ЯМНК
XXIII
2022

ПРИОРИТЕТНЫЕ НАПРАВЛЕНИЯ ПРАВОВОГО РЕГУЛИРОВАНИЯ ЦИФРОВОЙ ТРАНСФОРМАЦИИ В РОССИЙСКОЙ ФЕДЕРАЦИИ. ВНЕДРЕНИЕ В НОРМОТВОРЧЕСТВО СИСТЕМЫ ОЦЕНКИ ГУМАНИТАРНОГО ВОЗДЕЙСТВИЯ (2022–2025 годы)

Доклад НИУ ВШЭ

ВЫСШАЯ ШКОЛА ЭКОНОМИКИ
НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ
Москва, 2022

К XXIII Ясинской (Апрельской) международной научной конференции по проблемам развития экономики и общества

2022 г.

ВЫСШАЯ ШКОЛА ЭКОНОМИКИ
НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ

ПРИОРИТЕТНЫЕ НАПРАВЛЕНИЯ ПРАВОВОГО РЕГУЛИРОВАНИЯ ЦИФРОВОЙ ТРАНСФОРМАЦИИ В РОССИЙСКОЙ ФЕДЕРАЦИИ. ВНЕДРЕНИЕ В НОРМОТВОРЧЕСТВО СИСТЕМЫ ОЦЕНКИ ГУМАНИТАРНОГО ВОЗДЕЙСТВИЯ (2022–2025 годы)

Доклад НИУ ВШЭ

Издательский дом
Высшей школы экономики
Москва, 2022

УДК 347.73
ББК 67.401
П76

Руководитель авторского коллектива:
М.В. Якушев

Авторский коллектив:
М.В. Якушев, М.С. Журавлёв, Р.С. Ибрагимов, А.В. Майоров

П76 **Приоритетные направления правового регулирования** цифровой трансформации в Российской Федерации. Внедрение в нормотворчество системы оценки гуманитарного воздействия (2022–2025 годы) [Текст] : докл. к XXIII Ясинской (Апрельской) междунар. науч. конф. по проблемам развития экономики и общества, Москва, 2022 г. / М. В. Якушев (рук. авт. кол.), М. С. Журавлёв, Р. С. Ибрагимов, А. В. Майоров; Нац. исслед. ун-т «Высшая школа экономики». — М. : Изд. дом Высшей школы экономики, 2022. — 67 с. — ISBN 978-5-7598-2662-0 (в обл.). — ISBN 978-5-7598-2474-9 (e-book).

В докладе представлены результаты исследований Института права цифровой среды НИУ ВШЭ, проводимых в 2020–2022 гг. в целях определения приоритетных направлений совершенствования российского законодательства для обеспечения оптимальных условий цифровой трансформации. Обозначены основные проблемы («узкие места») в действующем регулировании в сфере обработки и защиты данных, применении систем искусственного интеллекта и установления ответственности за причиненный ими вред, в существующей системе охраны интеллектуальной собственности и др. Выявлена целесообразность обязательного учета этических аспектов цифровой трансформации и обоснована необходимость скорейшего внедрения системы оценки гуманитарного воздействия (ОГВ) в нормотворческом процессе.

УДК 347.73
ББК 67.401

Опубликовано Издательским домом Высшей школы экономики
http://id.hse.ru

ISBN 978-5-7598-2662-0 (в обл.)
ISBN 978-5-7598-2474-9 (e-book)

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Созданный в 2020 г. Институт права цифровой среды НИУ ВШЭ проводит комплексные исследования актуальных и перспективных вопросов правового регулирования цифровых технологий. Основная цель таких исследований заключается в научном обосновании оптимальных направлений и методов развития российского законодательства в условиях цифровой трансформации. В теоретическом плане такие вопросы находятся на самом начальном этапе осмысления, но в практическом они уже сейчас активно обсуждаются в рамках нормотворческого процесса на различных уровнях государственного управления.

Для достижения указанной цели должны быть решены следующие задачи:

- анализ основных проблем действующего регулирования в Российской Федерации и основных зарубежных юрисдикциях, изучение возможностей применимости иностранного опыта;
- выявление «узких мест», требующих нормативной корректировки уже в ближайшее время (несколько лет), а также
- определение приоритетных сфер совершенствования российской правовой системы для обеспечения максимально благоприятных условий цифровой трансформации.

Существующее «цифровое» правовое регулирование в значительной степени основано на подходах конца 1990-х — начала 2000-х годов и с учетом существенно изменившегося «ландшафта» общественных отношений, связанных с использованием современных технологий, требует безусловного обновления. Перечень «узких мест», пробелов в регулировании, примеров избыточного (неэффективного) регулирования и т.д. достаточно обширен, и довольно быстро пополняется новыми возникающими проблемами. Впрочем, это не является чем-то принципиально неожиданным – нормативное (в том числе правовое) всегда отстает не только от уровня развития тех или иных технологий, но и от уровня их фактического использования в соответствующих общественных отношений. Вследствие этого принципиально важно выбрать верные направления и определить приоритетность принятия соответствующих нормативных актов.

Ответы на поставленные вопросы требуют задействования всего арсенала научных методов исследований — эмпирические методы описания и экспертных оценок; общенаучные методы анализа, синтеза, абстрагирования, индукции, дедукции; а также сравнительно-правовые и формально-юридические методы. При этом, помимо традиционных правовых способов, в ситуации ускоренного развития и применения технологий искусственного интеллекта становится абсолютно необходимым принимать во внимание иные способы социального регулирования — в первую очередь этическое регулирование. В свою очередь, в качестве необходимого компонента нормотворческого процесса в сфере цифровой трансформации представляется внедрить систему оценки гуманитарного воздействия (ОГВ), по аналогии с уже существующей системой оценки регулирующего воздействия (ОРВ).

В настоящем докладе изложены результаты указанных исследований. Исходя из перечня поставленных задач, структуру доклада составляют разделы со следующей тематикой: (1) оценка состояния «цифрового законодательства» России на примере регулирования данных; (2) предложения по основным направлениям совершенствования российской правовой системы; (3) обоснование внедрения системы ОГВ как необходимого компонента нормотворчества в сфере цифровой трансформации.

В 2022 г. планируется продолжение указанной аналитической работы в рамках реализуемого НИУ ВШЭ Стратегического проекта «Цифровая трансформация: технологии, эффекты, эффективность».

I. ПРАВОВЫЕ АСПЕКТЫ ЦИФРОВОЙ ТРАНСФОРМАЦИИ В РОССИЙСКОЙ ФЕДЕРАЦИИ: РЕГУЛИРОВАНИЕ ДАННЫХ

1. *Цифровая трансформация* определена в качестве одной из национальных целей развития Российской Федерации на период до 2030 г.[1] В 2020 г. в Конституции РФ появилась норма, предусматривающая отнесение к предметам ведения РФ обеспечение безопасности личности, общества и государства *при обороте цифровых данных*. Стратегия развития информационного общества в Российской Федерации на 2017–2030 годы[2] предусматривает необходимость «обеспечить баланс между своевременным внедрением современных технологий обработки данных и защитой прав граждан, включая право на личную и семейную тайну». Важным направлением цифровой трансформации является активное применение технологий искусственного интеллекта (ИИ) в экономической деятельности и повседневной жизни хозяйствующих субъектов, государственных организаций и жителей России. Это потребовало научного анализа прежде неизвестных юридической науке теоретических проблем и возможностей применения существующего и перспективного правового регулирования ИИ в прикладных сферах — таких как алгоритмизация гражданско-правовых сделок, автономные («беспилотные») транспортные системы, цифровая медицина и др. В свою очередь, появилась и необходимость переосмысления становящихся устаревшими принципов охраны результатов интеллектуальной деятельности («интеллектуальной собственности») в условиях цифровой трансформации.

2. Правовое регулирование цифровой трансформации в Российской Федерации находится на начальном этапе развития. Соответствующие общественные отношения еще не приобрели достаточную устойчивость, чтобы можно было бы однозначно

---

[1] Указ Президента РФ от 21.07.2020 № 474.

[2] Утверждена указом Президента РФ от 09.05.2017 № 203.

рекомендовать тот или иной способ их правовой регламентации. Напротив, как будет показано ниже, по многим аспектам цифровой трансформации целесообразным был бы анализ сопутствующих этических проблем (потенциального «гуманитарного воздействия») для определения конкретных направлений правового регулирования. В то же время накопленный к настоящему времени опыт, практические результаты цифровой трансформации, а также обширный существующий нормативный массив законодательных норм в области информационных технологий позволяют уже сейчас дать оценку текущему состоянию и перспективам развития российского права в сфере цифровой трансформации. Соответствующие исследования были проведены по следующим направлениям.

• **Регулирование данных**, включая понятийный аппарат, тенденции регулирования «больших данных», персональных данных и их обезличивания, обеспечение конфиденциальности (тайны связи) и т.д.

• **Общетеоретические и практические вопросы применения систем искусственного интеллекта**, включая субъектный и объектный состав правооотношений, связанных с использованием ИИ, вопросы распределения ответственности, алгоритмическую прозрачность и др.

• **Охрана результатов интеллектуальной деятельности (интеллектуальной собственности)**, создаваемых в процессе цифровой трансформации, и сопутствующие правовые вопросы (например, так называемое машинное обучение).

• **Прикладные вопросы использования цифровых технологий** — сетевые цифровые платформы, гражданско-правовые сделки в цифровой форме, цифровая медицина, и смежные вопросы, включая статус людей с имплантированными киберфизическими системами.

3. В настоящем разделе представлен анализ регулирования такой важнейшей для цифровой трансформации правовой категории, как данные. Несмотря на то что *информация* в человеческом обществе существует с момента его зарождения, а его эволюция немыслима без использования информации, *как таковая* информация долгое время (за отдельными исключениями) не являлась объектом правовых отношений. Правовой институт *данных* тесно связан с понятием информации, выделение которой в качестве отдельного

объекта правоотношений было обусловлено как социально-экономическим развитием, так и собственно эволюцией юридической теории. Информация — одна из правовых категорий, относительно определения которой нет единой точки зрения. Действующее федеральное законодательство[3] определяет информацию как «*сведения (сообщения, данные) независимо от формы их представления*». Таким образом, в настоящее время ставится *знак равенства* между такими понятиями, как «информация», «сведения», «сообщения», «данные». Такая позиция является неточной и устаревшей.

4. Следует отметить, что в нормативных правовых актах до последнего времени в основном использовался термин «информация», однако применительно к определенным правовым институтам используется именно термин «данные» (*персональные данные, базы данных, большие данные, открытые данные* и т.д.). При этом замена термина «данные» на равнозначный согласно законодательному определению термин «информация» приводит к качественному изменению смысла регулируемых категорий: например, «*открытые данные*» и «*открытая информация*» имеют существенно различное содержание и объемы понятий. Ситуация с используемой терминологией изменилась с развитием нормотворчества в рамках цифровой трансформации. Термин «информация» практически вышел из употребления и почти повсеместно был заменен «данными»[4], которые рассматриваются как *ключевой актив цифровой трансформации*. В определении *цифровой экономики*, приведенном в упомянутой выше Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы, цифровая экономика рассматривается как «хозяйственная деятельность, в которой *ключевым фактором производства являются данные в цифровом виде*, обработка больших объемов и использование результатов анализа которых [...] позволяют существенно повысить эффективность различных видов производства [...]».

---

[3] Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» // СЗ РФ. 31.07.2006. № 31 (ч. 1). Ст. 3448 (далее — ФЗ об информации).

[4] См., напр.: *Талапина Э.В., Южаков В.Н., Двинских Д.Ю., Ефремов А.А., Черешнева И.А.* Оборот данных в государственном управлении: перспективы правового регулирования. М.: РАНХиГС, 2020. С. 13. URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3678040 (дата обращения 20.03.2022).

5. В настоящее время понятия «данные» и «информация» используются в нормативных документах как синонимичные. Однако становится очевидным, что в правоприменительной практике такая синонимичность создает определенные сложности[5]. При этом отмеченные в нормотворческом процессе попытки дать какое-то «особое» определение правовой категории данных не были успешными. В этой связи[6] следует зафиксировать, что понятие данных, вне анализа юридических нюансов его содержания, успешно используется в специальной литературе в соответствии с определением Международной организации по стандартизации, согласно которому «данные — это представление информации (фактов, концепций или инструкций) в виде, пригодном для передачи, связи или обработки как человеком, так и автоматическими средствами»[7].

6. *Конституция Российской Федерации* содержит значительное число статей, имеющих отношение к информации, в разных аспектах. Это и ст. 23, гарантирующая неприкосновенность частной жизни, личную и семейную тайну, тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений, и ст. 24, запрещающая сбор, хранение, использование и распространение информации о частной жизни лица без его согласия, и ст. 29, гарантирующая каждому свободу мысли и слова и устанавливающая право каждого свободно искать, получать, передавать, производить и распространять информацию любым законным способом, одновременно допускающая существование государственной тайны, и провозглашение свободы массовой информации с запретом цензуры, и целый ряд иных статей и их положений. Указанные нормы заложили основы правового режима информации, и они

---

[5] В частности, использование понятия «информация» стало намного более частотным для актов, относящихся к публично-правовой (в том числе административной) сфере, а понятия «данные» — к сфере гражданского оборота и хозяйственной деятельности.

[6] *Савельев А.И.* Гражданско-правовые аспекты регулирования оборота данных в условиях попыток формирования цифровой экономики // Вестник гражданского права. 2020. № 1. С. 60–92.

[7] Representation of facts, concepts, or instructions in a manner suitable for communication, interpretation, or processing by humans or by automatic means. См.: Документ ISO/IEC/IEEE 24765:2010(en) // ISO [Электронный ресурс]. URL: https://www.iso.org/ru/standard/50518.html (дата обращения 28.03.2022).

остаются стабильными на протяжении всего срока действия Конституции. После внесения в 2020 г. в Конституцию Российской Федерации изменений в ней присутствуют *и* информация, *и* данные. При этом если в отношении информации по-прежнему сохраняются права свободно искать, получать, передавать, производить и распространять информацию любым законным способом, то применительно к данным речь уже идет об их *обороте*. Включение в Конституцию упоминания об обороте цифровых данных ставит целый ряд вопросов, требующих теоретического осмысления. Это, в частности, вопросы о специфическом правовом *режиме именно цифровых данных*, о свободном или ограниченном *обороте определенных категорий данных* (либо о запрете таковых), о лицах, обладающих *правами на различные действия* с этими данными, об *основаниях их возникновения и прекращения* и, разумеется, об обеспечении *безопасности оборота* цифровых данных. Целесообразно уточнить, что принципиальным моментом для понимания смысла и цели включения цифровых данных в Конституцию является ответ на вопрос, почему цифровые данные, в отличие от информации, не были включены ни в какие другие статьи Конституции, где тем не менее присутствует информация. Цифровые данные появились именно в статье, определяющей федеральную компетенцию, и именно в п. «м», определяющем компетенцию в сфере обеспечения безопасности, при этом речь идет не просто о цифровых данных, а об их *обороте*. Очевидно, что включение цифровых данных в Конституцию Российской Федерации и определение их места в ней показывают направленность поставленных задач во взаимосвязи с безопасностью оборота цифровых данных и никоим образом не затрагивают установленных Конституцией основ правового режима информации, остающихся неизменными.

