ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«РОССИЙСКАЯ АКАДЕМИЯ НАРОДНОГО ХОЗЯЙСТВА И ГОСУДАРСТВЕННОЙ СЛУЖБЫ ПРИ ПРЕЗИДЕНТЕ РОССИЙСКОЙ ФЕДЕРАЦИИ»
(РАНХиГС)

ПРЕПРИНТ
(НАУЧНЫЙ ДОКЛАД)

по теме:

АКТУАЛЬНЫЕ НАУЧНО-МЕТОДОЛОГИЧЕСКИЕ ПОДХОДЫ К ОБЕСПЕЧЕНИЮ ФУНДАМЕНТАЛЬНЫХ ПРАВ ЧЕЛОВЕКА ПРИ ОБРАБОТКЕ ДАННЫХ В ГОСУДАРСТВЕННОМ УПРАВЛЕНИИ

Талапина Э.В., в.н.с. ЦТГУ, д.ю.н., 0000-0003-3395-3126, talapina-ev@ranepa.ru

Южаков В.Н., директор ЦТГУ, д.ф.н., проф., 0000-0002-5687-1863,
yuzhakov-vn@ranepa.ru

Черешнева И.А., м.н.с. ЦТГУ, 0000-0001-8135-4166, chereshneva-ia@ranepa.ru

Москва 2021

Аннотация
Обеспечение фундаментальных прав человека является конституционной обязанностью российского государства; в цифровых условиях риски нарушений прав человека возрастают, что **актуализирует** необходимость реализации последовательной государственной политики, в частности, при обработке данных в государственном управлении. **Цель** исследования – анализ научно-методологических подходов к обеспечению фундаментальных прав человека при обработке данных в государственном управлении и возможностей их учета в российском государственном управлении. **Предмет** исследования составили научные публикации, судебные кейсы, нормативные правовые акты международного и национального уровня, в том числе зарубежных государств. В исследовании применены формально-правовой и историко-правовой **методы**, сравнительно-правовой метод, метод юридического толкования, логический анализ, общенаучные методы классификации и моделирования. **Результатами** стали аналитический обзор зарубежных и российских научно-методологических подходов к обеспечению фундаментальных прав человека при обработке данных в цифровом государственном управлении; систематизация базовых правовых основ обеспечения фундаментальных прав человека при обработке данных в государственном управлении; предложения по правовому обеспечению фундаментальных прав человека при обработке данных в российском государственном управлении. Исследование позволяет сделать **выводы** о недостаточном внимании в российской доктрине и практике к проблематике фундаментальных прав. Поскольку российское законодательство в данной области базируется на европейском законодательстве, рекомендуется реализация европейских подходов к защите данных. Необходимо создать специальное законодательство об обработке данных в государственном управлении, с определением критериев надлежащей обработки и хранения данных, дифференциацией видов сбора данных и их обработки, обеспечением транспарентности. Правила обработки данных в государственном секторе на основе продвинутых цифровых технологий должны быть более строгими и прозрачными, чем в частном секторе. **Научная новизна** исследования определяется недостаточной урегулированностью процесса оборота данных в государственном управлении, в рамках которого конституционная задача обеспечения и защиты фундаментальных прав человека не получает специального нормативного оформления. **Рекомендации** по итогам исследования заключаются в использовании полученных результатов при формировании соответствующей государственной политики обеспечения фундаментальных прав человека при обработке данных в российском государственном управлении.

Ключевые слова:
Государственное управление, большие данные, данные, персональные данные, цифровизация, права человека, обработка данных, искусственный интеллект, алгоритм

Коды JEL Classification
H11; H83; K38

RUSSIAN PRESIDENTIAL ACADEMY OF NATIONAL ECONOMY AND PUBLIC ADMINISTRATION (RANEPA)

PREPRINT
(SCIENTIFIC REPORT)

THE RELEVANT SCIENTIFIC AND METHODOLOGICAL APPROACHES TO ENSURING FUNDAMENTAL HUMAN RIGHTS IN DATA PROCESSING IN PUBLIC ADMINISTRATION

Talapina Elvira V., lead researcher, Center of Public Administration Technologies, Dr. Sci. (Law), ORCID 0000-0003-3395-3126, talapina-ev@ranepa.ru
Yuzhakov Vladimir N., director, Center of Public Administration Technologies, Dr. Sci. (Philosophy), professor, ORCID 0000-0002-5687-1863, yuzhakov-vn@ranepa.ru
Chereshneva Irina A. junior researcher, Center of Public Administration Technologies, ORCID 0000-0001-8135-4166, chereshneva-ia@ranepa.ru

Abstract
Enforcing fundamental human rights is a constitutional obligation of the Russian Federation. In the digital age, the risks of human rights violations are increasing, making it

increasingly relevant to implement a consistent state policy related specifically to data processing in public administration. **The objective** of this paper is to analyze the scientific and methodological approaches to enforcing fundamental human rights in data processing in public administration and the possibilities for consideration of human rights in the Russian public administration. The **subject** of the study includes scientific publications, court cases, international and national laws and regulations, including foreign countries. The study uses formal legal and historical legal **methods**, comparative legal method, method of legal interpretation, logical analysis, general scientific methods of classification and modeling. The **results** of the study are an analytical review of foreign and Russian scientific and methodological approaches to enforcing fundamental human rights in data processing in digital public administration; systematization of the basic legal grounds for enforcing fundamental human rights in data processing in public administration; the proposals for legal enforcement of fundamental human rights in data processing in the Russian public administration. The study allows drawing **conclusions** about the lack of attention in the Russian doctrine and practice to the issue of fundamental rights. Since Russian legislation in this area is based on the European model, the implementation of European approaches to data protection is recommended. It is necessary to create special legislation on data processing in public administration, to define the criteria for proper data processing and data storage, to differentiate the types of data collection and data processing, to ensure transparency. Based on advanced digital technologies, data processing rules in the public sector should be stricter and more transparent than in the private sector. The **scientific novelty** of the research is determined by insufficient regulation of data processing in public administration, where the constitutional function of enforcement and protection of fundamental human rights is not sufficiently regulated. Based on the results of the study, **recommendations** are to use the findings in the formation of an appropriate state policy to enforce fundamental human rights in data processing in the Russian public administration.

Keywords:
Public administration, big data, data, personal data, digitalization, human rights, data processing, artificial intelligence, algorithm

JEL Classification
H11; H83; K38

Оглавление

Введение

В органах государственной власти сосредотачивается колоссальный объем данных из самых разных источников – от граждан, коммерческих организаций, из других государственных органов. Они собираются в различных целях, циркулируют внутри различных ведомственных информационных систем, используются в разных целях многими органами государственного управления. При их обработке возникает множество рисков, при этом один из главных - риск нарушения фундаментальных прав человека, одним из основных источников которого является нарушение правил обработки данных (в том числе необоснованное раскрытие персональных данных ввиду неопределенности правил их обработки).

Статья 18 Конституции России устанавливает, что права и свободы человека и гражданина «определяют смысл, содержание и применение законов, деятельность законодательной и исполнительной власти», а статья 2 Конституции называет признание, соблюдение и защиту прав и свобод человека обязанностью государства. Для того чтобы эта обязанность надлежаще выполнялась, необходимо ее организационное, нормативное, кадровое и пр. обеспечение, встраивание защиты прав человека непосредственно в логику государственного управления. Это требует выстраивания системной политики в отношении обработки данных в государственном управлении, что, в свою очередь, предполагается п. м) ст. 71 Конституции в редакции 2020 года, закрепившей в ведении Российской Федерации вопросы обеспечения безопасности личности, общества и государства при применении информационных технологий, обороте цифровых данных. Государство – активный участник оборота цифровых данных, но соответствующая политика пока не сформулирована. Поэтому весьма актуальна задача выявления и анализа имеющихся в мировой практике методологий, научно-методологических подходов, позволяющих обрабатывать данные в целях госуправления с соблюдением фундаментальных прав человека. Это поспособствует тому, чтобы обосновать и предложить собственные правовые меры обеспечения фундаментальных прав человека при обработке данных в государственном управлении России.

Целью настоящего исследования является анализ научно-методологических подходов к обеспечению фундаментальных прав человека при обработке данных в государственном управлении и возможностей их учета в российском государственном управлении.

Для достижения цели выполнены следующие задачи:

1) Подготовка обзора и анализ зарубежных и российских научно-методологических подходов к обеспечению фундаментальных прав человека при обработке данных в государственном управлении, в том числе при ее цифровизации и автоматизации;

2) Оценка возможностей учета в российском государственном управлении зарубежных и российских научно-методологических подходов к обеспечению фундаментальных прав человека при обработке данных в государственном управлении, в том числе при ее цифровизации и автоматизации.

3) Определение базовых правовых основ обеспечения фундаментальных прав человека при обработке данных в государственном управлении, в том числе при ее цифровизации и автоматизации, включая:

3.1 классификацию и анализ фундаментальных прав человека, затрагиваемых при обработке данных в государственном управлении, в том числе при ее цифровизации и автоматизации;

3.2 классификацию и анализ возможных нарушений фундаментальных прав человека, затрагиваемых при обработке данных в государственном управлении, в том числе при ее цифровизации и автоматизации;

3.3 разработку критериев надлежащей обработки данных в государственном управлении в целях обеспечения фундаментальных прав человека при обработке данных в государственном управлении, в том числе при ее цифровизации и автоматизации.

4) Подготовка предложений по правовому обеспечению фундаментальных прав человека при обработке данных в российском государственном управлении, в том числе при ее цифровизации и автоматизации.

Новизна такого исследования определяется недостаточной урегулированностью процесса оборота данных в государственном управлении и их обработки, в результате чего конституционная задача защиты фундаментальных прав человека не получает специального нормативного оформления.

Результаты данной НИР могут быть использованы в интересах Департамента информационных технологий и связи Правительства Российской Федерации, Министерства экономического развития Российской Федерации, Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации, для научно-методологического обоснования мер, предпринимаемых в рамках реализации мероприятий по цифровизации государственного управления.

Полученные результаты могли бы стать основой соответствующей государственной политики обеспечения фундаментальных прав человека при обработке данных в российском государственном управлении.

1 Анализ научно-методологических подходов к обеспечению фундаментальных прав человека при обработке данных в цифровом государственном управлении

Ввиду остроты тематики цифровизации и автоматизации в настоящий период, можно наблюдать относительное разнообразие подходов к проблематике прав человека в условиях цифровизации. «Географически» можно выделить подходы: 1) развиваемые на американском континенте, характеризуемые, во-первых, большим эмпирическим материалом, в связи с более продвинутой практической стадией использования цифровых технологий, во-вторых, более гибким и адаптивным правовым аппаратом, в-третьих, заметной тенденцией к экспансии собственного опыта; 2) европейские подходы, традиционно уделяющие повышенное вниманием правам человека и защите данных; 3) формирующиеся российские подходы, для которых характерно заимствование тех или иных зарубежных механизмов (довольно бессистемное). В качестве четвертого направления выделим китайский подход к обработке данных, квинтэссенцией которого стала система социального рейтинга граждан, который отвергается демократическими государствами. Его реализация в Российской Федерации также невозможна ввиду очевидного конфликта с правами человека, признанными в подписанных Россией (в отличие от Китая) международных актах и имплементированных в главу 2 российской Конституции, а также распространившихся в отраслевых актах законодательства.

