, не интерфейса между машиной и человеком). Указанный подход имел место среди специалистов отрасли[7] и в научной литературе на протяжении достаточного количества времени[8]. В отношении персональных данных он получил обобщенное название Privacy by Design (англ. дословно — частная жизнь (конфиденциальность) по замыслу)[9]. Европейский совет по персональным данным даже выпустил проект рекомендаций по соблюдению ст. 25 GDPR[10], т.е. принципов проектирования систем. И реальностью стало то, что в Европейском Союзе компании сурово наказывают за несоблюдение такого подхода.

В поддержку своей позиции законодатель выпустил два акта: Регламент о свободном движении данных и Директиву об открытых данных и повторном использовании информации публичного сектора, которые не касаются персональных данных и призваны улучшить обработку таких данных. Таким образом, что касается обработки информации, не затрагивающей непосредственно и прямо права граждан, то ее оборот был облегчен. Это касается в том числе и анонимной информации.

Подобный подход, который ставит во главу угла интересы граждан как слабой стороны, а не компаний, продемонстрировала Европейская комиссия в подходе

---

[7] *Cavoukian A.* [комиссар по информации и частной жизни в Онтарио, Канада]. Privacy by Design. The 7 Foundational Principles, в ред. янв. 2011 г. // URL: https://www.ipc.on.ca/wp-content/uploads/resources/7foundationalprinciples.pdf (дата обращения: 20.01.2020).

[8] *Edwards L., Veale M.* Slave to the Algorithm? Why a 'Right to an Explanation' Is Probably Not the Remedy You Are Looking For (May 23, 2017). 16 Duke // Law & Technology Review. 2017. 18 ; *Spiekermann S., Cranor L. F.* Engineering Privacy. Jänner/Februar 2009 // IEEE Transactions on Software Engineering. Vol. 35. 2009. No. 1 ; *Richards Neil M., Smart W. D.* How Should the Law Think About Robots? May 10, 2013 ; *Rubinstein I., Good N.* Privacy by Design: A Counterfactual Analysis of Google and Facebook Privacy Incidents. August 11, 2012. 28 Berkeley // Technology Law Journal. 2013. 1333 ; NYU School of Law, Public Law Research Paper. No. 12—43 ; *Singh J., Walden I., Crowcroft J., Bacon J.* Responsibility & Machine Learning: Part of a Process. October 27, 2016.

[9] Встречаются и другие названия, например Privacy-by-architecture (конфиденциальность-по-архитектуре).

[10] Guidelines 4/2019 on Article 25 Data Protection by Design and by Default. В феврале — марте 2020 г. ожидается дополненная и измененная редакция после публичных консультаций // // URL: https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_201904_dataprotection_by_design_and_by_default.pdf (дата обращения: 20.01.2020).

к регулированию такой цифровой технологии, как искусственный интеллект (ИИ). «Утекший» к СМИ проект[11] позиции[12] законодателя указывает на риски из-за таких характеристик ИИ, как автономия, непрозрачность и способность увеличения производительности с помощью обучения.

Так, в частности, существующее в Европейском Союзе законодательство уже покрывает риски, связанные с использованием ИИ, в отношении фундаментальных прав человека (охрана данных, недискриминация, равенство полов, убежище, авторское право), защиты прав потребителя, безопасности товаров и ответственности за их несоблюдение. Одним из рисков также называется отсутствие регуляторных инструментов, чтобы убедиться в соответствии ИИ нормам текущего законодательства. Предлагается основывать регулирование на ценностях, и сто́ит вспомнить, что одним из учредительных документов Союза является Хартия ЕС об основных правах, по сути, первый документ, основанный на ценностном подходе.

Справедливо замечено: несмотря на то, что предвзятость может быть элементом решений и человека, и ИИ, в случае с ИИ это может затронуть большее количество людей, чем в случае с человеком, над которым существует множество социальных элементов контроля. Более того, ИИ может нарушить и другие основные права человека: свободу выражения, свободу собрания, человеческое достоинство. Эта же позиция выражена в одном из исследований0, Совета Европы[13]. Причем эти риски могут реализовываться как из-за ущербной архитектуры системы (или непосредственных настроек системы), так и из-за предвзятых данных, загруженных в систему. Но такие же риски могут быть реализованы и из-за практических примеров данных, их корреляций. Технология ИИ также может использоваться во вред и праву на охрану персональных данных: системы могут следить за пользователями, деанонимизировать (персонализировать) их, на основе больших массивов неперсонализированных данных вычислять конкретных людей.

Выделяются также риск безопасности для людей, которые используют товары или услуги со встроенным ИИ. Следует отметить, что выделяется и риск потери связи ИИ со связанным товаром или услугой (или наоборот). Это увеличивает проблемы при наложении ответственности согласно законодательству ЕС или национальному законодательству, так как непрозрачность, автономность и сложность могут затруднить доступ компетентных органов к информации о том, как решение ИИ было принято, на основании чего, были ли соблюдены установленные правила? А разные подходы государств к решению проблем этих рисков могут фрагментировать единый рынок ЕС.

---

[11] Structure on the White Paper on Artificial Intelligence — European Approach // URL: https://www.euractiv.com/wp-content/uploads/sites/2/2020/01/AI-white-paper-EURACTIV.pdf (дата обращения: 20.01.2020).