7. Действующее российское законодательство в сфере данных характеризуется *фрагментарностью, внутренней несогласованностью* в регулировании информационных отношений, *отсутствием должной координации* разработки новых правовых актов и внесения изменений в уже существующие[8]. Помимо «базового» ФЗ об информации, отдельные аспекты использования данных (как

[8] *Терещенко Л.К., Якушев М.В.* Влияние цифровой экономики на правовые режимы информации // Информационное право. 2021. № 2. С. 4–10.

разновидности правовой категории информации) регулируются в кодексах (Гражданском, Уголовном, Налоговом кодексах, Кодексе об административных правонарушениях), двух федеральных законах о доступе к информации[9], Федеральном законе «О персональных данных»[10] и нескольких десятках иных федеральных законов. В ФЗ о персональных данных таковые определяются как «*любая информация,* относящаяся к прямо или косвенно определенному или определяемому физическому лицу» — то есть и здесь *данные определяются как информация*. Положения российского законодательства, регулирующие отношения в сфере предоставления доступа к открытым данным, открытыми данными называют *форму представления информации*, размещаемой в Интернете в установленном законом формате[11]. Законодательство о тайнах (о коммерческой, государственной, врачебной и иных видах тайны) определяет информацию, составляющую ту или иную тайну, через категорию *сведений*. Таким образом, единообразный подход к пониманию различий между категориями «информация», «данные», «сведения», «сообщения» *не соблюдается*. Понятия «информация» и «данные» чаще всего определяются одно через другое, в результате чего анализ содержания указанных понятий в законодательстве представляет собой безрезультатный замкнутый круг. Такая ситуация не может считаться допустимой, поскольку излишняя синонимичность может вредить юридической технике и, как следствие, влиять на качество правового регулирования[12].

---

[9] Федеральный закон от 09.02.2009 № 8-ФЗ «Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления» // СЗ РФ. 16.02.2009. № 7. Ст. 776; Федеральный закон от 22.12.2008 № 262-ФЗ «Об обеспечении доступа к информации о деятельности судов в Российской Федерации» // СЗ РФ. 29.12.2008. № 52 (ч. 1). Ст. 6217.

[10] Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» // СЗ РФ. 31.07.2006. № 31 (ч. 1). Ст. 3451 (далее — ФЗ о персональных данных).

[11] ФЗ об информации. Ч. 4. Ст. 7.

[12] *Суслопаров А.В.* Соответствие норм Уголовного кодекса России принципу единства и определенности терминологии на примере терминов «информация», «сведения», «данные» // Законы России: опыт, анализ, практика. 2017. № 11. С. 94–98.

8. В российской Конституции речь идет о *цифровых* данных, то есть четко обозначена их форма, что *не согласуется* с дефиницией ФЗ об информации, основывающейся на независимости предоставления информации (данных) от формы. Тем самым необходимо определение оптимального варианта «разведения» понятий «информация» и «цифровые данные». В дальнейшем потребуется более четкое разграничение различных категорий данных с определением особенностей их правового режима. Принципиальным моментом для определения правового режима является правовая регламентация условий включения цифровых данных в экономический и неэкономический оборот, основным из которых является, как следует из Конституции РФ, обеспечение безопасности личности, общества, государства.

9. На доктринальном уровне признается, что данные становятся информацией только тогда, когда они *помещены в определенный контекст и воспринимаются человеком*. При этом возможен и представляется более продуктивным подход, при котором данные (как информация, представленная в форме, пригодной для последующей обработки) могут рассматриваться в правовом смысле по аналогии с извлеченными полезными ископаемыми и представлять собой «сырье» для последующей обработки и изготовления продуктов, имеющих потребительскую ценность и востребованных на рынке конечных потребителей. В этом случае информация, представляющая собой предмет преимущественно публично-правовых отношений, будет являться почти полной аналогией природным ресурсам (полезным ископаемым) до их извлечения и введения в гражданский оборот последующей переработкой (обработкой). Появление категории данных как «*сырья*» для информационных продуктов связано с процессами развития цифровых технологий, в том числе технологий обработки «больших данных», искусственного интеллекта, интернета вещей. Развитие таких технологий привело к своеобразному исключению человека из процесса сбора и обработки информации, сделав сам фактор человеческого восприятия указанных сведений на определенных этапах их обработки *не значимым*.

10. Первоочередные меры в сфере развития *общих норм законодательства о данных* должны быть направлены на:

• унификацию и согласование юридической *терминологии*, используемой для регулирования информационных отношений в различных законодательных актах;

• устранение коллизий между различными правовыми режимами информации (между правовым режимом персональных данных и профессиональными тайнами, государственной тайной и информацией служебного характера и др.);

• усиление «цифровой» составляющей информационного законодательства, закрепление правового режима цифровых данных, учет особенностей обработки данных современными информационными технологиями («большие данные», машинное обучение) и защита законных интересов субъектов правоотношений при такой обработке (интересов личности при автоматизированной обработке данных, интересов общества и государства в части обеспечения информационной открытости, коммерческих интересов — в части защиты конфиденциальных сведений и охране интересов инвесторов в цифровую экономику);

• адаптацию традиционных правовых режимов информации к условиям цифровой среды (необходим пересмотр старой парадигмы *оборота данных* с учетом современных технологических реалий в части защиты информации, составляющей коммерческую, государственную тайну и др.).

11. Система защиты *прав субъектов персональных данных* в рамках адаптации к цифровой трансформации должна развиваться по следующим направлениям:

• изменение требований к согласию на обработку персональных данных в сторону большей гибкости моделей согласия для обеспечения баланса между автономией воли субъектов персональных данных и публичными интересами, интересами третьих лиц;

• увеличение роли организационно-технических средств защиты информации, развитие инструментов «мягкого» права и саморегулирования операторов по вопросам защиты персональных данных;

• оптимизация института юридической ответственности за нарушения в сфере персональных данных с целью усиления превентивной (профилактической) функции;

• обеспечение прозрачности и доверия граждан к алгоритмам обработки данных, защита интересов субъектов персональных дан-

ные от дискриминации в процессе принятия автоматизированных решений.

12. В эпоху «*больших данных*» и *машинного обучения* возможности по преобразованию данных в *полезную* информацию многократно возросли, что увеличило актуальность правового регулирования отношений в сфере оборота данных. Объектом охраны в отношении данных является не конкретная смысловая единица (либо совокупность таких смысловых единиц), а *массивы данных*, представленные, как правило, в цифровом виде и обрабатываемые в компьютерных информационных системах — при том, что традиционный объект регулирования совокупности данных (*базы данных*) относится к интеллектуальной собственности и охраняет не контент (собственно данные), а структуру баз данных по аналогии с литературными произведениями. Определение понятия *набора данных* содержится в Национальной стратегии развития искусственного интеллекта на период до 2030 года[13], в соответствии с которой под ним понимается «совокупность данных, *прошедших предварительную подготовку (обработку)* в соответствии с требованиями законодательства Российской Федерации об информации [...] и необходимых для разработки программного обеспечения на основе искусственного интеллекта». Данное определение носит достаточно узкий характер, в том числе с точки зрения указанной в нем цели — разработки программного обеспечения.

13. Существенное практическое значение имеет решение вопроса о *принадлежности данных*. Ни в одной из юрисдикций единообразный подход к пониманию категории «принадлежность данных» не сформировался. В зарубежной правовой литературе (особенно в американской[14] и европейской[15]) ведутся активные

---

[13] Утверждена Указом Президента РФ от 10.10.2019 № 490.

[14] См., напр.: *Contreras J.L.* The False Promise of Health Data Ownership. NYU Conference — Data Law in a Global Economy // University of Utah College of Law Research Paper No. 304. 2018. URL: https://ssrn.com/abstract=3328258 (дата обращения 20.03.2022); *Elvy S.A.* Paying for privacy and the personal data economy // Columbia Law Review. 2017. No. 117 (6). P. 1369–1460. URL: https://columbialawreview.org/content/paying-for-privacy-and-the-personal-data-economy/ (дата обращения 20.03.2022).

[15] См., напр.: *Boerding A., Culik N., Doepke Ch., Hoeren Th., Juelicher T., Roettgen Ch., Schoenfeld M.* Data Ownership — A Property Rights Approach from

дискуссии о целесообразности применения концепции принадлежности данных (либо владения данными — *data ownership*) к отношениям в сфере оборота данных. Идея признания в отношении данных некоего *аналога имущественных прав* (правомочий владения, распоряжения, пользования и т.д.) неоднозначно оценивается учеными-юристами. С одной стороны, четкое закрепление прав на данные должно способствовать охране законных интересов участников экономического оборота, что особенно актуально в условиях цифровой экономики[16]. С другой стороны, попытки закрепления за данными свойств объекта имущественных прав сталкиваются с серьезными сложностями юридического и этического характера[17]. Во-первых, данные ввиду своей неисчерпаемости (копируемости, дублируемости, тиражируемости) не могут быть полноценным объектом имущественных прав в их классическом понимании (как объекты вещных прав)[18]. Во-вторых, концепция владения данными вступает в конфликт с признаваемым во всех государствах конституционным принципом свободы информации[19] (правом на доступ к информации)[20]. В-третьих, позициони-

---

a European Perspective // Journal of Civil Law Studies. Vol. 11. 2018. URL: https://digitalcommons.law.lsu.edu/jcls/vol11/iss2/5 (дата обращения 20.03.2021).

[16] Как отмечают европейские авторы, «право должно следовать за экономической реальностью и решать юридические неопределенности». См.: *Boerding A. et al.* Data Ownership... P. 352.

[17] См.: *Hummel P., Braun M., Dabrock P.* Own Data? Ethical Reflections on Data Ownership // Philosophy & Technology. 2021. No. 34. P. 545–572. URL: https://doi.org/10.1007/s13347-020-00404-9 (дата обращения: 20.03.2022).

[18] Названная особенность, однако, не препятствует установлению в отношении данных режима «квазисобственности», как это сделано в праве интеллектуальной собственности в форме исключительных прав на результаты интеллектуальной деятельности и средства индивидуализации, которые по своей сути являются информацией.

[19] Некоторыми зарубежными авторами выдвигается компромиссная концепция коллективного владения данными (*community data ownership*). См.: *Singh P.J., Vipra J.* Economic Rights Over Data: A Framework for Community Data Ownership // Development. 2019. No. 62. P. 53–57. URL: https://doi.org/10.1057/s41301-019-00212-5 (дата обращения: 20.03.2022).

[20] Впрочем, право на доступ к информации не является абсолютным, оно может ограничиваться в целях защиты иных прав и свобод, охраняемых конституцией публичных и частных интересов.

рование данных (в первую очередь персональных) как имущества в целях их коммерциализации сталкивается с негативными этическими оценками.

14. Очевидно, что простое *признание данных объектом имущественных прав* и применение к ним положений об объектах вещных прав по аналогии не является адекватным решением. Оборот данных ввиду своей специфики нуждается в правовом режиме с иной, более сложной настройкой[21]. В наиболее общем виде субъектный состав правоотношений в сфере оборота данных сводится к фигурам *обладателей* (лиц, имеющих доступ к данным, возможность их использованиях и/или ограничения к ним доступа) и «*интересантов*» (*заинтересованных лиц* — то есть лиц, имеющих законные интересы в получении доступа к данным, их использовании и/или ограничении к ним доступа). Обладание данными, как правило, рассматривается не в значении обладания титулом (обладания законными полномочиями), а в фактическом смысле. В отношении одних и тех же данных может быть несколько обладателей, как связанных между собой какими-то правоотношениями, так и не связанных друг с другом. Лицо может стать обладателем данных в результате их создания, сбора и обработки, при получении данных от других обладателей на основании закона или договора. *Первичным* обладателем можно назвать субъекта, который изначально инициировал процесс записи и обработки данных экономическими, техническими, информационными средствами. К числу заинтересованных лиц относятся любые лица, имеющие охраняемый законом интерес в отношении конкретных данных. Интересы могут быть *позитивными* (в получении доступа к данным, их использовании) либо *негативными* (в ограничении досту-

[21] В дискуссии о целесообразности признания права владения данными, развернувшейся в зарубежной теории, отмечается, что возникновение права владения на данные чрезвычайно проблематично, поскольку они представляют собой объект, в отношении которого может быть множество интересов. Право владения данными представляется грубым инструментом для согласования конфликтующих интересов, оно может снизить гибкость и увеличить сложности правового регулирования. См.: *Scassa T.* Data Ownership // CIGI Papers No. 187. Ottawa Faculty of Law Working Paper No. 2018-26. 2018. URL: https://ssrn.com/abstract=3251542 or http://dx.doi.org/10.2139/ssrn.3251542 (дата обращения 20.03.2022).

па к данным, запрете использования). Эти интересы могут иметь как *публичный* характер (например, интерес в получении доступа к данным в целях осуществления государственных функций; интерес в доступе к информации о состоянии окружающей среды; интерес в ограничении доступа к запрещенной информации и т.д.), так и *частный* (например, интерес субъекта персональных данных в получении доступа либо ограничении доступа к своим персональным данным, запрете их использования; интерес хозяйствующего субъекта в использовании данных в предпринимательских целях и т.д.). В отношении одних и тех же данных могут существовать разнонаправленные интересы различных лиц. Обладатель данных также, как правило, является заинтересованным лицом в отношении этих данных, а заинтересованное лицо может стать обладателем данных в результате реализации своих интересов в получении доступа к ним. Ключевым субъектом правоотношений в сфере оборота данных является, в сущности, не обладатель данных, а именно *заинтересованное лицо*, поскольку именно оно реализует свои интересы посредством закрепленных в законодательстве правовых механизмов. Правовой статус обладателя данных в части его прав основывается на принципе свободы информации (если у лица есть фактический доступ к данным, по общему правилу, оно свободно в их использовании), в части же обязанностей — включает комплекс ограничений и обязательств, имеющих своей целью защитить публичные и частные интересы заинтересованных третьих лиц.

15. Для эффективного решения вопроса *о принадлежности данных* в российском законодательстве необходимо уточнение правового статуса *обладателя информации* (фактического владельца данных) и введение правовой категории *заинтересованных лиц*. Подход к регулированию оборота данных между обладателями и заинтересованными лицами может использоваться для установления уточненного правового режима *обезличенных данных*[22]. Если характер данных и цели обработки данных, находящихся у оператора (обла-

[22] В 2019–2021 гг. были разработаны и представлены на обсуждение несколько законопроектов, уточняющих правовой режим обезличенных данных, однако до сих пор регулятор и бизнес-сообщество не сформировали единую позицию об оптимальном регулировании.

дателя данных), не затрагивают интересы субъекта персональных данных и не создают угрозы неприкосновенности частной жизни, такие данные должны быть доступны для использования в интересах оператора, третьих лиц, в публичных интересах. Универсальным условием, исключающим субъектов персональных данных из круга интересантов, является обезличивание данных. В случае необратимого обезличивания данных утрачивается любая связь с физическими лицами, чьи персональные данные подверглись обезличиванию. Такие данные перестают быть персональными данными, хотя в отношении них могут существовать иные заинтересованные лица (сам оператор, обладатель данных, государство, третьи лица и др.). Необратимо обезличенные данные теряют статус персональных данных, но продолжают оставаться данными и, в терминологии российского законодательства, по общему правилу, становятся свободно распространяемой информацией (ч. 3 ст. 5 ФЗ об информации), что, однако, автоматически не обязывает обладателя такой информации предоставлять к ней доступ неограниченного круга лиц.