Проанализированные зарубежные (американские и европейские) и российские подходы к обеспечению фундаментальных прав человека при обработке данных в государственном управлении можно систематизировать по нескольким направлениям.

1.1.1 Правовое регулирование использования алгоритмов для обработки данных в государственном управлении

Алгоритм является базовым понятием в проблематике автоматизированной обработки данных. Развитие информационных технологий, успех науки

информатики прочно связали понятие алгоритма с информационным обеспечением. Алгоритмы хорошо знакомы праву в качестве объектов регулирования, но праву гражданскому, частному. Для полноценного использования алгоритмов в государственном управлении необходимо публично-правовое регулирование возникающих отношений, что позволит обеспечить защиту прав граждан посредством публично-правовых механизмов.

В Европе с 1981 года используется термин «автоматизированная обработка данных», который напоминает алгоритм по содержанию (совокупность действий): автоматизированная обработка включает в себя следующие операции, осуществляемые полностью или частично с помощью автоматизированных средств: хранение данных, осуществление логических и/или арифметических операций с этими данными, их изменение, уничтожение, поиск или распространение (Конвенция Совета Европы о защите физических лиц при автоматизированной обработке персональных данных от 28 января 1981 года) [1].

Нетрудно заметить, что сфера применения автоматизированной обработки данных ограничена персональными данными. То есть публично-правовая защита сконцентрирована на человеке с его частной жизнью и персональными данными. Собственно, так и произошло право на защиту персональных данных и была заложена традиция «сопротивления» индивидуальным автоматизированным решениям. Так, Регламент № 2018/1725 Европейского парламента и Совета Европейского Союза «О защите физических лиц при обработке персональных данных» (п.43) определяет, что субъект данных должен иметь право не подчиняться решению, которое может включать принятие мер, оценивающих личные аспекты, относящиеся к нему или к ней, которое основывается исключительно на автоматизированной обработке и результатом которого являются юридические последствия в отношении его или ее, или которое сходным образом может значительно повлиять на него или на нее, такое как практики электронного подбора кадров без вмешательства человека [2].

В русле европейских правовых позиций выстроен и российский закон. Согласно ст.16 ФЗ от 27.07.2006 года «О персональных данных» [3] субъект персональных данных имеет право отказаться от принятия в отношении него решения на основании исключительно автоматизированной обработки персональных данных. К признакам такого решения относится то, что оно порождает юридические последствия в отношении субъекта персональных данных

или иным образом затрагивает его права и законные интересы. Отметим, что в данной нормативной установке центр тяжести принятия решения (право выбора) лежит на субъекте персональных данных, гражданине. Действия государства данная норма не ограничивает.

При этом имеется в виду самый широкий круг решений – как управленческих, так и любых иных. Обработка персональных данных, осуществляемая в частном секторе, порождает вопросы при заключении и исполнении «договора в онлайн-среде в полностью автоматизированном режиме, например при размещении заказа на приобретение цифрового контента, который становится доступным для загрузки по факту оплаты» [4].

Напомним, что управленческие решения принимаются органами власти на общем уровне - в отношении неопределенного или значительного круга лиц (в отношении охраняемых законом ценностей), и на индивидуальном уровне - в отношении граждан на основе автоматизированной обработки данных. Если в первом случае нарушения прав человека могут иметь место в обобществленном и массовом виде (официальное утверждение нормативного порядка предоставления льгот на дискриминационной основе), то во втором – будет иметь место нарушение права человека как субъективного права, защитить которое можно уже только в индивидуальном порядке. Любопытно, что внедрение алгоритмов, по сути, нивелирует это разграничение, и, к примеру, дискриминационная практика реализации алгоритма в отношении конкретных лиц одновременно является массовой.

Нужно учитывать, что сама идея алгоритма как совокупности инструкций, позволяющих решить проблему и достичь определенного заданного результата, как нельзя лучше отвечает концепции надлежащего, качественного государственного управления, нацеленного на достижение заранее запланированных, ожидаемых результатов, – ведь результат управленческой деятельности можно легко заложить в алгоритм принятия управленческого решения. Это дает основания полагать, что в ближайшие годы государство активно займется подобной автоматизацией управленческих решений, а потому необходимо заранее изучить возможные риски. Во всяком случае, положение о совместимости алгоритмов и концепции надлежащего государственного управления выдвигается нами в качестве гипотезы настоящего исследования.

1.1.2 Равенство и дискриминация при обработке данных

Одной из фундаментальных проблематик, дающей начало целому спектру научно-методологических подходов в области обработки данных в контексте соблюдения прав человека, является выработка недискриминационных способов обработки данных. Именно возможная дискриминация является наиболее часто упоминаемым риском в разнообразных исследованиях – правовых, управленческих, политологических.

В теории прав человека равенство и недискриминация являются основополагающими ценностями. В обоих случаях речь идет о равенстве прав с тем отличием, что право на недискриминацию имеет более узкое содержание и в этом смысле производно от права на равенство.

Концепт равенства можно считать центральным принципом правового государства; в основе системы естественных прав человека лежит представление о том, что люди рождаются свободными и равными в своем достоинстве и правах [5]. Разумеется, в юридическом смысле речь идет о формальном равенстве как равенстве возможностей, обусловленных личными усилиями и личной волей субъектов права [6].

Дискриминация посягает на равенство, представляя угрозу для правового государства. Дискриминация - это не просто различие в обращении. Не каждое различие незаконно и представляет собой дискриминацию. Также дискриминация - не просто неравное обращение. Различие в обращении может быть незаконным, но не представлять собой дискриминацию. Дискриминация имеет место в тех случаях, когда неблагоприятное различие в обращении является незаконным и основано на критерии, на основании которого закон запрещает проведение юридических различий [7].

В современный период дискриминация, осуществляемая людьми в отношении других людей, не искоренена, но уже выработаны определенные критерии ее установления, доказывания и привлечения виновных к ответственности. Однако с распространением автоматизированной обработки данных, в особенности на базе технологий больших данных, возникла другая проблема – дискриминации людей со стороны искусственного интеллекта. Вторгаясь в существующее правовое поле, искусственный интеллект затрагивает целый спектр имеющихся норм (защита данных, транспарентность, информационное самоопределение), а также создает новые риски принятия ошибочных решений в отношении конкретных лиц, в основе

которых часто лежит дискриминация. Все перечисленные проблемы входят в спектр научных исследований по вопросам обработки данных.

Принцип всеобщего равенства является главным принципом правового государства. Если нет равенства, права и свободы теряют смысл – ведь тогда ими можно наделять одних и лишать их других. В равенстве выделяется несколько компонентов – равенство перед законом, равенство перед судом, перед государственными органами, равенство в смысле притязания на государственную помощь. Впрочем, это не означает, что законодатель не может по-разному регулировать различные ситуации, и даже в некоторых случаях поступиться равенством во имя публичных интересов (как, например, произошло во время пандемии коронавируса) или для защиты уязвимых либо перспективных групп населения (например, не будет являться дискриминацией государственная поддержка талантливых детей).

Разумеется, формальное равенство нарушается в повседневной жизни, но для его обеспечения выстроена вся система правового государства. В эпоху алгоритмов озвучивается надежда на то, что они облегчат бюрократическую работу и за счет своей технологической нейтральности обеспечат равенство в публичной деятельности.

Но так ли все однозначно? Смысл юридического равенства не только в том, что все подчинены закону одинаково, но и в том, что общая норма применяется к частному случаю, индивидуализировано, то есть с учетом всевозможных обстоятельств. Особенно наглядно это демонстрирует институт юридической ответственности, для которого индивидуализация наказания (ответственности) обретает исключительное значение в смысле достижения справедливости. В индивидуализации - смысл уголовного наказания, административных санкций, гражданско-правовой ответственности.

Управленческую практику индивидуализирует мотивация административных решений. Право на надлежащее государственное управление включает в себя обязанность государственных органов мотивировать свои решения (ст. 41 Хартии фундаментальных прав ЕС) [8]. А алгоритм формализует мотивацию решений, делает ее стереотипной. Поиск баланса между быстрым и эффективным решением на основе алгоритма и учетом индивидуальных обстоятельств дела ставит перед наукой новые задачи – выработать правила обработки данных, базирующиеся на подобном балансе. Выполнимая ли это задача? Верно замечено, что

правоприменение по своей природе далеко не всегда способно осуществляться в рамках строгих алгоритмов. В праве существуют пробелы, а любое социальное взаимодействие бывает многоаспектным, допускает различные и порой неоднозначные оценки [9].

В целом необходимо упомянуть, что случаи дискриминации, рассмотренные судами, редко касались автоматизированной обработки данных. Но легко спрогнозировать, что алгоритмы и в особенности искусственный интеллект способны так же дискриминировать людей, как и сами люди.

1.1.3 Дискриминационный потенциал искусственного интеллекта при обработке данных в государственном управлении

Алгоритмы лежат в основе многих технологий – искусственный интеллект, распределенный реестр, поддержка принятия решений, интернет, роботы. Стоит напомнить, что привлечение искусственного интеллекта к принятию решений не связано с цифровой эпохой - первые экспертные системы (юридические и медицинские) на основе искусственного интеллекта появились в 1970 годах [10].

Почему возникла идея не просто автоматически обрабатывать данные, а использовать искусственный интеллект? Система оценок позволяет квалифицировать склонность, но не помогает понять точно специфику, которая лежит в основании этой склонности. А смысл хорошего решения – в понимании специфики и контекста феномена [11]. Глобальность статистического подхода и скоринга перевела ставки на искусственный интеллект как технологический подход.

Поскольку все зависит от того, каким алгоритмом руководствуется искусственный интеллект, в науке формулируется задача достижения беспристрастности классификации, кладущейся в основу алгоритма. Самый простой путь – усовершенствовать классификатор, удалив самые «чувствительные» параметры, наиболее очевидно свидетельствующие о дискриминации. Обратимся к примерам из «автоматизированной» кадровой политики частных компаний, которая применима и к конкурсному набору на государственную службу. Найм на работу основывается на отборе «лучших» параметров кандидатов, что в дальнейшем способно привести к дискриминации (если в качестве ориентира избраны лучшие работники с наиболее высокой зарплатой за определенный период, которые все оказались мужчинами, женщины-претенденты будут отсекаться автоматически). Такой, казалось бы, нейтральный параметр, как место жительства, может косвенно указывать на национальность или расу (не секрет, что во многих городах мира

существуют кварталы компактного заселения по национальному признаку). Адрес проживания может свидетельствовать и о социальном положении лица, его достатке. Сложность состоит еще и в том, что механическое отсечение некоторых параметров не всегда приводит к недискриминации (посредством обработки больших данных можно извлечь даже ту информацию, которая кандидатами не предоставлялась) [12]. Все эти случаи могут иметь место и при конкурсном отборе государственных служащих, и при распределении общественно значимых благ.

