РОССИЙСКАЯ АКАДЕМИЯ НАУК

**ИНСТИТУТ НАУЧНОЙ ИНФОРМАЦИИ
ПО ОБЩЕСТВЕННЫМ НАУКАМ**

ГОСУДАРСТВО И ПРАВО В НОВОЙ ЦИФРОВОЙ РЕАЛЬНОСТИ

Монография

Под общей редакцией
доктора юридических наук, профессора И.А. Умновой-Конюховой
и доктора технических наук, профессора Д.А. Ловцова

**МОСКВА
2020**

УДК 340
ББК 67.4
Г 72

Серия
«Правоведение»

Центр социальных научно-информационных исследований

ИНИОН РАН

Рецензенты:
Гребенщикова Е.Г., руководитель Центра научно-информационных исследований по науке, образованию и технологиям ИНИОН РАН, доктор философских наук;
Лапаева В.В., главный научный сотрудник Института государства и права РАН, доктор юридических наук;
Фролова Н.А., профессор кафедры теории государства и права имени Г.В. Мальцева РАНХиГС, доктор юридических наук, профессор

Г 72

Государство и право в новой цифровой реальности : монография / под общ. ред. д-ра юрид. наук, проф. И.А. Умновой-Конюховой и д-ра техн. наук, проф. Д.А. Ловцова. – М.: РАН. ИНИОН, 2020. – 259 с.
ISBN 978-5-248-00959-6

Исследуются теоретико-методологические и философские основы влияния техники и технологий на цифровое развитие государства и права, воздействие инновационных технологий на формирование новых отраслей права – информационного права, цифрового права, права информационной безопасности. Рассматриваются проблемы цифровой трансформации права, правотворчества, правоохранительной системы и судебной деятельности. Анализируются современные взгляды на роль права в регулировании Интернета, сетевого общения и выражения мнения онлайн.

Адресуется научным работникам, преподавателям, аспирантам и студентам юридических вузов и факультетов, сотрудникам органов государственной власти и управления, законодателям.

УДК 340
ББК 67.4

ISBN 978-5-248-00959-6

УДК 340
ББК 67.4
Г 72

Series
«Jurisprudence»

Center for social scientific and information research

INION RAS

Reviewers:
Grebenshchikova E.G., Head of the Center of Scientific Information Studies in Science, Education and Technologies of the Institute of Scientific Information for Social Sciences of the Russian Academy of Sciences (INION RAN), Doctor of Science in Philosophy.
Lapaeva V.V., Principal Research Fellow at the Institute of State and Law of the Russian Academy of Sciences, Doctor of Science in Law.
Frolova N.A., Professor of the Department of theory of state and law named after G.V. Maltsev, Russian Academy of National Economy and Public Administration, doctor of law, Professor

Г 72 **State and law in the new digital reality : a monograph** / ed. by Doctor of Science in Technology, Professor D.A. Lovtsov, Doctor of Science in Law, Professor I.A. Umnova-Konyukhova. – Moscow: RAN. INION, 2020. – 259 p.
ISBN 978-5-248-00959-6

The book seeks to cover the theoretical, methodological and philosophical foundations of technology's influence on the digital development of State and law, the impact of innovative technologies on formation of new branches of law – information law, digital law, information security law. It provides discussion of the problems of digital transformation of law, law-making, law enforcement and judicial activity. The book also reviews the modern perspectives on the role of law in regulation of the Internet, network communication and online expression.

The volume is aimed at researchers, lecturers, postgraduate and undergraduate law students, employees of public authorities, legislators.

УДК 340
ББК 67.4

ISBN 978-5-248-00959-6

Коллектив авторов

Алешкова Ирина Александровна – старший научный сотрудник ИНИОН РАН, кандидат юридических наук, доцент (Irina Aleshkova – senior research fellow at the Institute of Scientific Information for Social Sciences of the Russian Academy of Sciences (INION RAN), candidate of sciences in law, associate professor) – (2.3 – в соавт. с О.Х. Молокаевой).

Алферова Елена Васильевна – ведущий научный сотрудник ИНИОН РАН, заведующая отделом правоведения ИНИОН РАН, кандидат юридических наук (Elena Alferova – leading research fellow at the INION RAN, Head of the Law Department of the INION RAN, candidate of sciences in law) – (Введение; 1.1: Магия техники и горизонты цифрового будущего; 1.2; 1.3).

Захаров Тимофей Владимирович – научный сотрудник ИНИОН РАН (Timofey Zakharov – research fellow at the INION RAN) – (3.1).

Иванова Ангелина Петровна – младший научный сотрудник ИНИОН РАН (Angelina Ivanova – junior research assistant at the INION RAN) – (2.5).

Коданева Светлана Игоревна – старший научный сотрудник ИНИОН РАН, кандидат юридических наук (Svetlana Kodaneva – senior research fellow at the INION RAN, candidate of sciences in law) – (1.1: Технологии, право и государство в эпоху блокчейн; 3.2).

Кравчук Наталья Вячеславовна – старший научный сотрудник ИНИОН РАН, кандидат юридических наук, доцент (Natalia Kravchuk – senior research fellow at the INION RAN, candidate of sciences in law, associate professor) – (3.3; 4.3).

Красиков Дмитрий Владимирович – старший научный сотрудник ИНИОН РАН, заведующий кафедрой международного права ФГБОУ ВО «Саратовская государственная юридическая академия», кандидат юридических наук, доцент (Dmitry Krasikov – senior research fellow at the INION RAN, Chair of international law department at the Saratov State Law Academy, candidate of sciences in law, associate professor) – (4.1).

Ловцов Дмитрий Анатольевич – заместитель по научной работе директора Института точной механики и вычислительной техники им. С.А. Лебедева РАН, заведующий кафедрой информационного права, информатики и математики Российского государственного университета правосудия, доктор технических наук, профессор, заслуженный деятель науки РФ (Dmitry Lovtsov – Deputy Director of the Lebedev Institute of precision mechanics and computer engineering of the Russian Academy of Sciences, Chair of the information law, informatics and mathematics department of the Russian State University of Justice, doctor of sciences in technology, professor Honored scientist of the Russian Federation) – (2.2).

Молокаева Оксана Хараевна – научный сотрудник ИНИОН РАН, доцент кафедры конституционного права им. Н.В. Витрука Рос-сийского государственного университета правосудия, кандидат юридических наук – (Oksana Molokaeva – research fellow at the IN-ION RAN, associate professor at the N.V. Vitruk Constitutional law Department of the Russian State University of justice, candidate of sciences in law) – (2.3 – в соавт. с И.А. Алешковой).

Скурко Елена Вячеславовна – старший научный сотрудник ИНИОН РАН, кандидат юридических наук (Elena Skurko – senior research fellow at the INION RAN, candidate of sciences in law) – (4.2).

Умнова-Конюхова Ирина Анатольевна – старший научный сотрудник ИНИОН РАН, руководитель конституционно-правовых исследований Российского государственного университета правосудия, доктор юридических наук, профессор (Irina Umnova-Konyukhova – senior research fellow at the INION RAN, Head of constitutional and legal research at the Russian State University of Justice, doctor of sciences in law, professor) – (2.1, заключение).

Черных Андрей Михайлович – доцент кафедры информационного права, информатики и математики Российского государственного университета правосудия, кандидат технических наук

(Andrew Chernykh – associate professor at the Information law, computer science and mathematics Department of the Russian State University of Justice, candidate of science in technology) – (3.4).

Четвернина Александра Владимировна – научный сотрудник ИНИОН РАН (Alexander Chetvernina – research fellow at the INION RAN) – (2.4).

СОДЕРЖАНИЕ

Глава 3.
ЦИФРОВЫЕ АЛГОРИТМЫ И ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ В ГОСУДАРСТВЕННОМ УПРАВЛЕНИИ, СУДЕБНОЙ И ИНОЙ ЮРИДИЧЕСКОЙ ДЕЯТЕЛЬНОСТИ

Глава 4.
ИНТЕРНЕТ-ПРАВО И ИНТЕРНЕТ-ТЕХНОЛОГИИ: ПРАВОВЫЕ ВОЗМОЖНОСТИ И РИСКИ

CONTENTS

Chapter 3.
DIGITAL ALGORITHMS AND ARTIFICIAL INTELLIGENCE IN PUBLIC ADMINISTRATION, JUDICIAL AND OTHER LEGAL ACTIVITIES

Chapter 4.
INTERNET LAW AND INTERNET TECHNOLOGIES: LEGAL OPPORTUNITIES AND RISKS

Введение

Цифровые технологии стали важным фактором нашей жизни, они стремительно изменяют мир, политические и культурные традиции, производственные и социальные процессы. Формируется новая цифровая реальность в виде «больших данных» («Big data»), искусственного интеллекта (ИИ), блокчейн, умных городов (smart city), Интернет вещей, гипертекстовых библиотек, электронных баз данных и др. Эти технологии одни называют «прорывными», другие – «подрывными». Для этой реальности характерны кардинальная трансформация экономики, прозрачность мира, индивидуализация поведения человека, социальное расслоение в обществе, исчезновение многих старых профессий и появление новых. Эти перемены затрагивают каждого, они беспрецедентны в истории человечества.

Исследователи ведут речь о Четвертой промышленной революции[1]. С одной стороны, открываются широкие возможности для развития человека, общества и государства в новой цифровой среде, позволяющие решать многие насущные проблемы. С другой стороны, появляются новые проблемы и угрозы национальной и личной безопасности. Многочисленные социальные сети и интернет-сервисы делают человека открытым, не защищенным, несмотря на все рассуждения о праве на конфиденциальность, тайну личной и семейной жизни, коммерческую тайну и пр. С каждым днем деятельность человека всё больше зависит от его умения работать и жить в условиях, которые диктует эта новая действительность:

[1] Четвертая промышленная революция: Интернет вещей, циркулярная экономика и блокчейн. – URL: http://www.furfur.me/furfur/changes/changes/216447-4-aya-promyshlennaya-revolyutsiya; Четвертая промышленная революция https://ru.wikipedia.org/wiki/Четвёртая_промышленная_революция

даже такая простая, казалось бы, операция, как оплата услуг ЖКХ онлайн или получение пенсии и зарплаты с банковской карточки и др., требует определенных знаний, навыков и умений. Не случайно философы, юристы, социологи и представители других социальных и гуманитарных наук, а также специалисты в области информационных, в том числе цифровых, технологий предлагают вести открытые междисциплинарные дискуссии и «всеобуч» по внедрению их в экономику, управление, правотворчество и правоприменение, в повседневную жизнь каждого. Положительные и отрицательные стороны цифровизации предстоит еще выяснить науке в ближайшем будущем.

Как показывает исследование, внедрение новых информационных технологий невозможно без четкой стратегии научно-технологического развития страны, ее информационной безопасности, изменения правового регулирования общественных отношений, складывающихся в цифровой среде. Соответственно, проблемы трансформации государства и права в условиях тотальной цифровизации представляют значительный интерес как для российских, так и зарубежных ученых.

В данной монографии коллектива ученых и научных сотрудников ИНИОН РАН и Российского государственного университета правосудия отражены точки зрения многих ведущих исследователей на актуальные проблемы, как то: теоретико-методологические и философские основы влияния техники и технологий на цифровое развитие государства и права; формирование информационного права как новой отрасли права и его подотраслей (кибернетическое право, сетевое право, цифровое право, право информационной безопасности, право киберпреступности и др.); кодификация информационного права и регулирование интернет-пространства и интернет-общения. Особое внимание уделяется проблемам функционирования цифровых социальных сетей, в том числе морально-этического поведения в Интернете, и юридической ответственности провайдеров социальных сетей за запрещенные выражения и выражения ненависти онлайн, а также различным моделям правового регулирования информационных отношений, развиваемых, например, в США, ЕС, а также в правовых системах незападной традиции.

Перемещение в цифровую среду подвергает права человека беспрецедентным рискам. Основными из них являются личная конфиденциальность, автономия и демократия. Как следует из

анализа работ многих юристов, цифровой век перевернул многие социальные и правовые нормы и ценности, которые существовали и развивались на протяжении столетий. То же право на свободу выражения мнения в наши дни ограничивается фильтрацией контента или блокированием доступа к нему. В монографии отмечается, что адаптация как национальных, так и международных правил, применимых к новым технологиям, происходит медленно, а действующее право не способно адекватно регулировать ситуации, порожденные технологическими инновациями. Нарушаются границы конфиденциальности и информационной безопасности. Эпоха «больших данных» создает угрозы, связанные с сохранением личной информации и защитой персональных данных. Прослеживается утопизм в оценке взаимосвязи между свободой человека и информационно-коммуникационными технологиями, нарастание разрыва между институтами защиты прав человека и самим человеком в эпоху информационного капитализма.

На международном уровне эта проблема была зафиксирована в Резолюции Генеральной Ассамблеи ООН 2450 (XXIII) «Права человека и технический прогресс» (1968), в которой было предложено начать процесс междисциплинарных исследований на национальном и международном уровнях, нацеленных на определение стандартов защиты прав человека и фундаментальных свобод от потенциального воздействия новых технологий. Резолюция призывала сконцентрировать усилия на установлении баланса между научным и техническим прогрессом и интеллектуальным, духовным, культурным и моральным продвижением гуманности.

Прошло много лет с момента принятия этой Резолюции, сегодня действуют новые документы, отражающие современные тенденции и проблемы. С учетом современных стратегических доктринальных актов и национального законодательства, принятого в последние годы во многих странах мира, в данной работе рассмотрены концептуальные и правовые аспекты формирования цифрового пространства, электронной алгоритмизации экономики, политики, государственного управления и правосудия, в том числе обеспечения информационной безопасности личности, общества и государства. Дана общая оценка состояния информационной безопасности, обусловленного применением перспективных средств и технологий. Обоснована парадигма и определены условия обеспечения информационной безопасности функционирования эргатических систем. Показано, как прорывные технологии влияют на

существующие институты государства и права, как они перестраиваются и адаптируются к новым условиям, какое будущее ждет человечество в эпоху блокчейн и искусственного интеллекта (ИИ).

В монографии отмечено, что «подрывные» инновации не вписываются в существующие правовые парадигмы. В действующих актах существуют пробелы или противоречивые положения, так как в момент принятия данных актов «деструктивные» технологии просто еще не появились. Так, экономика свободного заработка в своих сущностных характеристиках не вписывается в концепцию дихотомии наемных работников и независимых подрядчиков.

Искусственный интеллект всё активнее используется практически во всех сферах жизни общества, не стало исключением и государственное управление. Наибольшее число дискуссий возникает относительно перспектив его использования в правотворческой, правоохранительной, правоприменительной, в том числе судебной деятельности. В связи с этим исследуются проблемы реализации своевременных подходов сбора и качественного анализа больших массивов многоаспектной динамической статистической судебной информации (многомерных данных) в целях выявления устойчивых социально-правовых закономерностей и повышения эффективности информационного обеспечения судебной системы; предложен путь и рассмотрены концептуально-логические и организационно-технические аспекты реформирования современной судебной статистики на основе внедрения новой геоинформационной технологии, базирующейся на знаниях о технологии ведения баз данных и моделях пространственных данных.

Отдельный вопрос, рассматриваемый в монографии, посвящен влиянию цифровых технологий на юридические профессии. Обращается внимание на контролируемое использование технологий в целях повышения эффективности работы судей, прокуроров, следователей, адвокатов и др., ибо программы с элементами искусственного интеллекта, призванные заменить собой юриста, могут привести к ущербу для пользователя. Однако это не означает, что следует отказаться от использования программ в этой сфере. Исследование показывает, что будущее юридической профессии лежит между двумя точками зрения – утопической фантазии о том, как искусственный интеллект облегчит работу всем юристам, и алармистским утверждением, что он полностью заменит людей.

Научный интерес у ученых-юристов вызывают также такие актуальные вопросы, как трансформация права в условиях цифро-

визации, формирование цифрового права и др. Право в условиях новой реальности рассматривается не только как средство, инструмент, обеспечивающий цифровизацию экономики, управления и других сегментов социального бытия, но и как объект воздействия «цифровизации», в результате которого оно претерпевает изменения своей формы, содержания, системы, структуры, механизма действия и демонстрирует тенденцию к усилению наметившихся трансформаций. В связи с этим возникает ряд фундаментальных задач, связанных с регулированием общественных отношений в условиях цифровой реальности, которые правовой науке необходимо решать. Среди них: выявление закономерностей и механизмов воздействия цифровизации на право; развитие методологии юридической науки, позволяющей изучать право с позиции соотношения реального и виртуального; «оцифровка» юридических технологий, применяемых в правотворчестве, правовом мониторинге, юридическом прогнозировании, юридическом моделировании, экспертизе проектов нормативных правовых актов и др.[1]

Данное исследование продолжает темы: «Государство и право в новой информационной реальности»[2], «Право будущего: Интеллектуальная собственность, инновации, Интернет», «Большие данные в социальных и гуманитарных науках», над которыми более четырех лет работает отдел правоведения ИНИОН РАН в сотрудни-

---

[1] См.: Хабриева Т.Я., Черногор Н.Н. Право в условиях цифровой реальности // Журнал российского права. – М., 2018. – № 1. – С. 85, 101.