16. В условиях цифровой трансформации правовой институт *государственных (муниципальных) информационных систем* должен развиваться в направлении интеграции с иными информационными системами, в которых обрабатываются данные, имеющие общественное значение. Для этих целей предлагается ввести в законодательство институт *публичных информационных систем*, которые будут объединять все общественно значимые информационные системы в единую экосистему, построенную на принципах интероперабельности и единых стандартах информационного взаимодействия. Данные, обрабатываемые в публичных информационных системах, должны соответствовать требованиям полноты, точности, достоверности, актуальности и непротиворечивости, при этом любые отклонения от указанных требований должны иметь объективные основания и быть понятны пользователям данных, для чего на операторов/поставщиков данных должны быть возложены обязанности по обеспечению прозрачности сбора и обработки данных.

17. Выявлена целесообразность легализации (точнее, упорядочения использования в юридическом контексте) правовой категории «*запись*». Это понятие широко применяется в актах россий-

ского и зарубежного законодательства (запись актов гражданского состояния, записи в судовом/корабельном журнале, в трудовой книжке, в едином государственном реестре юридических лиц и др.). В зарубежных юрисдикциях под термином «запись» понимают определенный массив документированной информации, который имеет доказательственную силу. Записью могут быть договор, справки, выписки, свидетельства и многое другое. Записи могут использоваться в судебных делах в качестве доказательств, подтверждать наличие правоотношений или факт их прекращения и т.д. В эпоху бумажного документооборота речь шла, соответственно, о *бумажных* записях (*paper records*). Технологический прогресс стал основанием для развития записей *в электронной форме* (*digital records*). Такая запись может быть прочтена и верифицирована с использованием ЭВМ. Вариативность таких записей крайне высокая: электронная запись может представлять собой строку в базе данных, быть сообщением электронной почты или сообщением в мессенджере, электронной записью может также признаваться выписка из геолокационной информационной системы или сведения на веб-странице. Появление электронных записей значительно упрощает обмен большим количеством информации и, по сути, рождает собой электронный документооборот. Исходя из анализа правовых актов, где употребляется термин «запись» в их системной связи, можно сделать вывод, что речь идет о внесении сведений в базы данных различного формата (специализированные информационные системы, государственные реестры, судовые журналы и т.д.), зафиксированные уполномоченными субъектами с целью удостоверения подлинности фактов или событий. В каких-то случаях запись порождает юридические последствия (запись о списании утилитарного права), а в каких-то является просто фиксацией установившихся фактов, поскольку напрямую запись с возникновением или прекращением правоотношений не связана (например, в трудовых правоотношениях, когда речь идет об осуществлении записи на приказе или распоряжении при невозможности ознакомления с приказом об увольнении сотрудника).

18. В основе записи лежат прежде всего данные (*запись состоит из данных*), поэтому видится вполне логичным рассматривать в качестве правовых синонимов понятия «*цифровые данные*» и «*электронные записи*». Выделение *цифровых* данных в какую-либо

особую, отличную от *просто* данных категорию, может привести к искажению сущности данных в цифровой среде. В этой связи теоретический вывод о *правовой эквивалентности* понятий «цифровые данные» и «электронная запись (электронные записи)» имеет безусловное практическое значение, избавляющее от необходимости разработки новых правовых конструкций и позволяющее использовать уже имеющееся в законодательстве категории. Достаточно лишь упорядочить их использование и в необходимых случаях дать им определения в целях единообразного применения. Так, данные в записи всегда фиксированы, то есть они имеют упорядоченную форму существования, выражаемую через совокупность признаков: четко определен субъект, который осуществил внесение записи, имеются полномочия по изменению записи и фиксируется факт ее изменения, четко упорядочено место ее расположения, а главное, понятно ее значение и правовое последствие, которое запись порождает или о котором информирует. То есть в ряде случаев (цифровые) данные обретают вид электронной записи как уже известной правовой категории.

19. Упорядочение использования в законодательстве правовой категории «*запись*», возможно, например, путем введения соответствующего определения в ФЗ об информации как «юридически значимых сведений, внесенных (созданных, сохраненных) уполномоченным лицом в информационной системе или иным установленным законодательством образом». Такое определение позволит однозначно понимать «запись» не только в электронной форме (в информационной системе), но и в иных форматах (в частности, в традиционной бумажной форме). Рассмотрение записей в информационных системах позволит понимать таковые как *цифровые данные* без необходимости давать определение данным «вообще», поскольку сложилось общепринятое понимание данных как информации в виде, пригодном для передачи, связи или обработки как человеком, так и автоматическими средствами. При этом было бы разумным уточнить определение информационной системы как «совокупность записей (цифровых данных), содержащихся в базах данных и обеспечивающих их обработку информационных технологий и технических средств». Закрепление статуса записи как юридически значимой информации должно сопровождаться рядом критериев, о которых должно быть сказа-

но в самом законодательстве: запись находится (хранится) в определенной информационной системе, оператор которой установлен в решении о создании такой системы; запись вносится уполномоченным лицом в определенном, нормативно регламентированным (с точки зрения процедуры) порядке; установлена ответственность за неправомерное изменение записи, которое повлекло негативное последствие для того, в отношении кого запись сделана; само лицо, в отношении которого внесена запись, осведомлено о факте существования такой записи и имеет право оспорить ее правомерность.

20. Отдельным аспектом регулирования данных является их охрана в случае передачи их по сетям электросвязи (соблюдение *тайны связи*, гарантированной ст. 23 Конституции Российской Федерации). Такая охрана традиционно рассматривается как составная часть системы основных прав и свобод человека, его правового статуса. В то же время в действующем законодательстве (в частности, в Федеральном законе «О связи»[23]) понятие «тайна связи» не раскрывается, равно как не имеется и однозначного представления, на какой круг субъектов должны распространяться соответствующие конституционные требования. Поскольку в условиях цифровой экономики соблюдение режима конфиденциальности тех или иных видов данных требует однозначного понимания, какими методами и в каком объеме должна обеспечиваться их конфиденциальность, имеющиеся пробелы в правовом регулировании должны быть устранены. В частности, речь идет об определении прав и обязанностей операторов связи и иных лиц, обязанных соблюдать тайну связи; о круге лиц, в отношении которых тайна связи должна соблюдаться; а также о правильной и единообразной квалификации сведений, составляющих тайну связи. Большинство авторов, предпринимающих попытку дать определение понятия «тайна связи»[24], делают акцент на «личном» характере соответствующих сведений, а также на том, что институт тайны связи имеет своей целью защиту интересов граждан. На

---

[23] Федеральный закон «О связи» от 07.07.2003 № 126-ФЗ (далее — ФЗ о связи).

[24] *Апанасенко С.С., Гладких Е.Л.* Тайна телефонных переговоров в уголовном праве России // Ростовский научный журнал. 2019. Вып. 1. Январь. С. 278–293; *Рязанов Н.Ю.* Эволюция права на тайну связи // Право и государство: теория и практика. 2015. № 8 (128). С. 111–115.

этом основании нередко делается вывод о том, что тайна связи не распространяется на коммуникации с участием юридических лиц, а также на переписку и переговоры делового (профессионального) характера. В современных условиях такие выводы должны рассматриваться как ошибочные. Несмотря на то что правовой институт тайны связи исторически тесно связан с обеспечением права на неприкосновенность частной жизни, в действительности тайна связи имеет *самостоятельную сферу* правовой охраны. В частности, в Конституции Российской Федерации право на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений отделено от права на неприкосновенность личной жизни. Законодательство об информации[25] также не разделяет субъектов, чья тайна связи подлежит защите, используя универсальный подход об охране тайны связи любых субъектов (физических, юридических лиц и публично-правовых субъектов).

21. Право на тайну связи является самостоятельным правом, имеющим собственное содержание, структуру, субъектно-объектный состав, механизмы и гарантии его реализации. Право на неприкосновенность частной жизни защищает информацию, определяемую *по содержательному* признаку, то есть информацию, которая характеризует обстоятельства, относящиеся к личности физического лица (например, *персональные данные*, которые являются таковыми только в том случае, если они могут быть соотнесены с идентифицированным или идентифицируемым лицом). В свою очередь, тайна связи охватывает данные, которые определяются не по содержательному, а *по формальному* критерию: соответствующие данные должны иметь форму сообщений, которые находятся в состоянии передачи или уже были переданы по каналам связи. Данная логика в некоторой степени нарушается, когда речь заходит об охране тайной связи *метаданных* — информации, которая характеризует сообщения, но не раскрывает их содержание (например, информации об адресатах сообщений, времени их направления и т.д.). Однако такая информация охраняется тайной связи только в том случае, если она относится к упомянутым выше сообщениям, а сообщения, в свою очередь, все равно определяются по формальному критерию. Соответственно, формальный

[25] См. ФЗ об информации, а также ФЗ о связи.

характер критерия, с использованием которого происходит выделение сведений, составляющих тайну связи, косвенно охватывает не только сами сообщения, но и их метаданные. Описанное разделение наглядно иллюстрирует российское законодательство о связи, которое проводит различие между *сведениями об абоненте* и сведениями, *составляющими тайну связи*, о которых говорится в ст. 53 и 63 ФЗ о связи соответственно. Нормативные положения, посвященные охране сведений об абоненте, во многом дублируют положения законодательства о персональных данных, требуя от оператора связи обеспечить конфиденциальность сведений, позволяющих идентифицировать абонента или иным образом относящихся к нему. В свою очередь, нормы о тайне связи в принципе не содержат какой-либо привязки к характеру передаваемых сведений: ознакомление с корреспонденцией не допускается независимо от того, позволяет она идентифицировать абонента или нет.

22. С учетом вышеизложенного тайна связи может быть охарактеризована как *режим конфиденциальности*, который применяется к *любым* сведениям, передаваемым или переданным в составе переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений, а также к информации о таких сообщениях. В рамках такого подхода можно констатировать, что тайна связи защищает не только частную переписку, но и *коммуникации, связанные с профессиональной деятельностью*. Неслучайно значительное место в отечественной и зарубежной судебной практике занимают споры, связанные с соблюдением права на тайну корреспонденции в отношении рабочих коммуникаций. Также в настоящее время отсутствуют основания для исключения из сферы правовой охраны сообщений, передаваемых юридическими лицами или иными корпоративными структурами. При оценке содержания тайны связи доминирует широкий подход, согласно которому тайной связи охватывается не только содержание осуществляемых коммуникаций, но и сам факт таких коммуникаций и связанные с ними сведения, которые получили в законодательстве наименование «информация о соединениях»[26]. Вместе с тем такой подход подвергается критике со стороны отдельных ученых ввви-

[26] *Терещенко Л.К.* Отдельные вопросы, возникающие в судебной практике при применении норм о тайне связи // Комментарий судебной практики /

ду расширительного толкования тайны связи и необоснованного распространения режима тайны связи на сведения о соединениях[27]. Также в науке ставится под сомнение целесообразность отнесения технических идентификаторов абонентского оборудования к тайне связи, основывая свою позицию на существенно меньшей ценности такой информации для абонента в сравнении с содержанием коммуникаций[28].

23. Знаковой для регулирования отношений в области тайны связи была попытка *Конституционного Суда* Российской Федерации в 2003 г.[29] дать определение содержанию тайны связи, отсутствующему в действующем законодательстве: «Право каждого на тайну телефонных переговоров по своему конституционно-правовому смыслу предполагает комплекс действий по защите информации, получаемой по каналам телефонной связи, независимо от времени поступления, степени полноты и содержания сведений, фиксируемых на отдельных этапах ее осуществления. В силу этого информацией, составляющей охраняемую Конституцией Российской Федерации и действующими на территории Российской Федерации законами тайну телефонных переговоров, считаются любые сведения, передаваемые, сохраняемые и устанавливаемые с помощью телефонной аппаратуры, включая данные о входящих и исходящих сигналах соединения телефонных аппаратов конкретных пользователей связи; для доступа к указанным сведениям органам, осуществляющим оперативно-розыскную деятельность, необходимо получение судебного решения. Иное означало бы несоблюдение требования ст. 23 (ч. 2) Конституции Российской Фе-

---

отв. ред. К.Б. Ярошенко. Вып. 21. М.: Институт законодательства и сравнительного правоведения при Правительстве РФ, ИНФРА-М, 2016. С. 145–153.

[27] *Чечетин А.* Ограничение тайны связи // Законность. 2005. № 7. С. 40; *Богдановский А.* Может ли ошибаться Конституционный суд? // Законность. 2006. № 8. С. 34.

[28] *Рего А.В., Мацкевич А.Ю.* Проблема доступа антимонопольных органов к тайне связи // Российское конкурентное право и экономика. 2019. № 3. С. 18.

[29] Определение Конституционного Суда РФ от 02.10.2003 № 345-О «Об отказе в принятии к рассмотрению запроса Советского районного суда города Липецка о проверке конституционности части четвертой статьи 32 Федерального закона от 16 февраля 1995 года “О связи”».

дерации о возможности ограничения права на тайну телефонных переговоров только на основании судебного решения». Следует отметить, однако, что указанное определение носит «отказной» (то есть процессуальный, не содержательный) характер, в связи с этим вряд ли можно основывать на нем однозначные выводы о перспективах регулирования тайны связи, тем более что по существу вопроса действовало регулирование прежнего Федерального закона «О связи» (от 16.02.1995 № 15-ФЗ), который утратил силу с 1 января 2004 г. Его заменил действующий ФЗ о связи, содержащий схожие, но не полностью аналогичные нормы. Тем самым Конституционный Суд РФ дал расширительное по сравнению с действующим законодательством толкование понятию тайны связи, поскольку, согласно его разъяснениям, получение любой информации, связанной с оказанием услуг связи, поставлено в зависимость от наличия судебной санкции. Действующий ФЗ о связи, к тому же, «получение сведений об услугах связи» не относит к охраняемой Конституцией РФ тайне связи.

24. Для устранения выявленных пробелов и неопределенностей[30] в регулировании *тайны связи* предлагается:

- распространить (однозначно уточнить, что) правовой режим тайны связи на сообщения, передаваемые не только физическими, но и юридическими лицами и иными организациями.
- включать те или иные данные в категорию тайны связи в зависимости от критериев, которыми они характеризуются. Основным критерием предлагается считать факт наличия сообщения, (а) имеющего определенное содержание и (б) являющегося объектом коммуникации, информационного обмена. К данным, составляющим тайну связи, безусловно относится *содержание* («*контент*») сообщений электросвязи, независимо от технологий их передачи. Помимо содержания сообщений следует различать *сведения об абонентах* (правовая охрана которых во многом совпадает с режимом персональных данных), а также *сведения о соединениях* (включая, в частности, геоинформационные данные) с *различающимся* по сравнению с тайной связи правовым режимом;

---

[30] *Изотова А.Н.* Правовое регулирование тайны связи в информационном обществе // Вестник РУДН. (Юридические науки). 2020. Т. 4. № 4. С. 985–1004.