Упоминавшийся выше Регламент № 2018/1725 Европейского парламента и Совета Европейского Союза «О защите физических лиц при обработке персональных данных» установил обязательность оценки воздействия на защиту данных (data protection impact assessment). Если тип обработки данных, в частности, использование новых технологий с учетом характера, масштаба, контекста и целей обработки, может привести к возникновению высокой степени риска для прав и свобод физических лиц, контролер перед обработкой должен провести оценку воздействия предполагаемых операций по обработке на защиту персональных данных (ст.39). Для оценки соблюдения основных прав могут использоваться большие данные, которые содержат потенциал выявления систематических предубеждений и дискриминации [13].

Углубленные исследования утверждают, что суждение о нейтральности технологий, в частности алгоритмов, несколько преувеличено. Алгоритм составляется людьми. Они отбирают его составные части, преследуя определенную цель. Это означает, что в алгоритм уже закладывается предпочтение, связанное с определенным ожидаемым поведением или характеристиками [14]. Получается, что выбор (в пользу заранее предполагаемого решения) может быть сделан уже на стадии разработки алгоритма.

В качестве нейтрализатора подобных рисков в публичной сфере обычно называется транспарентность. Поэтому транспарентность алгоритмов относят к первичному «барьеру» на пути дискриминации.

1.1.4 Дискриминационные риски технологии профилирования

Большие данные сами по себе не являются информацией, а просто цифровыми данными. Чем больше данных мы собираем, тем труднее извлекать полезную информацию - так как огромные объемы данных превосходят человеческие возможности рассмотрения. Следовательно, данные нуждаются в мощных инструментах для использования в качестве управленческого ресурса.

Профилирование является конкретным методом интеллектуального анализа данных. В этой перспективе профилирование рассматривается как автоматизированный либо полуавтоматизированный процесс для изучения больших наборов данных в целях построения классов или категорий характеристик [15]. Важными компонентами профилирования являются: поиск информации по определенным критериям, связь этой информации с конкретным лицом, использование ее для идентификации лица или для обращения с лицом неким заданным образом.

При профилировании обрабатываются как персональные, так и неперсональные данные. Из этого посыла сразу ясно, что основной конфликт профилирования в плоскости законодательства возникает с законодательством о защите данных. Но это конкретный аспект, который в целом все-таки нормативно регулируется, хоть и неидеально.

Гораздо более проблемной становится обработка данных в условиях незнания граждан о том, что их данные обрабатываются и используются для принятия решений. Таким образом, в более общем плане профилирование «сталкивается» с либеральной демократией, прежде всего потому, что провоцирует информационную асимметрию. В общем-то, асимметрия знаний - явление распространенное, но именно в технологиях профилирования достигает нового пика. Потому, что в большинстве случаев граждане не знают о распространяемой информации и о том, как ее можно использовать в будущем.

Очевидно, что такие технологии, как профилирование, не оставляют большого пространства для автономии и самоопределения личности. Изначально заложенное противоречие между закрытостью частной жизни и открытостью публичной сферы обретает новые грани - частная жизнь тяготеет к непрозрачности, а условием защиты данных является прозрачность. Вопрос – как в таких условиях защитить частную жизнь? – становится трудноразрешимым.

Особенно показательно демонстрирует возникающие риски американский опыт в области профилирования и влияния на права человека, где разрешено использовать алгоритмы для принятия решения о предварительном заключении или условно-досрочном освобождении. В частности, речь идет о приложениях PSA (Public Safety Assessment) или COMPAS (Courcional Offender Management Profiling for Alternative Sanctions). Критика подобного алгоритмического прогнозирования поведения человека основана на том, что предиктивный результат вовсе не дает

100% верную истину - его средняя предиктивность оценивается лишь в 65%. заслуживает подробного рассмотрения ввиду довольно устоявшейся практики и потенциальной полезности (по крайней мере, частичной). В знаковом деле «State v. Loomis» [16] Верховным судом штата Висконсин были даны разъяснения нижестоящим судам при вынесении приговора с использованием алгоритмической оценки.

Так, к общим разъяснениям можно отнести запрет на использование данной оценки в отношении того, может ли обвиняемый быть лишен свободы, а также для определения тяжести приговора. Тем самым, судьи, использующие оценку риска в процессе вынесения приговора, должны объяснить отличные от такой оценки факторы, которые легли в основу принятого решения.

В свою очередь, к специальным разъяснениям могут быть отнесены пять письменных предупреждений для судей, которые должны включаться в предприговорный отчет о проведении расследования, если он содержит оценку COMPAS:

1) необходимо учитывать «проприетарный» характер COMPAS, который не допускает раскрытия процесса подсчета баллов;

2) баллы COMPAS не могут идентифицировать конкретных лиц с высоким уровнем риска, поскольку для подсчета используются групповая выборка;

3) несмотря на то, что COMPAS опирается на национальную выборку данных, не было проведено исследование перекрестной проверки населения штата Висконсин;

4) в научных исследованиях были подняты вопросы относительно того, что при оценке осуществляется непропорциональная классификация правонарушителей из числа меньшинств как имеющих более высокий риск рецидива;

5) COMPAS не был разработан для использования судьями в процессе вынесения приговоров, напротив, он был создан для Службы исполнения наказаний в целях оказания содействия при определении различного рода мер (исправление преступников, надзор, условно-досрочное освобождение), применяемых к осужденным, после вынесения приговора.

Тем самым, вынося эти предупреждения, суд ясно выразил свое желание привить как общий скептицизм в отношении точности применяемого инструмента, так и более целевой – в отношении оценки риска правонарушителей из числа меньшинств. Несмотря на то, что вышестоящий суд оставил приговор без

изменений, трудности в эффективном оспаривании оценки риска все-таки были признаны судом, который указал, что инструменты оценки риска должны постоянно контролироваться, а нормы обновляться в целях обеспечения точности результатов [16].

1.1.5 Генетическое профилирование в контексте дискриминации

Пожалуй, самой яркой моделью дискриминационного профилирования служит генетическое профилирование. Генетический профиль может раскрыть информацию не только о человеке, но и о его родственниках, включая их текущий и будущий профиль здоровья и ранее неизвестные семейные отношения [17]. Следует иметь в виду, что генетическая информация значительно отличается от иных медицинских данных, этому помогает понятие генетической исключительности. Разумеется, диапазон использования подобного рода информации чрезвычайно широк, что неминуемо создает риски, в том числе дискриминационные. Генетические данные наряду с прочими могут обрабатываться для решения управленческих задач.

Сформировавшиеся в различных государствах законодательные позиции по этому вопросу можно представить следующим образом:

1) полный запрет на использование генетической информации в страховании (Австрия, Норвегия, Франция), в том числе в контексте охраны прав на защиту персональных данных третьих лиц (Испания, Португалия);

2) дифференциация условий использования генетических данных в зависимости от сумм страхового покрытия при страховании жизни, страховании от несчастного случая (в том числе на производстве); конкретных обстоятельств, определенных законодателем, и причин проведения генетического исследования (Швейцария); участия страхователя в программе по выявлению и профилактике врожденных заболеваний (Израиль) [18].

Что касается США, в законодательстве (Genetic Information Nondiscrimination Act (GINA), 2008) преследуются две явные цели - предотвращение генетической дискриминации в медицинском страховании и предотвращение генетической дискриминации на рабочем месте. Медицинским страховщикам запрещено требовать прохождения генетического тестирования для оформления страховки или принимать решения о возмещении вреда на основании генетической информации. Аналогично – работодателям запрещено требовать прохождения генетического тестирования и принимать решения о найме, увольнении и пр. на основе

генетической информации. Заметим, что речь идет именно о медицинском страховании, а не о страховании жизни. К тому же законодательство о генетической дискриминации не распространяется на военных [17].

Проведенное исследование позволяет выделить три проблемы.

Во-первых, с учетом практики легальной дискриминации, она иногда может быть полезной и даже необходимой. Например, как утверждает эстонский исследователь Nõmper [19], работодатель должен иметь право требовать прохождения генетического тестирования как до поступления на работу, так и во время существования трудовых отношений, в той мере, в какой такое тестирование необходимо для определения существования генетического заболевания, которое может привести к выполнению должностных обязанностей с риском для здоровья работника или других сотрудников и иных лиц, активов работодателя или клиентов. Так, проявление болезни Хантингтона (симптомами которой являются непроизвольные движения) создает потенциальный риск для пилота самолета, его пассажиров и др.

Во-вторых, в литературе обращается внимание на сложности защиты прав в контексте генетической дискриминации. В частности, по эстонскому законодательству одним из заметных процедурных преимуществ общего Закона о равном обращении (который, напомним, не распространяется на генетическую дискриминацию) является распределение бремени доказывания. Общий Закон (пункт 8 (1)) устанавливает совместное бремя доказывания, оговаривая, что заявление лица в суд, комитет по трудовым спорам или Уполномоченному по вопросам гендерного равенства и равного обращения основывается на фактах, из которых можно предположить, что дискриминация произошла. Затем бремя доказывания перекладывается на ответчика, который в ходе разбирательства должен доказать сам, что нарушения принципа равного обращения не было (пункт 8 (2)). Если ответчик отказывается представить такие доказательства, это приравнивается к признанию дискриминации [20]. А по Закону об исследованиях генов человека доказывать дискриминацию должен заявитель (как и то, что работодатель использовал генетическую информацию), что, конечно же, крайне сложно на практике.

Кроме того, по Общему Закону предусмотрены конкретные правила возмещения за ущерб по делам о дискриминации. Помимо имущественных убытков, предоставляется право требовать возмещения нематериального ущерба. Из

вышеизложенного можно сделать вывод о том, что наиболее важное процедурное преимущество Общего Закона о равенстве (правило совместного бремени доказывания) не применяется к случаям генетической дискриминации.

По утверждению эстонского специалиста, хотя запреты на генетическую дискриминацию четко установлены эстонским законодательством, регулирующий подход к недискриминации является фрагментарным. В частности, Общий Закон о равном обращении содержит исчерпывающий перечень оснований для дискриминации, не включающий генетическую дискриминацию [20].

В-третьих, нельзя отрицать предиктивного потенциала генетической информации. Пока генетическая информация не является точной на все 100%. Однако, если она станет таковой (в том смысле, что можно со 100%-ной уверенностью установить индивидуальный риск), мы столкнемся с трудным выбором между отказом от использования предсказательной силы генетической информации и явной дискриминацией людей на основе качеств, над которыми они не имеют никакого контроля [17].

1.1.6 Перспективы появления новых форм дискриминации при обработке данных

В зарубежных работах выявлению новых потенциальных форм дискриминации при дальнейшем расширении использования цифровых технологий уделяется значительное внимание. Этот контекст представляется крайне важным в свете государственного управления, перед которым стоит задача сгладить фактическое неравенство, в том числе посредством так называемой позитивной дискриминации (предоставления льгот отдельным нуждающимся в этом категориям населения).

Дискриминационный потенциал в реализации права на труд

Как отмечалось выше, вопросы равенства применительно к занятости населения и оплате труда почти всегда становятся предметом специального конституционного внимания. Реже применяется модель защиты от дискриминации на основании общих норм. Например, в Италии, Ирландии, Дании и некоторых других странах защита работников от преследований на рабочем месте строится на применении общих норм законодательства, чаще всего принципа запрета дискриминации. Специализированные нормы не закрепляются прямо в законодательстве, а суды широко трактуют необходимость защиты личности работника. Примечательно, что в исходных антидискриминационных документах

речь идет о дискриминации в вопросах оплаты труда и найма на работу, в то время как в настоящий период отдельным направлением стала борьба с дискриминацией на работе в процессе осуществления трудовых обязанностей работником.