[2] См.: Государство и право в новой информационной реальности: сб. науч. тр. / РАН. ИНИОН. Центр социал. науч.-информ. исслед. Отдел правоведения; Рос. гос. ун-т правосудия. Каф. информационного права, информатики и математики; отв. ред. Е.В. Алферова, Д.А. Ловцов. – М., 2018. – 268 с. – (Сер.: Правоведение). – URL: https://www.elibrary.ru/item.asp?id=41318623; Право будущего: Интеллектуальная собственность, инновации, Интернет: Ежегодник. – М., 2011. – Вып. 1 / РАН. ИНИОН. Центр социал. науч.-информ. исслед. Отдел правоведения; каф. предпринимательского права МГУ им. М.В. Ломоносова; отв. ред. Е.Г. Афанасьева. – 207 с. – (Сер.: Правоведение); Указ. соч. Вып. 2. – М., 2019. – 192 с.; Большие данные в социальных и гуманитарных науках: сб. обзоров и рефератов / РАН. ИНИОН. Центр науч.-информ. исслед. по науке, образованию и технологиям; отв. ред. Е.Г. Гребенщикова. – М., 2019. – 193 с. – (Сер.: Наука, образование и технологии); Социальные и гуманитарные науки: Отечественная и зарубежная литература. Сер. 4: «Государство и право»: РЖ. – URL: http://elibrary.ru/defaultx.asp; http://inion.ru/ (официальный сайт ИНИОН РАН: см. рубрики: «Новые издания ИНИОН РАН»; «Ресурсы»).

честве с коллегами из Центра научно-информационных исследований по науке, образованию и технологиям ИНИОН РАН и учеными-преподавателями кафедры информационного права, информатики и математики и отдела конституционно-правовых исследований (ныне – направления конституционно-правовых исследований) Российского государственного университета правосудия, а также с кафедры предпринимательского права МГУ им. М.В. Ломоносова.

Глава 1.
ТЕОРЕТИКО-МЕТОДОЛОГИЧЕСКИЕ ОСНОВЫ ИССЛЕДОВАНИЯ ВЛИЯНИЯ ТЕХНИКИ И ТЕХНОЛОГИЙ НА ЦИФРОВОЕ РАЗВИТИЕ ГОСУДАРСТВА И ПРАВА

1.1. Философские концепции цифрового общества и государства: Культ техники и технологий

Магия техники и горизонты цифрового будущего. В цифровой технике и технологиях современного типа заключена идея совершенно новой человеческой среды, которая неоднозначно воспринимается исследователями и ее критиками. Однако критика техники оказывается столь же древней, как и сама техника. «Из истории почти всех высоких культур, – признает доктор философии, немецкий историк Р.П. Зиферле, – до нас дошли голоса, в которых можно уловить скептическую настроенность по отношению к технике и пользе изобретений, или по крайней мере техника рассматривается в демонически-зловещем свете»[1]. Ученый выделяет несколько моделей критики техники, культуры, цивилизаций. Первоначальные движения «разрушителей машин» как форма протеста были весьма популярным феноменом начала XIX в. Ремесленники и квалифицированные рабочие видели в машине конкурента, угрожавшего их рабочему месту и социальному статусу. В последнее десятилетие XIX в. сформировалось движение интеллектуального «антимодернизма», видевшего в технике и экономике важнейший предмет своей критики. Р.П. Зиферле называет ее консервативной. «Консервативная критика цивилизации нападала почти на все аспекты современного индустриального общества, которое тогда уже обретало свои основные признаки и строила свою аргументацию исходя из перспективы упразднения существующего положения вещей. Оно смотрело назад, на лучшее

[1] Зиферле Р.П. Исторические этапы критики техники // Философия техники в ФРГ. – М., 1989. – С. 257.

прошлое, которому грозила гибель… Обычно использовалась излюбленная метафора о “господине и рабе”, с помощью которой пытались понять технику»[1].

Господство техники проявилось в том, что человек сам приобрел черты машины: он стал автоматом, безвольно оказавшимся во власти самодвижущихся технических систем, которые уже не являются средствами для достижения цели, а стали самоцелью. Возникла мысль об автономии техники, которая связывалась со способом аргументации, исходящей из понятия «отчуждение».

Этот мотив автономии техники сделал в XX в. примечательную «карьеру». Сложилось три типа аргументации:

1) модель критики техники, согласно которой техника спонтанно несется к автоматическому «совершенству» (Ф.Г. Юнгер), подминающему под себя подлинно человеческое;

2) технократическая модель (О. Шпенглер, Э. Юнгер). В 20-е годы XX в. технический мир рассматривался уже «как судьба», которую следует осилить. Она внесет структурный порядок в мир, который иначе может стать нестабильным и духовно опустошенным. Поэтому «технократия» – точное отражение отчужденной техники, с той лишь разницей, что теперь уже не ждут, будто техника может быть подчинена «человеческим целям». И именно в этом – ее структурирующая функция;

3) неомарксистская модель (Г. Маркузе, Ю. Хабермас). В XX в. экономика и техника рассматриваются как «опредмеченности», ставшие чуждыми человеку, которые, однако, деятельностью «разума» должны быть вновь приведены в подчинение человеку. Этот мотив обнаруживается и у представителей Франкфуртской школы от Г. Маркузе до Ю. Хабермаса. Здесь много точек соприкосновения с консервативной критикой техники, однако перспектива иная: если культурологическая критика направлена против процесса модернизации в целом, то неомарксистская модель ориентирует на прогрессивное завершение «проекта модернистов» (следовательно, на полное подчинение всей техники, экономики и общества «господству разума»).

В современных движениях протеста можно увидеть слияние консервативной и неомарксистской критики техники. Это проявляется в том, пишет Р.П. Зиферле, что данные движения до сих

[1] Зиферле Р.П. Исторические этапы критики техники // Философия техники в ФРГ. – М., 1989. – С. 266.

пор еще не выработали никаких, достойных внимания теоретических проектов, с помощью которых можно было бы ввести устойчивый порядок в этот каталог восприятий и требований. Многие проекты исключают друг друга, иные же, если бы они были осуществлены, привели бы к катастрофическим последствиям. Они едины лишь в том, что индустриально-технический мир грозит нам бесчисленными опасностями, так что каждое нововведение вызывает прежде всего мысль о дальнейшем ухудшении[1].

Напротив, сторонники идеи прогресса отдают предпочтение культу техники и технологий, машины. В машине человек видит собственное продолжение. Миф машины настойчиво предлагает человечеству более совершенную альтернативу развития. Однако, по Э. Дэвису, «миф машины – утопическая вера в то, что машина может открыть человеку в другие миры»[2]. Миф машины создавался для расширения власти над природой и людьми. По мнению И.А. Исаева, идея власти была заложена как в основу мифа машины, так и в основу самой ее деятельности. «Технологический миф, – пишет он, – теперь обретает новые черты. Становящаяся суверенной техника оказывается на стороне политического глобализма. Тотальный характер технизации, когда все связано со всем, уже очевиден. Множественность властных центров, которая свойственна техническим системам, разрушает представления о государственном суверенитете. Техника космополитична, но не нейтральна. Политика государств и их законодательство приспосабливаются к ее настойчивым требованиям. Целые отрасли – промышленное право, экологическое право, аграрное право и др. – уже включены в сферу ее императивного воздействия, Экономика уже давно находится под контролем технологий: джинн вырвался наружу – и все переменилось…»[3].

Технологии могут принести пользу всем, однако наибольшие преимущества имеют те, кто обладает необходимыми средствами и знаниями и желанием учиться использовать новые инструменты[4]. Ник Бостром (N. Bostrom), профессор Оксфордского

---

[1] См.: Зиферле Р.П. Указ. соч. С. 267–269.

[2] Дэвис Э. Техногнозис: миф, магия и мистицизм в информационную эпоху. – Екатеринбург, 2017. – С. 158–159 (цит. по: Исаев И.А. Технология власти. Власть технологии. – М.: Проспект, 2019. – С. 41–42).

[3] Исаев И.А. Технология власти. Власть технологии. – С. 42–43.

[4] См.: Бостром Н. FAQ по трансгуманизму. – URL: https://www.libfox.ru/567046-nik-bostrom-faq-po-transgumanizmu.html (дата обращения: 24.02.2020).

университета, директор Института «Будущее человечества», пытается доказать, что будущее влияние искусственного интеллекта (ИИ) является самой важной проблемой, с которой когда-либо сталкивалась человеческая раса. По Бострому, существует множество вариантов экспертных оценок относительно будущего, уготованного искусственному интеллекту. Разногласия касаются и времени его появления, и того вида, в каком он когда-нибудь предстанет перед миром. Прогнозы перспектив развития ИИ, по мнению Бострома, – различны и не в состоянии дать полную картину всех современных положений по этой теме. Однако проведенные автором опросы специалистов и высказанные ими частные мнения по вопросу: что они ожидают от появления искусственного интеллекта человеческого уровня (ИИЧУ) (причем *уровень,* замечает автор, определялся как «способность освоить большинство профессий, по крайней мере тех, которыми мог бы владеть среднестатистический человек»), строились на предположении, что «научная деятельность в этом направлении будет продолжаться без серьезных сбоев». По данным выборки получились следующие средние оценки:

- 2022 г. – средний прогноз с 10%-ной вероятностью;
- 2040 г. – средний прогноз с 50%-ной вероятностью;
- 2075 г. – средний прогноз с 90%-ной вероятностью.

Результаты этого исследования Н. Бостром рассматривает с некоторой долей скептицизма. «На сегодняшний день, если брать уровень общего интеллектуального развития, машины абсолютно уступают людям, – пишет он… – Но однажды – разум машины превзойдет разум человека... Это ознаменует собой начало новой эры»[1].

Какой будет эта эра? Одни исследователи смотрят в будущее с надеждой, другие – с тревогой. Так, Н. Бостром, рассуждая о генной модификации клеток живого организма, создании новой генерации людей путем биологического улучшения интеллектуальных способностей, особенно основанного на генетической селекции, выделяет три важных момента: «1) при помощи биотехнологических методов мы способны прийти к существованию сверхразума, по крайней мере к его начальной стадии; 2) появле-

[1] Бостром Н. Искусственный интеллект: Этапы. Угрозы. Стратегии / пер. с англ. С. Филина. – М., 2016. – URL: https://royallib.com/read/bostrom_nik/iskusstvenniy_intellekt_etapi_ugrozi_strategii.html#0 (дата обращения: 04.03.2020).

ние интеллектуально усовершенствованных людей увеличивает возможность осуществить когда-нибудь развитие искусственного интеллекта до высокоразвитых форм, поскольку сама задача создания ИИ будет абсолютно доступна и проста для усовершенствованных людей нового поколения…; 3) … вполне допустимо появление поколения генетически усовершенствованных групп людей: избирателей, изобретателей, ученых, причем показатели улучшения их когнитивных функций будут увеличиваться от десятилетия к десятилетию»[1]. Что это звучит провокационно, соглашается сам исследователь, но прогресс на пути биологического развития, полагает он, вполне реален.

Современные футурологи пытаются предсказать развитие технологий и будущее человеческой цивилизации. Р. Курцвейл в своей книге «Сингулярность уже близка» («The Singularity is Near») предвещает, что время, когда искусственный интеллект превзойдет человеческий, наступит совсем скоро, это событие произойдет в 2045 г., после чего люди «*преобразуют биологию и будут существовать во Вселенной в качестве бессмертных киборгов*»[2].

Анализируя в своей книге «Цифровой тоталитаризм» работы ведущих трангуманистов, О.Н. Четверикова, описывает тревожную картину нового мира. «Их излюбленная тема, – замечает автор, – “научный иммортализм”, т.е. достижение бессмертия путем “цифрового метемпсихоза” (переселения души), при котором происходит полное копирование человеческого мозга на компьютере для создания цифровой копии человека. Поскольку человеческая личность рассматривается как носитель генной информации, закодированной в ДНК, а мозг – как нейрокомпьютер, то бессмертия собираются достичь путем “динамического переноса” сознания с одного медианосителя в другой»[3]. О.Н. Четверикова утверждает, что трансгуманисты не только декларируют свои цели, но и открыто демонстрируют методы их достижения, абсолютно не скры-

---

[1] Бостром Н. Искусственный интеллект: Этапы. Угрозы. Стратегии / пер. с англ. С. Филина. – М., 2016. – URL: https://royallib.com/read/bostrom_nik/iskusstvenniy_intellekt_etapi_ugrozi_strategii.html#0 (дата обращения: 04.03.2020).

[2] Человек, который предсказал всё: Рэй Курцвейл о будущем технологий. – URL: https://vc.ru/future/6626-kurzweil (дата обращения: 17.02.2020).

[3] См.: Четверикова О.Н. Цифровой тоталитаризм: как это делается в России. – М., 2019. – URL: https://www.litmir.me/br/?b=668249&p=1 (дата обращения: 17.02.2020).

вая, что речь идет *о создании системы всеобъемлющего электронного контроля над человечеством*[1].

Э. Шмидт и Дж. Коэн в книге «Новый цифровой век: Преобразуя будущее народов, стран и бизнеса» также заявляют о конце частной жизни и анонимности как таковой[2]. Аналогичного мнения придерживается Ю.Н. Харари. Предстоящая технологическая революция, пишет он, может установить власть алгоритмов, и тогда об индивидуальной свободе можно забыть. По его мнению, сегодняшний человек труда с каждым годом чувствует себя все более неуместным. Робототехника способна вытеснить огромное количество людей с их рабочих мест. «Небольшая элита может править с помощью цифровой диктатуры благодаря алгоритмам больших данных. Большинство людей будет страдать не от нещадной эксплуатации, а от полной бесполезности… Технологическая революция может обернуться катастрофой, если что-то пойдет не так»[3].

Технологии, замечает Харари, способствуют глобализации, но «как знать – возможно, полезнее будет повернуть вспять, вновь вернуться к национальным государствам, к древним религиозным традициям?.. Возможно, когда искусственный интеллект еще больше усовершенствуется, в финансах вскоре не сможет разобраться никто, так что правительства будут слепо полагаться на алгоритмы... Люди не должны полагаться на алгоритмы, вместо этого они могут обслуживать их и правильно использовать»[4].

К 2050 г., предполагает автор, развитие искусственного интеллекта и машинного обучения изменит все привычные формы трудовой занятости. Каким будет характер изменений? Мнения разделились: одни эксперты предполагают, что за несколько десятилетий миллиарды людей останутся без работы, другие – что рабочие места просто станут другими, и для них потребуется другая квалификация. Кто из них прав, сегодня сказать трудно.

Как видим, с одной стороны, перед читателем встает картина фантастического будущего, населенного людьми со сверхспособ-

---

[1] См.: Четверикова О.Н. Цифровой тоталитаризм: как это делается в России. – М., 2019. – URL: https://www.litmir.me/br/?b=668249&p=1 (дата обращения: 17.02.2020).

[2] Schmidt E., Cohen J. The new digital age: Transforming nations, businesses and our lives. – New York, 2013.

[3] Харари Ю.Н. 21 урок для XXI века. – М.: Синдбад, 2019. – URL: https://www.litmir.me/br/?b=649347&p=1 (дата обращения: 15.03.2020).

[4] Там же.

ностями и имплантатами в виде нейрокомпьютерных интерфейсов, позволяющими человеку использовать всю мощь электронных вычислений, и сверхразумными роботами, с другой – все выгоды и риски, которые связаны с новыми цифровыми технологиями, идеи, методы и реальность, составляющие основания техницизма, приобретают в современном мире совершенно новые значения.

Магическая вера в технику и эйфория массового сознания, обусловленная компьютеризацией, декларирование создания цифровой экономики и цифрового правительства рождают вместе с новыми идеями и новую реальность, к которой следовало бы относиться с осторожностью, как до конца не познанной тенденции. Уже сегодня в результате использования систем наблюдения, осуществляемых на добровольной или обязательной основе, накоплены огромные объемы информации о поведении человека. На сайтах социальных сетей многие люди делятся своей личной информацией. Автоматизированный анализ этих потоков информации может быть использован как во благо, так и во зло. «Что нужно сделать?» – задают вопросы исследователи. С их точки зрения, следует сосредоточить силы на проблемах, не просто важных, но неотложных в том смысле, что их нужно разрешить раньше, чем произойдет взрывное развитие интеллекта, воздерживаться от работы над задачами с отрицательной ценностью, т.е. решений, которые могут принести вред. Отрицательную ценность могут иметь некоторые технические задачи в области искусственного интеллекта, поскольку их решение может подстегнуть развитие этого направления, опережающее создание методов контроля, которые все-таки призваны помочь человечеству пережить революцию машинного интеллекта и получить выгоду от нее[1].

Современный мир мало чем отличается от того, что мы привыкли видеть в фантастических романах: внедрение тотальной автоматизации, новые виды транспорта, биотехнологии, искусственный интеллект, генная инженерия и т.п. Многие уже не мыслят себя без социальных сетей, электронных сервисов, поисковых систем и мессенджеров, электронной торговли, цифровых платформ и технологий по типу «блокчейн», удаленных сервисов, применяемых в самых разнообразных областях человеческой деятельности.

[1] См.: Бостром Н. Указ соч.

Мир усложняется с каждым днем, «ослепляя иллюзией новых знаний и технологий»[1].

Технологии, право и государство в эпоху блокчейн. Технология «блокчейн» ставит перед юристами новые вызовы, что подняло волну обсуждений и предположений о будущем государства, его суверенитета и права. Наибольшей популярностью пользуется тема криптовалют и их влияния на финансовые рынки, легализация и отмывание денег, что заставляет некоторых исследователей говорить о том, что финансовые системы становятся нерегулируемыми. Менее обсуждаемыми, но более значимыми в долгосрочной перспективе являются иные возможности данной технологии, начиная от возможностей регистрации (например, недвижимости) и заканчивая смарт-контрактами, влияние которых на правовые системы и государство еще менее очевидно.