• установить обязанность обеспечивать информацию, составляющую тайну связи, операторам сервисов электронной почты, а также компаниям, которые по факту оказывают услуги связи, однако не должны по законодательству иметь лицензию (по аналогии с курьерскими службами доставки);

• распространить режим тайны связи на субъектов правоотношений, привлекаемых для целей оказания услуг связи, а также расширить перечень целей обработки сведений, составляющих тайну связи для оператора услуг связи;

• уточнить требования к работе с «большими данными» в контексте соблюдения тайны связи. Режим персональных данных и тайна связи являются дополняющими, а не совпадающими, поэтому при работе с «большими данными» операторам таких данных требуется вменить обязанность соблюдать требования к обработке не только персональных данных, но и тайны связи;

• установить правовую возможность предоставления согласия на машинный анализ сведений, составляющих тайну связи, в условиях обеспечения соблюдения прав человека. Для решения данного вопроса требуется нормативное закрепление функциональных и технических требований к средствам автоматической обработки сведений, составляющих тайну связи, поскольку при машинной обработке одной из главных задач является обеспечение высоких стандартов защиты в условиях агрегирования больших массивов данных.

25. Приведенные в настоящем разделе результаты исследований в сфере регулирования данных как основы цифровой экономики иллюстрируют использовавшуюся методологию правового анализа, которая также применялась и к другим изученным предметным областям, что позволило сформулировать предложения по дальнейшему развитию правовой системы Российской Федерации, кратко суммированные в следующем разделе.

II. СОВЕРШЕНСТВОВАНИЕ ПРАВОВОЙ СИСТЕМЫ РОССИИ ДЛЯ ОБЕСПЕЧЕНИЯ ОПТИМАЛЬНЫХ УСЛОВИЙ ЦИФРОВОЙ ТРАНСФОРМАЦИИ: ОСНОВНЫЕ НАПРАВЛЕНИЯ

26. Желательность системной модернизации нормативного массива информационного права обусловлена цифровой трансформацией и вызвана необходимостью приведения его в соответствие с текстом внесенных изменений в Конституцию Российской Федерации и ликвидации правовой неопределенности в регулировании возникающих общественных отношений, связанных с новейшими (цифровыми) технологиями. Одним из выходов могла бы стать кодификация всего комплекса «информационных» законодательных актов, однако все попытки создания *Информационного («инфокоммуникационного») кодекса* до настоящего момента были безуспешными. Возможна разработка не Кодекса, а *Основ информационного законодательства*, которые включали бы базовые положения, понятийный аппарат и принципы регулирования в сфере информации, оборота данных, применения систем искусственного интеллекта и иных прикладных аспектов цифровой трансформации.

27. В то же время в краткосрочной перспективе (без учета комплексной кодификации «цифрового права») целесообразно использовать как (1) *корректировку действующего законодательства* в целях его соответствия новым реалиям (применительно к различным категориям данных речь идет о персональных данных, иных охраняемых законом видов информации, идентификации и аутентификации, электронном документообороте и др.), так и (2) разработку *новых законодательных и подзаконных актов*, в том числе в случае появления новых объектов правоотношений (применительно к данным речь может идти о «больших данных», обезличенных данных, открытых данных, цифровом профиле и т.д.). Возможно также (3) *сохранение действующего регулирования* без внесения каких-либо изменений, с учетом возможностей *саморе-*

гулирования и *применения правовых норм по аналогии*. Следует помнить, что на разных этапах развития экономических отношений наблюдается разное соотношение государственного регулирования, дерегулирования и допустимости саморегулирования в тех или иных сферах, что зависит от целого ряда причин. Отказ от правового регулирования может быть обусловлен различными факторами, в частности, применительно к общественным отношениям, которые государство *не считает нужным* регулировать, или *неэффективно регулировать* правом, или *невозможно регулировать* правом.

28. С учетом выявленных «узких мест» в регулировании наиболее актуальных правовых проблем цифровой трансформации, целесообразно обозначить следующие основные (приоритетные) *направления* совершенствования правовой системы России.

Систематизация *основных принципов и базовой терминологии* информационного законодательства в целях обеспечения единообразия их применения в нормативных правовых актах различного уровня. В перспективе — решение назревшего вопроса о кодификации российского информационного («цифрового», «инфокоммуникационного») законодательства.

Актуализация нормативного регулирования основных объектов (*правовых категорий*), связанных с цифровой трансформацией («информация», «данные», «персональные данные», «цифровые данные», «большие данные», «(публичные) информационные системы» и т.д.

Разработка *концепции регулирования систем искусственного интеллекта* (робототехники) с учетом использования этических стандартов, «мягкого права», механизмов саморегулирования, а также нормативно-технического регулирования.

Развитие (корректировка) законодательства об *интеллектуальной собственности*, обеспечивающее адекватную защиту правообладателей и возможности беспрепятственной творческой деятельности в интересах цифровой трансформации.

«Точечное» регулирование отдельных *прикладных аспектов использования современных технологий*, с устоявшейся практикой хозяйственных деятельности и сложившимся представлением о соответствующих общественных отношений.

Внедрение *системы оценки гуманитарного воздействия* (ОГВ) в нормотворчество, связанное с цифровой трансформацией.

29. Быстрое развитие *технологий искусственного интеллекта (ИИ)* ставит вопрос о правовом статусе использования систем ИИ, обладающих разной степенью автономности: по некоторым прогнозам, к 2075 г. мыслительные процессы роботов уже нельзя будет отличить от процессов мышления человека[31]. Можно полагать, что системы ИИ могут выступать *не только как объект регулирования,* но и зачастую одновременно как *потенциальный инструмент применения и/или обеспечения соблюдения регулирования*[32], в частности *при принятии юридически значимых решений*, и в самое ближайшее время во всем мире будет наблюдаться процесс постепенного правового признания тех или иных «действий» системы ИИ и их последствий, а также формализации этих действий. Именно в сфере использования ИИ верно утверждение, что право осуществляет свои регулятивные функции не изолированно и обособленно, а в едином комплексе и тесном взаимодействии с другими социальными регуляторами[33]. В этой связи требует особой проработки отражение в проектируемых нормах *этических принципов* использования систем ИИ, которые, как подтверждает мировой опыт, приобретают особое значение в этой сфере. Среди *правовых* проблем, относящихся к использованию ИИ, выделяются:

- определение субъектного и объектного состава правоотношений, связанных с системами ИИ;
- допустимость использования ИИ при *принятии юридически значимых решений*;
- регулирование *ответственности* в сфере ИИ;
- совершение *гражданско-правовых сделок* с использованием систем ИИ;
- обеспечение *алгоритмической прозрачности* в процессах принятия решений.

---

[31] *Etzioni O.* No, the Experts Don't Think Superintelligent AI is a Threat to Humanity // MIT Technology Review. September 20, 2016 [Электронный ресурс]. URL: https://www.technologyreview.com/2016/09/20/70131/no-the-experts-dont-think-superintelligent-ai-is-a-threat-to-humanity/ (дата обращения 28.03.2022).

[32] Regulating Artificial Intelligence / T. Wischmeyer, T. Rademacher (eds). 2020. URL: https://link.springer.com/book/10.1007/978-3-030-32361-5 (дата обращения 28.03.2022).

[33] *Нерсесянц В.С.* Философия права: учебник для вузов. М.: Норма, 2004. С. 77.

30. Проведенный анализ *субъектного и объектного состава* правоотношений, связанных с использованием систем ИИ, в значительной степени был обусловлен дискуссиями о возможности наделения таких робототехнических систем той или иной степенью правосубъектности (дееспособности) и позволил сделать следующие выводы:

• потенциальное наделение робота (системы ИИ) правосубъектностью в настоящее время *не решает* каких-либо задач, помимо ограничения ответственности лиц, причастных к созданию или эксплуатации соответствующего робота;

• в текущих социально-экономических условиях признание робота (системы ИИ) субъектом права *не имеет* надлежащих политико-правовых оснований. Хотя роботы потенциально способны нести ретроспективную имущественную ответственность, которая может быть реализована посредством применения механизмов страхования, возложение ответственности на робота как такового приводит к невозможности достижения одной из основных целей ответственности — превенции правонарушений;

• оставаясь *объектом правоотношения*, система ИИ может выступать средством реализации прав субъектов оборота (например, средством трансляции волеизъявления на совершения сделки) или средством нарушения прав (в частности, в случаях причинения вреда с использованием систем ИИ). В обоих случаях ключевым является вопрос о том, каким образом активность ИИ должна влиять на правовое положение субъектов, причастных к применению ИИ (в первую очередь лиц, осуществляющих использование ИИ для решения тех или иных задач);

• в контексте реализации прав специфичная роль ИИ проявляется только в контексте *потенциального несоответствия действий робота волеизъявлению или интересам лица, волю которого робот призван выразить* во вне (прямо или опосредованно, через формирование собственного решения, призванного учесть интересы субъекта). Как явно следует из анализа существующих положений ГК РФ, посвященных оспоримым сделкам, нарушающим интересы одной из сторон (например, ст. 174 ГК РФ), правопорядок отдает предпочтение интересам добросовестного контрагента, который не знал и не должен был знать, что контрагент действует без надлежащих полномочий (в нарушение интересов представляемого лица);

• в контексте определения обязанностей субъектов в ходе эксплуатации систем ИИ представляют интерес следующие критерии

классификации соответствующих систем[34] — степень *автономности* (неавтономные и автономные системы ИИ); степень *автоматизации* (системы, предполагающие предварительный контроль человека, последующий контроль человека и отсутствие контроля со стороны человека); степень *риска* (системы ИИ, результаты деятельности которых могут привести к причинению вреда жизни или здоровью человека, имуществу, безопасности общества или государства и т.д.); степень *объяснимости*.

31. Принятие юридически значимых решений может обладать характером властного воздействия, то есть, по сути, система ИИ фактически будет *наделена властью*, в этом случае должен быть определенно решен вопрос о порядке ответственности в случае такого автоматизированного принятия решения. При этом юридически значимые решения — это группа решений, которая охватывает разные по своей сложности и содержанию действия. Выделяются следующие признаки юридического действия: их волевой характер, внешнее проявление воли лица, должно быть доступно восприятию со стороны третьих лиц, его формализация и его закрепление в норме права, направленность на правовые последствия. Выражение воли лица будет формироваться в момент начала использования системы ИИ, то есть лицо осознает и заранее нацелено на получение всех юридических последствий такого использования системы. При этом в тот же момент у пользователя системы ИИ должна быть возможность отказаться от принятия автоматизированного юридического решения в отношении него. Важно отметить, что в частном праве в качестве обязательного условия наступления юридически значимых последствий является *добросовестность* участников отношений при создании и эксплуатации систем ИИ. Процесс принятия решения сосредоточен вокруг принимающего решение (*агента, человека или автоматизированной системы*), который делает выбор из доступных ему вариантов. Принимающий решение будет считаться разумным, если в основе его выбора лежит *механизм рассуждения*[35], то есть этот элемент является ключевым при квалификации определенного действия в качестве решения. Принятие решения относится

---

[34] Отчасти основаны на ГОСТ Р 59277-2020.

[35] *Rosenfeld A., Kraus S.* Predicting Human Decision-Making: From Prediction to Action. Morgan & Claypool, 2018. P. 7.

к действиям лиц, то есть фактам, которые прямо зависят от воли и сознания людей. При этом если мы говорим о юридически значимых действиях, то воля должна быть направлена *на наступление правовых последствий*. Это в полной мере будет относиться и к ситуациям, когда принятие решения будет делегировано системе ИИ, можно предположить, что при создании системы ИИ воля и сознание людей будут *выражены в коде*.

32. Разработка концептуальных правовых документов в области *применения искусственного интеллекта* должна учитывать накопленный опыт отраслевого саморегулирования и использования механизмов этического регулирования[36] в этой новой для права сфере (наиболее показательный пример — разработанный и принятый в 2021 г. Кодекс этики в сфере искусственного интеллекта[37]). Тем не менее уже сейчас очевидны, как минимум, следующие принципы для дальнейшей их реализации на различных уровнях системы российского права применительно к вопросу об ответственности за вред, причиненный системами ИИ:

- юридическую ответственность за причинение вреда должны нести «*традиционные*» субъекты права. Санкции и объем ответственности «традиционных» субъектов права *должны определяться человеком*. Правоприменение, исключающее участие человека, *недопустимо*;
- основным ответственным должно являться то лицо, с кем ассоциирован *риск операционного использования, или лицо, являющееся непосредственным выгодоприобретателем* от использования системы ИИ;
- пользователь системы ИИ должен нести *ответственность за выбор технологии*, не соответствующей задаче, за нарушение правил по использованию, контролю и техническому обслуживанию системы;
- производитель систем ИИ должен нести *ответственность за вред, причиненный недостатками системы* с ИИ, полученными во время производства системы;

---

[36] См., напр.: *Ибрагимов Р.С., Сурагина Е.Д., Чурилова Д.Ю.* Этика и регулирование искусственного интеллекта // Закон. 2021. № 8. С. 85–95.

[37] Кодекс этики в сфере искусственного интеллекта. URL: https://www.profiz.ru/upl/2021/Кодекс_этики_в_сфере_ИИ_финальный.pdf (дата обращения 28.03.2022).

• разработчик и производитель систем ИИ должен обеспечивать *соответствие проекта и правил разработки задачам*, полное раскрытие информации о системе ИИ, недопустимость рекламы или распространения иной информации и системе с ИИ, вводящей в заблуждение потенциальных пользователей;

• при использовании систем ИИ возможно применение *ответственности без вины* (источник повышенной опасности) в тех случаях, когда такая система с ИИ может квалифицироваться как источник повышенной опасности и когда это не противоречит природе отношений;

• высокая степень автономности ИИ *не может служить основанием для уменьшения ответственности* разработчиков, производителей.

33. Среди *сфер*, в которых возможно и фактически осуществляется или планируется осуществлять делегирование полномочий, функций, обязанностей системам ИИ, возможно выделить следующие: государственные услуги и управление; правоохранительная деятельность (распознавание лиц, назначение штрафов, обработка данных в уголовных делах); судебная деятельность (поддержка решений судьи, обеспечение единообразия судебной практики, скоринговые системы, оценивающие вероятность совершения рецидива, рассмотрение определенных категорий споров); таможенная деятельность; сфера здравоохранения; автоматизированный транспорт (беспилотный транспорт, использование дронов для проверки трубопроводов); экология; банковская деятельность (кредитный скоринг, предложение персонализированных услуг); подбор персонала; рынок недвижимости (скоринг благонадежности арендаторов). Среди *ключевых требований* к системам ИИ, которым могут быть делегированы какие-либо полномочия, функции, обязанности, следует привести следующие: отслеживаемость, объяснимость, прозрачность и проверяемость; подотчетность и ответственность за действия таких алгоритмов, эффективность решений, принимаемых алгоритмами; отсутствие необъективности, дискриминации, неравенства, несправедливых решений, порождаемых алгоритмами, предвзятости алгоритмов; соответствие систем ИИ не только нормам права, но и этики; возможность контроля со стороны человека; устойчивость и безопасность. Чем меньше человеческого контроля предполагает конкретный слу-

чай делегирования полномочий системам ИИ, тем более жесткие требования должны предъявляться к тестированию и системному управлению технологиями ИИ.