Дискриминация лиц с лишним весом

Уже сегодня на вопрос, стигматизированы ли люди с избыточным весом, можно четко ответить утвердительно. Если дискриминация представляет собой правовой эквивалент социальной стигматизации, то сразу становится очевидным, что дискриминация лиц с избыточным весом имеет место [21]. Но несмотря на то, что в доктрине начинают подниматься подобные проблемы, в законодательствах разных государств практически нет попыток «легализовать» понятие дискриминации лиц с лишним весом. Заметным исключением в этом отношении является так называемый закон Эллиота Ларсона штата Мичиган (США) 1976 года, который в области трудового права запрещает наем и увольнение по причинам религии, расы, цвета кожи, национального происхождения, возраста, пола, роста, веса или семейного положения [22].

Однако с юридической точки зрения весьма важна квалификация понятия – считать ли избыточный вес в смысле дискриминации болезнью или инвалидностью? Или это новый самостоятельный критерий дискриминации?

Дискриминация в связи с освоением космоса

Физическая конфиденциальность лица может быть нарушена с помощью цифровых средств, таких как дистанционное зондирование, которое может вызвать проблемы с правами на неприкосновенность частной жизни, особенно когда ожидаемое высокое разрешение станет доступным широкому кругу коммерческих игроков. Пока же вопросы, касающиеся неприкосновенности частной жизни и прав человека, поднимались только в связи с беспилотными летательными аппаратами [23].

Спутники будут размещаться в космическом пространстве, которое не имеет суверенных границ и сможет обеспечить глобальный охват видео и изображений в высоком разрешении в режиме реального времени. С коммерциализацией космоса и снижением затрат как на запуск, так и на производство, а также и в сфере услуг и конечных продуктов, технология станет все более доступной для частных компаний или даже частных лиц. Подобное вторжение может стать опасным, и ожидается, что с появлением ИИ оно станет более продвинутым, получив возможность обработки больших данных из космоса. Исследователи считают данное направление весьма

перспективным и в плане потенциальной угрозы правам человека, и в плане необходимости расширения средств их защиты.

Также в научной литературе высказываются опасения о возможных рисках дискриминации для людей с меньшими финансовыми ресурсами, людей, страдающих редкими заболеваниями, или людей, ведущих нездоровый образ жизни (употребление алкоголя, курение) [24]. Обнаружение таких лиц не составит труда для ИИ, а следовательно, приведет к их дискриминации.

1.1.7 Обработка данных в рамках наблюдения (слежки)

Вопрос о технологии наблюдения заслуживает более подробного рассмотрения, поскольку в государственном управлении предполагается использовать интернет вещей при осуществлении государственного контроля. Более того, наблюдение уже активно используется государством для обеспечения безопасности (видеокамеры, геолокация), что происходит практически вне правового поля.

В общем виде наблюдение (surveillance) можно представить в качестве процесса сбора информации о физических лицах, отношение к которым будет различаться, в зависимости от ранее полученной информации, предварительно распределенной по тем или иным классам и группам. Подчеркнем, что данная дефиниция наблюдения не содержит принципиально новых характеристик, однако необходимо обозначить ряд нюансов.

Во-первых, возрастающая роль частных субъектов в выполнении задач, традиционно возложенных на государственные органы, таких как обеспечение здравоохранения, образования и даже внутренней и внешней безопасности. В настоящее время во многих странах подобная деятельность все чаще осуществляется в рамках государственно-частного партнерства или делегируется государственными органами частным компаниям [25]. Кроме того, частные субъекты могут заниматься наблюдением независимо от осуществления какой-либо государственной функции. Например, в целях маркетинга частные компании регулярно «следят» за потребителями [26].

Во-вторых, наступление цифровой эры и быстрое развитие вычислительных методов, включая интеллектуальный анализ данных. Отдельно следует выделить концепт «ассамбляж наблюдения» (surveillant assemblage). Метафора ассамбляжа, начиная с нулевых годов нашего века, активно используется в качестве аналитической модели в различных междисциплинарных полях. «Ассамбляж

наблюдения» — нечто, позволяющее соединить разнородные потоки информации, базы данных, информационные системы, технологии передачи и кодирования информации [27].

Применительно к технологии наблюдения сказанное означает, что отдельные люди «разделяются» на ряд фрагментов информации, а затем вновь собираются в виртуальном пространстве. Эти данные циркулируют в виртуальном пространстве, хранятся, тщательно изучаются, используются для расчетов и, что еще более важно, служат маркерами доступа к ресурсам, услугам и власти такими способами, которые часто неизвестны их референту [28].

Отношение к массовой слежке менялось под влиянием ситуации с терроризмом и других событий на международной арене, причем не только со стороны общества, но и со стороны судов. Во многом этим объясняется принятие постановления Европейского Суда по правам человека по делу Биг Бразер Вотч и другие против Соединенного Королевства [29], которое вызвало неоднозначную оценку, в частности, утверждение, что массовая слежка per se не нарушает Конвенцию о защите прав человека и основных свобод: Решение о введении режима массового перехвата для того, чтобы идентифицировать тем самым неизвестные угрозы национальной безопасности, подпадает под широкие пределы усмотрения, которые есть у государств при выборе того, как лучше достигнуть легитимную цель по защите безопасности. ЕСПЧ сделал упор на то, что новыми технологиями воспользовались «террористы и преступники», которым это помогает «избежать обнаружения в Интернете». По мнению Суда, режим массового перехвата данных имеет упреждающую функцию и потому эффективен.

Наблюдение предлагается рассматривать и с другой точки зрения, как результат бюрократии и стремления к эффективности, скорости, контролю и координации. В данном контексте инструменты наблюдения, основанные на больших данных, могут значительно повысить качество государственной политики и услуг [30].

Нюансы различных видов наблюдения, цели наблюдения имеют значение для оценки степени вторжения в частную жизнь человека. Суд Европейского Союза подчеркнул такую черту наблюдения, как интрузивность, в деле Digital Rights Ireland и Seitlinger: наблюдение способно породить в сознании у соответствующих лиц ощущение, что их частная жизнь является предметом постоянного наблюдения [31]. Таким образом, в процессе наблюдения (слежки) возникает угроза частной жизни.

1.1.8 Обеспечение фундаментальных прав в рамках законодательства о защите данных

Нарушение неприкосновенности частной жизни и дискриминация на основе обработки данных являются двумя наиболее частыми и наиболее серьезными последствиями злоупотребления персональными данными. Именно поэтому исследователи особенно активно изучают возможности совмещения законодательства и защите данных с антидискриминационным законодательством, адаптации защиты данных к развитию цифровых технологий. В этом плане можно выделить несколько направлений.

Обоснования перехода от априорного контроля в защите данных к апостериорному

Защита персональных данных основана на априорных процедурах (как правило, уведомления и запросы на авторизацию), то есть осуществляется независимо от того, понесло ли какое-либо лицо какой-либо фактический ущерб или вред, и охватывает неспособность выполнить необходимые предварительные формальности, даже без специальных намерений. Первоначально защита персональных данных была призвана контролировать силу знаний. В отличие от этого, положения о защите частной жизни и о борьбе с дискриминацией в большей степени относятся непосредственно к контролю над действием: правонарушение фиксируется только в том случае, если лицо фактически пострадало от нарушения неприкосновенности частной жизни или от неблагоприятного решения, которое было незаконно принято на основании дискриминационного критерия.

В соответствии с европейским законодательством, выполнение предварительных формальностей контролером данных является одним из условий законности обработки персональных данных. Но в современных условиях априорная проверка обработки данных становится низким барьером. Антидискриминационные правила в европейских странах в отношении применения законодательства о защите данных развиваются в направлении более сильного акцента на апостериорных проверках, этот сдвиг оправдан растущей сложностью контроля за сбором данных, что повышает необходимую бдительность при использовании данных.

Тревожный феномен, который на самом деле может рассматриваться как переработка, а также как сбор данных - это автоматическая генерация новых знаний с использованием интеллектуального анализа данных. В подобной ситуации субъект может игнорировать не только процесс, но и само генерируемое знание, даже если

это знание его касается (например, его предпочтений). Положения о защите персональных данных изначально были разработаны с целью решения проблем первого типа ситуации. Конечно, предпринимаются усилия по их адаптации к сложным проблемам, возникающим в связи со вторым типом сбора данных, но они, как правило, все более неэффективны в этих ситуациях. Главной причиной такой неэффективности является основополагающая философия - априорный и процедурный контроль. Цифровой мир основан на обороте и обработке данных, и сбор данных - уже не одноразовое событие, а обычное явление, процесс, который становится постоянным с появлением вездесущего вычисления. Кроме того, границы между персональными и неперсональными данными становятся все более размытыми, как и границы между частными и открытыми доменами, а также различия между сбором и обработкой данных.

С учетом этих изменений априорные проверки и процедуры представляются слишком жесткими, или же их просто невозможно осуществить, и предусмотренные законодательством средства защиты данных становятся чисто формальными обязательствами.

Обоснования перехода от встроенной конфиденциальности к минимальному вреду

В литературе предлагается еще один подход, позволяющий «приспособить» защиту данных к соблюдению недискриминации, ориентированный на механизмы гражданского права. А именно – принцип Privacy by design (PbD, конфиденциальность по дизайну, встроенная конфиденциальность) предлагается трансформировать в Minimum harm by design (MHbD, минимальный вред от дизайна) [26]. Концепция PbD была изначально задумана для делового сектора как способ повышения доверия потребителей за счет улучшения защиты частной жизни, чтобы в дальнейшем распространить его на другие области, включая государственную политику [26].

MHbD отличается от PbD двумя критическими способами. Во-первых, он признает, что возможный вред от наблюдения выходит за рамки только нарушения неприкосновенности частной жизни и попыток предоставить рекомендации по их решению. Во-вторых, он отказывается от беспроигрышного принципа PbD и перекладывает бремя доказывания на стороны, осуществляющие наблюдение.

Это дает два преимущества по сравнению с PbD. Во-первых, позволяет нам оценить потенциальный вред от наблюдения, в том числе вред, который не будет

признан в соответствии с правилами PbD. Во-вторых, устанавливает меры наблюдения под более строгим контролем, чем PbD, поскольку нарушения неприкосновенности частной жизни являются существенным моментом. В целом можно ожидать, что такая система обеспечит более надежную защиту от рисков наблюдения, чем полиция [26].

Обоснования перехода к целевой таксономии данных

Суть данного подхода – в новой таксономии, основанной на цели, а не на ожидаемой чувствительности к собранным персональным данным [24].

В Европе, как и в Соединенных Штатах, классический подход к защите данных о здравоохранении состоит в том, чтобы данные прошли через строгие правила анонимизации или деидентификации. Именно так и представлена защита персональных данных в их нынешнем виде – анонимизация и деидентификация. В то время как Европейский Союз концентрируется на защите персональных данных, определенных в широком смысле, США пытаются контролировать поток персональной идентифицируемой информации, особенно в момент раскрытия. Некоторые исследователи считают такую стратегию более перспективной.