Технология блокчейн обладает тремя ключевыми признаками: 1) это система регистрации последовательного ряда элементов; 2) она использует криптографию, что практически исключает возможность подделки реестра; 3) она основана на согласованном процессе хранения копий и добавления новых записей. Следовательно, если не сводить блокчейн исключительно к криптовалютам, то станет очевидным, что данная технология может использоваться в самых разных вариациях. Например, блокчейн может быть создан консорциумом, который установит собственные правила, по которым будет происходить обработка информации, включая персональные данные. Кроме того, вместо распределенного механизма консенсуса стороны могут согласиться использовать своего рода «консенсус по полномочиям».

Соответственно, в долгосрочной перспективе блокчейн может привести к изменениям в том, как работают государственные институты и правовые системы. Одна из многих интересных особенностей технологии blockchain заключается в том, что она не только основана на правилах (как и многие информационные технологии), но и может быть развернута таким образом, чтобы автоматизировать работу процессов, основанных на правилах, как для запуска, так и для документирования событий новыми способами и в очень больших масштабах. Два десятилетия назад Джоэл Рейденберг предположил, что пришло время для «Lex Informatica»,

[1] Харари Ю.Н. Указ. соч.

когда «политики… должны использовать нормы Lex Informatica в качестве эффективной замены закона, где желательны самоисполняющиеся, индивидуальные правила». Кристофер Миллард полагает, что этот тезис, радикальный в то время, соответствует эпохе блокчейна[1].

И действительно, лица, создающие вычислительные транзакционные системы и формирующие институты разрешения споров и правоприменения, в настоящее время являются «нормотворцами», решающими, какие формы поведения разрешены и какие формы права установлены. Во многих отношениях эти инженеры создают собственные правовые стандарты, по которым осуществляются сделки на их платформах. При этом их санкционирующей силой является доминирование на рынке.

При этом возникает разрыв между технологиями и правом, потому что юристы рассматривают стандарты функционирования блокчейн как технический вопрос, в то время как технические специалисты рассматривают стандарты как «юрисдикционный» вопрос. Однако, на наш взгляд, стандарты принимают характер и тех и других, и их следует рассматривать как гибридные технико-правовые инструменты. В любой конкретной области стандарты представляют собой мозаику правил, которые структурируют модели поведения. Несмотря на то что в целом они создаются частными лицами, рыночные и инфраструктурные властные отношения делают установление стандартов процессом нормотворческим и квазизаконодательным.

Для примера обратимся к истории Средних веков, когда только происходило формирование общего права в форме властных предписаний. Эти ранние предписания были технологическими артефактами, которые связывали человеческое поведение с исполнительными институтами судов. Причем составлялись они не судьями, а юристами, которые разрабатывали первые юридические стандарты. Эти стандарты становились основой предписаний, издаваемых Королевским судом. В XII в. тяжба между частными лицами могла дойти до Королевской канцелярии только в том случае, если стороны были вызваны самим королем. Средством вызова служили специальные юридические формулы, предписания. Как описывает Мэтью Хейл в своей истории общего права,

[1] См.: Millard C. Blockchain and law: Incompatible codes? // Computer law & Security review. – 2018. – Vol. 34. – P. 846.

после того как юристы превращают обычаи в законные предписания судебной власти, происходит формирование общего права, которое определяет, какие из существующих обычаев являются хорошими и разумными, а какие – неразумными и неприменимыми[1]. Далее, общее право придает тем обычаям, которые оно считает разумными, обязательную силу. Оно определяет, что такое продолжительность времени, достаточная для того, чтобы создать такой обычай, наконец, общее право решает вопрос о толковании, ограничениях и распространении таких обычаев.

Иными словами, средневековое общее право представляло собой формулярную систему, содержание и базовая структура которой в значительной степени определялись реестром судебных актов. Соответственно, возможность обращения в суд с иском полностью зависела от наличия подходящей формы в реестре.

Аналогичный процесс происходит и сейчас: по мере того, как формы правового поведения на блокчейн-платформах становятся все более понятными, современная практика разработки юридически приемлемых сделок создает библиотеку возможных взаимодействий с техно-правовым миром.

Однако возникает фундаментальный вопрос о том, кто будет «верховным судьей» в этой системе, а также о том, на основании каких правовых норм будут разрешать споры. Формирующийся сейчас тип права, тип сделок, которые разрешаются и запрещаются, и процедуры разрешения споров, которые задействованы, – это вопросы политические и технические. Разрешение споров может принимать различные формы: это могут быть односторонние решения руководящих органов или судебное вмешательство. Однако техническая и нормативная форма этих механизмов оспаривания еще не определена.

Ключевые проблемы связаны с тем, что судебные и исполнительные органы власти не имеют возможности технически повлиять на исполнение смарт-контрактов, а также с их географической децентрализацией. Соответственно, возникает конкуренция между наднациональными институтами арбитража и национальными правительствами. Следовательно, возникает вопрос о юрисдикции – должны ли это быть принципиально новые международ-

[1] См.: Goldenfein J., Leiter A. Legal engineering on the blockchain: ‘Smart Contracts’ as legal conduct // Law critique. – 2018. – Vol. 29. – P. 145. – URL: https://doi.org/10.1007/s10978-018-9224-0 (дата обращения: 10.01.2020).

ные нормы или, к примеру, должно применяться английское право, как в морском арбитраже. Вопрос о суде – не просто формальность; это юрисдикционный механизм, который делает закон действующим. Юрисдикция отсылает нас, прежде всего, к вопросам власти и полномочиям говорить от имени закона.

Различные методы и подходы к урегулированию деловых споров отражают постоянное напряжение между обладателями экономической власти, которые оказывают давление, чтобы контролировать то, как их конфликты решаются, и относительно небольшим числом юристов-практиков, которые стремятся получить большую долю прибыльного рынка, представленного коммерческими спорами. Разрешение споров на блокчейне теперь становится полем борьбы такого же рода, только теперь между создателями Эфириума, Меттериума и подобных платформ, с одной стороны, и национальными правительствами, стремящимися стать «Силиконовой долиной криптоэкономики», – с другой. Кроме того, есть еще и сторонники либертарианской идеологии, которые поддерживают арбитражные механизмы, основанные на индивидуальной свободе в форме согласия сторон.

Вопрос о юрисдикции в мире блокчейн – это также вопрос суверенитета. Так, Сара и Бэн Мански отмечают, что, по мнению многих исследователей широкое распространение технологии блокчейн будет означать конец современного суверенного государства. Особенно часто такие предсказания звучат в банковской сфере[1].

Быть суверенным – значит обладать «высшей, непреодолимой, абсолютной, бесконтрольной властью» и быть свободным от ответственности за свои поступки. Понятие суверенитета вошло в широкое употребление в ходе демократических и республиканских революций XVIII в., когда божественное право монарха на управление заменялось принципом народного суверенитета «Vox Populi, Vox Dei». Тогда концепция суверенитета была призвана узаконить ту или иную форму территориального господства и воспрепятствовать оспариванию этого господства. Если обобщить все последующие дискурсы, то под суверенитетом подразумевается всеобщее признание исключительного права устанавливать правила поведения в пределах определенной области действия.

[1] См.: Manski S., Manski B. No gods, no masters, no coders? The future of sovereignty in a blockchain world // Law critique. – 2018. – Vol. 29. – P. 152.

Можно выделить пять возможных сценариев влияния технологии блокчейн на суверенитет государства.

1. Формирование индивидуального суверенитета, основанного на децентрализующей функции блокчейна. Создатель этой технологии Сатоши Никамото (Satoshi Nakamoto) помимо сугубо технологических подробностей указывал и на идеологическую составляющую – на возможность создать общество, которое лучше всего способствует реализации индивидуальной воли в условиях свободной рыночной экономики, свободной от регулирования со стороны государств или крупных корпораций. Этой идеологии придерживаются либертарианцы – энтузиасты технологии блокчейн.

2. Народный суверенитет. Блокчейн дает новое дыхание идеям народной кооперации. Авторы отмечают, что на базе этой технологии уже сейчас начинается фактическое строительство «глобального технологического содружества», созданного с использованием передовых технологий обмена, связи и управления. В настоящее время существует много примеров приложений, которые делают возможным глобальное децентрализованное осуществление народного суверенитета и экономической демократии, свободной от логики капитализма.

3. Технологический суверенитет – это власть технократов (тех, кто владеет техническими знаниями). Она может быть использована для достижения различных целей – как средство сопротивления капитализму, как средство личной выгоды или как путь к консолидации власти. По мере того, как приложения блокчейн становятся более прибыльными, наблюдается рост числа миллиардеров-разработчиков. Это может привести к суверенитету не технологов, а самой технологии. Развитие технологии может позволить создавать блокчейн-компании, которые работают сами с распределенными и децентрализованными доходами, управлением и услугами. Эти независимые децентрализованные автономные организации автоматически будут использовать различные смарт-контракты, тем самым устраняя юристов, бухгалтеров и чиновников, чья работа заключается в подтверждении надежности и юридической силы контрактов между сторонами. То есть фактически они станут обладать властными полномочиями, традиционно присущими суверенному государству. Мански подчеркивают, что, по какому бы пути ни пошло дальнейшее общественное развитие,

технологический суверенитет в большем или меньшем объеме будет присутствовать непременно[1].

4. Корпоративный суверенитет. Фактически это разновидность третьего сценария, когда разработчики платформ блокчейн либо сами станут корпорациями, либо будут работать на крупные корпорации, которые завладеют всеми преимуществами данной технологии в целях их монетизации. Это приведет к укреплению иерархии, централизации власти, усилению неравенства и в целом ослаблению демократии. Корпорации фактически будут формировать государственную политику в своих интересах.

5. Тоталитарный государственный суверенитет. Авторы указывают на ошибочность безоговорочных суждений о том, что блокчейн непременно разрушит традиционный суверенитет национальных государств. Они полагают, что потенциально вполне возможно прямо противоположное: государства постараются использовать такие свойства блокчейна, как открытость и неизменность транзакций и глобальность для вмешательства в повседневную жизнь людей. Эти технологические возможности потенциально делают возможным появление новых технологических тоталитарных форм государственного суверенитета. Государства не могут легко контролировать то, что они не могут измерить, а Интернет вещей с поддержкой блокчейна, усиленный искусственным интеллектом, повышает степень, с которой государства могут контролировать материальный и социальный мир. Когда в каждый материальный объект, с которым мы взаимодействуем, встроен крошечный чип, связанный с блокчейном, государственные учреждения, несомненно, будут стремиться контролировать личную, политическую и экономическую деятельность своих граждан.

Таким образом, сегодня трудно предсказать, по какому пути пойдет общество. Очевидно, что решающее слово остается за инженерами, как непосредственными «конституционалистами» нового мира блокчейна. И наше общее будущее зависит от того, какой из перечисленных сценариев окажется наиболее приемлемым для них.

[1] См.: Manski S., Manski B. Op. cit.

1.2. Развитие современного государства: От «электронного» и «сервисного» к «государству как платформе»

Технический прогресс, порожденный фундаментальными знаниями в области физики, математики, информатики, биологии и других наук, создал новые предметные для государства и права реалии, новые объекты цифровой природы, новые вызовы и угрозы, которые нередко имеют высокотехнологическое содержание: они замешаны на применении нанотехнологий и высокого интеллекта. Поэтому одной из самых актуальных задач юридической науки в настоящее время является мобилизация теоретических и методологических исследований, направленных на осмысление новых цифровых феноменов и на разработку соответствующих им правовых инструментов.

Ф. Юнгер, немецкий философ и писатель, в своей книге «Совершенство техники. Машина и собственность» в предисловии замечает, что «все мы постепенно становимся все более зависимыми» от техники, «рабочие являются пленниками сложной технической аппаратуры и организации», «все государства находятся в одинаковом положении: они похожи на корабль, оснащенный хорошо отлаженным и превосходно функционирующим двигателем, который неуклонно движется навстречу неведомому айсбергу»[1].

Влияние техники на власть и государство попытался проанализировать доктор юридических наук, профессор И.А. Исаев в книге «Технология власти. Власть технологии». Опыт истории, пишет он, убедительно доказывает, что вслед за происходившими в мире технологическими революциями чаще всего следовали революции социальные, культурные и политические. Рационализация, без которой не обходилась ни одна техническая революция, меняла ранее когнитивные и институциональные структуры общества, внося свой вклад в революционные процессы. Вместе с тем техника предполагала отечественному и индивидуальному сознанию собственную логику и свой язык общения. Структуры властвования и права принимали их, часто оказываясь в ситуации риска,

[1] Юнгер Ф.Г. Совершенство техники. Машина и собственность. – URL: https://gtmarket.ru/laboratory/basis/3152 (дата обращения: 12.03.2020).

порождаемого иррациональным и «бездуховным» характером техники. Машина становилась богом и демоном существования[1].

Раскрыть технологию власти, действие «мегамашины властвования», в котором государство составляет центр этой машины, – цель, которую преследует в своем исследовании И.А. Исаев. Со времен камеристов и Т. Гоббса, пишет ученый, политика все больше рассматривалась как техническая задача, когда особое значение придавалось не добродетельности и справедливости, сколько целесообразному построению эффективного государственного аппарата. По Гоббсу, «искусство строительства и сохранения государства, подобно арифметике и геометрии, основано на определенных правилах, а не только практике»[2]. Ф Юнгер писал: «…государство только тогда начинает по-настоящему справляться со своими задачами, когда оно целиком технизировано, когда само понятие государства и его цели определяются централизованным функционализмом, который охватывает все сферы жизни»[3].

Л. Мамфорд, американский историк, социолог, философ XX в., подчеркивал, что существование автоматизированных фабрик и компьютерного управления помогает скрыть человеческие составляющие машины власти и религиозную идеологию, важную даже для наступившей эры автоматизации. Но на вершине иерархических организаций по-прежнему стоят «царь и жрец», обеспечивающие работу всего комплекса власти[4].

Аналогичное впечатление создается, замечает И.А. Исаев, что в цифровом обществе – царстве количества и анонимности, правит Никто, но это гипотетическое единство вполне реальных экономических общественных отношений правит не менее деспотично оттого, что не привязано ни к какому конкретному лицу[5].

Этот философский подход сущности цифрового общества и государства в аспекте властных отношений дополняется позицией современных ученых относительно развития государства и его функционала в условиях цифровизации. Именно в связи с информатизацией, а теперь цифровизацией современного социума и раз-

---

[1] См.: Исаев И.А. Технология власти. Власть технологии. – С. 2.

[2] Цит. по: там же. – С. 56.

[3] Юнгер Ф. Указ соч.

[4] Мамфорд Л. Миф машины. Техника и развитие человечества. – М., 2001. – С. 262–264.

[5] См.: Исаев И.А. Указ соч. – С. 63.

личных сегментов общественной жизни в дискурс были введены понятия «электронное государство» («электронное правительство»)[1], «сервисное государство»[2]; «государство-платформа»[3] и т.п.

Концепция электронного государства («e-government») появилась в 90-х годах XX в. Этот термин использовался наряду с дефиницией «электронное правительство», который в отличие от первого был закреплен в «Концепции формирования в Российской Федерации электронного правительства до 2010 года», утвержденной распоряжением Правительства РФ от 6 мая 2008 г. № 632-р.

Вместе с тем ученые заметили, что развитие «электронного государства» на практике ознаменовалось распространением бюрократических механизмов во все сферы общественной жизни благодаря широкому развитию информационно-телекоммуникационных технологий. В результате дискуссии утвердилась идея, что развитие электронной информационной коммуникации и интеграция компьютерных технологий в системы управления обеспечивают лишь исходные условия, но не автоматическую трансформацию данных систем в соответствии с идеалами гуманизма и свободы личности, вследствие чего необходимо социально-ценностное обоснование стратегии и практики их внедрения. Эффективное использование

---

[1] См.: Электронное государство и энтропийные процессы в управлении в условиях информационного коллапса: доклад / И.В. Башелханов, Н.А. Трусов, А.И. Иванус, Е.А. Колмыкова. – М., 2016. – URL: https://old.integras.com/seminar/conference/11p.pdf (дата обращения: 11.03.2020); Васильева Е.Г., Кононенко Д.В. Современные интерпретации концепции электронного государства (электронного правительства) // Вестн. Волгогр. гос. ун-та. Сер. 5: Юриспруденция. – Волгоград, 2016. – № 1 (30). – С. 10–16; Кузнецов П.У. Социальная миссия электронного государства: Ценности и терминологические проблемы // Информационное общество и социальное государство: сб. науч. тр. – М.: ИГП РАН, 2011. – С. 14–19, и др.

[2] См.: Бачило И.Л. Государство социальное или сервисное? (Информационно-правовой аспект) // Право. Журнал высшей школы экономики. – М., 2010. – № 1. – С. 3–11. – URL: https://socionet.ru/publication.xml?h=spz:cyberleninka:7346:16027016 (дата обращения: 11.03.2020); Васильева А.Ф. Сервисное государство: Административно-правовое исследование оказания публичных услуг в Германии и России. – М., 2012, и др.

[3] См.: Крупеня Е.М. Законотворчество: к проблеме понимания в условиях цифровизации общества и функционирования государства-платформы // Трансформация правовой реальности в цифровую эпоху: сб. науч. тр. / под общ. ред. Д.А. Пашенцева, М.В. Залоило. – М., 2019. – С. 76.

информационных технологий предполагает их оценку с двух точек зрения – социальной целевой определенности (приемлемости целей их применения) и инструментальности (управляемости), задаваемой требованиями программной разработки. Доминирование «алгоритмизированной функциональности», при которой разработчики систем оперируют элементами, часто не имеющими целевого назначения, а человек рассматривается только как система для обработки данных, приводит к конфликтам, нивелирующим значение технологии[1].