[12] Выражен в форме white paper (англ. — белая книга) — детального документа, в котором отражены позиции всех субъектов отношений.

[13] Algorithms and human rights. Study on the human rights dimensions of automated data processing techniques and possible regulatory implications. Council of Europe // URL: https://rm.coe.int/algorithms-and-human-rights-en-rev/16807956b5 (дата обращения: 20.01.2020).

Европейская комиссия четко выделяет акты о традиционных основных правах человека в качестве основы для законодательства ЕС в области ИИ: Хартия ЕС об основных правах, Директива о равенстве рас, Директива о равенстве при найме на работу, GDPR и др. Такое же значение придается и Общему регламенту о безопасности товаров[14].

Выделяются слабости текущего регулирования. Так, обращается внимание на ограничения сферы применения актов об основных правах человека, которые не всегда применяются в частном секторе. Ограничено и законодательство о безопасности товаров на рынке ЕС: услуги не подпадают под его сферу действия. Действие законодательства о безопасности товаров не распространяется на разработчика системы ИИ, только если он не производитель такой системы (как видно, ответственность разработчиков, т.е. фактически технических инженеров, возможно, близится). Внедрение ИИ изменяет сущность и функции товаров: новые риски безопасности возникают уже после продажи товара. Упоминается опять и сложность расследования инцидентов, возможной дискриминации.

Предполагается, что сто́ит различать роль операторов в цепочке создания товара с системой ИИ: разработчику действительно легче заложить что-то изначально, но на этапе использования он не всегда может воздействовать, а вот продавец или производитель, наоборот, может делать это гораздо чаще. Представляется, что выяснение этой роли в определенный момент времени для наложения ответственности или же какого-либо обязательства выглядит логично и обоснованно, однако может столкнуться, во-первых, в начальный период с трудностями у разработчиков, а во-вторых, с длительностью выяснения обстоятельств с целью вынесения справедливого решения.

Предлагается также налагать обязательства как до, так и после выпуска системы в оборот (например, как и должное проектирование, так и устранение ошибок), что выглядит разумным предложением.

Конкретные предложения мер регулирования состоят из 5 инициатив. Добровольная маркировка предполагает, что разработчики (производители) систем ИИ будут использовать таковую, самостоятельно выполнив требования по этике или комплаенсу ИИ. Секторальные требования для государственной администрации (и здесь Европейская комиссия использует ссылку на недавно принятый подобный акт в Канаде — Директиву об автоматическом принятии решений[15]) и распознавания лиц предполагают исследование всех рисков и их влияние на жизни людей и соответствующий запрет на использование технологии распознавания лиц на 3—5 лет.

Обязательные дополнительные требования к высокорисковым приложениям ИИ предполагаются в таких областях, как здравоохранение, транспорт, полиция, судебная система; и для эффектов в виде ранения, смерти или существенного материального вреда предусматривают также самооценку рисков и их уровня. Безопасность и ответственность — два принципа, которые остаются незыбле-

[14] Directive 2001/95/EC of the European Parliament and of the Council of 3 December 2001 on general product safety // *OJ L. 11. 15.01.2002.* P. 4—17.

[15] Directive on Automated Decision-Making // URL: https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=32592 (дата обращения: 20.01.2020).

мыми и должны быть оценены на предмет расширения по секторам, продуктам и системам. Управление предполагает прозрачность, а также активную позицию национальных органов, а органам ЕС будет поручено множество задач по изучению влияния систем ИИ на жизни людей и рисков в связи с таким влиянием.

Как видно, ответ на вопрос об ответственности разработчиков систем все еще не очевиден, но точно стал яснее в том, что в Европейском Союзе скоро разработчики должны будут учитывать требования законодательства как минимум при проектировании систем искусственного интеллекта.

Сделано это для главного — не забывать о правах человека, сохранить возможность их реализации, не нарушив функционирование в новом типе общества хрупкого послевоенного мира, базирующегося на фундаментальных актах в области прав человека. Поэтому цифровизация немыслима без гуманизации. Невозможно оцифровывать жизнь человека без того, чтобы его самого не ставить во главу угла, не давать ему возможность управлять цифровыми технологиями, не считаться с ним самим и его правами.

БИБЛИОГРАФИЯ

1. *Edwards L., Veale M.* Slave to the Algorithm? Why a ‘Right to an Explanation’ Is Probably Not the Remedy You Are Looking For. — May 23, 2017. — 16 Duke // Law & Technology Abstract. — 2017. — 18.
2. *Richards Neil M., Smart W. D.* How Should the Law Think About Robots? — May 10, 2013.
3. *Rubinstein I., Good N.* Privacy by Design: A Counterfactual Analysis of Google and Facebook Privacy Incidents. — August 11, 2012. — 28 Berkeley // Technology Law Journal. — 2013. — 1333 ; NYU School of Law, Public Law Research Paper. — No. 12—43.
4. *Singh J., Walden I., Crowcroft J., Bacon J.* Responsibility & Machine Learning: Part of a Process. — October 27, 2016.
5. *Spiekermann S., Cranor L. F.* Engineering Privacy. — Jänner/Februar 2009 // IEEE Transactions on Software Engineering. — Vol. 35. — 2009. — No. 1.