Не отказываясь от идеи регулирования сбора и хранения данных, сторонники данного подхода основываются на существующем принципе целеустремленности для создания надежных и актуальных категорий. Суть в том, чтобы сместить фокус с ограничительного сбора и сохранения данных на контроль данных в самый важный момент, а именно в момент их использования, не забывая при этом, однако, о первоначальном назначении, для которого они были собраны. Такой подход просто адаптировать как к европейским, так и к американским правовым рамкам, поскольку принцип цели является ключевым принципом в директиве ЕС о защите данных 1995 года, также как в Законе США о неприкосновенности частной жизни 1974 года [24].

1.1.9 Влияние использования цифровых технологий в период пандемии COVID-19 на права человека

В настоящий период государства сталкиваются с трудными задачами в стремлении защитить свое население от угрозы Covid-19. Это может изменить и изменяет нормальное функционирование демократических обществ и привести к мерам, которые могут ущемлять права и свободы. В европейской практике можно выделить три основных подхода:

- принятие общих чрезвычайных мер, наделяющих правительство особыми полномочиями (в частности, на основе законов или указов, в соответствии с конституционным законодательством);

- принятие чрезвычайных мер в конкретных секторах, часто основанных на правилах общественного здравоохранения или пандемии;

- принятие чрезвычайных мер без конкретной законодательной базы.

Чаще всего законодательными мерами были разрешены следующие виды практик:

- использование мобильных приложений для различных целей;

- использование данных о трафике и местоположении с мобильных телефонов и приложений;

- использование других технических средств (электронные браслеты, умные камеры с системой распознавания лиц, тепловое сканирование, дистанционное управление дронами и роботами, обязательное тестирование) [32].

1.1.10 Нормативный потенциал регулирования оборота данных: лучшие практики

К иллюстрациям успешного урегулирования оборота данных посредством специального законодательства можно отнести опыт Ирландии и Австралии. В Ирландии Законом 2019 года «О совместном использовании и управлении данными» (Data Sharing and Governance Act) под совместным использованием данных (data sharing) понимается раскрытие информации, в том числе персональных данных, одним государственным органом другому государственному органу. Закон подробно регламентирует случаи, когда допускается раскрытие персональных данных. В Австралии законопроектом «О доступности и транспарентности данных» 2020 года (Data Availability and Transparency Bill) предусматривается внедрение целой системы авторизации и регулирования доступа к государственным данным.

Результаты проведенного анализа имеют значение для формирования собственного российского подхода к обработке данных в государственном управлении. В частности, целый ряд позиций может быть учтен после их комплексной оценки, а именно: 1) переход в защите данных от априорного контроля к апостериорному; 2) подход к соблюдению прав человека как к комплексной задаче, а не как к ничем не обеспеченной декларации публичного права или субъективному праву; 3) усиление и конкретизация публично-правовых механизмов обеспечения фундаментальных прав (в том числе посредством расширения цифровых

компетенций государственных служащих, введения должности инспектора по обработке данных, создания независимого органа по защите данных); 4) привлечение гражданско-правовых механизмов защиты прав (в случае причинения конкретного вреда); 5) дифференциация видов сбора данных для нужд государственного управления (строго формализованный, наблюдение, опосредованный (из больших данных)), дифференциация целей обработки данных (стандартная, экстренная, прогностическая и др.).

Систематизируя результаты анализа, отметим, что для цифрового государственного управления и обработки данных будут иметь значение четыре крупных направления – переосмысление прав человека в цифровых условиях, персонализация и предиктивность как эффекты алгоритмической обработки данных, соотношение публичного и частного права в регулировании обработки данных, развитие антидискриминационного законодательства. Остановимся на них подробнее.

1.2.1 Переосмысление прав человека в цифровых условиях

Технологии очевидно имеют положительный эффект на человеческую жизнь; вероятно, возникает даже право человека на использование определенных технологий. Однако большинство технологий имеет двойственные эффекты, которые мы часто не можем даже предсказать. Часть из этих эффектов может в конечном счете стать значительными для прав человека, а некоторые затронут жизни людей, которые еще не родились [33].

Режим прав человека был установлен на основе сотрудничества между национальными государствами, в то время как новые технологии проводят в жизнь наднациональные регулирующие режимы и вынуждают нас спросить, как будущие люди включены в эти режимы в таких обстоятельствах, когда долгосрочные эффекты технологий сомнительны и неопределенны [33]. Если, например, частная жизнь не может эффективно быть обеспечена, или если нет никакого пути к установлению демократического контроля над технологиями, это затрагивает самую суть человеческого достоинства и могло бы послужить причиной сомнений относительно законности таких технологий [33].

С этой точки зрения предлагается поместить человеческое достоинство в центр нормативной оценки технологий. Поскольку технологии существенно меняют человеческие жизни и мир, место человека в мире, возникает вопрос не просто о применимости прав человека в эпоху интернета, но о том, подходит ли вообще

существующая нормативная структура прав человека для регулирования. И если не подходит, это не основание для отказа от нее, а основание для переосмысления структуры прав человека в свете человеческого достоинства, в качестве соответствующего ответа новым технологиям [33].

1.2.2 Персонализация и предиктивность как эффекты алгоритмической обработки данных

Полагаем, что уже сейчас можно вести речь о двух основных преимуществах алгоритмической обработки данных, а именно персонализации и предиктивности, которые существенно влияют на традиционное понимание государственного управления.

Персонализация права стала довольно популярным направлением исследований в последние годы. Отправной точкой служит констатация проблем, которые создает или усугубляет появление цифровых технологий. Во-первых, разрывы между пользователями по отношению к сбору и защите их персональных данных, при этом опросы пользователей подчеркивают чувство потери управления, которому не соответствует расширение использования средств шифрования или защиты устройств, вполне доступных на цифровом рынке. Во-вторых, возможности заключения «эксплуататорских» контрактов в результате так называемой «асимметрии вычислительной мощности» между продавцами с технологическими возможностями и покупателями с технологическими недостатками. В-третьих, растущая угроза дискриминации с помощью поведенческих алгоритмов [12].

В качестве решения проблем предлагаются разные выходы – обеспечение прозрачности алгоритмов, активная роль регулирующего органа. Или «переход» к персонализированному праву. Потенциал цифровизации в трансформации публичной деятельности нуждается в отдельном дополнительном изучении, поскольку может привести к исчезновению публичных услуг или к созданию заново публичных услуг [14]. Таким образом, персонализация, с одной стороны, привлекательна для государственного управления, с другой – остается задача соблюдения юридического равенства, в частности, при оказании персонализированных государственных услуг.

Предиктивность, или возможность предсказать и предугадать дальнейшее развитие событий, называют одним из преимуществ алгоритмов, используемых искусственным интеллектом. Это звучит довольно безобидно, когда речь идет о построении планов развития экономики на государственном уровне, о

маркетинговых прогнозированиях частных компаний. Но совсем другое дело, когда предиктивные способности искусственного интеллекта используются для юридической оценки поведения конкретного человека, как в сформировавшейся уже судебной практике.

Представляется, что многие правила, разработанные к алгоритмической обработке данных в судебных системах, могут быть адаптированы для принятия решений в государственном управлении ввиду следующего.

Во-первых, судебная власть является органичной частью системы государственного управления в широком смысле слова, на которую распространяются единые принципы государственного управления.

Во-вторых, принятие судебного и административного решения с правовой точки зрения представляют собой индивидуализацию общей нормы применительно к конкретному человеку, а потому эти процессы не могут и не должны принципиально различаться. Более того, в обоих случаях решение принимается в отношении конкретной личности, обладающей полным набором прав человека, соблюдение которых – обязанность правоприменителя. Однако для этого необходимо обеспечить:

- установление нормативно-правовым актом порядка, в соответствии с которым будет исключено использование оценки, проведенной алгоритмом, в качестве единственной основы для принятия решения должностным лицом, обладающим соответствующей компетенцией и наделенным соответствующими дискреционными полномочиями;

- полную транспарентность и доступность (объяснимость и понятность работы) алгоритма для широкой общественности; это позволит минимизировать возможные негативные последствия предиктивного характера алгоритмов.

1.2.3 Соотношение публичного и частного права в регулировании обработки данных

Традиционная защита прав, связанных с цифровыми технологиями, происходит в режиме защиты фундаментальных прав, то есть в праве публичном. При этом в частных отношениях гражданин защищен как потребитель (по законодательству о защите потребителей).

Если изначально защита персональных данных регулировалась только публичным правом (как и в целом - право на информацию и информационное право возникли в публичной сфере), то теперь подобными вопросами все больше

занимается частное право, а также уголовное и международное. В итоге обостряется конфликт публичного и частного, одновременно усредняются их подходы; благодаря такого рода комплексным институтам взаимодействие между подсистемами и отраслями права усиливается.

Другой важный аспект – так называемое право собственности на данные. Основное отличие права на персональные данные как фундаментального от права собственности в том, что фундаментальные права принадлежат любому физическому лицу и неотделимы от него. Их нельзя передать другому лицу, и даже если их не осуществлять, они не исчезают. И в принципе, их нельзя наследовать. Развитие же ситуации с цифровыми данными пошло явно по частноправовому пути (мы имеем в виду в том числе право на цифровую смерть). Правда, проблемой остается правовая квалификация того права, которое возникает в отношении цифровых данных, – это не традиционное право собственности, и не право интеллектуальной собственности, и вообще они плохо сочетаются с защитой персональных данных.

Ключевым элементом обращения с персональными данными служит согласие обладателя. Но согласие – это центральный элемент гражданско-правовой сделки. Но есть ли у человека возможность не давать такое согласие на обработку данных? На работе? В банке? Ответы на эти вопросы очевидны. Получается, в некоторых случаях человек не в состоянии дать свободное и четкое согласие на обработку данных. Сказанное актуализирует проблематику создания законодательства, в котором публично-правовые и частноправовые начала будут сбалансированы и не провоцировать внутренний конфликт норм, выливающийся в разнонаправленное правоприменение.

1.2.4 Развитие антидискриминационного законодательства

В западной литературе нормативное обеспечение прав человека при обработке данных часто связывается с развитием антидискриминационного законодательства. В качестве ключевой предпосылки для противостояния возможной дискриминации со стороны ИИ рассматривается концептуальная переориентация антидискриминационного права ЕС с чистой парадигмы причинно-следственной связи к парадигме корреляции.

Согласно классической правовой доктрине, запрещенная дискриминация предполагает причинно-следственную связь между запрещенным основанием для дискриминации и конкретным неблагоприятным обстоятельством. Соответственно,

действие или бездействие с открытым намерением провести неблагоприятное различие между людьми по признаку пола или расы и т.д. квалифицируется как (прямая) дискриминация.

Однако традиционная модель причинно-следственной связи антидискриминационного права оказалась не в состоянии противостоять другим более сложным проблемам дискриминации. Доктринальный сдвиг от причинно-следственной связи к простым корреляциям произошел, когда суды начали изучать «косвенную» дискриминацию (что известно в антидискриминационном праве США как the doctrine of ‘adverse effect’): во многих случаях даже одного снижения бремени доказывания недостаточно для того, чтобы законно санкционировать неравное обращение.