В 90-е годы XX в. социальное значение электронной коммуникации через институт электронного государства (электронного правительства) мыслилось преимущественно в контексте требований информационной свободы и открытого общества, т.е. дискуссия имела в большей мере политический контекст. Основным итогом дискуссии стала концептуализация социальных целей электронного государства через идеалы общественной демократии и свободного рынка. Развитие информационных технологий начало рассматриваться в качестве важнейшей предпосылки для формирования открытого общества, а открытое общество отождествлялось со свободой функционирования информации и обеспечением прав информационного доступа для граждан и организаций. В соответствии с этим основное предназначение электронного правительства усматривалось в возможностях максимально широкого информирования о властно-управленческих решениях в противоположность «закрытости» административно-бюрократических процессов, а само развитие различных информационных систем (в том числе негосударственных) трактовалось как фактор безусловного социального прогресса, обеспечивающего возможности общественного контроля за действиями власти и равноправной рыночной конкуренции[2].

Соответственно, электронное правительство также рассматривалось в рамках функционально-инструментального подхода: как коммуникативная технология и информационная управленческая среда, интенсифицирующая и интегрирующая управленче-

---

[1] См.: Информационная технология и проблемы информатизации современного общества: реф. сб. / В.А. Виноградов, А.М. Кулькин, В.П. Зиноченко и др. – М.: ИНИОН РАН, 1991. – С. 153.

[2] См.: Васильева Е.Г., Кононенко Д.В. Современные интерпретации концепции электронного государства (электронного правительства) // Вестник Волгогр. гос. ун-та. – Сер. 5: Юриспруденция. – Волгоград, 2016. – № 1 (30). – С. 10.

ские процессы; как целевая стратегия развития социальных электронных коммуникаций и информационных систем управления, обеспечивающая взаимодействие граждан и государства и реализацию государственных функций. Социальное значение электронного правительства определяется и сегодня его ценностно-функциональным содержанием, которое, с одной стороны, соотносится с общесистемными целями социального развития и принципом эффективного управления, а с другой – с целевыми задачами органов государственной власти и требованиями эффективной коммуникации.

Как отмечала И.Л. Бачило, стратегия развития электронного государства (правительства) определяется направленностью, во-первых, на поддержку управленческой инфраструктуры – процессов технико-технологической информатизации и развитие интегрированной информационной среды; во-вторых, на формирование коммуникационных сервисов и дифференциацию подсистем информационного обмена в соответствии с потребностями управляющего развития[1].

В целях создания «электронного государства» («электронного правительства») И.Л. Бачило предложила разработать четыре платформы в инфраструктуре современного информационного общества. Платформа № 1 должна быть ориентирована на производство коммуникационных и информационных технологий и соответствующее им правовое регулирование. Платформа № 2 – на формирование и действие рынка ИТ-продукции, услуг в информационной сфере (в данной сфере есть проблемы новой цензуры, качества телевидения, блогов в Интернете и др.). Платформа № 3 – на производство и рынок. Здесь должен осуществляться лозунг «информация для всех» при условии, что она социальна, креативна, достоверна, доступна, своевременна. В результате создается «информационный гражданин». Платформа № 4 «интегрирует полученные результаты по уже продвинутым участникам информационного пространства, которое одновременно является и образцово управляемым»[2].

[1] См.: Бачило И.Л. Электронное правительство и инновации в области государственных функций и государственных услуг // Информационные ресурсы России. – М., 2010. – № 1. – С. 13–17.

[2] Бачило И.Л. Государство и право XXI века: Реальное и виртуальное. – М.: Юркомпани, 2012. – С. 254–256.

Как видим, речь идет о сближении концептуальных составляющих электронного государства и собственно государства, а также границ гражданского общества и государства.

На следующем этапе так называемый «менеджериальный подход» трансформировался в концепцию «сервисного государства», которая конкретизирует электронное управление применительно к целевым задачам и функциям государственных институтов и связывает его с созданием интегрированных многоуровневых информационных систем, обеспечивающих межведомственное взаимодействие и информационную коммуникацию граждан (организаций) и государства[1]. Эта тема в 2006–2010 гг. стала исследовательским проектом сектора информационного права Института государства и права РАН, возглавляемого в то время И.Л. Бачило. В этот период в исследованиях ученых акцент делался на модернизации концепции электронного государства (электронного правительства), и «сервисное государство» рассматривалось как его главная составляющая[2].

Однако отдельные ученые высказывали мнение о неполном содержательном совпадении категорий «сервисное государство» и «электронное государство (правительство)»[3]. Основное содержание и социальное значение так называемого «сервисного государства» исследователи связывали с его пониманием как процесса предоставления социальных услуг. Сервисная идея развития государственной системы, с точки зрения Я.В. Коженко, основывается на классической экономической схеме: «производитель услуг – потребитель», где устойчивость и легитимность государственных институтов связаны с эффективностью выявления, моделирования

[1] См.: Бачило И.Л. Электронное правительство и инновации в области государственных функций и государственных услуг. – С. 13–17.

[2] См.: там же; Бачило И.Л. Государство социальное или сервисное? (Информационно-правовой аспект) // Право. Журнал высшей школы экономики. – М., 2010. – № 1. – С. 3–11. – URL: https://socionet.ru/publication.xml?h=spz:cyberleninka:7346:16027016 (дата обращения: 11.03.2020); Кононенко Д.В. Модернизация концепций электронного правительства: сравнительно-правовой анализ (РФ и США) // Вестник Волгогр. гос. ун-та. Сер. 5: Юриспруденция. – 2013. – № 2 (19). – С. 34–38.

[3] См.: Кононенко Д.В. Указ. соч. С. 34–35.

и реализации индивидуальных и групповых интересов и потребностей[1].

Преимущества электронного государства (правительства) как сервисного государства усматриваются: 1) в целевой ориентации исполнительных структур государственной власти на потребности различных социальных групп населения (что в значительной мере обусловлено перенесением стандартов и правил бизнеса в систему государственного управления); 2) в новых качествах управления, основанных на «гибком реагировании» в соответствии с принципами интерактивной коммуникации и обратной связи посредством пользовательских запросов; 3) в возможностях реализации социальных функций государства на основе качественного предоставления государственных услуг широкому кругу потребителей; 4) в снижении государственных издержек управления, связанных с децентрализацией бюрократических структур и открытостью процессов принятия решений; 5) в возможности гражданского контроля процессов управления[2].

По задумке разработчиков, проект «Сервисное государство 1.0 (2010–2018)» включает четыре составляющие: «государственные услуги», «государственные порталы», «межведомственное взаимодействие» и «государственные данные». Этот проект ставил задачу создания «электронного правительства» и «электронного государства», определяемого как гибридная цифроаналоговая надсистема гармонично (в математическом и гуманитарном аспектах) взаимодействующих систем и подсистем граждан, цифро-программных, информационно-коммуникационных устройств, обеспечивающих безопасность каждого человека, соблюдение его прав и свобод[3].

Вместе с тем Минкомсвязи России была предложена Концепция цифровизации государственного управления на 2018–2024 гг. – «Сервисное государство 2.0». Новая модель «Сервисного

---

[1] См.: Коженко Я.В. Концепции «сильного» и «сервисного» государства в контексте модернизации государственного управления в России: общее и отличное // Фундаментальные исследования. – 2012. – № 3–3. – С. 744–748.

[2] См.: Васильева Е.Г., Кононенко Д.В. Современные интерпретации концепции электронного государства (электронного правительства). – С. 11.

[3] См.: Электронное государство и энтропийные процессы в управлении в условиях информационного коллапса: доклад на IX Междунар. конф. «Электронный город – Электронная губерния – Электронное государство». Москва, 18 мая 2016 г. / И.В. Башелханов, Н.А. Трусов, А.И. Иванус, Е.А. Калмыкова. – С. 4. – URL: https://old.integra-s.com/seminar/conference/11p.pdf (дата обращения: 01.03.2020).

государства», по мнению зам министра цифрового развития, связи и массовых коммуникаций РФ М. Паршина, позволит комплексно решать жизненные ситуации граждан на основании автоматизированных бизнес-процессов («суперсервисы»), минимизировать участие чиновников в принятии решений по оказанию услуг, исключить бумажные документы как в процессе оказания услуг, так и между ведомствами. Этот проект предусматривает развитие сервисного государства по шести направлениям: «суперсервисы», «цифровой профиль», «единый фронт», «единый транспорт», «единая модель данных» и «единая платформа услуг и сервисов». Предполагается, что в рамках первого направления в ближайшие три года будет запущено 25 цифровых суперсервисов, среди которых рождение ребенка, оформление пособий и льгот, электронный больничный, полис ОСАГО, полис обязательного медицинского страхования и трудовая книжка.

Второе направление связано с развитием Единой системы идентификации и аутентификации (ЕСИА), к которой относятся цифровой профиль, облачная электронная подпись, биометрическая идентификация и реестр полномочий и согласий. «*Единый фронт*» означает, что все официальные информационно-сервисные интернет-порталы, сайты, мобильные и интернет-приложения, создаваемые и выпускаемые органами власти, будут объединены в одну систему. Направление «*единый транспорт*» касается данных и документов, связанных с облегчением электронного взаимодействия ведомств и юридически значимого документооборота. «*Единая модель данных*» подразумевает создание и развитие Национальной системы управления данными (НСУД). Сюда относится, в частности, внедрение единого стандарта управления жизненным циклом данных. «*Единая платформа услуг и сервисов*» будет представлять единую бэк-платформу услуг и сервисов, где будет осуществляться, в частности, контроль сроков и качества предоставления услуг[1].

С 2017 г. в научных публикациях начал активно использоваться термин «*государство-платформа*», который можно рассматривать как аналог понятия «цифровые платформы». Данный термин применяется, когда речь идет о поисковых платформах

[1] Сервисное государство нового поколения. – URL: https://www.comnews.ru/content/115366/2018-10-16/servisnoe-gosudarstvo-novogo-pokoleniya?utm_source=telegram& utm_medium=general&utm_campaign=general (дата обращения: 27.02.2020).

(системах), социальных сетях, платформах электронной торговли, шеринговых платформах и др. Эти платформы отражают различные виды социально-экономической активности населения, взаимодействия и сотрудничества компаний, людей, создают возможности расширения знаний, общения и развлечения и пр.

К крупнейшим цифровым платформенным компаниям сегодня относятся Apple, Microsoft, Amazon, Google, Facebook, Alibaba, Tencent, совокупная рыночная капитализация которых составляет около 4,5 трлн долл. США, что более чем в 7 раз превышает объем российского фондового рынка (625,2 млрд долл. США). Большинство крупных платформенных компаний базируется преимущественно в США и КНР, есть они также в Великобритании, Индии, Японии, Германии, России и в других странах[1]. Цифровые платформы в России представлены в формате социальных сетей, мессенджеров, поисковых систем, платежных систем, платформ в сфере электронной торговли, финансов, туризма, занятости, образования, пассажирских перевозок и т.п.

Считается, что идея «государства как платформы» была предложена Тимом О'Рейли в 2010 г., и в дальнейшем она получила поддержку в ряде стран, где приобрела характер практической идеи и была положена в основу соответствующих административных реформ[2].

«Государство как платформа» – метафора, ее также можно рассматривать как аналог понятия «кибергосударство», применяемого в цифровой экономике. Начиная с 2017 г. эта идея, используя опыт таких стран, как Сингапур, Великобритания, США, Австралия, Франция, Норвегия и др., получила свое развитие и в России. Акцент разработчиков данной концепции в нашей стране (Центра стратегических разработок) был сделан на роль государства в условиях трансформации информационного общества и его перехода на уровень цифровизации. Предполагается, что значительная часть функций государства как посредника в движении

[1] См.: Гелисханов И.З., Юдина Т.Н., Бабкин А.В. Цифровые платформы в экономике: сущность, модели, тенденции развития // Научно-технические ведомости С.-Петерб. гос. политех. ун-та. Сер. Экономические науки. – 2018. – Т. 11, № 6. – С. 28.

[2] O'Reilly T. Government as a platform // Open government: collaboration, transparency, and participation in practice / ed. by D. Lathrop, L. Ruma. – Sebastopol, 2010. – P. 11–40. – URL: https://books.google.ru/books?id=JQJ5LF3h4ikC&redir_esc=y (дата обращения: 10.02.2020).

такой информации, как налоговая, кадровая, статистическая, персональных данных и др., будет выполняться алгоритмами без участия человека[1].

В апреле 2018 г. Центром был подготовлен доклад под названием «Государство как платформа»[2]. Целевой функцией реализации этой идеи является, по словам ее разработчиков, благополучие граждан и содействие экономическому росту, основанному на внедрении технологий. Основная идея концепции – взаимодействие трех групп – граждан, государства и бизнеса.

Внедрение рассматриваемых платформ, по мнению авторов доклада, приведет к ряду принципиальных изменений по следующим направлениям:

1) модель государственного участия: позволит внедрять модель сервисного государства – культуры «государство для меня»; государство как координатор возьмет на себя управление взаимодействием всех участников платформы, будет выступать создателем экосреды взаимодействия;

2) государственные процессы: государственная инфраструктура станет единым центром для всех обращений за государственными сервисами; позволит использовать достоверные и единые данные для принятия решений; даст новые возможности для определения целей, оценки результатов, позволит снизить коррупцию;

3) государственная служба: разовьется «цифровой менталитет»: принятие цифровой реальности, умение в ней эффективно работать, цифровые навыки и персональное развитие; возникнет единая цифровая платформа взаимодействия для государственных служащих, бизнеса и граждан[3].

Реализовать цифровую трансформацию, которая подразумевает переход к государству-платформе, как признают сами разработчики, достаточно сложно. Эту же точку зрения разделяют и некоторые ученые, полагая, что создание цифрового правительств

---

[1] См.: Крупеня Е.М. Законотворчество: к проблеме понимания в условиях цифровизации общества и функционирования государства-платформы // Трансформация правовой реальности в цифровую эпоху: сб. науч. тр. / под общ. ред. Д.А. Пашенцева, М.В. Залоило. – М., 2019. – С. 76.

[2] См.: Государство как платформа: Люди и технологии. (Кибер)государство для цифровой экономики. Цифровая трансформация: доклад / М. Петров, В. Буров, М. Шклярук, А. Шаров. – URL: https://www.csr.ru/upload/iblock/313/3132b2de9ccef0db1eecd56071b98f5f.pdf (дата обращения: 15.02. 2020).

[3] См.: там же. – С. 8–10, 21.

будет вестись еще довольно долго[1]. Объясняется это тем, что существующая система управления заинтересована в консервации своего текущего состояния на максимально долгий срок.

Вместе с тем цифровые технологии развиваются быстрыми темпами, и к 2024 г. уже планируется создание не менее десяти отраслевых (индустриальных) цифровых платформ для основных предметных областей экономики (в том числе для создания цифрового здравоохранения, цифрового образования, «умного города»), предусмотренных программой «Цифровая экономика Российской Федерации»[2].

Однако есть проблемы, которые еще предстоит решить: 1) на каких правовых платформах следует строить «электронное (цифровое) государство» и «электронное правительство»; 2) причины и суть эволюции государственных и правовых институтов в условиях цифровизации; 3) как изменятся человек, его профессиональные функции, общество и государство в условиях технологических и иных информационно-коммуникационных процессов; 4) как трансформируются отношения между людьми, общающимися сегодня посредством многочисленных социальных сетей и месседжей, гражданином и государством в так называемую «цифровую эпоху»; 5) какие новые проблемы возникают в связи с процессами социализации и демократизации, развитием социальных сетей и др.[3]

Следует признать, что далеко не все исследователи однозначно оценивают идею «государства-платформы». С одной стороны, многие признают платформу технологически продвинутым инструментом и базой для использования больших данных в различных приложениях. С другой стороны, использование этой идеи основано на технологическом оптимизме и не учитывает сложную структуру публичного государства. Проект «государство как платформа», считает Л.В. Сморгунов, превращает государство в управляющего «рынка», «социальное предприятие»[4]. Историк

---

[1] См.: Павлютенкова М.Ю. Электронное правительство vs цифровое правительство в контексте цифровой трансформации // Мониторинг общественного мнения: экономические и социальные перемены. – М., 2019. – № 5 (153). – С. 132.

[2] См.: Государство как платформа: Люди и технологии. (Кибер) государство для цифровой экономики. Цифровая трансформация: доклад. – С. 20–21.

[3] См.: Там же.

[4] См.: Сморгунов Л.В. Партисипаторная государственная управляемость: платформа и сотрудничество // Власть. – М., 2019. – С. 10, 15.

О.Н. Четверикова в серии своих видеоинтервью ставит такие вопросы: «Сегодня государство выполняет уже не функции, а оказывает услуги – социальные, образовательные, медицинские и пр.? Кто будет управлять государством – владелец платформы?»[1].

Основными направлениями критического подхода к технологической и рыночно-потребительской теории «государства (правительства) как платформы» признаются суждения о характере использования ИКТ: в политике и государственном управлении; потребительском подходе к платформенной организации государственного управления в связи с доминированием идеологии неолиберализма; преобладающем акценте на информацию, ее хранение, распространение и использование на государственных порталах в виде больших данных и отсутствии внимания к тому, что современное государственное управление в большей степени основано на знаниях, чем на информации; либерально-индивидуалистической модели демократии, на которой основывается идея «государства как платформы»[2].

Очевидно то, что проблемы цифрового правительства не являются полностью техническими; коммерческие усилия мало подходят для решения социально-культурных и других функций правительства, в частности, решения вопросов, касающихся конфиденциальности и доверия, которые носят юридический и политический характер.