34. Что касается последствий автономного принятия решений (АПР) системами ИИ — физическое лицо (гражданин) должно иметь безусловное *право на оспаривание* такого решения. Делегирование принятия решения ИИ может требовать получения согласия физического лица, в отношении которого принимается такое решение. Необходимость получения согласия может проистекать из регулирования персональных данных. Среди дополнительных прав субъектов, в отношении которых системами ИИ принимаются решения, предлагаются следующие: право знать, что решение принимается ИИ; право иметь возможность контролировать генерируемые в процессе использования ИИ данные и знать, куда в дальнейшем они направляются и как взаимодействуют с устройствами и с другими людьми; право быть уведомленным о том, как связаться с человеком и как удостовериться в том, что принимаемые системой решения могут быть проверены или скорректированы; право на получение объяснений. Данное требование может быть трудновыполнимым в случае с ИИ, чью логику решения не всегда могут описать даже разработчики. Специальные принципы правового регулирования делегирования принятия юридически значимых решений с использованием систем ИИ должны учитывать и основываться на *общих принципах справедливости, разумности и добросовестности*. Вместе с тем в связи с особенностями использования технологий ИИ, например, справедливость наполняется новым содержанием, которое охватывает в том числе соблюдение общечеловеческих ценностей, равный и недискриминационный подход, социальную справедливость, права человека, включая свободу, достоинство, независимость, защиту частной жизни, защиту персональных данных. Такие принципы могут рассматриваться как «нормативное ядро» принципиального подхода к этике и управлению в сфере ИИ с поправкой на разрыв между концептуальными формулировками и реальной имплементацией, а также на возможные различия в отдельных ценностных подходах в зависимости от юрисдикции.

35. При делегировании принятия решений ключевыми проблемами ответственности, выходящими на первый план, становятся

определение субъекта ответственности, определение *случаев наступления* такой ответственности и определение *вида ответственности*. Праву известны ситуации, когда ответственность за действия одного субъекта перелагается на другого субъекта. К таким ситуациям, например, относятся ответственность работодателя за действия работника при исполнении им трудовых функций, ответственность родителей за действия несовершеннолетних детей, ответственность юридического лица или государственного органа за действия его должностных лиц, ответственность владельца источника повышенной опасности. При рассмотрении ответственности ИИ целесообразно говорить в первую очередь о *деликтной* ответственности, то есть меры ответственности должны быть установлены как реакция на вред, который ИИ может причинить или причиняет. При этом речь не всегда идет о *линейной* ответственности, то есть ответственности одного лица за вред, который он причинил, а скорее о *совмещенной* ответственности, то есть, когда помимо причинителя вреда к ответственности могут быть призваны и другие субъекты[38]. В случае признания ИИ объектом также есть несколько вариантов возложения деликтной ответственности:

1) на *обладателя прав* на устройство, снабженное интеллектом;

2) на *разработчика* программного обеспечения;

3) на *оператора*, обслуживающего ИИ.

36. Складывающаяся практика разработки и применения систем АПР показывает, что в процессах обработки данных, используемых для принятия юридически значимых решений, а также в самих алгоритмах установления закономерностей и выводов на их основе существуют недостатки. В частности, выборки данных, на основе которых принимаются решения, могут являться недостоверными, а сами алгоритмы принятия решений — несбалансированными, что приводит к ложным выводам и некорректным результатам. Логика, по которой система АПР приходит к тому или иному выводу, не всегда объясняется либо принципиально не объяснима. В таких условиях возникает естественный конфликт между интересами лиц, в отношении которых применяются си-

---

[38] См.: *Тихомиров Ю.А, Крысенкова Н.Б., Нанба С.Б., Маргушева Ж.А.* Робот и человек: новое партнерство? // Журнал зарубежного законодательства и сравнительного правоведения. 2018. № 5. С. 5–10.

стемы АПР и которые заинтересованы в максимальной прозрачности применяемых механизмов, и разработчиками соответствующих решений, заинтересованными в снижении административного бремени при внедрении инновационных технологий. Под *прозрачностью* системы АПР понимается доступность документации о коде программы, а также сведений о параметрах и наборе данных, используемых для ее обучения (если для системы АПР характерно применение машинного обучения). В отличие от прозрачности, *объяснимость* требует предоставления информации не только о самой системе, но и о причинах, по которым она принимает те или иные решения. При этом объяснимость рассматривается не только как способность объяснять технические процессы. Объяснения могут касаться, например, выбора сферы применения системы АПР и принимать различную форму в зависимости от целевой аудитории, целей и контекста объяснений. С указанными выше характеристиками тесно связано требование *подотчетности* — обязанность обосновать действия, совершаемые с использованием системы, и претерпевать санкции в случае неудовлетворительности обоснования.

37. Применительно к системам (АПР) на уровне федерального законодательства имеет смысл реализовать, в частности, следующие меры, направленные в первую очередь на обеспечение большего *доверия* к таким системам, использующим ИИ:

• установление на нормативном уровне *классификационных критериев*, позволяющих осуществить категорирование систем АПР с учетом характерного для их применения уровня риска (так, для систем высокой степени риска может быть установлено требование об обязательном логировании всех действий, происходящих в системе АПР в ходе принятия решения. При этом важно избежать дублирования со смежными сферами регулирования — в частности, законодательством о критической информационной инфраструктуре);

• введение требования об *обязательном осуществлении предварительной самостоятельной и/или внешней оценки алгоритмического воздействия* системы АПР на предмет справедливости, отсутствия дискриминации, точности и релевантности обучающих данных. Вид оценки, применимый к системе АПР, должен зависеть от типа рисков, характерных для системы АПР (с учетом классификационных критериев, упомянутых выше);

• установление *запрета на использование в наиболее рискованных сферах* алгоритмов, не обеспечивающих достаточный уровень объяснимости;

• формирование государственными органами *регулярных отчетов* об использовании систем АПР;

• *создание единого реестра систем АПР, используемых в государственном управлении*, а также *наиболее опасных* частных систем АПР. В отсутствие такого реестра формирование единой политики в отношении использования систем АПР будет существенно затруднено. Российское законодательство имеет достаточно богатый опыт создания реестров как одного из инструментов определения объектов специального регулирования, который может быть органично распространен на сферу применения АПР;

• введение требования *об обязательном размещении уведомления* о применении системы АПР на соответствующем сайте государственного органа или иной организации, использующей систему АПР. Одновременно желательно закрепить правило, в соответствии с которым любое решение, принятое на основе исключительно алгоритмической обработки, должно содержать отметку о том, что оно было принято без участия человека.

38. Несмотря на то что в настоящее время применение автономных систем ИИ *в гражданском обороте* пока не осуществляется, отсутствие специальных положений, устанавливающих возможность совершать сделки без участия человека, может создать риск возникновения большого количества споров об оспаривании договоров, совершенных системой ИИ. Важно отметить, что сделка обладает свойствами факта, то есть явления объективной действительности, которое может быть воспринята другими людьми[39]. Вопрос восприятия совершения сделки связан с обеспечением прозрачности и объяснимости операций системы ИИ. Анализ российской судебной практики в исследуемой сфере показал, что суды не квалифицируют договоры, в которых оферта формируется компьютерной программой, как автоматизированные. При этом, делая выводы о заключении или не заключении договора, когда оферта была размещена с существенной ошибкой, например,

[39] *Скловский К.И.* Сделка и ее действие. Комментарий главы 9 ГК РФ. Принцип добросовестности. 4-е изд., доп. М.: Статут, 2019.

ценой товара в 1 руб., судьи применяют различные подходы. Так, например, в одном из дел суд признал договор незаключенным в связи с тем, что не была согласована цена товара, поскольку она была указана с ошибкой, то есть отсутствовала воля одной из сторон на заключение такого договора[40], в другом же аналогичном деле суд презюмировал волю на заключение договора и признал его юридическую силу[41]. Тем не менее суды признают ответственность пользователей программного обеспечения за их действия и ошибки. Для целей регулирования сделок представляется значимой корректная *классификация систем ИИ* в зависимости от степени автономности. В случае если сторона использует программу, которая действует без участия человека, но в рамках заложенного алгоритма, можно утверждать, что воля стороны на заключение договоров данной программой была выражена путем, во-первых, формирования конкретного алгоритма; во-вторых, использования программы. По сути, программа, за некоторыми исключениями и при отсутствии ошибок, не принимает каких-либо решений, которые изначально не были заложены. В то же время, когда речь идет об использовании систем ИИ, способных самостоятельно анализировать информацию, самообучаться и выходить за рамки изначально заложенного алгоритма, могут возникать проблемы, связанные с тем, что изначально запроектированные в системе ИИ параметры совершения сделок могут отличаться от итоговых решений, принимаемых этой системой.

39. Особенность совершения сделок системой ИИ заключается в том, что в цифровой среде необходима система *непрерывной цифровой фиксации операций*, осуществляемых технологиями, всех данных, которые система использует и создает, а также соответствующего хранения всех этих данных. Также необходимо поддерживать эту систему, осуществляя периодический мониторинг на ее соответствие качеству, надежности и безопасности. Это требуется также в целях минимизации рисков оспаривания заключенных сделок, необходима проектируемая система фиксации всех операций

---

[40] Например, решение Краснооктябрьского районного суда г. Волгограда от 19.09.2019 по делу № 2-2461/2019.

[41] Например, решение Ворошиловского районного суда г. Волгограда от 11.07.2019 по делу № 2-1569/2019.

системы ИИ, которая будет доступна для восприятия человеком в случае необходимости для представления в качестве доказательства по делу в случае спора либо контролирующему органу. Все лица, которые, так или иначе, являются участниками отношений, связанных с созданием и эксплуатацией систем ИИ, применяемых для совершения сделок, должны иметь *одинаковый уровень правовой защиты* и порядок осуществления прав, независимо от того, осуществляются сделки обычным способом или в цифровой среде.

40. Вопрос *охраны результатов интеллектуальной деятельности, созданных с использованием систем ИИ*, поднимался еще с начала широкого применения вычислительной техники. Однако в течение десятилетий этот вопрос носил скорее теоретический, чем практический характер ввиду того, что использование вычислительной техники дополняло творческую деятельность человека, но в редких случаях заменяло ее. Однако в настоящее время ситуация кардинально изменилась. ИИ достиг уровня, когда он может вполне успешно конкурировать с человеком в части создания результатов интеллектуальной деятельности, более того, современное индустриальное создание результатов интеллектуальной деятельности практически невозможно без использования сложных вычислительных систем. Вопросы охраны результатов интеллектуальной деятельности, созданных ИИ или с его значительным участием, активно обсуждаются уже более десяти лет[42]. И тем не менее говорить о формировании общепризнанных моделей регулирования или даже понятийного аппарата пока не приходится.

41. Применительно к охране результатов интеллектуальной деятельности Концепция развития регулирования отношений в сфере технологий ИИ и робототехники до 2024 года в п. 12 установила, что, в частности, необходимо определить:

1) целесообразно ли *расширить толкование понятия творческого вклада* и/или предоставить правовую охрану таким результатам

---

[42] См. подробнее: *Рудяков А.Н., Майоров А.В., Минченков Е.Н.* Права на интеллектуальную собственность как основной объект инвестиционной деятельности в сфере искусственного интеллекта и робототехники // Ленинградский юридический журнал. 2020. № 3 (61). С. 80–95; *Абышко А.О., Сабиров Г.С.* Искусственный интеллект и произведения машинного творчества: применимость опыта стран общего права к российскому регулированию // Патенты и лицензии. Интеллектуальные права. 2021. № 12. С. 60–71.

как объектам интеллектуальной собственности в другом формате. Если целесообразно то, кто должен быть субъектом, обладающим исключительным правом на результат интеллектуальной деятельности, в каком режиме и с какими возможными изъятиями должна быть предоставлена правовая охрана таким результатам интеллектуальной деятельности;

2) при каких условиях *допустимо использование* при разработке и эксплуатации систем ИИ и робототехники (в частности, при машинном обучении) результатов интеллектуальной деятельности третьих лиц.

Данная проблематика не оказывается в зоне правового вакуума, а попадает в сферу достаточно развитого регулирования. В настоящее время в Российской Федерации отношения по созданию результатов интеллектуальной деятельности и обороту прав на нах регулируются частью четвертой ГК РФ. Являясь достаточно современным законом, тем не менее ГК РФ жестко ориентирован на создание результатов интеллектуальной деятельности человеком. Так, п. 1 ст. 1228 ГК РФ определяет, что автором результата интеллектуальной деятельности признается гражданин, творческим трудом которого создан такой результат. В то же время ИИ по своей природе может рассматриваться как программа для ЭВМ — понятие, хорошо известное праву (согласно ст. 1261 ГК РФ программой для ЭВМ является представленная в объективной форме совокупность данных и команд, предназначенных для функционирования ЭВМ и других компьютерных устройств в целях получения определенного результата, включая подготовительные материалы, полученные в ходе разработки программы для ЭВМ, и порождаемые ею аудиовизуальные отображения). Учитывая, что в настоящее время наиболее распространенным взглядом на ИИ является рассмотрение его как инструмента, используемого в деятельности человека, и, соответственно, выступающего в качестве объекта права, в этом случае вопрос о праве на результат, создаваемый ИИ, фактически заменяется на вопрос о том, участвовал ли в создании данного объекта человек, внесший творческий вклад в его создание. С одной стороны, это позволяет применять *традиционные подходы* к регулированию прав на такие результаты интеллектуальной деятельности, что позволяет разрешать возникающие вопросы уже сегодня — на базе действующего законодательства,

но с другой — ослабляет охрану объектов, в создании которых человек не проявил явной творческой активности[43].

42. Несмотря на широкий диапазон мнений, сложившийся в доктрине и законодательных системах разных стран мира, ряд подходов заслуживает внимания при решении вопросов о перспективах регулирования интеллектуальной собственности в современных условиях[44]. Во-первых, проведение в законодательстве *прямого разграничения* между результатами интеллектуальной деятельности, *созданными ИИ*, и результатами интеллектуальной деятельности, *созданными с использованием ИИ*. Во-вторых, закрепление прав на результаты интеллектуальной деятельности, созданные ИИ, за лицом, *организующим процесс использования ИИ*. Преимуществом данной модели является стимулирование процесса создания новых результатов интеллектуальной деятельности и обеспечение владельцу ИИ возможности эффективно осуществлять его коммерческую эксплуатацию. В-третьих, установление в законодательстве *специального исключения* в сфере авторских прав в отношении возможности использования результатов интеллектуальной деятельности, исключительные права на которые принадлежат иным лицам, *для создания и обучения ИИ*.

43. *Корректировка регулирования* в сфере интеллектуальной собственности как минимум должна включать:

• введение в перечень случаев *свободного использования* произведений таких способов использования, как воспроизведение и переработка объектов авторского произведений и баз *данных исключительно для автоматизированного анализа в целях разработки и обучения искусственного интеллекта* с исключением возможности использования этих объектов за пределами указанной цели и обязанностью удалить соответствующую копию при отпадании такой цели. Это может быть реализовано и в форме *специальных ограни-*

---

[43] Применительно к проблематике принудительных лицензий в этой сфере см.: *Калятин В.О.* Определение условий принудительных лицензий в отношении зависимых изобретений // Патенты и лицензии. Интеллектуальные права. 2021. № 6. С. 33–39.