И вмененная причинно-следственная связь, и понятие косвенной дискриминации в настоящее время расцениваются исследователями как важный первый шаг во введении ИИ в поле антидискриминационного законодательства с юридической точки зрения [34]. Их изучение, оценка и возможное заимствование полезны для сферы государственного управления, поскольку они предлагают новые правовые механизмы привлечения к ответственности.

2 Фундаментальные права, соблюдение которых необходимо при обработке данных в государственном управлении

Беспрецедентное развертывание информационно-коммуникационных технологий привело к тому, что сделалось возможным развитие мириад новых услуг, но одновременно оно породило разнообразные угрозы правам человека, к которым следует относиться очень серьезно. В последние годы активно продвигаются идеи нового поколения прав, таких как соматические («телесные») права, права генома, биоправа, права, порожденные новыми технологиями (в частности, право на защиту персональных данных) [35], цифровые права. Необходимо понимать, что, во-первых, не все государства в мире признают права человека, во-вторых, многие апеллируют к национальным особенностям прав и тем самым подвергают сомнению их универсальный характер (евразийская теория прав человека), в-третьих, не все права напрямую защищены, например, Европейской конвенцией, в-четвертых, национальные законодательства могут воспроизводить как максимальный, так и избранный круг прав человека. Однако и в науке, и в прикладных исследованиях и

опросах к правам, которые наиболее часто связываются с автоматизированной обработкой данных, относят право на конфиденциальность, право на защиту персональных данных и право на равенство и недискриминацию,

Право на уважение частной жизни и конфиденциальность

Термин «неприкосновенность частной жизни», используемый в статье 12 Всеобщей декларации прав человека и в статье 17 Международного пакта о гражданских и политических правах, или «частная жизнь», используемый в статье 8 Европейской конвенции по правам человека, прямо не упоминает аспект неприкосновенности частной жизни, но представляет собой лишь общий термин, «зонтичное» понятие, которое заявлено настолько широко, что даже обеспечивает защиту тех аспектов частной жизни, которые не упоминаются. Конфиденциальность не является абсолютным правом, и сама по себе может быть ограничена в некоторых случаях. Но вторжение в частную жизнь должно быть законным, то есть пропорционально благу общества в целом. В противном случае, положения статьи 12 Всеобщей декларации очень четко ограничивают произвольное вмешательство в частную и семейную жизнь, жилище или переписку. Право на неприкосновенность частной жизни является одним из основных элементов Всеобщей декларации и имеет большое значение для защиты человеческого достоинства и свободного развития человеческой личности. В целом, неприкосновенность частной жизни может пониматься как право на защиту физического лица путем четкого определения того, кому будет предоставлен законный доступ к его частной деятельности, коммуникациям и информации. В основе права на неприкосновенность частной жизни лежат, по крайней мере, две конкурирующие идеи: одна из них касается частной жизни как свободы от общества, то есть защита информации от других; другая - это неприкосновенность частной жизни, понимаемая как достоинство, означающая защиту интимных отношений и общественной репутации.

В цифровых условиях средства, предлагаемые интернетом для публикации и доступа к информации, приводят к увеличивающемуся количеству нарушений конфиденциальности. В контексте государственного управления проблематика высвечивает нарастающее противоречие между вторжением в частную жизнь для целей государственного и ее защитой: используемые государством технологии становятся чересчур интрузивными для частной жизни его граждан. На основе Доклада Верховного комиссара ООН по правам человека от 03 августа 2018 года

A/HRC/39/29 «Право на неприкосновенность частной жизни в цифровой век» можно выделить следующие тенденции и проблемы, связанные с посягательством на неприкосновенность частной жизни:

1) расширение использования личных данных правительствами и компаниями:

- усиление цифрового следа;
- обмен и сведение данных: постоянно происходит обмен данными (а также их сведение) между организациями государственного и частного секторов, причем ключевая роль отводится последнему;
- биометрия;
- расширение аналитического потенциала технологий (большие данные, ИИ и, как следствие, профилирование);

2) государственное слежение и перехват сообщений:

- массовая слежка;
- доступ к данным пользователей, находящихся у частного сектора, в виду того, что государства часто полагаются на компании в деле сбора и перехвата личных данных;
- взлом: внедрение «скрытого» программного обеспечения на цифровые устройства физических лиц;
- попытки ослабления шифрования и анонимности (например, кейс с блокировкой работы Telegram на территории РФ в связи с отказом предоставления Telegram ключей шифрования органам государственной безопасности);
- обмен разведывательными данными;
- трансграничный доступ к данным, находящимся в распоряжении компаний [36].

Право на защиту персональных данных

Пожалуй, наиболее растиражированной в мире является европейская модель законодательства о защите данных, которую восприняли и Россия, и бывшие советские республики, и страны Латинской Америки (Аргентина, Уругвай, Мексика, Перу, Коста-Рика, Никарагуа, Колумбия и Доминиканская Республика) [37]. Несмотря на четкую структуру законодательства о защите данных, в этой сфере наблюдается неформальное мягкое влияние, институциональным воплощением которого служит созданная в 1980 Международная рабочая группа по защите данных в телекоммуникациях («Берлинская группа») [38].

Защита данных зиждется на ясных принципах, среди которых принцип цели и принцип минимизации данных. Кроме того, нужно уделять должное внимание технологическим способам защиты данных. Но хуже всего было бы создать ложное

впечатление полной защиты, которая привела бы людей к меньшей заботе об их частной жизни: технология может играть ключевую роль в защите частной жизни, но только если она не используется изолированно или рассматривается как удобный способ забыть о частной жизни [39].

На правовую защиту персональных данных в последнее время оказывается значительное экономическое влияние. Дело в том, что персональные данные стали базовым экономическим элементом цифрового мира, монетизировавшись на различных сайтах и в соцсетях, в частности в рекламных целях [40]. Это коммерческое использование угрожает частной жизни (1), к чему добавляются угрозы безопасности (2). Утверждается, что бесплатность интернета основана на коммерциализации наших персональных данных [41].

Коммерциализация (монетизация) персональных данных – острая дискуссионная тема во всем мире. Если в странах общего права к этой идее относятся скорее заинтересованно, то в Европе – скорее отрицательно. В контексте государственного управления необходимо определиться с принципиальным подходом к персональным данным граждан и оценить возможности и риски их монетизации (в том числе посредством «обмена» данных на услуги и формулирования права на информационное самоопределение).

В защите персональных данных особо выделяется европейский опыт, который можно систематизировать на основе судебной практики, сформированной Европейским судом по правам человека и Судом ЕС. Так, ст. 8 «Право на уважение частной и семейной жизни» Европейской конвенции о защите прав человека и основных свобод служит основной нормой, которая применяется в делах, связанных с вопросами защиты данных. Наиболее часто нарушения, дошедшие до рассмотрения европейских судов, связаны со сбором персональных данных и соблюдением необходимых процедур (ЕСПЧ, дело L.H. v. Latvia), хранением и использованием персональных данных (ЕСПЧ, дело S. and Marper v. the United Kingdom), перехватом сообщений, прослушиванием телефонных разговоров и тайным наблюдением (ЕСПЧ, дело Roman Zakharov v. Russia) и др.

Право на равенство и недискриминацию

Право на недискриминацию и право на равенство являются основополагающими нормами в смысле международного права прав человека. В обоих случаях речь идет о равенстве прав, с тем отличием, что право на недискриминацию имеет более узкое содержание и подпадает под право на

равенство. Это следует из Appendix E to the Report of the Global Citizenship Commission, “Article 7: The Equality and Non-Discrimination Provision”.

В переложении на цифровое государственное управление это означает непосредственную связь с его качеством. Целью государственного управления является качественное выполнение государственных функций в отношении всех граждан, без какого бы то различия в обращении. Государственное управление, результатом которого становится дискриминация граждан, не может считаться ни обоснованным, ни результативным, ни эффективным, поскольку исключает из круга «получателей» отдельных граждан или целые их группы. В более широком контексте это ведет к постановке вопроса о демократичности и легальности управления.

Основную опасность для права на равное обращение представляет профилирование. Методы автоматической обработки данных могут быть применены к огромному количеству доступной информации для создания индивидуальных и групповых профилей, которые можно использовать для различного обращения с людьми, что ведет к сдержанной дискриминации в больших масштабах. Возникает реальная опасность системной цифровой дискриминации

Существующие исследования дискриминационных рисков при обработке данных выделяют несколько категорий недостатков и нарушений. В своей считающейся основополагающей статье Barocas и Selbst [42] выделяют пять способов, с помощью которых решение, принимаемое искусственным интеллектом, способно непреднамеренно привести к дискриминации. В широком плане проблемы связаны с 1) определением целевой переменной и классовых меток; 2) маркировкой тренировочных данных; 3) сбором тренировочных данных; 4) выбором характеристик; и 5) выбором прокси-данных. Кроме того, 6) системы искусственного интеллекта могут преднамеренно использоваться в дискриминационных целях [43].

При этом к наиболее часто анализируемым в зарубежной литературе видам недостатков, которые способны привести к дискриминационной обработке данных, относят: 1) дефекты сбора данных, 2) агрегирование ошибочных данных, и 3) нормативная невосприимчивость.

1. *Дефекты сбора данных*

Общая причина недостаточных или даже дискриминационных результатов в решениях искусственного интеллекта - создание ошибочных обучающих данных.

Смещенные входные данные с большей вероятностью приведут к смещенным выходным данным. Такое смещение на входе может быть вызвано либо недостаточной, либо избыточной представленностью данных.

2. *Агрегирование ошибочных данных*

Еще одной причиной дискриминационного подхода со стороны искусственного интеллекта является неправильная агрегация данных. В этом случае исходные данные для обучения как таковые репрезентативны, но проявления предвзятости возможны позднее, в процессе обработки.

Во-первых, искусственный интеллект может быть обучен на основе изначальной ручной агрегации данных и воспроизводить предвзятость конкретных лиц, ранее принимавших решения на основе этих данных. То есть решения, принятые когда-то людьми, становятся примером для искусственного интеллекта. Например, разные дефекты маркировки данных при ручном обучении – когда, например, нельзя считать кредитоспособным человека из этнических меньшинств, если он допустил три просрочки выплат по кредитам, в то время как для «белых» допускаются четыре задержки выплат по кредиту.

Во-вторых, дефекты могут быть спровоцированы и после подготовительного периода. Например, если выполнить поиск через Google женских причесок в деловом стиле и причесок неделового стиля, то поисковик показывает в первом случае в основном фотографии белых женщин со светлыми волосами, и фотографии темнокожих женщин - во втором. Гипотетически, если работодатель разрешает искусственному интеллекту отсканировать заявления на работу и разобраться с ними по критерию «непрофессиональный» вид, это способно привести к юридически значимой расовой дискриминации [34].

3. *Невосприимчивость к нормативным установкам*

Искусственный интеллект при принятии решений основывается на статистике, которая может оценивать будущее только с учетом прошлого. Нормативные же соображения обусловлены оценкой фактов. Это значит, что перевести такие соображения на язык, понятный искусственному интеллекту, может быть весьма проблематично.