Ключевые вопросы, которые необходимо решать, полагает Л.В. Сморгунов, касаются пригодности технологий в государственных процессах, а не развития правильных технологий. Попытка свести использование идеи «государства как платформы» к прагматической версии государства как эффективного механизма предоставления государственных услуг не учитывает сложный характер внедрения каких-либо технологий в жизненное пространство государственной политики[3].

Таким образом, сегодня многое, что делает государство, уже обретает цифровую форму, а цифровизация процессов управления

---

[1] См.: Четверикова О.Н. На кону будущее: Кому будет принадлежать власть. – Режим доступа: https://yandex.ru/video/preview/?filmId=8944479208871745276&text=четверикова%20о%20на%20кону%20будущее&path=wizard&parent-reqid=1585568943458909-1063547403033497729400179-vla1-0672&redircnt=1585569071.1

[2] См.: Сморгунов Л.В. Указ. соч. – С. 15.

[3] См.: там же. – С. 17.

начинает превалировать при разработке стратегических программ развития, происходит трансформация многих сфер экономической, социальной, политической и культурной жизни общества. Ученые выдвигают новые идеи и проекты, которые, с одной стороны, воодушевляют, с другой – заставляют задуматься: не слишком ли мы увлеклись виртуальной жизнью, забыв о реальной?

1.3. Трансформация права в условиях цифровизации

Проблемы, связанные с трансформацией права в условиях алгоритмизации, правовым регулированием цифровой экономики, «цифровизацией» правотворчества и судебной деятельности, стали в последние годы предметом отдельных направлений научных исследований[1].

Научный интерес вызывает как право в условиях цифровизации государства и общества, так и цифровое право как таковое[2].

Право в условиях новой реальности рассматривается не только как средство, инструмент, обеспечивающий цифровизацию экономики, управления и других сегментов социального бытия, но

[1] См.: Трансформация правовой реальности: сб. науч. тр. / под общ. ред. Д.А. Пашенцева, М.В. Залоило. – М.: Ин-т законодат. и срав. правоведения при Правительстве РФ: ИНФРА-М, 2019. – 213 с.; Цифровизация правотворчества: монография / под общ. ред. Д.А. Пашенцева. – М.: Ин-т законодат. и срав. правоведения при Правительстве РФ: ИНФРА-М, 2019. – 233 с.; Правовое регулирование цифровой экономики в современных условиях развития высокотехнологического бизнеса в национальном и глобальном контексте: монография / под общ. ред. В.Н. Синюкова, М.А. Егоровой. – М.: Моск. гос. юрид. ун-т им. О.Е. Кутафина (МГЮА): Проспект, 2019. – 240 с.; Цифровая экономика: проблемы правового регулирования: монография / Моск. гос. юрид. ун-т им. О.Е. Кутафина (МГЮА); отв. ред. В.В. Зайцев, О.А. Серова. – М.: Кнорус, 2019. – 200 с.; Антимонопольное регулирование в цифровую эпоху: как защищать конкуренцию в условиях глобализации и четвертой промышленной революции / Нац. исслед. ун-т «Высшая школа экономики»; ФАС России; под ред. А.Ю. Цариковского, А.Ю. Иванова и Е.А. Войниканис. – М.: Изд. дом Высшей школы экономики, 2018. – 311 с., и др.

[2] См.: Хабриева Т.Я., Черногор Н.Н. Право в условиях цифровой реальности // Журнал российского права. – М., 2018. – № 1. – С. 87; Полякова Т.А. Актуальные проблемы развития системы правового обеспечения информационной безопасности в цифровую эпоху и юридическое образование // Вестник Ун-та им. О.Е. Кутафина (МГЮА). – М., 2019. – № 12. – С. 41 и др.

и как объект воздействия «цифровизации», в результате которого оно претерпевает изменения своей формы, содержания, системы, структуры, механизма действия и демонстрирует тенденцию к усилению наметившихся трансформаций[1]. Утверждается, что право изменяет свою природу, и, соответственно, предъявляет новые требования к правовой науке и юридической практике[2].

В связи с этим возникает ряд фундаментальных задач, связанных с регулированием общественных отношений в условиях цифровой реальности, которые правовой науке необходимо решать. Среди них: выявление закономерностей и механизмов воздействия цифровизации на право; развитие методологии юридической науки, позволяющей изучать право с позиции соотношения реального и виртуального (например, что такое «цифровая личность» или «виртуальная вещь»); изучение природы «циклических правовых массивов», механизма их формирования и влияния на общественные отношение, право и правоприменительную практику; разработка моделей правового регулирования общественных отношений, связанных с использованием цифровых технологий; разработка стратегии, тактики и юридического инструментария управления цифровыми трансформациями; появление новых нормативных комплексов в системе социальных норм наряду с уже существующими (моралью, религией, правом); создание концепции опережающего отражения в праве общественных отношений в сферах, сопряженных с использованием цифровых технологий; «оцифровка» юридических технологий, применяемых в правотворчестве, правовом мониторинге, юридическом прогнозировании, юридическом моделировании, экспертизе проектов нормативных правовых актов и др.[3]

Обобщение научных работ российских исследователей в рассматриваемой сфере, проведенное А.А. Дорской, позволило ей выделить следующие векторы развития юридической науки в условиях цифровизации производства и общественных процессов: 1) эволюция теоретико-правовых конструкций, в том числе определение понятия «цифровизации права», характеристика субъек-

[1] Хабриева Т.Я., Черногор Н.Н. Указ. соч. – С. 85.

[2] См.: Шабаева О.А. Право в условиях цифровой реальности: постановка проблемы // Сибирский юридический вестник. – Иркутск, 2019. – № 1 (84). – С. 20.

[3] См.: Хабриева Т.Я., Черногор Н.Н. Указ. соч. – С. 101.

тов («виртуальная личность» или цифровой образ)[1]; объектов, правоотношений, судьба права как нормативной системы цифрового права; 2) вопросы безопасности; 3) развитие отдельных институтов, подотраслей и отраслей права; 4) защита прав человека; 5) цифровизация процесса отправления правосудия; 6) подготовка юридических кадров[2].

Следует подчеркнуть, что приоритетные направления правового регулирования в связи с нарастанием процессов цифровизации определены в Стратегии развития информационного общества в Российской Федерации на 2017–2030 гг., утвержденной Указом Президента РФ от 9 мая 2017 г. № 203. В их числе названы: формирование информационного пространства знаний и развитие правосознания граждан и их ответственного отношения к использованию информационных отношений, в том числе потребительская и пользовательская культура, а также обеспечение создания и развития систем нормативно-правовой, информационно-консультативной, технологической и технической помощи в обнаружении, предупреждении и отражении угроз информационной безопасности граждан и ликвидации последствий их проявления (подп. «н» и «о» п. 26).

В рамках реализации Указа Президента РФ от 7 мая 2018 г. № 204 «О национальных целях и стратегических задачах развития Российской Федерации на период до 2024 года», в том числе в целях решения задачи по обеспечению ускоренного внедрения цифровых технологий в экономике и социальной сфере, Правительством РФ на базе программы «Цифровая экономика Российской Федерации», утвержденной распоряжением Правительством РФ от 28 июля 2017 г. 3 1632-р (данный документ распоряжением Правительства РФ от 12 февраля 2019 г. № 195-р утратил силу), сформирован паспорт национальной программы «Цифровая экономика Российской Федерации», утвержденный протоколом заседания президиума Совета при Президенте РФ по стратегическому развитию и национальным проектам от 4 июня 2019 г. № 7. В состав национальной программы «Цифровая экономика Российской Федерации» входят следующие федеральные проекты, утвержденные

[1] См.: Талапина Э.В. Право и цифровизация: новые подходы и перспективы // Журнал российского права. – М., 2018. – № 2 (254). – С. 6–10.

[2] См.: Дорская А.А. Проблема цифровизации правовой сферы: основные направления исследований // Трансформация правовой реальности в цифровую эпоху. – М., 2019. – С. 19–24.

протоколом заседания президиума Правительственной комиссии по цифровому развитию, использованию информационных технологий для улучшения качества жизни и условий ведения предпринимательской деятельности от 28 мая 2019 г. № 9: «Нормативное регулирование цифровой среды»; «Кадры для цифровой экономики»; «Информационная инфраструктура»; «Информационная безопасность»; «Цифровые технологии»; «Цифровое государственное управление»[1]. Система управления утверждена постановлением Правительства РФ от 2 марта 2019 г. № 234 «О системе управления реализацией национальной программы «Цифровая экономика Российской Федерации».

На рассмотрении Государственной Думы Федерального Собрания РФ находятся проекты федеральных законов: «О цифровых финансовых активах», «О привлечении инвестиций с использованием инвестиционных платформ» и «О внесении изменений в отдельные законодательные акты (в части уточнения процедур и аутентификации)».

Минэкономразвития разработан проект федерального закона «Об экспериментальных правовых режимах в сфере цифровых инноваций в Российской Федерации» (12 марта 2020 г. он одобрен Правительством РФ). В данном проекте определяется порядок инициирования, установления, реализации, мониторинга реализации, оценки результативности экспериментальных правовых режимов в сфере цифровых инноваций («регуляторных песочниц»), состоящих во временном адресном контролируемом установлении экспериментального (в отсутствие существующего или отличающегося от существующего) нормативного правового регулирования для применения цифровых инноваций или осуществляемой с их использованием деятельности в Российской Федерации.

Цифровая инновация в проекте понимается как новое средство, поддерживающее использование цифровых процессов, ресурсов и сервисов. Это – новая система средств, созданных на основе технологий больших данных, нейротехнологий и искусственного интеллекта, квантовых и новых производственных технологий, промышленного Интернета, компонентов робототехники и сенсорики, технологий беспроводной связи, техноло-

[1] См.: Цифровая экономика РФ. – URL: https://digital.gov.ru/ru/activity/directions/858/ (дата обращения: 11.03.2020).

гий виртуальной и дополненной реальностей, а также иных технологий. Эти технологии получают отражение в нормативных правовых актах, утверждаемых высшими органами государственной власти РФ в качестве технологий, относящихся к категории цифровых или к сфере цифровой экономики. В том числе определяются: полномочия органов государственной власти РФ в области экспериментальных правовых режимов в сфере цифровых инноваций; объекты экспериментальных правовых режимов, критерии их допустимости и ограничения; гарантии прав и законных интересов участников экспериментальных правовых режимов; порядок установления экспериментального правового режима (внесение предложения, его рассмотрение, принятие решения), его срок; требования к программе экспериментального правового режима, порядок его реализации, в том числе приостановления и отмены[1].

С одной стороны, ученые признают, что нормативный массив, образующий правовую основу цифровой экономики, уже не только формируется, но и функционирует[2]. С другой стороны, исследователи отмечают, что «нормативное описание цифровых процессов значительно отстает от фактического развития цифровых институтов»[3], наблюдается «прогрессирующее отставание правовых норм от потребностей реальной жизни»[4], «…правовое регулирование не работает “на перспективу”, так как законодатель способен реагировать лишь на факты негативного влияния современных информационных технологий на жизнь общества, не представляя, каким оно будет в будущем»[5]. Прежнее нормативно-правовое регулирование различных сфер социальной жиз-

---

[1] Минэкономразвития России предлагает устанавливать временные правовые режимы. – URL: http://www.consultant.ru/law/hotdocs/56430.html/ (дата обращения: 02.03.2020).

[2] Хабриева Т.Я., Черногор Н.Н. Указ. соч. – С. 89.

[3] См.: Наумов В.Б. Право в эпоху цифровой трансформации: в поисках решений // Российское право: Образование. Практика. Наука. – М., 2018. – № 6. – С. 5.; Вайпан В.А. Правовое регулирование цифровой экономики // Приложение к журналу «Предпринимательское право». – М., 2018. – № 1. – С. 12.

[4] См.: Пашенцев Д.А. К вопросу о влиянии цифровых технологий на правотворчество и правоприменение (постановка проблемы) // Российское государствоведение. – М., 2018. – № 4. – С. 134.

[5] Полякова Т.А., Минбаев А.В., Наумов В.Б. Форсайт-сессия «Информационная безопасность в XXI веке: вызовы и правовое регулирование // Труды Института государства и права РАН. – М., 2018. – № 5. – С. 194.

ни, считает В.Д. Зорькин, нуждается в существенной модернизации[1].

О формировании нового цифрового права как самостоятельного направления правового регулирования пишут многие ученые-правоведы. Дискуссии ведутся главным образом в направлении поиска оптимальных решений и разработки моделей правового регулирования общественных отношений, сопряженных с применением цифровых технологий в области финансов, публичного управления, создания искусственного интеллекта и др.

Так, по мнению А.А. Карцхия, логика развития правоотношений с использованием цифровых технологий может быть использована для формирования концепции (доктрины) цифрового права как формы выражения правового регулирования с использованием цифровых технологий в так называемом «цифровом киберпространстве»[2]. Автор полагает, что есть объективная потребность создания самостоятельного неоклассического правового направления, использующего не только традиционные, классические институты и правовые конструкции частного или публичного права. Речь идет, по сути, о «создании цифрового права в широком правовом смысле, не ограниченного классической частноправовой доктриной», а также об «адаптации («форматировании») в самой ближайшей перспективе классического гражданского права для применения новых цифровых технологий в правовом регулировании»[3]. При формировании цифрового права как самостоятельного направления правового регулирования, с его точки зрения, оправдан подход с позиции цифровой системы – разновидности информационной системы. При этом цифровое право представляет собой не только развитие современной системы права, но и развитие системы правовых норм различной отраслевой принадлежности, объединяемых предметом регулирования отношений между субъектами виртуального (цифрового) пространства – киберпространства. В то же время система цифрового права не ограничена рамками информационной системы, как ее определяет Федеральный закон от 21 июля 2006 г. № 149-ФЗ

[1] Зорькин В.Д. Право в цифровом мире: Размышления на полях Петербургского международного юридического форума // Рос. газета. – 2018. – 18 мая, № 115.

[2] Карцхия А.А. Цифровая транформация права // Мониторинг правоприменения. – М., 2019. – № 1. – С. 26.

[3] См.: Там же.

«Об информации, информационных технологиях и защите информации». В частности, в п. 3 ст. 2 этого Закона информационная система определяется как «совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств».

Цифровое право в объективном смысле, резюмирует А.А. Карцхия, представляет собой структуру нормативных правовых актов (включая международные договоры) и акты локального действия в технологических платформах[1].

Близкую позицию высказывают и другие ученые. Так, П. Хлебников предлагает рассматривать цифровое право как новую отрасль российского права – систему общеобязательных, формально-определенных, гарантированных государством правил поведения, складывающуюся в области применения или с помощью применения цифровых технологий, в том числе посредством специального программного обеспечения[2].

В *субъективном* смысле – это цифровые права на объекты цифрового оборота (криптовалюты, токены и др.), обладающие объявленной или действительной экономической ценностью, признаваемые законом и основанные на принципах создания и действия технологических платформ распределенного реестра или иных цифровых технологий (технологии искусственного интеллекта, технологии виртуальной или дополненной реальности, технологии криптографии и др.)[3].

Федеральным законом от 18 марта 2019 г. № 34-ФЗ «О внесении изменений в части первую и вторую и ст. 1124 части третьей Гражданского кодекса Российской Федерации» в Гражданский кодекс РФ была введена новая ст. 141.1, названная «Цифровые права». Согласно п. 1 и 2 указанной статьи «*Цифровыми правами признаются названные в таком качестве в законе обязательственные и иные права, содержание и условия осуществления которых определяются в соответствии с правилами информационной системы, отвечающей установленным законом признакам. Осуществление, распоряжение, в том числе передача, залог, обременение цифрового права другими способами или ограничение*

[1] См.: Карцхия А.А. Указ. соч. – С. 26.

[2] См.: Хлебников П. Цифровизация права как следствие цифровизации // Жилищное право. – 2017. – № 9. – С. 93–94.

[3] См.: Карцхия А. А Указ соч. – С. 26.

распоряжения цифровым правом возможны только в информационной системе без обращения к третьему лицу.

2. Если иное не предусмотрено законом, обладателем цифрового права признается лицо, которое в соответствии с правилами информационной системы имеет возможность распоряжаться этим правом. В случаях и по основаниям, которые предусмотрены законом, обладателем цифрового права признается иное лицо».

Следовательно, введение в перечень имущественных объектов децентрализованных информационных систем, основанных на блокчейне, полагает Н.Ю. Комлев, свидетельствует о реагировании отрасли гражданского права на изменения в социально-экономической жизни и цифровизации гражданского оборота, т.е. способности объектов гражданского права быть востребованными на рынке информационных технологий[1].

В первоначальной редакции законопроекта, как отмечают многие исследователи, цифровым правом предлагалось назвать совокупность электронных данных (т.е. цифровой код), существующую в информационной системе, отвечающей установленным законом признакам децентрализованной информационной системы. Но в такой редакции получалось, что цифровое право – это имущественное право (об этом говорилось в обновленной ст. 128 ГК РФ), но в то же время – это цифровой код. В итоге от этой идеи решено было отказаться. В последнем варианте определение было сформулировано по модели описания ценной бумаги в ст. 142 ГК РФ[2].

---

[1] См.: Комлев Н.Ю. Правовая природа токена (цифрового права) как нового объекта гражданских правоотношений // Ученые записки Казанск. юрид. ин-та МВД России. – Казань, 2019. – Т. 4, № 2 (8). – С. 59.