[44] См., напр.: *Назаров Н.А.* Закрепление прав на результаты интеллектуальной деятельности, созданные с использованием искусственного интеллекта // Патенты и лицензии. 2021. № 7. С. 59–65; № 8. С. 50–57.

чений исключительного права, дающих возможность использовать чужие результаты при разработке, обучении и совершенствовании ИИ. Указанные изменения позволят быстрее и с меньшими расходами разрабатывать и совершенствовать ИИ. Без таких изменений законодательства разработчики ИИ в России будут проигрывать конкурентную борьбу с иностранными производителями;

• предоставление лицу, *организовавшему создание результата* интеллектуальной деятельности с использованием искусственного интеллекта, *самостоятельного права на ограниченный срок*. В качестве ориентира для формирования модели такого права может быть использована конструкция исключительного права изготовителя фонограммы, изготовителя базы данных или публикатора;

• уточнение в ст. 1357 ГК РФ, что право на получение патента *может также принадлежать лицу, организовавшему создание результата* интеллектуальной деятельности искусственного интеллекта. В случае если в создании такого результата принимал участие человек, право на получение патента должно принадлежать им совместно. Данное изменение позволит устранить риски для лиц, использующих искусственный интеллект в сфере технического творчества, связанные с возможностью признания неохраноспособности созданных технических решений;

• минимизация юридических возможностей для формирования «*фейковой реальности*» («дипфейков»), поскольку уже сейчас уровень развития вычислительной техники позволяет формировать объекты, в отношении которых средний потребитель не будет в состоянии определить, что они не отражают существующую реальность, а являются искусственно сфабрикованными. Наиболее взвешенным вариантом представляется введение в законодательстве (например, о защите прав потребителей) обязанности создателя произведения указывать на использование ИИ, а также на то, что произведение передает реальность в измененном виде.

44. Способы, форматы и технические решения использования цифровых технологий весьма разнообразны, а анализ их экономических, организационных, правовых и иных аспектов является предметом многочисленных и интенсивных научных дискуссий. Наиболее очевидной специфика регулирования бизнес-процессов цифровой трансформации становится при сопоставлении с «традиционными» деловыми практиками такого феномена, как

сетевые (цифровые) платформы или экосистемы. Отличия бизнес-модели *в цифровой среде* от «классического» *линейного* бизнеса (под которым принято понимать ситуации, где для продвижения продукции производитель создает товар, и крупным оптом продает посреднику) можно указать следующие:

1) основным активом становится не ресурс для производства продукции, а средства связи. Владелец платформы ничего не производит сам, для него важно то, что произойдет между участниками платформы. И чем больше таких участников, тем эффективнее работает платформа. Платформа сама не порождает тот конечный товар, который потребляет клиент (например, услуга такси или приобретение вещи). Платформа только создает условия для потребления услуг и вещей более удобным способом за счет связей, которые без этой платформы не были бы доступны ни той, ни другой стороне потенциальных транзакций;

2) отсутствуют «классические» транзакционные издержки. У цифровых платформ другая архитектура транзакций, некоторые полностью взаимодействуют в киберпространстве, у кого-то есть расходы на складские помещения и логистику, однако ключевое взаимодействие происходит в интернет-среде, где основная ценность заключается в обмене информацией и способе обеспечения обмена этой информацией. Основные и ключевые действия происходят в самой цифровой платформе, а далее — и только после подтвержденных платформенных транзакций — происходят другие операции, в том числе связанные с расходами, свойственными линейному бизнесу;

3) мобильность в части расширения объемов рынка (интернет делает доступной возможность функционировать по всему миру или одновременно в нескольких точках города, упрощает логистические процессы и порой создает такой бизнес, который мобилен географически и быстрее откликается предложением на спрос).

45. Цифровая платформа *одновременно представляет собой*:

• *бизнес-модель*, обеспеченную высокими технологиями, которая создает стоимость, облегчая обмены между двумя или большим числом взаимозависимых групп участников;

• *информационную систему*, обеспечивающую взаимодействие участников платформы в интернете;

• *элемент* (инструмент, аппаратное или программное решение, инфраструктуру) функционирования *технологической систе-*

мы, обеспечивающей обмен данными между владельцами и пользователями;

• *организацию*, обеспечивающую взаимовыгодные взаимодействия между сторонними производителями и потребителями, которая создает открытую инфраструктуру для участников и устанавливает правила взаимодействия между участниками.

С учетом указанных особенностей и с учетом законодательного регулирования в России под цифровой платформой следует понимать *информационную систему*, обеспечивающую взаимодействие ее участников в определенных целях с использованием интернет-технологий, *доступ к которой предоставляет оператор* такой информационной системы.

46. Для правового регулирования цифровых платформ (экосистем) наиболее значимыми являются следующие теоретические и практические вопросы, требующие доктринального осмысления и нормативного закрепления.

1) Субъектный состав правоотношений по использованию цифровых платформ. Среди *субъектов* правоотношений, связанных с использованием цифровых платформ, выделяются две основные группы: оператор платформы, выполняющий функцию информационного посредника, и пользователи (потребители, поставщики и др.). Круг пользователей в таких правоотношениях достаточно широкий, охватывающий как субъектов предпринимательской деятельности, так и лиц, которые используют возможности цифровых платформ в целях обеспечения личных, семейных, бытовых нужд. Оператор цифровой платформы среди названных субъектов играет особо важную роль, являясь лицом, которое осуществляет эксплуатацию платформы (либо собственником технических средств, посредством которых обрабатывается информация, содержащаяся в базе данных цифровой платформы, либо лицом, которому таким собственником поручена эксплуатация технических средств, если законодательством не предусмотрено иное). Одним из таких операторов цифровой платформы является торговый агрегатор (*оператор маркетплейса*) — агрегатор информации о товарах и услугах, правовые основы деятельности которого закреплены в Законе РФ от 07.02.1992 № 2300-1 «О защите прав потребителей».

2) Понятие *сетевых эффектов* и их роль для цифровых платформ. Одной из наиболее характерных особенностей цифровых

платформ является мультипликативный эффект от их использования большим количеством потребителей соответствующих разнообразных услуг. Сетевой эффект может быть разным: прямым, косвенным, двусторонним, локальным и т.д. Сетевой эффект — зависимость *потребительской ценности* товара от *количества потребителей* одной и той же группы (*прямой* сетевой эффект) либо изменение ценности товара для одной группы потребителей при уменьшении или увеличении количества потребителей в другой группе (*косвенный* сетевой эффект). С целью поиска решений для регулирования новых моделей бизнеса, в том числе цифровых платформ, которые оказывают влияние на рынок, Федеральная антимонопольная служба России в качестве законотворческой инициативы предложила новые способы и методы определения *доминирующего положения*.

3) Особенности функционирования *государственных* цифровых платформ[45]. Цифровые платформы бывают не только коммерческого, но и государственного назначения (например, *портал госуслуг*). Существенная разница между такими платформами в том, что последние не представляют собой бизнес-модель, а являются способом предоставления *некоммерческих* (государственных, муниципальных) услуг, при этом такой способ рассматривается как наиболее оптимальный и современный, позволяющий воссоздать в государстве идею *электронного правительства*. Несмотря на цифровую трансформацию в процессах осуществления государственных функций (оказания государственных услуг населению и бизнесу), роль и функция государства остаются неизменными.

47. Важным аспектом выявления правовой специфики цифровых платформ является проведение их *классификации* по критериям, позволяющим определить существенные характеристики цифровых платформ для целей правового регулирования. Так, помимо наиболее распространенных *прикладных* платформ существуют платформы *инструментальные*, представляющие собой аппаратные или программные комплексы, на чьих базах уже строятся прикладные платформы (Java, IOS, Intel), и *инфраструктур-*

---

[45] *Ибрагимов Р.С., Кислый В.А.* Развитие государственных ИТ-сервисов. Как это влияет на конкуренцию на цифровых рынках // Конкуренция и право. 2021. № 5. С. 45–54.

ные платформы, цель которых — предоставить технологически инфраструктуру для принятия решений на основе данных (ArcGIS, Эра-Глонас и др.). Деление платформ на инструментальные, инфраструктурные и прикладные позволяет нам говорить о том, что не каждую платформу правильно называть бизнес-моделью или технологическим решением. Та же идея лежит в основе деления цифровых платформ на категории *транзакционных* и *нетранзакционых*. К первым относят платформы *прикладного характера*, ко вторым — все остальные. Платформа как бизнес-модель может рассматриваться только в случае, если мы говорим о прикладной (транзакционной) платформе. Следовательно, и большее значение для правового регулирования будет иметь прикладная платформа, поскольку на ней происходит обмен экономическими ценностями, развитие таких платформ напрямую влияет на экономику страны, у такой платформы широкий круг участников, которые совершают действия, имеющие для них юридически значимые последствия. Это, впрочем, не означает, что инструментальные и инфраструктурные платформы не нуждаются в регулировании, просто в большинстве своем инструментальные платформы как программно-аппаратные решения подпадают под регулирование гражданского законодательства, а инфраструктурные платформы действуют также по правилам гражданского законодательства и требуют дополнительно соблюдения правил работы с информацией. Классификация прикладных цифровых платформ может производиться по разным критериям. Однако для правового регулирования в первую очередь значение имеет та *предметная область*, в которой функционирует цифровая платформа, поскольку именно область регулирования и создает определенные правила функционирования. Например, в области медицины действуют правила о лицензировании, в сфере СМИ — необходимость регистрации, существуют ограничения на распространение информации и т.д. В наиболее обобщенном виде такая классификация может включать: 1) платформы для коммуникаций (в том числе электронное взаимодействие с государственными органами); 2) платежные платформы; 3) игровые платформы; 4) платформы для обмена товарами и услугами; 5) инвестиционные платформы. Соответственно, для каждого вида платформ характерна своя совокупность правил, учитывающая прежде всего специфику отрас-

ли, которую цифровая платформа затрагивает. Также в правовом регулировании необходимо принимать во внимание, что бизнес-модель строится исключительно в цифровой среде.

48. Одним из видов цифровых платформ, требующим отраслевого нормативного регулирования, являются *телемедицинские платформы*, актуальность использования которых (в первую очередь для оказания дистанционных услуг в условиях пандемии COVID-19) резко повысилась в последнее время. Телемедицинскую платформу можно определить как технологическое решение (информационную систему), используемое в сфере охраны здоровья граждан с целью профилактики заболеваний, сохранения и укрепления физического и психического здоровья пациентов, поддержания активной жизни, предоставления медицинской помощи и позволяющее осуществлять сбор, хранение и обмен данными и дистанционное оказание медицинской помощи. К числу специфических правовых вопросов регулирования телемедицинский платформ относятся: *правовой статус агрегатора* (оператора) телемедицинской платформы и требования, в том числе лицензионные, предъявляемые к нему; *требования к телемедицинской платформе как информационной системе* (связанные с защитой информации, с порядком документирования информации и ведением медицинской отчетности, с взаимодействием с другими — в том числе государственными — информационными системами, а также требования к регистрации телемедицинских платформ); условия *обработки персональных данных* телемедицинскими платформами (персональные данные пациентов, персональные данные врачей, обезличивание персональных данных); разрешительные процедуры в сфере использования телемедицинских платформ (лицензирование деятельности по оказанию медицинских услуг с использованием телемедицинских платформ, требования к обращению лекарственных средств и т.д.). Далеко не все эти вопросы получили адекватное отражение в действующем законодательстве.

49. В более широком плане цифровая трансформация в сфере охраны здоровья не сводится только к использованию телемедицинских платформ. Современные информационные технологии предоставляют возможности для *повышения гарантий права на охрану здоровья и медицинскую помощь*. Дистанционное оказание медицинской помощи, мониторинг состояния здоровья, авто-

матизированный анализ медицинской информации — это лишь некоторая часть преимуществ, заключенных в потенциале «электронной медицины», которая обеспечивает равный доступ к качественной медицинской помощи, способствует оптимизации государственных расходов на систему здравоохранения[46]. Главным барьером развития телемедицины (электронной, цифровой медицины) является отсутствие адекватных механизмов правового регулирования общественных отношений, складывающихся в процессе *оказания медицинской помощи с использованием цифровых (телемедицинских) технологий*. В настоящее время российское законодательство фактически запрещает использование телемедицинских технологий для дистанционного диагностирования заболеваний и назначения лечения, что препятствует реализации права граждан на медицинскую помощь в условиях цифровой среды. Кроме того, в законодательстве имеются пробелы и коллизии, препятствующие эффективному использованию медицинских данных в исследовательских целях, с применением технологий искусственного интеллекта и машинного обучения. Ключевая проблема заключается в обеспечении баланса частных и публичных интересов, закреплении гарантий реализации прав граждан (пациентов) при оказании им медицинских услуг с применением телемедицинских технологий, защите персональных данных о состоянии здоровья при их обработке в медицинских и исследовательских целях. Несмотря на предпринятые Правительством Российской Федерации меры по повышению эффективности борьбы с пандемией в 2020–2021 гг., требуется системный *пересмотр имеющихся ограничений* на оказание медицинских услуг с использованием телемедицинских технологий (невозможность *постановки диагноза* без очного приема, невозможность *назначения* лечения и, соответственно, *назначения лекарственных средств* без очного приема, невозможность *дистанционного наблюдения* за состоянием пациента без предшествующего очного приема).

50. В целом использование цифровых технологий (в частности, систем ИИ) *для диагностики и лечения заболеваний* имеет широкие перспективы и обеспечивает наиболее полную реализацию кон-

---

[46] *Zhuravlev M., Blagoveshchenskaya O.* Telemedicine: Current State and COVID-19 Lessons // Legal Issues in the Digital Age. 2020. No. 2. P. 92–143.

ституционного права на охрану здоровья и медицинскую помощь. Применение ИИ может рассматриваться и как *критерий качества* оказываемой медицинской помощи — но при условии *обеспечения доступности* технологий ИИ (устранения цифрового неравенства) и определения случаев *обязательного вмешательства человека* (квалифицированного медика). Правовые вопросы, требующие решения в связи с этим, включают установление *информационных прав пациента* и проблематику *алгоритмической гигиены*, *управление рисками* (например, установление обязательных требований к медицинским изделиям с ИИ и страхования медицинских рисков), а также пересмотр требований к обработке медицинских данных пациентов (с обязательным обезличиванием медицинских персональных данных как основания для их обработки в целях обучения искусственного интеллекта). Как мы видим, здесь в полном объеме подлежат учету все отмеченные выше этические и правовые аспекты использования систем ИИ для обеспечения максимальной безопасности пациентов[47].

51. Отдельный интерес в сфере электронного здравоохранения *представляют имплантируемые киберфизические системы* (КФС) — «вживляемые» в тело человека системы, состоящие из нескольких блоков — как технических, так и программных. Имплантируемые КФС, в зависимости от вида, могут оказывать различное по степени и характеру влияние на человека, в тело которого они имплантированы, а также формировать, собирать и передавать информацию и данные как об этом человеке, так и о самом имплантированном носителе. Предвестником использования имплантируемых КФС являются протезирование и использование медицинских средств мониторинга, например, кардиостимуляторов. По сути, многие из этих устройств являются предшественниками КФС, выполняющими одну из их функций — сбор информации. Но в отличие от них КФС может использоваться мультифункционально, собирать и передавать дистанционно информацию, давать возможность медицинскому персоналу удаленно корректировать работу сопряженных устройств и адаптировать лечение в зависимости от характера полученной информации. Имплантируемые КФС могут использоваться в здравоохранении для целей диагностики и про-

[47] Ibid.