3 Критерии надлежащей обработки данных в государственном управлении в целях обеспечения фундаментальных прав человека

В целях формирования нового правового регулирования обработки данных в государственном управлении на основе цифровых технологий, которое не вступало бы в конфликт с защитой фундаментальных прав человека, необходимо начать с формулировки основополагающих критериев, режим соблюдения которых можно назвать надлежащей обработкой данных.

полагаем возможным сформулировать следующие критерии надлежащей обработки данных и использования алгоритмов в российском государственном управлении, в режиме, гарантирующем обеспечение прав человека:

- транспарентность,
- специальная оценка воздействия алгоритма на права человека,
- определение пределов использования алгоритмов,
- контроль качества данных для создания и обучения алгоритма,
- нормативное регулирование хранения и обмена данными.

А. *Транспарентность*. В нашем случае транспарентность понимается максимально широко и наполненно. Она включает открытость, подотчетность, контроль, доступность и объяснимость, распространяющиеся на каждый этап создания и использования алгоритма.

Б. *Специальная оценка воздействия алгоритма на права человека*. Основанный на правах человека подход предусматривает целый ряд мер, которыми руководствуются государства, а также коммерческие организации при осуществлении и практической реализации своих обязательств по предотвращению и обеспечению защиты прав человека. Например, Управление Верховного комиссара ООН по правам человека определяет прямое предупреждение как направленное на устранение факторов риска и создание правовой, административной и политической основы, которая направлена на предотвращение нарушений [44].

Крайне важно, чтобы государства создали такие механизмы рассмотрения жалоб, как омбудсмены и эффективные средства судебной защиты. Определение того, какой субъект (или субъекты) несет ответственность за конкретный ущерб, в равной степени важно для того, чтобы распределить ответственность за предоставление эффективного средства правовой защиты. В том случае, если будет

установлено, что нарушения имели место быть, основанный на правах человека подход предъявляет ряд требований: должны быть приняты меры для предотвращения любых повторений, пострадавшим должно быть предоставлено эффективное возмещение, а виновные должны быть привлечены к ответственности.

В. *Определение пределов использования алгоритмов*. Использование подхода, основанного на правах человека, направлено на обеспечение реализации заложенного в цифровую технологию потенциала с одновременным служением этой технологии обществу.

Во-первых, *существуют ли определенные случаи, в которых использование алгоритмической обработки данных запрещено?*

1. Запрет на использование алгоритмов в процессе принятия решений, в случае если он нацелен на обход основанного на правах человека подхода. Это может произойти, если цель использования алгоритма непосредственно направлена на дискриминацию определенной группы или если эффект от использования алгоритма таков, что он приводит к косвенной дискриминации, даже если она непреднамеренна.

2. Запрет на исключительное использование алгоритмов для принятия определенных решений. Основанный на правах человека подход может запретить определенные решения, которые принимаются исключительно на основе алгоритмической обработки данных в отсутствие возможности вмешательства со стороны человека. Сказанное означает, что алгоритмы не могут использоваться в качестве единственного основания для принятия управленческого решения, поскольку, как правило, их выборка основывается на групповых, а не индивидуальных данных, тем самым, велика вероятность отсутствия учета индивидуальных характеристик человека, которые могут иметь принципиальное значение при принятии того или иного решения. Отсюда следует, что при использовании алгоритмов необходимо участие человека или требуется надзор.

Г. Контроль качества данных, используемых для создания и обучения алгоритма

Значение качества данных, используемых для создания и обучения алгоритма, было обосновано выше. В целях государственного управления необходимо определить, какой состав данных может использоваться (нормативные акты, статистика, судебные решения, обобщения правоприменительной практики и пр.). Важно, чтобы отбор данных был недискриминационным (что предполагает

отдельную проверку), была обеспечена полнота и достоверность данных. Отдельную проблему представляет и то, что многие первичные данные были созданы в доцифровом режиме и существуют в бумажном варианте; их приведение в машиночитаемый вид может оказаться процессом длительным и дорогостоящим.

Д. *Нормативное регулирование хранения и обмена данными.* Урегулирование проблемы хранения данных связано с несколькими аспектами. Прежде всего, это локализация хранения данных. Многие государства избрали путь национальной «прописки» данных своих граждан, что в некотором смысле улучшает возможности контроля за их использованием. Разумеется, не в абсолютном масштабе.

Другой аспект проблемы связан с организационно-правовой принадлежностью организаторов хранилищ, поскольку использование частных хранилищ ставит слишком много вопросов о безопасности данных.

4 Предложения по правовому обеспечению фундаментальных прав человека при обработке данных в российском государственном управлении на основе цифровых технологий

Проведенное исследование позволяет сформулировать основные позиции, касающиеся наиболее актуальных направлений правового обеспечения фундаментальных прав человека при обработке данных в российском государственном управлении на основе цифровых технологий.

Представляется, что данному вопросу должно быть посвящено специальное законодательство, в частности, закон об обороте данных (лучшие практики в этой сфере были приведены выше).

Представляется, что законодательство об обработке данных в России необходимо выстраивать с опорой на европейский опыт. Россия является участницей ряда важных международных конвенций, входит в Совет Европы и применяет его рекомендации, правовая система относится к континентальному типу, действующее законодательство о персональных данных основано на европейских нормах. Все это достаточно крепко «привязывает» Россию к Европе.

Итак, *правовое обеспечение фундаментальных прав при обработке данных в государственном управлении на основе цифровых технологий*, на наш взгляд, должно учитывать следующие принципиальные позиции.

1. Необходимо разработать специальное законодательство об обработке данных в государственном управлении, в том числе на основе прорывных цифровых технологий. Важно подчеркнуть, что это – отдельное направление государственной политики, требующее системного и комплексного правового обеспечения. Отправным стимулирующим понятием здесь служит т.н. волюнтаризм данных – понимание того, что все, что происходит с, вокруг, внутри, с помощью или перед цифровыми технологиями, можно превратить в данные. Это означает, что в цифровую эпоху государственное управление почти полностью строится на основе данных, получаемых, хранящихся и используемых на основе цифровых технологий, а такие данные подвергаются постоянным опасностям, нейтрализовать которые – задача государства.

В правовом государстве любые задачи государство решает посредством права, соответственно, и государственное управление, и обработка данных в процессе его осуществления должны быть регулируемы. Так, автоматическое распознавание данных и их сопоставление превращает наблюдение в контроль за данными, для предотвращения всеобъемлющего наблюдения требуются новые правовые положения для сбора, хранения, пересылки, совместного использования и обработки цифровых данных [45]. В целом совершенствование законодательства рассматривается как «аналоговый фундамент» для получения цифровых дивидендов [46].

2. Правила обработки данных в государственном секторе на основе продвинутых цифровых технологий должны быть более строгими и прозрачными, чем в частном секторе, поскольку государственная деятельность монопольна и не предполагает наличия у граждан свободного выбора контрагентов и услуг.

Построение правил обработки данных с точки зрения соблюдения прав человека требует комплексного решения: никакое из фундаментальных прав человека не может остаться ничем не обеспеченной декларацией в актах публичного права или подчиниться лишь режиму субъективного права, отстаиваемого самим гражданином. Фундаментальные права принадлежат конкретному человеку и не могут отчуждаться, передаваться по наследству и пр., в том числе и тогда, когда их реализация связана с использованием цифровых технологий.

3. Обработка данных в государственном управлении на основе цифровых технологий должна опираться на усиление и конкретизацию публично-правовых механизмов обеспечения фундаментальных прав.

Это означает, во-первых, расширение цифровых компетенций государственных служащих и государственных органов, а во-вторых, - введение в государственных органах должности инспектора по обработке данных, и наконец, в-третьих, - установление механизмов ответственности государственных служащих за несоблюдение правил обработки данных.

4. Необходимо создать и нормативно урегулировать статус независимого органа по защите данных в условиях цифровизации их оборота в государственном управлении.

Изучение практического опыта зарубежных государств в вопросах защиты персональных данных от преступных посягательств объективно доказывает, что наличие специализированных органов, предоставляющих защиту персональных данных субъектов информационного взаимодействия (например, Комиссариат по защите информации) является одним из достоинств, что позволяет создать более качественный механизм ее обеспечения [47].

5. Базовым принципом обработки данных в государственном управлении является транспарентность (открытость, подотчетность, объяснимость, доступность).

6. Исходя из позиции о том, что права человека в цифровую эпоху нуждаются в более приспособленной к учету технологических особенностей защите, необходимо внедрить оценку алгоритмов на предмет нарушений прав человека, при их создании и периодический аудит – в процессе их использовании. Особое внимание стоит уделить обеспечению права на частную жизнь, праву на защиту персональных данных и праву на равное обращение (недискриминацию).

7. Необходимо нормативно урегулировать сбор и отбор данных для обучения ИИ, обеспечить контроль качества данных для создания и обучения алгоритма.

8. Отдельные нормативные правила должны быть посвящены хранению данных, а также обмену данными (внутри государственного органа, между государственными органами, между государственными органами и другими субъектами, задействованными в государственном управлении, между государственными органами и частными субъектами).

9. При организации обработки данных в государственном управлении и его нормативном закреплении необходимо там, где это логично, обеспечить переход в защите данных от априорного контроля к апостериорному, одновременно предусмотрев использование гражданско-правовых механизмов защиты прав (в

случае причинения конкретного вреда), с разработкой методик возмещения причиненного вреда.

10. Нужно нормативно дифференцировать виды сбора данных для нужд государственного управления (строго формализованный, наблюдение, опосредованный (из больших данных)), дифференцировать также цели обработки данных (стандартная, экстренная, прогностическая и др.).

11. Необходимо нормативно предусмотреть использование алгоритмов (ИИ) для участия в принятии решений в государственном управлении, как общего характера, так и индивидуальных административных решений (легализация алгоритмов).

При этом нужно установить правило, согласно которому принятие решения в отношении человека не может основываться исключительно на обработке данных на основе алгоритма (ИИ), а контроль за принятием окончательного решения остается за человеком – государственным служащим.

Заключение

Проведенным исследованием охвачено значительное число современных исследований, посвященных использованию ИИ и возникающим в связи с этим рискам фундаментальным правам человека. В результате удалось выделить американский и европейский подходы, элементы которых могут оказаться полезными при формировании российского механизма. Обнаруженный широкий диапазон проблем в целях настоящего исследования систематизирован и сужен до анализа правовых аспектов, имеющих решающее значение при обработке данных в государственном управлении (цифрового государственного управления), а именно: переосмысление прав человека в цифровых условиях; персонализация и предиктивность как эффекты алгоритмической обработки данных; соотношение публичного и частного права в регулировании обработки данных; развитие антидискриминационного законодательства.