[2] См.: там же. – С. 59: Конобеевская И.М. Цифровые права как новый объект гражданских прав // Изв. Сарат. ун-та. Сер.: Экономика. Управление. Право. – 2019. – Т. 19, вып. 3. – С. 331; см.: Бардина П. Цифровые права как новый вид объектов гражданских прав. Что еще поменялось в ГК РФ? – URL: https://www.eg-online.ru/article/396138/ (дата обращения: 06.03.2020); Василевская Л.Ю. Токен как новый объект гражданских прав: проблемы юридической квалификации цифрового права // Актуальные проблемы российского права. – 2019. – № 5. – С. 111–119; см.: Шестакова М. Цифровые права как новый вид объектов гражданских прав. Что еще поменялось в ГК РФ? – URL: https://www.eg-online.ru/article/396138/ (дата обращения: 06.03.2020).

Как следует из ст. 141.1 ГК РФ, осуществление и распоряжение цифровым правом возможны только в информационной системе без обращения к третьему лицу. Если иное не предусмотрено законом, обладателем цифрового права признается лицо, которое в соответствии с правилами информационной системы имеет возможность им распоряжаться. В случаях и по основаниям, которые предусмотрены законом, обладателем цифрового права признается иное лицо. Переход цифрового права на основании сделки не требует согласия лица, обязанного по цифровому праву.

Выражение воли в Интернете согласно п. 3 указанной статьи приравнено к письменной форме сделок. Например, когда на интернет-странице или в мобильном приложении описаны условия для нажатия клавиши «ОК», из которых следует, что такого нажатия достаточно для выражения волеизъявления. Письменная форма будет считаться соблюденной в случае совершения сделки с помощью электронных либо иных технических средств, позволяющих воспроизвести на материальном носителе в неизменном виде содержание этой сделки. А требование о наличии подписи будет считаться выполненным, если использован любой способ, позволяющий достоверно определить лицо, выразившее волю. Законом и соглашением сторон может быть предусмотрен специальный способ достоверного определения лица, выразившего волю. На основании этих норм будут считаться заключенными сделки, совершаемые дистанционно, в том числе путем заполнения формы в Интернете или путем отправки смс. Кроме того, можно будет заочно голосовать с помощью технических средств на собраниях гражданско-правовых сообществ.

В вышеупомянутом Федеральном законе № 34-ФЗ предусмотрены положения, касающиеся сбора и обработки обезличенной информации о пользователях, т.е. большие данные (big data). В частности, в ГК РФ появилась ст. 783.1, регулирующая договор об оказании услуг по предоставлению информации. В таком договоре может быть предусмотрена обязанность сторон не совершать в течение определенного периода действий, в результате которых информация может быть раскрыта третьим лицам. Исследования российских ученых позволяют им констатировать появление следующих тенденций и процессов в современном праве: 1) формируются новые понятия и легальные дефиниции, составляющие основу будущих правовых институтов; 2) меняется внутреннее строение права, что может поставить под вопрос общепринятые

представления об отраслевом делении права, а также его разделение на частное и публичное; 3) закрепляются и оформляются новые правовые институты, подотрасли права; 4) меняются некоторые формальные параметры источников права; 5) конкретизируются права человека, возникает новое поколение прав – «цифровых»; 6) для целей создания цифровой экономики широко применяются инструменты публичного права; 7) в частное право вводятся новые понятия и институты; 8) изменяется соотношение между законами и подзаконными актами; 9) происходит перенастройка законодательства на решение задач, возникших в связи с цифровизацией, посредством «цифровой прививки» гражданскому, трудовому, административному, уголовному и многим другим отраслям законодательства и др.[1]

Можно утверждать, что цифровизация обусловливает появление новых общественных отношений, которые ранее не существовали, и, соответственно, активно влияет на развитие законодательства. Как замечает Т.Я. Хабриева, в сфере правового регулирования наблюдается появление отношений: 1) субъектами которых являются виртуальные или цифровые «личности»; 2) связанных с юридически значимой идентификацией личности в виртуальном пространстве; 3) возникающих в связи с реализацией прав человека в виртуальном пространстве (право на доступ в Интернет, право на забвение, право на «цифровую смерть» и др.); 4) ориентированных на применение робототехники; 5) складывающихся по поводу нетипичных объектов – информации, цифровых технологий (финтех, регтех и др.), создаваемых посредством применения новых цифровых сущностей (криптовалюты) и объектов материального мира, а также связанных с использованием и оборотом того и другого; 6) сопряженных: с использованием оцифрованных информационных массивов – информационных баз данных; переводом в цифровую форму действий и операций, посредством которых реализуются государственные функции, оказываются государственные и муниципальные услуги, обеспечивается электронное участие граждан в управлении обществом и государством; совершением действий в виртуальном простран-

[1] См.: Хабриева Т.Я. Право перед вызовами цифровой реальности // Журнал российского права. – М., 2018. – № 9. – С. 12.; Николаев А.И. Вопросы цифровизации права в современной юридической доктрине // Вестник МГПУ. Сер.: Юрид. науки. – М., 2019. – № 4 (36). – С. 45, и др.

стве, направленных на возникновение, изменение и прекращение правоотношений, реализацию прав и исполнение обязанностей, образующих их юридическое содержание; применением автоматизированных действий (Интернетом вещей), обеспечением информационной безопасности и др.[1]

В структуре информационной сферы есть и такие общественные отношения, которые на данном этапе объективно не могут быть регламентированы правом. Например, известная ситуация с блокировкой мессенджера Telegram на территории России. Юристы пока не могут ответить на вопрос, как осуществлять контроль за деятельностью подобных субъектов права. Вопрос этот сложный и не однозначный. Представители интернет-сообществ отстаивают идею саморегулирования в Сети, органы государственной власти в целях информационной безопасности пытаются усилить регулятивное воздействие путем введения новых ограничений и запретов.

Высказывается мысль о том, что одним из социальных регуляторов общественных отношений может стать программный код. В связи с этим В.Д. Зорькин видит несколько вариантов дальнейшего развития событий: 1) право трансформируется в иной социальный регулятор, допуская появление программного кода или некой гибридной формы; 2) право сохранит свои субстанциональные признаки и будет мирно сосуществовать с программным кодом; 3) появится новая нормативная система, которая займет свое место в системе социальных норм наряду с правом, моралью, религией. Однако этот вариант можно прогнозировать на самую отдаленную перспективу[2].

Таким образом, анализ процессов цифровизации и их правового регулирования позволяет ученым-юристам прийти к выводу, что цифровая реальность формирует поведение человека, нормы социальных отношений, создается новое цифровое право, актуализируется запрос общества на дальнейшее совершенствование режима цифровых прав, на правовое регулирование сегмента цифро-

[1] См.: Хабриева Т.Я. Право перед вызовом правовой реальности: доклад. – URL: https://izak.ru/img_content/pdf/Право%20перед%20вызовами%20цифровой%20реальности.pdf (дата обращения: 03.03.2020).

[2] Зорькин В.Д. Право в цифровом мире: размышления на полях Петербургского международного юридического форума // Рос. газета. – 2018. – 18 мая, № 115.

вых услуг и закрепление права на виртуальные объекты цифрового пространства и др. Исследования российских ученых показывают, что цифровые технологии все шире проникают в общественные отношения, порождая новое явление, именуемое цифровизацией; право под воздействием алгоритмизации трансформируется в целях сохранения своего ключевого свойства – быть эффективным регулятором общественных отношений. Требуется продолжение научных исследований вопросов цифровизации права и тех изменений, которые происходят в правовой среде под влиянием прорывных цифровых технологий. Соответственно, для реализации целей эффективного правового регулирования общественных отношений необходимы не только нормативная правовая база, но и подготовка нового поколения юристов, владеющих этими технологиями, и новые технологии, алгоритмизирующие их труд.

Глава 2.
ВОЗДЕЙСТВИЕ ЦИФРОВЫХ ТЕХНОЛОГИЙ НА ИНФОРМАЦИОННОЕ ПРАВО И ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

2.1. Информационное право как отрасль права нового поколения: Развитие в цифровую эпоху

В современную эпоху информационные отношения оказались объектом всестороннего международного и внутригосударственного правового регулирования. Информация стала одним из ценнейших товаров и источников получения прибыли. Ее значимость непрерывно возрастает в условиях интенсивного развития цифровых технологий, расширения интернет-пространства, формирования сетевых систем управления обществом. Появление вычислительной техники и цифровых видов связи создало возможности для использования информации как универсального средства взаимодействия в системах экономических, бюджетно-финансовых, политических, социальных и иных отношений. Цифровизация существенным образом затрагивает практически все социальные отношения, что требует переосмысления многих базовых юридических понятий[1]. Одно из направлений научного поиска состоит в доктринальном освоении новых явлений и процессов, возникших и протекающих в государственно-правовой сфере под воздействием цифровизации экономики, управления и права[2].

В истории человечества выделяются четыре этапа информационно-технологической революции, которые заметно изменили характер цивилизационного развития. Первый этап увязывается с возникновением и интенсивным развитием кибернетики, созданием на ее основе информационных систем управления. Второй – характеризуется массовым внедрением персональных компьюте-

[1] См.: Варламова Н.В. Цифровые права – новое поколение прав человека? // Тр. Ин-та государства и права РАН. – М., 2019. – Т. 14, № 4. – С. 9–46.

[2] См.: Хабриева Т.Я., Черногор Н.Н. Право в условиях цифровой реальности // Журнал российского права. – М., 2018. – № 1. – С. 87.

ров, третий этап соотносится с развитием телекоммуникационных технологий, объединением персональных компьютеров в компьютерные сети, сначала в локальные, а затем в глобальные – Internet, Fidonet и др. Выстраивание информационных сетей вызвало острые дебаты о том, существует ли необходимость в отдельном законе, регулирующем информационные технологии, допустимы ли такие термины, как «киберпространство», «интернет-право» и «киберправо»[1].

Для четвертого этапа, который начался в конце XX в. и продолжается до сих пор, характерно формирование глобального информационного пространства, обеспечиваемого цифровизацией и сетевой взаимозависимостью. Информация становится ключевым коммуникативным ресурсом в международном масштабе, в создании транснациональных информационных сетевых пространств, в возникновении сетевой взаимозависимости государств и социума, в сетевом обслуживании всех видов отношений. Разработка и внедрение цифровых технологий способствовали ускорению взаимообмена и развития, с одной стороны, и глобализировали негативные виды деятельности (киберпреступность, кибертерроризм, цифровое мошеничество и пр.) – с другой.

Развитие информационных отношений, в том числе информационных цифровых технологий, в 1990-х годах и в начале нового столетия обусловило необходимость принятия немалого числа законов и иных нормативных правовых актов, направленных на их регулирование. Наличие разветвленной нормативной правовой базы позволило ученым поставить вопрос о формировании новой комплексной отрасли права – информационного права.

В 1980–1990-х годах термин «информационное право» начинает всё более широко использоваться в российской научной литературе[2], и постепенно растет число ученых, которые признают информационное право в качестве самостоятельной отрасли права[3]. С начала нового столетия в Российской Федерации публикуется широкая сеть учебников по информационному праву, обосно-

[1] См.: Cohen J. Cyberspace as/and space // Columbia law review. – 2007. – Vol. 107. – P. 210–256.

[2] См.: Готт В.С., Семенюк Э.П., Урсул А.Д. Социальная роль информатики. – М., 1987; Батурин Ю.М. Проблемы компьютерного права. – М., 1991.

[3] См.: Копылов В.А. О теоретических проблемах становления информационного права // Информационные ресурсы России. – М., 1998. – № 3. – С. 15–21.; Рассолов М.М. Информационное право. – М., 1999.

вывающих его именно как самостоятельную комплексную отрасль права, в этих учебниках соответственно даются определения данной отрасли права[1].

В современных условиях развития информационное право приобрело характер интегрированной отрасли права нового поколения[2]. Универсальная природа глобальных интегрированных отраслей права проявляется в том, что они одновременно охватывают нормы международного права и национального права. По степени значимости новое поколение отраслей права относится к типу глобального права, так как предназначено либо для противодействия глобальным вызовам и угрозам человечеству (право выживания), либо для перехода на новую реальность путем сущностного преобразования или трансформации регулируемых общественных отношений (право развития)[3].

Для глобальных отраслей права нового поколения характерно тесное соединение публичных и частных интересов при очевидном доминировании публичной значимости их правовых норм. Такое сочетание дает основание относить данные отрасли к комплексным отраслям права, т.е. смешанного типа. Главное предназначение отраслей права нового поколения – обслуживание новых или преобразованных (расширенных, модифицированных) функ-

---

[1] См.: Лапина М.А., Ревин А.Г., Лапин В.И. Информационное право. – М., 2004; Бачило И.Л., Лопатин В.Н., Федотов М.А. Информационное право / под ред. акад. РАН Б.Н. Топорнина. – СПб., 2005; Копылов В.А. Информационное право. – М., 2005; Тедеев А.А. Информационное право. – М., 2006; Кузнецов П.У. Информационное право: метод. материалы по учебному курсу. – Екатеринбург, 2006; Ястребов Д.А. Информационное право: учеб.-метод. комплекс для студентов юрид. высш. учеб. заведений. – М., 2006; Ковалева Н.Н. Информационное право России: учеб. пособие. – М., 2007; Акопов Г.Л. Информационное право. – М., 2008; Бачило И.Л. Информационное право. – М., 2009; Городов О.А. Информационное право. – М., 2009; Попов Л.Л., Мигачев Ю.И., Тихомиров С.В. Информационное право: учебник. – М., 2010; Чеботарева А.А. Информационное право: учеб. пособие. – М., 2014; Рассолов И.М. Информационное право: учебник. – 4-е изд. – М., 2015; Загородников С.Н., Шмелев А.А. Основы информационного права. – М., 2016 и др.

[2] См., напр.: Ловцов Д.А. Теория информационного права: базисные аспекты // Государство и право. – М., 2011. – № 11. – С. 43–51; Системология правового регулирования информационных отношений в инфосфере: монография. – М.: РГУП, 2016. – 316 с.

[3] Подробнее об отраслях права нового поколения см.: Умнова (Конюхова) И.А. Конституционное право и международное публичное право: теория и практика взаимодействия. – М., 2016. – С. 71–90.

ций государства. В юридической литературе постоянно обсуждается возникновение у государства всё новых функций[1], к числу которых относят информационную функцию государства[2].

В непрерывно развивающейся системе права можно было бы выделить три группы глобальных интегрированных отраслей права нового поколения: 1) сформировавшиеся, общепризнанные отрасли права; 2) интенсивно формирующиеся отрасли права; 3) обозначившие общие контуры своего развития правовые комплексы, тяготеющие в дальнейшем к оформлению в качестве отрасли права.

Информационное право относится к первой группе отраслей права нового поколения. Структура данной отрасли права представляет собой широкую систему непрерывно развивающихся, но устойчивых институтов, они предназначены для реализации определенной, ясно обозначенной информационной функции государства. В качестве основного источника информационное право имеет кодификационные акты – специальные законы (в данном случае законы об информации).

Особая значимость информационного права в современную эпоху очевидна. М.А. Кудрявцев образно сравнил информационное право с «дирижером оркестра» правовой системы, т.е. одним из важнейших ее организующих начал в информационном обществе[3].

Выделение информационного права в отдельную отрасль обосновывается наличием предмета, объекта и метода правового регулирования, а также с созданием на определенной стадии развития кодифицированного информационного законодательства.

---

[1] См.: Бобылев А.И. Функции государства: понятие, классификация, общая характеристика // Право и государство: теория и практика. – М., 2010. – № 3 (63). – С. 11.

[2] См.: Никодимов И.Ю. Информационно-коммуникативная функция государства и механизм ее реализации в современной России (теоретический и сравнительно-правовой анализ): дис. … д-ра юрид. наук. – СПб., 2001; Просвирнин Ю.Г. Информационная функция государства // Журнал российского права. – М., 2002. – № 3. – С. 29–35; Федосеева Н.Н. Влияние глобальной информатизации на функции государства // Государственная власть и местное самоуправление. – М., 2008. – № 4. – С. 9; Титов А.С. К вопросу о понятии информационной функции российского государства // Право и государство: теория и практика. – М., 2008. – № 11 (47). – С. 9–12.

[3] См.: Кудрявцев М.А. Новые горизонты информационного права // Информационное пространство: обеспечение информационной безопасности и права; сб. науч. тр. / РАН. Ин-т государства и права. – М., 2018. – С. 100.

Основным компонентом информационных отношений как объектов информационного права является информация (в переводе с латинского – ознакомление, разъяснение, изложение), по поводу которой формируется предмет правового регулирования – информационные правоотношения. В самом общем понимании информация – это сведения, несущие новые знания о чем-либо или о ком-либо. Исследователи-юристы по-разному определяют информацию, и, как правило, акцент делается на когнитивную, т.е. познавательную функцию человека. К примеру, по мнению А.Р. Алиева, «информация представляет собой систему идеальных (субъективных) образов объектов, процессов и явлений окружающего нас мира в сознании человека, а также множество признаков, присущих материи и формирующих идеальные образы»[1].

Другой важный аспект понимания информации – это ее привязанность к источнику, носителю, месту, времени и другим характеристикам ее идентификации. Иначе говоря, информация не может быть нейтральной.