гнозирования, сбора данных, для выявления лиц с высокими рисками развития заболеваний, разработки новых лекарств[48].

52. Необходимым *предварительным условием* для проведения процедуры имплантирования КФС должно быть информированное добровольное согласие в соответствии со ст. 20 Федерального закона «Об основах охраны здоровья граждан в Российской Федерации». Кроме того, в целом необходимо установление требований к процедуре имплантации, а также к лицам, проводящим имплантацию (исключительно медицинские сотрудники), и введение реестра для технически сложных имплантатов. В тело человека в результате медицинского или парамедицинского вмешательства оказывается помещена технически сложная система, отвечающая признакам КФС. Как следствие, возникает возможность программирования данной системы, она может влиять на тело, здоровье и функциональность человека, а также формирует данные, которые могут быть изъяты и использованы с помощью применения технологических процессов. Помимо заранее определенных целей имплантирования КФС, с развитием общественных отношений и технологий можно будет допустить, что такая система станет аккумулировать значительно больший объем сведений о реципиенте, чем планировалось изначально. Или появятся новые направления использования таких данных. С одной стороны, это дает потенциал для усовершенствования технологии, с другой — неограниченные возможности для злоупотреблений. Например, кардиостимулятор с технологией КФС собирает данные для целей телемедицины, а в дальнейшем собранные данные — с учетом риска смерти от сердечно-сосудистых заболеваний — используются страховой компанией для принятия решения о возможности заключения договора страхования жизни[49].

53. К КФС возможно применение нескольких правовых режимов: *вещь; орган; субъект*. До имплантации КФС является вещью по смыслу ст. 128 ГК РФ (иногда КФС должна рассматриваться как

---

[48] *Eley C.L.* Dr. A.I.: The Evolution of the Use and Regulation of Artificial Intelligence in Medical Practice and Drug Development. 2017. P. 4.

[49] Подробнее см.: *Майоров А.В., Тягай Е.Д.* Имплантируемые киберфизические системы: социально гуманитарные проблемы внедрения // Вестник ЛГУ им. А.С. Пушкина. 2021. № 1. С. 194–204.

сложная вещь, функционирование которой обеспечивается целым рядом механизмов и технических решений). Сразу после имплантации применение режима органов и тканей к КФС автоматически ставит вопрос об утрате правовой природы вещи и оборотоспособности[50]. Признание КФС органом, а не вещью, создает риск поражения реципиента в правах как собственника или владельца. В этой связи можно допустить, что *имплантированная КФС должна одновременно рассматриваться как вещь, ограниченная в обороте, и как орган*. Признание КФС органом позволит соблюсти права человека на личную неприкосновенность, на охрану здоровья и на неприкосновенность частной жизни[51], а режим вещи, ограниченной в обороте, — защищать права реципиента в порядке защиты прав потребителей, но при этом ограничит возможность заключению сделок с такой КФС.

54. Ключевым вопросом взаимодействия индивида с КФС и общества с КФС становится этическая проблема *доверия и прозрачности*. Принципы и методы функционирования КФС могут быть прозрачными, только если всем понятны принципы их работы и их возможности, в том числе и в области сбора и обработки информации, а также очевидны риски имплантирования и существует действенный механизм защиты от посягательств и злоупотреблений. Вопрос выработки этических принципов во взаимодействии с КФС обсуждался и на международном уровне. Европейским парламентом в 2016 г. была проведена форсайт-сессия в рамках проекта «Этические аспекты КФС», на которой были сформулированы

---

[50] Большинство ученых исключают у органов и тканей, не отделенных от человека, правовую природу вещей или рассматривают их как личное неимущественное благо. См., напр.: *Волож З.Л.* Право на кровь // Вестник советской юстиции. 1928. № 7; *Красавчикова Л.О.* Понятие и система личных неимущественных прав граждан (физических лиц) в гражданском праве Российской Федерации: автореф. дис. ... докт. юрид. наук. Саратов, 1997. Вещью органы и ткани могут признаваться после отделения от тела, либо смерти. См., напр.: *Малеина М.Н.* Статус органов, тканей, тела человека как объект права собственности и права на физическую неприкосновенность // Законодательство. 2003. № 11.

[51] Подробнее о правах на органы и ткани человека см.: *Трубина В.А.* Ткани и органы человека как объекты гражданских прав: дис. ... канд. юрид. наук. М., 2020.

основные этические подходы, а также потенциальные трудности, которые могут быть релевантны после широкого распространения КФС. Обращает на себя внимание и обозначенный в рамках данной проекта горизонт технического развития КФС: 2050 г.

55. Изложенные выше аспекты правового регулирования цифровой трансформации в Российской Федерации не исчерпают всего многообразия теоретических и прикладных правовых проблем, которые предстоит решить для создания эффективно действующей системы законодательного регулирования, но обозначают основные направления для соответствующей нормотворческой работы. Объединяющим фактором для выбора адекватного направления регулирования каждой из прикладных сфер цифровой трансформации является необходимость учета *неюридических* аспектов, и в первую очередь — *этических*. Указанное обстоятельство доказывает необходимость скорейшего внедрения в нормотворческую практику системы *оценки гуманитарного воздействия* (ОГВ).

III. ОЦЕНКА ГУМАНИТАРНОГО ВОЗДЕЙСТВИЯ: НЕОБХОДИМЫЙ КОМПОНЕНТ НОРМОТВОРЧЕСКОГО ПРОЦЕССА В СФЕРЕ ЦИФРОВОЙ ТРАНСФОРМАЦИИ

56. Нормотворческий процесс в сфере цифровой трансформации по очевидным причинам сопровождается вовлечением *широкого круга экспертов* в различных отраслях знаний. В целях повышения прозрачности законодательных процедур, как правило, в открытом доступе размещаются проекты нормативных правовых актов, законопроекты обсуждаются с экспертным сообществом до их официального рассмотрения, а также используются различные методы оценки предполагаемого нормативного материала. Можно в этой связи упомянуть «*регуляторную гильотину*», предполагавшую масштабный пересмотр и отмену нормативных правовых актов, негативно влияющих на общий бизнес-климат и регуляторную среду. Целью реализации «регуляторной гильотины», по мнению Министерства экономического развития Российской Федерации, является тотальный пересмотр обязательных требований, в соответствии с которым нормативные акты и содержащиеся в них обязательные требования должны быть пересмотрены с широким участием предпринимательского и экспертного сообществ[52]. Рассматривать реализацию «регуляторной гильотины» следует в совокупности с практикой применения *оценки регулирующего воздействия* (ОРВ)[53] проектов правовых актов и *оценки фактического воздействия* (ОФВ) действующих правовых актов. При применении оценки фактического воздействия действующего нормативного акта происходит сбор предложений с обоснованием избыточности регулирования либо информации об издержках

---

[52] Механизм «регуляторной гильотины» // Министерство экономического развития Российской Федерации [Электронный ресурс]. URL: https://www.economy.gov.ru/material/directions/gosudarstvennoe_upravlenie/mehanizm_regulyatornoy_gilotiny/ (дата обращения 28.03.2022).

[53] Подробнее см.: Оценка регулирующего воздействия [Электронный ресурс]. URL: http://orv.gov.ru (дата обращения 28.03.2022).

выполнения требований регулирования со стороны экспертов и предпринимателей. При этом важно отметить, что оценке подлежит не правовая форма регулирования общественных отношений, а сами экономические механизмы и прогноз социально-экономических последствий применения правовых норм[54]. ОФВ уже известна российским регионам, которые внедряли ее в пилотном порядке (в частности, Свердловская область в 2013 г.). Ключевой идеей механизма ОФВ является анализ достижения заявленных целей, которые были поставлены при принятии нормативного правового акта, что также позволяет выявлять взаимосвязь между целями принятия нормативного правового акта и тем эффектом, который повлекло его принятие. На федеральном уровне ОФВ осуществляется с учетом сроков, предусмотренных Планом проведения оценки фактического воздействия на календарный год. По ее итогам обнародуется заключение об оценке фактического воздействия, подлежащее рассмотрению Правительственной комиссией по административной реформе и учету органами-разработчиками[55].

57. Тем не менее нельзя не отметить, что механизм ОРВ *не имеет задачи комплексного социального анализа и возможных гуманитарных рисков*, так как изначально методология была рассчитана на процессы введения, изменения и отмены правовых норм, регулирующих экономическую деятельность, и обеспечение, как следствие, существенного повышения качества регулирования и предсказуемости и обоснованности возможных изменений в нормативно-правовой базе экономической деятельности. Сложившийся инструментарий оценки нормативных актов свидетельствует о доминировании экономически детерминированных подходов, когда риски и последствия изучаются с точки зрения возможных финансовых выгод и потерь, тогда как аспекты неэкономического характера либо отодвигаются на второй план, либо не анализируются

---

[54] Оценка законов и эффективности их принятия. Материалы международного семинара. М.: Издание Государственной Думы, 2013.

[55] Постановление Правительства РФ от 30.01.2015 № 83 «О проведении оценки фактического воздействия нормативных правовых актов, а также о внесении изменений в некоторые акты Правительства Российской Федерации» // СЗ РФ. 09.02.2015. № 6. Ст. 965.

вовсе. В этих условиях происходящая цифровая трансформация сформировала запрос на внедрение в сферу нормотворчества комплексного *социально-гуманитарного анализа* в сферу нормотворчества. Влияние современных инноваций уже приводит не только к широкомасштабным трансформациям экономических отношений, способов производства и форм труда, но и ожидаемо порождает множество новых проблем, лежащих в области этики и гуманитарного знания. Это вызвано не только глубокими изменениями в различных областях жизнедеятельности человека, но и тем, что, в сущности, технологии имеют двойственный характер: несмотря на те возможности, которые они дают или могут дать в будущем людям, их развитие неизбежно порождает новые вызовы. Так, например, резонансным кейсом является формирование *системы социального ранжирования* (цифрового учета) в Китае, в рамках которой оценивается благонадежность граждан посредством анализа образа жизни и их поведения с помощью цифровых технологий с потенциальной возможностью синхронизации такой системы с цифровым юанем.

58. Как явствует из представленных выше результатов анализа правовых проблем цифровой трансформации, именно *гуманитарная, этическая экспертиза* в области регулирования цифровых технологий должна стать основой в процессе формирования наиболее эффективной, комфортной и безопасной технологической среды для людей, а также сделать социокультурные и иные последствия развития, внедрения и использования цифровых технологий (в особенности это касается таких сложных и перспективных технологий, как искусственный интеллект) более понятными, прогнозируемыми и, как следствие, управляемыми, что крайне важно не только для государства, но и для российского бизнеса и общества. Решением данной задачи являются разработка, внедрение и использование механизма *оценки гуманитарного воздействия* (ОГВ), который представляет собой процесс оценки гуманитарных последствий принимаемых актов в сфере цифровой трансформации в целях их возможной корректировки в случае, если их принятие не даст ожидаемого позитивного гуманитарного эффекта либо повлечет негативный гуманитарный эффект (в том числе в отношениях, прямо не затрагиваемых нормативным правовым актом) с точки зрения прав и свобод человека, представлений о справедливости, свободе, морали и т.д.

59. Дополнительными аргументами для использования ОГВ являются:

• сохраняющееся *социальное недоверие* к новым технологиям и рост опасений по поводу негативного влияния таких технологий на жизнь людей (в первую очередь речь идет о физическом и ментальном здоровье, безопасности, правах человека), а также низкая вовлеченность общества в процессы принятия решений в сфере научно-технологического развития, напрямую затрагивающих и влияющих на права и свободы, а также образ жизни людей;

• отсутствие современного инструментария для *разоблачения антинаучных мифов и дезинформации граждан* в области научно-технологического развития, проявлений технофобии и неолуддизма (ярким примером является кейс мифологизации технологии 5G), а также выработки рекомендаций по решению связанных с этим;

• *дефицит* оценки и прогнозирования социальных (гуманитарных) эффектов развития, распространения и использования перспективных цифровых технологий в *российской* практике, в то время как за рубежом подобный опыт существует более 20–30 лет;

• «*лоскутное» нормотворчество*, когда правила поведения формируются по факту создания технологического продукта. Фактически цифровая трансформация «диктует» условия правового регулирования, обусловленные технологией и рынком. С точки зрения государственных интересов такую тенденцию можно считать негативной.

60. Оценка гуманитарного воздействия относится к одной *из новых уникальных форм общественного и экспертного участия* в анализе нормативных правовых актов на их соответствие существующим этическим нормам в сфере новых технологий и цифровой трансформации. ОГВ в нормотворчестве отличает следующее.

1) Охват не только нормативно-правового материала, но и *социальных тенденций, характеристик*. Так, навыки оценивания нормативно-правового акта с точки зрения норм этики являются элементом *гражданской компетентности*, поскольку с их помощью население должно определять свое отношение к работе органов власти и управления, тем самым демонстрируя правосознание и правовую культуру.

2) *Критерии оценки*. По сравнению с ОРВ, ОГВ *не предполагает внедрение оценок* и не исходит из формально закрепленных «жестких» критериев. Оценка производится с субъективной точки зрения на базисе этических норм, принятых в обществе, и их толковании в контексте проекта нормативно-правового акта. ОГВ не преследует цель формулировки итогового экспертного заключения, протокола, одобряющего или критикующего представленный на оценку текст проекта нормативно-правового акта. Сущность ОГВ в нормотворчестве заключается в формировании эмпирического материала, который помогает предвосхитить проблемы правового и неправового характера, указать авторам на возможные регуляторные последствия, научное обоснование этих последствий и представить общественное мнение.

3) *Общенаучные* философские методы анализа, применяющиеся совместно с некоторыми специфическими юридическими методами. ОГВ предполагает оценку текста проекта нормативно-правового акта с точки зрения расширительного толкования категории «права человека».

4) Предмет ОГВ имеет *дуалистический* характер:

• текст проекта нормативного акта;

• возможные (моделируемые, прогнозируемые) последствия действия нормативного акта для человека во всех сферах общественной жизни.

61. Резюмируя вышесказанное, можно отметить следующие *базовые отличия* ОГВ от ОРВ:

• ОРВ является *экономически детерминированным* инструментом и не охватывает гуманитарный аспект, что ограничивает его возможности с точки зрения проведения системного анализа. ОГВ позволяет ликвидировать существующий вакуум гуманитарной экспертизы, системно выявлять *социокультурные (этические)* риски научно-технологического развития, вырабатывать решения проблем, затрагивающих и/или имеющих значение для общества;

• проведение публичных консультаций с заинтересованными сторонами является важным элементом процедуры ОРВ, однако ОГВ предполагает *более глубокий уровень взаимодействия* с представителями общества и бизнеса за счет проведения социологических исследований, интервью и фокус-групп. Инструмент ОГВ не только позволит государственным органам власти и коммерческим ор-

ганизациям лучше понимать общественные интересы, установки, запросы и опасения, знакомиться с вненаучными знаниями, оценками, мнениями и опытом, но и даст стимул к включению граждан и представителей бизнеса в процессы принятия решений в сфере формирования нормативного правового регулирования научно-технологического развития;

• ОГВ предполагает проведение *обширной научно-исследовательской работы*, в то время как основным методом ОРВ является проведение консультаций с заинтересованными сторонами;

• по существу, ОГВ имеет больше общего не с ОРВ, а с *общественной экспертизой*. Однако ОГВ имеет свою уникальную методологию, основанную на научном подходе.