На богатом фоне зарубежных источников очевидно, что Россия и российская наука в рассматриваемом вопросе отстают от западной мысли, хотя и следуют при этом в основном за европейскими документами. Тому есть несколько причин: 1) неурегулированность процесса государственного управления в целом, и как следствие, недостаточное внимание к научному сопровождению инноваций в государственном управлении; 2) отсутствие нормативного регулирования обработки данных для целей государственного управления, что не дает возможности науке

(следующей часто за нормативными и конъюнктурными установками) оценить специфику управленческих отношений в условиях цифровизации; 3) разрыв между формальным закреплением защиты данных (ФЗ о персональных данных) и фактическими массовыми нарушениями прав граждан в данной сфере, отсутствие независимого органа по защите данных и внятной судебной практики; 4) слабость и неразвитость механизмов защиты прав человека в целом и т.н. цифровых прав, в особенности судебных механизмов (аргумент даже о «доцифровой» дискриминации практически неизвестен российским судам); 5) неготовность общества и среднестатистического гражданина к осмыслению собственных прав и их защите в новых, цифровых условиях. Каждая из этих причин – отдельное направление для теоретических и прикладных исследований.

Установлено, что в детализированной защите при обработке данных в государственном управлении нуждаются право на частную жизнь (конфиденциальность), право на защиту персональных данных, право на равенство (равное обращение) и недискриминацию. Разработанные в рамках настоящего исследования предложения по правовому обеспечению фундаментальных прав человека при обработке данных в российском государственном управлении позволяют создать системную основу будущего правового регулирования, определить ее приоритеты и принципиальные позиции, а также направления реформирования законодательства.

Благодарности

Материал подготовлен в рамках выполнения научно-исследовательской работы государственного задания РАНХиГС на 2021 год по научному направлению «Государственное управление и государственная служба. Реформа государственного управления на основе развития проектного и процессного подходов».

Список источников

1. Конвенция Совета Европы о защите физических лиц при автоматизированной обработке персональных данных от 28 января 1981 года//Доступ из справочно-правовой системы «КонсультантПлюс».

2. Регламент Европейского Парламента и Совета Европейского Союза 2018/1725 от 23 октября 2018 г. о защите физических лиц при обработке персональных данных, осуществляемой учреждениями, органами, службами и агентствами Союза, и о свободном обращении таких данных, а также об отмене

Регламента (ЕС) 45/2001 и Решения 1247/2002/ЕС. – URL: http://base.garant.ru/72759520/ (дата обращения 04.04.2021).

3. Федеральный закон от 27 июля 2006 года «О персональных данных»//СЗ РФ. 2006. № 31 (1 ч.). Ст. 3451.

4. Савельев А.И. Научно-практический постатейный комментарий к Федеральному закону «О персональных данных». М.: Статут, 2017, - 320 с.

5. Лапаева В. В. Правовой принцип формального равенства//Журнал российского права. – 2008. - № 2. – С. 67-80.

6. Нерсесянц В.С. К праву. О происхождении равенства (из неопубликованного)//История государства и права. - 2009. - № 17. - С. 2 - 7.

7. Miné M. Les concepts de discrimination directe et indirecte. – URL : http://www.era-comm.eu/oldoku/Adiskri/02_Key_concepts/2003_Mine_FR.pdf (дата обращения 24.03.2021).

8. Хартия Европейского союза об Основных правах. – URL: https://eulaw.ru/treaties/charter/ (дата обращения 24.05.2021).

9. Пашенцев Д. А. Особенности правоприменения в условиях цифровизации общественных отношений//Вестник Санкт-Петербургского университета. Право. - 2020. - № 1. – С. 35-49.

10. Bourcier D. De l'intelligence artificielle à la personne virtuelle : émérgence d'une entité juridique?//Droit et société. - 2001. - №3.

11. Huret A., Huet J.-M. L'intelligence artificielle au service du marketing//L'Expansion Management Review. - 2012. - №3.

12. Hacker Ph. The Ambivalence of Algorithms. Gauging the Legitimacy of Personalized Law//Bakhoum Mor, Conde Gallego Beatriz, Mackenrodt Mark-Oliver, Surblytė-Namavičienė Gintarė (Eds.). Personal Data in Competition, Consumer Protection and Intellectual Property Law. Towards a Holistic Approach? Springer, 2018, - 583 p.

13. BigData: Discrimination in data-supported decision making. – URL: https://fra.europa.eu/sites/default/files/fra_uploads/fra-2018-focus-big-data_en.pdf (дата обращения 13.05.2021).

14. Pauliat H. La décision administrative et les algorithmes: une loyauté à consacrer//Revue du droit public. - 2018. - №3.

15. Bosco F., Creemers N., Ferraris V. et al. Profiling Technologies and Fundamental Rights and Values: Regulatory Challenges and Perspectives from European

Data Protection Authorities//Reforming European Data Protection Law. S. Gutwirth, R. Leenes, P. de Hert (eds.). Springer, 2014, - 428 p.

16. State v. Loomis - 2016 WI 68, 371 Wis. 2d 235, 881 N.W.2d 749. – URL: https://caselaw.findlaw.com/wi-supreme-court/1742124.html (дата обращения 10.04.2021).

17. Feldman E.A., Quick E. Genetic Discrimination in the United States: What State and National Government Are Doing to Protect Personal Information//Khoury L., Blackett A., Vanhonnaeker L. (eds.). Genetic Testing and the Governance of Risk in the Contemporary Economy. Springer. 2020.

18. Суворова Е.И. Законодательные подходы к решению вопроса о генетической дискриминации в сфере страхования//Актуальные проблемы российского права. - 2020. - № 9. - С. 188 - 194.

19. Nõmper A. Geenitestide õiguslikust regulatsioonist. Juridica II. – 2001. - P.113–123.

20. Pormeister K. The Prohibitions Against Genetic Discrimination in Estonia//Khoury L., Blackett A., Vanhonnaeker L. (eds.). Genetic Testing and the Governance of Risk in the Contemporary Economy. Springer. 2020, - 364 c.

21. Richter D. Overweight and Obesity as Novel Grounds of Discrimination//Th. Giegerich (ed.). The European Union as Protector and Promoter of Equality. Springer. 2020.

22. Elliott-Larsen Civil Rights Act 453 of 1976. – URL: http://www.michigan.gov/documents/act_453_elliott_larsen_8772_7.pdf (дата обращения 20.04.2021).

23. Froehlich A., Mihai Tăiatu C. Space in Support of Human Rights. Springer. 2020.

24. Levallois-Barth C., Zylberberg H. A Purpose-Based Taxonomy for Better Governance of Personal Data in the Internet of Things Era: The Example of Wellness Data /R. Leenes, R. van Brakel, S. Gutwirth, P. De Hert (Eds.). Data Protection and Privacy: (In)visibilities and Infrastructures. Springer. 2017. P. 139-162.

25. Porcedda M G., Public-Private Partnerships: A “Soft” Approach to Cybersecurity? Views from the European Union//Security in Cyberspace: Targeting Nations, Infrastructures, Individuals, ed. Giampiero Giacomello. New York: Bloomsbury. 2014. P. 183–211.

26. Orrù E. Minimum Harm by Design: Reworking Privacy by Design to Mitigate the Risks of Surveillance//Data Protection and Privacy: (In)visibilities and Infrastructures. Law, Governance and Technology Series Issues in Privacy and Data Protection. – 2017. -Volume 36. – P. 107-138.

27. Разогреева А.М. Предупреждение преступлений при помощи средового проектирования: защищающее пространство и защищенное пространство//Всероссийский криминологический журнал. - 2017. Т. 11, - № 4. - С. 706–716.

28. Haggerty K. D., Ericson R. V. The Surveillant Assemblage//The British Journal of Sociology. – 2000. № 51 (4). – P. 605–622.

29. ECtHR. Big Brother Watch and Others v. the United Kingdom. Applications nos. 58170/13, 62322/14 and 24960/15. Judgment of 13 September 2018.

30. Viktor Mayer-Schönberger and Kenneth Cukier. Big Data: A Revolution That Will Transform How We Live, Work, and Think//Eamon Dolan/Houghton Miffl in Harcourt, - 2013, - 272 p.

31. European Court of Justice. Joined cases C-293/12 and C-594/12, Digital Rights Ireland (C-293/12) and Seitlinger (C-594/12), EU:C:2014:238, § 37.

32. Digital solutions to fight Covid-19. Data Protection Report. – URL: https://rm.coe.int/prems-120820-gbr-2051-digital-solutions-to-fight-covid-19-text-a4-web-/16809fe49c (дата обращения 7.10.2021).

33. Düwell M. Human Dignity and the Ethics and Regulation of Technology // The Oxford Handbook of Law, Regulation and Technology. – URL: https://www.oxfordhandbooks.com/view/10.1093/oxfordhb/9780199680832.001.0001/oxfordhb-9780199680832-e-8 (дата обращения 08.08.2021).

34. Tischbirek A. Artificial Intelligence and Discrimination: Discriminating Against Discriminatory Systems//Th.Wischmeyer, T. Rademacher. Regulating Artificial Intelligence. Springer. 2020. P. 103-121.

35. Ковлер А.И. Европейская конвенция в международной системе защиты прав человека: монография. М.: ИЗиСП, Норма, ИНФРА-М, 2019, - 304 с.

36. Доклад Верховного комиссара Организации Объединенных Наций по правам человека «Право на неприкосновенность частной жизни в цифровой век». – URL: https://ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/39/29 (дата обращения 27.10.2021).

37. Brian Nougrères A. Data Protection and Enforcement in Latin America and in Uruguay // Wright D., De Hert P. (eds.) Enforcing Privacy. Regulatory, Legal and Technological Approaches. Springer, 2016, p.176.

38. Dix A. The International Working Group on Data Protection in Telecommunications: Contributions to Transnational Privacy Enforcement // Wright D., De Hert P. (eds.) Enforcing Privacy. Regulatory, Legal and Technological Approaches. Springer, 2016, p.183-193.

39. Le Métayer D. Whom to Trust? Using Technology to Enforce Privacy // Wright D., De Hert P. (eds.) Enforcing Privacy. Regulatory, Legal and Technological Approaches. Springer, 2016, p.431.

40. Peyrou S. La protection des données à caractère personnel au sein de l'UE : des enjeux économiques et sécuritaires encadrés par le législateur sous le contrôle du juge // Revue du droit public et de la science politique en France et à l'étranger. 2016. № 1.

41. Urvoas J.-J. Le point de vue du Président de la Commission des lois de l'Assemblée Nationale // Revue du droit public et de la science politique en France et à l'étranger. - 2016. - № 1.

42. Barocas S., Selbst A.D. Big Data's disparate impact. California Law Review. - 2016. - Vol. 104. P. 671-732.

43. Zuiderveen Borgesius F. Discrimination, intelligence artificielle et décisions algorithmiques. Etude à l'intention du Service anti-discrimination du Conseil de l'Europe. 2018, - 53 p.

44. UN Human Rights Council, 'Report of the Office of the UN High Commissioner for Human Rights on 'The Role of Prevention in the Promotion and Protection of Human Rights' (16 July 2015) UN Doc A/HRC/30/20, para 9.

45. Ellebrecht, S., Kaufmann, S. Digitalization and Its Security Manifestations // European Journal for Security Research. 2020. doi:10.1007/s41125-019-00063-8.

46. Захарова Е.Н. Цифровая экономика как важнейший институт трансформации современных социально-экономических систем//Представительная власть. - 2018. - №5-6. - С. 63-67.

47. 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.