А.К. Вудс (доцент юридического колледжа Кентуккийского университета) находит общие черты информации как нематериального объекта с такими традиционными объектами правового регулирования, как акции, долги, деньги, банковские счета, а также подчеркивает ее неразрывную связь с объектами материальными – устройствами, на которых она хранится и которые всегда имеют конкретное территориальное местонахождение[2]. Соответственно, для государства открыт широкий спектр оснований для распространения своей законодательной юрисдикции на поведение тех или иных лиц за рубежом, если его последствия затрагивают территорию данного государства или его граждан. При этом, по мнению А.К. Вудса, ни один тест, взятый в отдельности, не является исключительным для установления юрисдикции государства. Скорее, соответствующих критериев – множество, включая местонахождение информации, место причинения вреда, гражданство подозреваемого лица, гражданство жертвы, гражданство контролирующего информацию лица[3].

---

[1] Алиев А.Р. Международно-правовое регулирование в сфере информационного противоборства. – М., 2017. – С. 8.

[2] См.: Woods A.K. Against data exceptionalism // Stanford law review. – Stanford, 2016. – Vol. 68, N 4. – P. 756–763.

[3] См.: Ibid. – P. 766–769.

Повышение значимости информации как компонента объектов правового регулирования способствовало юридизации данного понятия. В Российской Федерации легальное понятие информации впервые было дано в Федеральном законе от 20 февраля 1995 г. № 24-ФЗ «Об информации, информатизации и защите информации», в соответствии с которым это сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления. Новый Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (далее – Закон об информации) дал более емкое и краткое понятие информации, определив ее как сведения (сообщения, данные), независимо от формы их представления.

На примере России стоит отметить, что Закон об информации стал кодифицированным информационным кодексом, вбирающим в себя основные принципы и нормы права, касающиеся информационных отношений. На данный момент в нем, в том числе с учетом поправок, дано понятие информационных технологий и информационной системы, определены условия и гарантии реализации права на информацию (в частности, тщательно прописаны случаи ограничения доступа к информации); обозначена система защиты информации с помощью правовых, организационных и технических мер. Закон об информации постоянно совершенствуется и охватывает все новые сферы правового регулирования. В частности, особый резонанс вызвал Федеральный закон от 1 мая 2019 г. № 90-ФЗ «О внесении изменений в Федеральный закон "О связи" и Федеральный закон "Об информации, информационных технологиях и защите информации"», получивший название Закон о «суверенном Рунете». Данные изменения были призваны сохранить стабильную работу Рунета на случай отключения России от Глобальной сети.

Наряду с кодификацией норм информационного права в Законе об информации, источником общих положений информационного права являются доктрины и стратегии, утверждаемые главой государства. В Российской Федерации действуют Доктрина информационной безопасности РФ (Указ Президента РФ от 5 декабря 2016 г. № 646) и Стратегия развития информационного общества в Российской Федерации на 2017–2030 гг. (Указ Президента РФ от 9 мая 2017 г. № 203). В Доктрине определены стратегические цели, информационные угрозы, основные направления и организационные основы обеспечения информационной безопас-

ности. Стратегия развития информационного общества в РФ на 2017–2030 гг. определяет цели, задачи и меры по реализации внутренней и внешней политики РФ в сфере применения информационных и коммуникационных технологий, направленные на развитие информационного общества, формирование национальной цифровой экономики, обеспечение национальных интересов и реализацию стратегических национальных приоритетов.

Закон об информации и доктринально-стратегические акты главы государства пересекаются со многими законами, где различные виды информации являются объектом услуг или защиты, затрагивают условия и информационные технологии реализации политических, экономических, социальных и культурных прав (например, федеральные законы: от 13 марта 2006 г. № 38-ФЗ «О рекламе», от 27 июля 2006 г. № 152-ФЗ «О персональных данных», от 29 декабря 2012 г. № 273-ФЗ «Об образовании в Российской Федерации», от 29 июля 2004 г. № 98-ФЗ «О коммерческой тайне», от 21 ноября 2011 г. № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации» (тайна медицинской деятельности), а также Закон РФ» от 21 июля 1993 г. № 5485–1 «О государственной тайне» и др.).

Таким образом, в развитии информационного права в Российской Федерации просматриваются *две тенденции*: 1) кодификация основных положений в едином законе об информации и стратегически-доктринальных актах; 2) распространение принципов и норм информационного права по видам информационной деятельности в различных отраслях права и сферах правового регулирования. Аналогичные процессы развития информационного права характерны и для других стран.

В силу всеобъемлющего характера информации информационные отношения затрагивают самые различные сферы правового регулирования. Это обусловливает тесное взаимодействие информационного права с другими отраслями права. Базовыми отраслями права, регулирующими отношения, связанные с информационной деятельностью, являются конституционное право и административное право. Новые механизмы электронных финансовых расчетов испытывают потребность во внесении соответствующих дополнений в финансовое право. Институт интеллектуальной собственности относится одновременно к информационному и к гражданскому праву, институт правовой охраны информации и защиты от инфор-

мационных правонарушений касается административного и уголовного права.

По мнению современных исследователей, требуется формирование институтов, в рамках которых можно будет обеспечивать функционирование цифровой среды доверия и идентификацию субъектов в ней, внедрять искусственный интеллект и роботов, принимать решения на основе больших данных (Big data) и функционирования Интернета вещей и многое другое. В системе права всё чаще наблюдается негативная конкуренция отраслей, когда нормы из одной отрасли права попадают в законодательство другой отрасли права[1].

Являясь интегрированной отраслью права, информационное право использует методы, характерные для различных отраслей. Информационному праву присущи как императивные, так и диспозитивные методы правового регулирования. В информационном праве используются такие императивные методы, как предписания (например, в государственном управлении в сфере информации, использование информации с особым правовым режимом) и запреты (обязанность воздерживаться от совершения каких-либо деяний, представляющих собой информационные правонарушения). Императивность информационного права не подавляет, однако, его диспозитивные начала. В нем широко используются дозволения (права совершать какие-либо действия либо не совершать их по своему выбору); поощрения (рекомендует модель поведения и предоставляет какие-либо льготы или иные блага при ее выборе); рекомендации (например, при регулировании деятельности средств массовой информации в сети Интернет); согласования (для достижения какого-либо согласия, например, в сфере регулирования интеллектуальной собственности); иные диспозитивные методы правового регулирования.

Расширение норм права, регулирующих общественные отношения, обусловленное развитием информационных технологий, предопределило развитие двух параллельно развивающихся тенденций: *дифференциацию и глобализацию информационного права.*

Дифференциация информационного права обусловлена межотраслевым, комплексным характером информации и инфор-

[1] См.: Наумов В.Б. Право в эпоху цифровой трансформации: в поисках решений // Рос. право: образование, практика, наука. – 2018. – № 6. – С. 4–6.

мационных отношений. Можно выделить *три направления дифференциации информационного права*:

1) формирование новых подсистем информационного права – подотраслей и институтов, к которым можно отнести кибернетическое право, цифровое право, интернет-право (сетевое право), право информационной безопасности, информационные права человека, информационная ответственность и др.;

2) внутри традиционных отраслей права появились блоки норм и институты, связанные с информационными отношениями. Например, в уголовном праве – это «уголовная ответственность за киберпреступления», в финансовом праве и предпринимательском праве – новые цифровые технологии обслуживания денежно-финансовых потоков (биткойны, криптовалюта, блокчейн-технологии)»[1], в гражданском и предпринимательском праве – «цифровая экономика», в конституционном праве – «электронная демократия», «электронное голосование» и т.д.;

3) появились такие новые сферы правового регулирования информационных технологий, как биоинженерия, нанотехнологии, робототехника, искусственный интеллект, многомерная визуализация и др.

Дифференциация информационных прав человека в условиях цифровизации проявилась в формировании целой группы так называемых цифровых прав: на доступ в Интернет, на изображение (ст. 1521 ГК РФ), право на забвение. В информационном обществе свобода слова, право на информацию и доступ к ней трансформировались в универсальный товар, состоящий из данных о человеке и его сообщений в сети Интернет[2]. В этих условиях, как замечает Э.В. Талапина, проблема обеспечения прав человека в цифровом мире выходит на первый план[3].

По мнению экспертов, среди современных прорывных технологий самыми востребованными в условиях четвертой промышленной революции являются технологии, связанные с созданием и использованием роботов и искусственного интеллекта. Активно

---

[1] Подробнее об этом см., например: Beyond bitcoin – legal impurities and off-chain assets / Reed Ch., Sathyarayan U., Ruan Sh., Collins J. // International journal of law and information technology. – Oxford, 2018. – Vol. 26, N 2. – P. 160–182.

[2] См.: Родимцева М.Ю. Регулировать нельзя манипулировать (о рисках информационного общества) // Государство и право. – М., 2016. – № 7. – С. 72.

[3] См.: Талапина Э.В. Право и цифровизация: новые вызовы и перспективы // Журнал российского права. – М., 2018. – № 2. – С. 8.

формирующаяся робототехническая отрасль, обширные исследования технологий искусственного интеллекта и ожидаемое проникновение роботов во многие сферы общественной жизни, включая военную, уже сейчас требуют от мирового сообщества, правовой науки и юридической практики дать ответы на многочисленные прикладные и теоретические вопросы[1].

Одновременно с дифференциацией информационное право непрерывно глобализируется на международно-правовом уровне, т.е. государствами и международными организациями разрабатываются общие правовые информационные стандарты. Вместе с тем на данном этапе международное информационное право, рассматриваемое как совокупность правовых норм, регулирующих информационно-правовые отношения между государствами, в отличие от внутринационального права, идет по пути регламентации различных информационных аспектов в других отраслях и сферах правового регулирования. Оно как бы пронизывает их содержание и определяет те международно-правовые стандарты, которым следуют затем в своем внутреннем законодательстве государства мирового сообщества.

В частности, Всеобщая декларация прав человека 1948 г. закрепила право человека на информацию независимо от государственных границ, Международный пакт о гражданских и политических правах 1966 г. сформулировал принципы допустимости ограничения свободы информации в целях охраны государственной безопасности, здоровья и нравственности населения.

Началом глобальной кодификации международного информационного права можно считать Международные принципы создания информационного общества. В настоящее время они определены «мягким правом»: Окинавской хартией глобального информационного общества (2000), Декларацией принципов «Построение информационного общества – глобальная задача в новом тысячелетии» (2003), Планом действий Тунисского обязательства (2005).

Наиболее острые задачи противодействия вызовам современного технотронного общества – обеспечение кибербезопасности и противодействие киберпреступности – постепенно получают отражение в международном информационном праве. В 2002 г. под эгидой ООН был принят документ «Элементы для создания

[1] См.: Наумов В.Б. Указ соч. – С. 7.

глобальной культуры кибербезопасности». В 2003 г. ГА ООН выразила озабоченность ростом преступности в сфере информационных технологий, их трансграничным характером, заявлена необходимость принятия скоординированных международных мер для их предотвращения. В апреле 2005 г. состоялся III Международный конгресс по борьбе с киберпреступностью в целях поиска средств минимизации угроз в киберпространстве. На 11 Конгрессе ООН по предупреждению преступности и уголовному правосудию (2005) киберпреступность была поставлена в один ряд с международным терроризмом. В июле 2018 г. в Москве прошел I Международный конгресс по кибербезопасности, в работе которого приняли участие делегаты из 51 страны: России, США, Германии, Великобритании, Швейцарии, Турции, Японии, Китая и др.[1]

Наряду с универсальным международным информационным правом интенсивно развивается региональное информационное право. Наиболее ярко эта тенденция представлена в европейском праве. Так, в рамках Совета Европы приняты конвенции: о защите личности в связи с автоматической обработкой персональных данных 1981 г.; о преступности в сфере компьютерной информации 2001 г. (Конвенция о киберпреступности), а также Дополнительный протокол к ней 2002 г., который касается уголовной ответственности за криминализацию действий расистского и ксенофобного характера, совершаемых через компьютерные системы.

В 2005 г. Комитетом министров Совета Европы была принята Декларация о свободе выражения мнений и информации в СМИ в контексте борьбы с терроризмом, в которой подчеркивается, что свободное и беспрепятственное распространение информации является одним из наиболее действенных средств укрепления взаимопонимания и терпимости, способных помочь предупреждению терроризма и борьбе с ним. В Рекомендации Парламентской ассамблеи Совета Европы от 2005 г. № 1706 «Средства массовой информации и терроризм» отмечается, что терроризм не должен посягать на свободу слова в средствах массовой информации как на один из основополагающих принципов демократического общества.

Вышеуказанные процессы дифференциации и глобализации между собой взаимосвязаны и в свою очередь обусловлены преоб-

[1] См.: Международный конгресс по кибербезопасности. – URL: https://www.sberbank.com/ru/responsibility/cybersecurity (дата доступа: 24.01.2020)

разованием технократического общества в технотронное цифровое общество нового поколения. В таком обществе широкое распространение получила «сетевая коммерция» (e-Commerce, интернет-бизнес и др.), являющаяся интегральной частью сетевой экономики[1]. В современную обыденную жизнь стремительно вживаются интернет-технологии, электронная торговля, электронные платежи, электронный контроль, электронные госуслуги и пр. Доля интернет-экономики в ВВП государств неуклонно повышается.

Универсальная значимость Интернета как средства, обеспечивающего реализацию прав человека, актуализировало задачу обеспеченности права граждан на доступ к Интернету. Право на доступ к Интернету, по мнению Н.В. Варламовой, может рассматриваться как одно из новых проявлений индивидуальной свободы – свободы доступа в виртуальную среду (цифровое пространство) и функционирования в ней[2].

Право на доступ к Интернету не получило пока всеобщего признания на национальном и международно-правовом уровне и регулируется точечно. В настоящее время право на доступ к Интернету напрямую закреплено в ч. 6 ст. 35 Конституции Португалии (в ред. 2008 г.): «Каждому гарантирован свободный доступ к информационным сетям общего пользования». При этом в Конституции отдельно гарантируются свобода выражения и свобода информации, а также свобода прессы и других средств массовой информации (ст. 37–39). Частично право на информацию в новых условиях цифровизации и развития электронного сетевого пространства формулируется в Конституции Греции: все лица имеют право участвовать в информационном обществе; облегчение доступа к информации, передаваемой в электронном виде, а также ее производства, обмена и распространения признано обязанностью государства, которая реализуется при соблюдении гарантий прав на защиту персональных данных (ст. 5 А).

Правовая возможность доступа к Интернету определяется в законах об информации некоторых государств. Так, п. 33 «Доступ

---

[1] См.: Брацун Д.А. Сетевая экономика: учеб. пособие. – Пермь, 2013. – С. 87. – URL: http://diss.seluk.ru/m-informatika/30002617–1-d-bracun-setevaya-ekonomika-uchebnoe-posobie-dlya-studentov-ochnoy-zaochnoy-form-obucheniya-perm-2013-udk-bbk-recenzent-zaveduyusch.php (дата доступа: 15.02.2020).

[2] См.: Варламова Н.В. Цифровые права – новое поколение прав человека? // Тр. Ин-та государства и права РАН. – М., 2019. – Т. 14, № 4. – С. 35.

к сети передачи данных» в Законе Эстонии о публичной информации от 15 ноября 2000 г.[1] предусматривает, что каждому человеку должна быть предоставлена возможность иметь свободный доступ к публичной информации через Интернет в публичных библиотеках. Общий характер обязательств государства по обеспечению доступа к Интернету устанавливает Закон Испании об устойчивой экономике 2011 г., который предусматривает предоставление универсальной услуги соединения, обеспечивающего широкополосную передачу информации со скоростью 1 *Мбит в секунду*.

На международно-правовом уровне задачи обеспечения доступа к Интернету определены в Резолюции ГА ООН от 25 сентября 2015 г. N A/RES/70/1 «Преобразование нашего мира: Повестка дня в области устойчивого развития на период до 2030 года».

В рамках цели № 9 «Создание стойкой инфраструктуры, содействие всеохватной и устойчивой индустриализации и инновациям» предполагается «существенно расширить доступ к информационно-коммуникационным технологиям и стремиться к обеспечению всеобщего и недорогого доступа к Интернету в наименее развитых странах к 2020 году».

Показатели свободы доступа к Интернету содержатся в Приложении к Рекомендации Комитета министров Совета Европы государствам-членам о свободе Интернета от 13 апреля 2016 г. В частности это: предоставление пользователям программ цифровой грамотности, чтобы повысить их способность принимать обоснованные решения и уважать права и свободы других лиц; способствование доступу к просветительскому, культурному, научному, образовательному и другому контенту и его организация для населения пунктов доступа к Интернету в учреждениях, поддерживаемых государственной администрацией, образовательными организациями или частными лицами; принятие разумных мер для обеспечения доступа к Интернету лиц с низким уровнем дохода, лиц, проживающих в сельских или географически отдаленных районах, а также лиц с особыми потребностями, например, с ограниченными возможностями здоровья.

В современной международно-правовой и конституционной практике обращают на себя внимание технологическое выделение

[1] Public Information Act // Riigi Teataja. – URL: https://www.riigiteataja.ee/en/eli/ee/Riigikogu/act/518012016001/consolide (дата доступа: 14.02.2020).

доступа к информации и ее распространение двумя каналами: *online* (т.е. электронным путем) и *offline.* Система *online* выделяется не только в законах, но и в решениях судебных и квазисудебных органов. Так, Конституционный совет Франции в решении от 10 июня 2009 г.[1] отметил, что Декларация прав человека и гражданина 1789 г. провозглашает свободное распространение идей и мнений одним из самых ценных прав человека; это означает, что в нынешнем состоянии средств коммуникации и с учетом общего развития публичных *online*-коммуникационных услуг и их значимости для участия в демократических процессах и выражения идей и мнений это право предполагает свободу доступа к таким услугам. Данное решение Конституционный совет вынес, рассматривая законопроект, который предусматривал возможность приостановления доступа к Интернету лиц, неоднократно нарушающих права интеллектуальной собственности посредством распространения в Интернете нелегальных копий объектов авторских прав. Заявители утверждали, что установленная законодателем санкция, предусматривающая приостановление доступа к Интернету, не учитывает фундаментальный характер свободы выражения и коммуникации и является очевидно несоразмерной. Таким образом, Конституционный совет признал доступ к Интернету одним из необходимых в современных условиях способов реализации свободы выражения мнений.