62. В рамках развертывания системы ОГВ важным видится инициировать дискуссию о том, можем ли мы развивать «*проспективное нормотворчество*» (направленное в будущее), или в работе по совершенствованию российской правовой системы попрежнему практически полностью будут отсутствовать практики прогнозирования, нормотворчество будет носить *реактивный* характер, в то время как эффективная работа в условиях неопределенности технологического развития и геополитической ситуации требует *проактивного* подхода. Одним из фундаментальных вопросов развития ОГВ является вопрос о политической и идеологической нейтральности. Международные исследования и разработки не должны становиться абсолютной основой экспертной работы с российским законодательством: ключевое значение имеют исследования именно национального контекста, что позволит избежать излишних и прямых заимствований из зарубежных законодательных и политических систем. При этом крайне необходимо вовлекать представителей общества в процессы регулирования цифровой трансформации (в этой сфере достаточно остро стоят вопросы о неприкосновенности частной жизни и правах человека, статусе и использовании пользовательских данных). Цель такого подхода — не только обмен мнениями, но и разъяснительная работа с обществом на предмет того, что их ждет в будущем и как работают новые технологии, развитие которых государственные институты поддерживают через инвестиции и законопроекты. Вместе с этим для экспертов и представителей государственных органов власти мнение граждан в вопросах нормативно-правового регулирова-

ния должно носить преимущественно информативный характер, так как суждения людей могут быть противоречивы с точки зрения этики, отражать стереотипы и предрассудки.

63. Таким образом,

• система ОГВ позволит *эффективнее модерировать и развивать* систему нормативного регулирования процессов цифровой трансформации, а также ускорит процесс складывания практик «*мягкого права*» внутри страны;

• необходимость ОГВ в нормотворчестве обусловлена *широким методологическим потенциалом и гуманитарным подходом* к нормативному материалу в области цифровой трансформации;

• ОГВ имеет весомый *потенциал общественного участия*, что позволяет говорить о реальной сущностной оценке тех правовых новелл, которые будут затрагивать человеческий капитал в общественных отношениях. В результате — снижается вероятность технологической дискриминации в контексте цифровой трансформации;

• ОГВ может стать одним из *ключевых инструментов в рамках исследований* искусственного интеллекта и робототехники с точки зрения гуманитарного знания и дать импульс к переходу от технико-экономического детерминанта к более широкому взгляду на процессы научно-технологического развития и становления цифровой экономики в Российской Федерации. ОГВ позволит развивать такую систему регулирования, которая будет в наивысшей степени отвечать сложившимся в современном российском обществе ценностям и нормам, представлениям о справедливости, свободе и морали.

ЗАКЛЮЧЕНИЕ

Основные предложения, вытекающие из проводимых ИПЦС НИУ ВШЭ исследований, могут быть просуммированы следующим образом.

(1) Законодательство в сфере цифровой трансформации в Российской Федерации нуждается в *срочном и системном* обновлении. Оптимальной с точки зрения правовой теории представляется его систематизация в форме кодификации, однако с учетом текущих политических обстоятельств можно было бы ограничиться продолжением «точечных» поправок в действующие нормативные акты, но основанные на *единой логике, терминологии и принципах* регулирования.

(2) Ключевыми *правовыми институтами*, требующими переосмысления и обновленного в рамках цифровой трансформации, являются *данные* (включая персональные данные, «большие данные» и др.) и смежные с использованием и передачей данных вопросы *принадлежности данных* функционирования *публичных* (в первую очередь государственных) информационных систем, *тайны связи*, упорядочение применения правовой категории «*запись*».

(3) Применительно к регулированию использования систем искусственного интеллекта наибольшую актуальность имеют вопросы *делегирования юридически значимых решений*, *ответственности существующих субъектов права* за деятельность автономных («беспилотных») систем, обеспечение *алгоритмической прозрачности*.

(4) Развитие цифровых технологий неизбежно влечет за собой необходимость пересмотра подходов к *охране результатов интеллектуальной деятельности* (интеллектуальной собственности). Несмотря на важность защиты законных прав авторов с сохранением существующих международно признанных принципов охраны, использование систем искусственного интеллекта в создании объектов интеллектуальной собственности требует *новых подходов* к охране отдельных видов объектов (например, в целях *машинного обучения* или с учетом *отсутствия правосубъектности робототехнических систем*).

(5) Активное развитие и использование *цифровых платформ*, в первую очередь *телемедицинских*, в условиях эпидемических ограничений 2020–2022 гг., является убедительным примером того, в каких направлениях и при соблюдении каких требований в сфере защиты прав граждан и бизнеса должно осуществляться *регулирование новых форматов взаимодействия* государства, общества и жителей страны, *с отменой необоснованных ограничений и избыточных требовани*й к использованию цифровых технологий.

(6) *Общим* аспектом для всех частных проблем правового регулирования цифровых трансформаций является обязательный учет накопленного опыта отраслевого саморегулирования, использования формата «*мягкого права*» и механизмов *этического регулирования* (показательный пример — Кодекс этики в сфере искусственного интеллекта 2021 г.).

(7) В целях обязательного учета этических аспектов цифровой трансформации предложено обоснование скорейшего внедрения в нормотворческий процесс (на всех уровнях принятия решений) и требует дальнейшей проработки методология системы оценки гуманитарного воздействия (ОГВ), по аналогии с применяемой в Российской Федерации с 2010 г. системой оценки регулирующего воздействия (ОРВ).

* * *

Представленные результаты научно-исследовательской работы Института права цифровой среды, обобщенные выводы и сформулированные предложения по корректировке законодательства подтверждают, что в целом Российская Федерация имеет все шансы создать законодательные механизмы и гарантии для обеспечения дальнейшего устойчивого развития всех аспектов цифровой трансформации хозяйственной и общественной жизни, сохранив лидирующие позиции в глобальной цифровой экономике в силу накопленного технологического потенциала.

ЛИТЕРАТУРА

Федеральный закон «О связи» от 07.07.2003 № 126-ФЗ.

Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных».

Федеральный закон от 22.12.2008 № 262-ФЗ «Об обеспечении доступа к информации о деятельности судов в Российской Федерации».

Федеральный закон от 09.02.2009 № 8-ФЗ «Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления».

Кодекс этики в сфере искусственного интеллекта.

Абышко А.О., Сабиров Г.С. Искусственный интеллект и произведения машинного творчества: применимость опыта стран общего права к российскому регулированию // Патенты и лицензии. Интеллектуальные права. 2021. № 12. С. 60–71.

Апанасенко С.С., Гладких Е.Л. Тайна телефонных переговоров в уголовном праве России // Ростовский научный журнал. 2019. Вып. 1. Январь. С. 278–293.

Богдановский А. Может ли ошибаться Конституционный суд? // Законность. 2006. № 8.

Волож З.Л. Право на кровь // Вестник советской юстиции. 1928. № 7.

Ибрагимов Р.С., Кислый В.А. Развитие государственных ИТ-сервисов. Как это влияет на конкуренцию на цифровых рынках // Конкуренция и право. 2021. № 5. С. 45–54.

Ибрагимов Р.С., Сурагина Е.Д., Чурилова Д.Ю. Этика и регулирование искусственного интеллекта // Закон. 2021. № 8. С. 85–95.

Изотова А.Н. Правовое регулирование тайны связи в информационном обществе // Вестник РУДН. (Юридические науки). 2020. Т. 4. № 4. С. 985–1004.

Калятин В.О. Определение условий принудительных лицензий в отношении зависимых изобретений // Патенты и лицензии. Интеллектуальные права. 2021. № 6. С. 33–39.

Красавчикова Л.О. Понятие и система личных неимущественных прав граждан (физических лиц) в гражданском праве Российской Федерации : автореф. дис. ... докт. юрид. наук. Саратов, 1997.

Майоров А.В., Тягай Е.Д. Имплантируемые киберфизические системы: социально гуманитарные проблемы внедрения // Вестник ЛГУ им. А.С. Пушкина. 2021. № 1. С. 194–204.

Малеина М.Н. Статус органов, тканей, тела человека как объект права собственности и права на физическую неприкосновенность // Законодательство. 2003. № 11.

Назаров Н.А. Закрепление прав на результаты интеллектуальной деятельности, созданные с использованием искусственного интеллекта // Патенты и лицензии. 2021. № 7. С. 59–65; № 8. С. 50–57.

Нерсесянц В.С. Философия права: учебник для вузов. М.: Норма, 2004. С. 77.

Рего А.В., Мацкевич А.Ю. Проблема доступа антимонопольных органов к тайне связи // Российское конкурентное право и экономика. 2019. № 3. С. 18.

Рудяков А.Н., Майоров А.В., Минченков Е.Н. Права на интеллектуальную собственность как основной объект инвестиционной деятельности в сфере искусственного интеллекта и робототехники // Ленинградский юридический журнал. 2020. № 3 (61). С. 80–95.

Рязанов Н.Ю. Эволюция права на тайну связи // Право и государство: теория и практика. 2015. № 8 (128). С. 111–115.

Савельев А.И. Гражданско-правовые аспекты регулирования оборота данных в условиях попыток формирования цифровой экономики // Вестник гражданского права. 2020. № 1. С. 60–92.

Скловский К.И. Сделка и ее действие. Комментарий главы 9 ГК РФ. Принцип добросовестности. 4-е изд., доп. М.: Статут, 2019.

Суслопаров А.В. Соответствие норм Уголовного кодекса России принципу единства и определенности терминологии на примере терминов «информация», «сведения», «данные» // Законы России: опыт, анализ, практика. 2017. № 11. С. 94–98.

Талапина Э.В., Южаков В.Н., Двинских Д.Ю., Ефремов А.А., Черешнева И.А. Оборот данных в государственном управлении: перспективы правового регулирования. М.: РАНХиГС, 2020. С. 13.

Терещенко Л.К. Отдельные вопросы, возникающие в судебной практике при применении норм о тайне связи // Комментарий судебной

практики / отв. ред. К.Б. Ярошенко. Вып. 21. М.: Институт законодательства и сравнительного правоведения при Правительстве РФ, ИНФРА-М, 2016. С. 145–153.

Терещенко Л.К., Якушев М.В. Влияние цифровой экономики на правовые режимы информации // Информационное право. 2021. № 2. С. 4–10.

Тихомиров Ю.А, Крысенкова Н.Б., Нанба С.Б., Маргушева Ж.А. Робот и человек: новое партнерство? // Журнал зарубежного законодательства и сравнительного правоведения. 2018. № 5. С. 5–10.

Трубина В.А. Ткани и органы человека как объекты гражданских прав: дис. ... канд. юрид. наук. М., 2020.

Чечетин А. Ограничение тайны связи // Законность. 2005. № 7.

Boerding A., Culik N., Doepke Ch., Hoeren Th., Juelicher T., Roettgen Ch., Schoenfeld M. Data Ownership — A Property Rights Approach from a European Perspective // Journal of Civil Law Studies. 2018. Vol. 11.

Contreras J.L. The False Promise of Health Data Ownership. NYU Conference — Data Law in a Global Economy // University of Utah College of Law Research Paper No. 304. 2018.

Eley C.L. Dr. A.I.: The Evolution of the Use and Regulation of Artificial Intelligence in Medical Practice and Drug Development. 2017. P. 4.

Elvy S.A. Paying for privacy and the personal data economy // Columbia Law Review. 2017. No. 117 (6). P. 1369–1460.

Etzioni O. No, the Experts Don't Think Superintelligent AI is a Threat to Humanity // MIT Technology Review. September 20, 2016 [Электронный ресурс]. URL: https://www.technologyreview.com/2016/09/20/70131/no-the-experts-dont-think-superintelligent-ai-is-a-threat-to-humanity/.

Hummel P., Braun M., Dabrock P. Own Data? Ethical Reflections on Data Ownership // Philosophy & Technology. 2021. No. 34. P. 545–572.

Regulating Artificial Intelligence / T. Wischmeyer, T. Rademacher (eds). 2020.

Rosenfeld A., Kraus S. Predicting Human Decision-Making: From Prediction to Action. Morgan & Claypool, 2018. P. 7.

Scassa T. Data Ownership // CIGI Papers No. 187. Ottawa Faculty of Law Working Paper No. 2018-26. 2018.

Singh P.J., Vipra J. Economic Rights Over Data: A Framework for Community Data Ownership // Development. 2019. No. 62. P. 53–57.

Zhuravlev M., Blagoveshchenskaya O. Telemedicine: Current State and COVID-19 Lessons // Legal Issues in the Digital Age. 2020. No. 2. P. 92–143.

АВТОРЫ ДОКЛАДА

Якушев Михаил Владимирович
Заместитель директора Института права цифровой среды НИУ ВШЭ

Журавлёв Михаил Сергеевич
Старший научный сотрудник Института права цифровой среды НИУ ВШЭ

Ибрагимов Руслан Султанович
Директор по правовым исследованиям НИУ ВШЭ

Майоров Арсений Валерьевич
Руководитель Лаборатории права и этики цифровой среды Института права цифровой среды НИУ ВШЭ

Научное издание

Приоритетные направления правового регулирования цифровой трансформации в Российской Федерации. Внедрение в нормотворчество системы оценки гуманитарного воздействия (2022–2025 годы)

Доклад НИУ ВШЭ

Формат 60×88 1/16
Гарнитура Newton. Усл. печ. л. 4,1. Уч.-изд. л. 3,2
Изд. № 2633

Национальный исследовательский университет
«Высшая школа экономики»
101000, Москва, ул. Мясницкая, 20,
Тел.: +7 495 772-95-90 доб. 15285

ЯМНК XXIII 2022

ВЫСШАЯ • ШКОЛА • ЭКОНОМИКИ

При поддержке Фонда целевого капитала НИУ ВШЭ

ГЕНЕРАЛЬНЫЙ ИНФОРМАЦИОННЫЙ ПАРТНЕР

РОССИЯ 24

ГЕНЕРАЛЬНЫЙ РАДИОПАРТНЕР

87,5 BUSINESS FM
первое деловое радио

ГЛАВНЫЙ ИНФОРМАЦИОННЫЙ ПАРТНЕР

interfax

ИНФОРМАЦИОННЫЕ ПАРТНЕРЫ

ЭКСПЕРТ
Российская Газета
ОТР
ОБЩЕСТВЕННОЕ ТЕЛЕВИДЕНИЕ РОССИИ
Финам
ПОЛИТ.РУ
Агентство Социальной Информации
Индикатор
HON
журнал стратегия
ЭКОНОМИКА и ЖИЗНЬ
КАНАЛ НАУКА
ImScience.News
ECONS
Инвест-Форсайт
ДЕЛОВОЙ ЖУРНАЛ