Аналогичные обязательства признала за государством и Конституционная палата Верховного суда Коста-Рики, отметив в решении от 18 июня 2010 г. N 2010–10627, что отказ по техническим причинам в предоставлении государственной услуги по широкополосному доступу к Интернету нарушает основные права заявителя на коммуникацию и информацию, и обязала соответствующие службы продолжить предоставление данной услуги[2].

Растущая интенсивность информационного движения товаров, капитала и услуг, с одной стороны, упрощает нашу жизнь, экономит время человеческой жизнедеятельности, ускоряет про-

---

[1] Decision n° 2009–580 DC du 10 juin 2009 // Conseil constitutionnel. – URL: https://www.conseil-constitutionnel.fr/decision/2009/2009580DC.htm (дата доступа: 14.02.2020).

[2] См.: La Sala Constitucional ordena brindar servicio de internet. SC-CP–26 – 10. San Jose, 18 de junio de 2010 // Sala Constitucional Republica de Costa Rica. – URL: https://salaconstitucional.poder-judicial.go.cr/index.php/jurisprudenciasec (дата доступа: 14.02.2020)

цессы взаимообмена и доступа к информации. С другой стороны, человечество столкнулось с такими негативными явлениями, как «информационные войны», «информационный терроризм», «киберпреступность», «информационное мошеничество», «сетевые угрозы», «глобальное электромагнитное излучение» и др.

Средства, предоставляемые информационно-коммуникационными технологиями, и их преимущества были незамедлительно адаптированы многими государствами в военных целях. В политический и научный оборот вошли понятия «кибероружие», «кибератаки» и «кибервойна». К примеру, Киберстратегия Министерства обороны США 2015 г. устанавливает, что США будут применять киберсредства ведения войны как часть наступательных военных операций, а также как часть секретных операций в отношении потенциальных угроз. При определенных обстоятельствах Вооруженные силы США могут использовать киберсредства для разрушения военных систем противника, чтобы предотвратить их применение против национальных интересов США, т.е. в превентивных целях[1].

В условиях интенсивной цифровизации общества возникли также серьезные проблемы злоупотребления информацией, вторжения в личное пространство и массовые нарушения достоинства пользователей информацией. Это в свою очередь обусловило необходимость появления таких институтов права, как «информационная безопасность», «кибербезопасность», «информационная ответственность», «защита персональных данных», «электронное правосудие»[2] и др.

Интернет – не просто компьютерная сеть, возможность обмена информацией и распространения знаний. Это еще и возможность ограничения свободы и злоупотребления свободой. В этом контексте формируется правовое понятие «электронные ограничения прав и свобод».

Ф. Галиндо и Х.Г. Марко выделяют три вида такого ограничения:

---

[1] См.: Singer P., Friedman A. Cybersecurity and cyberwar: What everyone needs to know. – Oxford, 2014.

[2] Об электронном правосудии см., например: Сас В.В. «Электронное правосудие» как элемент «сетевого общества»: теоретические проблемы // Юридическая наука. – М., 2012. – № 2. – С. 101–104.

– ограничение свободы выражения мнения (при этом следует принимать во внимание, что защита одних прав и свобод может оказывать прямой и немедленный эффект на другие права и свободы);

– экономические ограничения (доступ в Интернет подразумевает наличие определенных устройств и возможности платить за услуги, что доступно не каждому);

– ограничение политических свобод (оно может быть достигнуто с легкостью как государственными, так и негосударственными акторами; к примеру, Китай и Турция в значительной мере регулируют доступ к определенным интернет-ресурсам, включая и те, что выкладываются в Сеть, и те, к которым могут получить доступ пользователи)[1].

Думается, однако, что это не полный перечень, и он будет непрерывно развиваться.

Ответом на сложное и противоречивое информационное развитие должно стать повсеместное совершенствование законодательного регулирования информационных отношений, а также правоприменительной, в том числе судебной практики разрешения информационных споров, включая споры, связанные с использованием информационных технологий. Современные исследователи практики информационного правотворчества и правоприменения выявляют общие потребности правового регулирования и обозначают перспективы его совершенствования.

В частности, распространение информационно-коммуникационных технологий и связанные с этим нарушения прав граждан собственниками компьютерных систем, ответственными за управление базами данных, привело к осознанию необходимости защиты данных. Практика защиты в США и в Европе пошла в разных направлениях[2].

Первое дело, рассматриваемое в Верховном суде США, было разрешено не на основании специального положения закона (по причине отсутствия такового), а на основании прецедента, касавшегося вмешательства в частную жизнь. В Европе государствами были приняты профильные законы, направленные на защиту лич-

[1] См.: Galindo F., Marco J.G. Freedom and the Internet: Empowering citizens and addressing the transparency gap in search engines // European journal of law and technology. – 2017. – Vol. 8, N 2. – P. 8.

[2] См.: Ibid. – P. 10.

ных данных. В каждой стране ЕС были учреждены отделы защиты данных (Data Protection Office), перед которыми отчитываются как государственные органы, так и операторы баз данных. Приняты процедуры, позволяющие отдельным лицам делать запросы относительно своей личной информации и ее использования, а также обжаловать действия операторов баз данных. Эксперты отмечают, что столь разный подход к регулированию свободы в Интернете неизбежно сказывается и на развитии технологий, что приводит к конфликту между разработанными в США программами (использующими такие механизмы сбора информации о пользователе, как «кукисы» (cookies)) и регулированием рассматриваемых прав в Европе[1].

Актуальные проблемы правового регулирования воздействия «больших данных», компьютерных алгоритмов, искусственного интеллекта и машинного обучения на конкурентные рынки, общее благосостояние потребителей, идеалы демократии и неприкосновенность частной жизни поднимаются в книге А. Эзраки и М.Э. Штука[2]. Они обращают внимание на то, как цифровые технологии меняют традиционную динамику конкуренции и создают принципиально новую экономическую среду. Виртуальная конкуренция выявляет проблемы антиконкурентной динамики ввиду использования новых алгоритмов и технологий. На первый взгляд, онлайн-рынки имеют все признаки конкурентных рынков: минимальные затраты и низкие барьеры для входа новых участников. Однако за этим «фасадом конкуренции» находится множество стратегий, основанных на сети сложных алгоритмов, способствующих максимизации прибыли в ущерб общественному благосостоянию. К примеру, Google, столкнувшись с интенсивным антимонопольным контролем в 2011 г., напрямую профинансировала ряд научных исследований, которые выявили интенсивную конкуренцию в отрасли, и отправила эти публикации государственным органам в целях оправдания своей деятельности. Исследователи высказывают опасения по поводу способности государственных органов справиться с негативными последствиями современных технологий и, осознав ценности персональных данных, защитить конфиденциальность потребителей. Для этого, по

[1] См.: Galindo F., Marco J.G. Op. cit. – P. 12–18.

[2] См.: Ezraphi A., Stupke M.E. Virtual competition: The promise and perils of the algorithm-driven economy. – Harvard, 2016.

их мнению, необходимы серьезные независимые эмпирические исследования[1].

Основные направления реструктуризации кибернетического права с учетом появления новых информационных сфер правового регулирования представлены в монографии «Переосмысление киберправа: Новое ви□дение интернет-права» Жаклин Липтон, директора Центра интеллектуальной собственности, права и технологий Школы права Университета Акрона (США)[2]. Она отмечает, что генеалогия развития информационных отношений проявилась в расширении цифрового ландшафта, появлении персональных данных как движущей силы инноваций в экономике, а также умных технологий (рейтинги поисковых систем, социальные логины, интернет-рынки и блокчейны), которые облегчают обмен контентом и взаимодействие. В то же время Липтон обращает внимание на появление интернет-элит, бизнес-модели которых обеспечивают контроль над рынками в своих интересах.

У экспертов вызывают озабоченность недобросовестная конкуренция в информационной среде, деятельность хакеров и электронные манипуляции[3]. Отсюда выдвигаются задачи переоценки роли законодательных и судебных органов, достижения интеллектуальной согласованности и управляемости[4]. Актуальное значение имеют модернизация правового регулирования авторского права и товарных знаков; правовое противодействие диффамации (распространение порочащих сведений) и онлайн-виктимизации, обеспечение конфиденциальности[5].

Близкую позицию по необходимости дальнейшей модернизации информационного и кибернетического права занимают Мэйв Макдон и Микаил О'Дауд в книге «Кибернетическое право в Ирландии»[6]. Среди институтов и актуальных проблем информа-

---

[1] См.: Ezraphi A., Stupke M.E. – Op. cit.

[2] См.: Lipton J. Rethinking cyberlaw: A new vision for Internet law. – Cheltenham, 2015.

[3] См.: See European Commission Antitrust: Commission Sends Statement of Objections to Google on Comparison Shopping Service (2015). – URL: http://europa.eu/rapid/press-release_MEMO-15-4781_en.htm (дата обращения: 12.01.2020)

[4] См.: Goldman E. Teaching cyberlaw // Saint Louis univ. law journal. – 2008. – N 52. – P. 749–764.

[5] См.: Lipton J. Op. cit. – P. 135, 160.

[6] См.: McDonagh M., O'Dowd M. Cyber law in Ireland. – Alphen aan den Rijn, 2015.

ционного права ими выделяются как материальные (авторское право и смежные права, телекоммуникации, законодательство о конкуренции, криптография, стандартизация и пр.), так и процессуальные вопросы (разрешение внесудебных споров, расследования киберпреступлений, судебное разбирательство по обмену файлами и блокированию Интернета).

М. Макдон и М. О'Дауд обращают внимание на электронные сделки и их реализацию в контексте действия ирландского Закона о правовом статусе электронных сделок, электронных подписей, электронных банковских услуг и защиты прав потребителей. Констатируется почти полное отсутствие ирландского прецедентного права в этих областях. В противоположность этому по посреднической ответственности в контексте диффамации и нарушения авторских прав в Ирландии состоялось значительно больше судебных разбирательств, что способствовало формированию внутреннего прецедентного права. В отношении киберпреступности авторы считают важным рассматривать в единстве основные правонарушения и процессуальные нормы, касающиеся их исполнения (такие, как право требовать расшифровки данных)[1].

На примере Ирландии видно, что в целях обеспечения конституционного права на частную жизнь создается развитое законодательство и широкая судебная правоприменительная практика по защите конфиденциальности. Существуют, однако, расхождения ирландского законодательства с требованиями Директивы ЕС N 95/46 «О защите данных», принятой в 1995 г. Данная Директива рассматривается Европейским союзом в качестве важнейшего компонента защиты частной жизни и прав человека. Указанные расхождения характерны и для других стран, так как касаются вопросов нахождения баланса между государственной безопасностью и вторжением в частную жизнь.

Правовая ответственность в информационной сфере тесно связана с этическими аспектами. Развитие фейковой информации, оскорбление и клевета «на весь свет» через соцсети, сложность верификации информации в Интернете, появление в соцсетях неконтролируемой личностной информации без согласия ее носителей – все эти проблемы обусловливают необходимость решения задач обеспечения достоверности сетевой информации, защиты

[1] См.: McDonagh M., O'Dowd M. Op. cit. – P. 330–334.

чести, достоинства и доброго имени, выявления правонарушителей и привлечения к ответственности.

«Учитывая громадный объем информации, проходящей через Интернет, – отмечает Э.В. Талапина, – у каждого человека появилась возможность оставить свой цифровой след. Но ведь далеко не все люди хотят этого. Из данной гипотезы родилось право на забвение (right to be forgotten), закрепленное в законодательстве ряда государств, в том числе в России»[1]. К этому добавилось и право на цифровую смерть. Оно предусмотрено, к примеру, французским Законом о цифровой республике (государстве) от 7 октября 2016 г. Как при завещании, лицо будет иметь право на соблюдение его воли по поводу дальнейшей судьбы своей персональной информации, опубликованной онлайн после его кончины поставщиками онлайн-услуг или доверенными лицами. Это означает, что права субъекта в определенной мере «продляются» после его смерти посредством Интернета.

Показательно, что изначально специалисты в области киберправа исходили из того, что киберпространство находится вне досягаемости и контроля как правительств, так и традиционной индустрии[2], к нему неприменимо традиционное право, виртуальный мир может быть подвержен лишь децентрализованному саморегулированию[3] и воздействию технологических устройств[4]. Однако возможности и угрозы, заложенные в интернет-технологии, заставили пересмотреть эти подходы. Признание доступа к Интернету в качестве права человека и необходимости обеспечения *online* всех традиционных прав человека закладывает надлежащие основы для правового регулирования отношений в цифровом пространстве.

---

[1] См.: Талапина Э.В. Указ. соч. – С. 8.

[2] См.: A Declaration of the Independence of cyberspace // Crypto anarchy, cyberstates, and pirate utopias / Ed. by P. Ludlow. – Cambridge, 2001. – P. 28. – URL: https://monoskop.org/images/4/42/Ludlow_Peter_Crypto_Anarchy_Cyberstates_and_Pirate_Utopias.pdf (дата обращения: 12.03.2020).

[3] См., напр.: Hardy I.T. The proper legal regime for «cyberspace» // University of Pittsburgh law review. – 1994. – Vol. 55. – P. 1015–1055; Johnson D.R., Post D.G. Law and borders – The rise of law in cyberspace // Stanford law review. – 1996. – Vol. 48, N 5. – P. 1367, 1387–1391; Perritt H.H. Cyberspace self-government: Town hall democracy or rediscovered royalism? // Berkeley technology law journal. – 1997. – Vol. 12, N 2. – P. 413, 419.

[4] См., напр.: Reidenberg J.R. Lex informatica: The formulation of information policy rules through technology // Texas law review. – 1998. – Vol. 76, N 3. – P. 553, 555.

Среди стран, чей опыт информационно-правового регулирования и судебной практики широко представлен в правовой науке, следует отметить США, которые интенсивно развивают и законодательную, и судебную правоприменительную деятельность в информационной сфере. При этом особое внимание уделяется вопросам защиты достоинства при пользовании информацией и ее распространении. В этом контексте интерес представляет статья Джеффа Коссеффа «Постепенная эрозия закона, который сформировал Интернет: Эволюция 230 раздела за два десятилетия»[1].

В 1996 г. Конгресс США, как известно, принял статут под названием Закон о соблюдении приличий в средствах коммуникации (Communications Decency Act – CDA). Дж. Коссефф считает, что хотя Верховный суд страны в решении по делу *Reno vs American Civil Liberties Union* отменил большую часть этого Закона через год после его принятия, однако одна статья – 230, которая осталась, оказала большее влияние на развитие современного Интернета. Ее влияние, по мнению Дж. Коссеффа, в первую очередь проистекает из следующего положения: «Ни один поставщик или пользователь интерактивной компьютерной услуги не должен рассматриваться как издатель или докладчик какой-либо информации, предоставленной другим поставщиком информационного контента». Дж. Коссефф замечает, что эта норма существенно изменила правовой ландшафт Интернета. Она означает, что вебсайты, приложения, интернет-провайдеры (ISP), компании социальных сетей и другие поставщики онлайн-услуг не должны нести ответственность за диффамацию, вторжение в частную жизнь и за практически любой иск, который возникает из пользовательского контента. Дж. Коссефф пишет, что трудно представить себе современные социальные сети и краудсорсинговые сайты в мире без этого раздела. Статья 230 CDA содержит лишь несколько исключений, позволяющих рассматривать интерактивные компьютерные услуги в качестве издателей или носителей контента. Эти узкие исключения охватывают нарушения федерального уголовного законодательства, законодательства об интеллектуальной собствен-

[1] См.: Kosseff J. The gradual erosion of the law that shaped the Internet: Section 230's evolution over two decades // The Columbia science & Technology law review. – N.Y., 2016. – Vol. 18, N 1. – P. 2–41. – URL: file:///C:/Users/Администратор/Downloads/SSRN-id3225774%20(1). pdf (дата обращения 04.02.2020).

ности и Закона о конфиденциальности электронной почты (Email Privacy Act)[1].

Рассмотренные Дж. Коссеффом судебные дела, связанные со ст. 230 в период с 1 июля 2015 г. по 30 июня 2016 г., позволили установить, что примерно в половине случаев суды отказывались полностью предоставить иммунитет по ст. 230. Чаще всего суды приходили к выводу, что интернет-провайдер фактически создал и опубликовал контент. Автор считает, что через 20 лет после того, как Конгресс принял ст. 230, и восемь лет с момента вынесения судебного решения *Fair Housing Council of San Fernando Valley vs Roommates.com,* ст. 230 остается сильным щитом для поставщиков онлайн-услуг во многих случаях. Однако, поскольку количество пользовательского контента в последние годы значительно возросло, суды постепенно уменьшили иммунитет для онлайн-посредников и расширили лазейки, которые позволяют истцам выигрывать дела.

Актуальные вопросы в сфере правового регулирования ответственности интернет-посредников, исследуются также в книге Джаани Риордана (Школа права и социальной справедливости Ливерпульского университета)[2]. Им рассматриваются вопросы, связанные со значительным ростом посреднических коммуникаций и услуг после принятия в 2000 г. Директивы ЕС об электронной торговле. Особое внимание Дж. Риордан уделяет таким новым элементам в процедуре ответственности интернет-посредника, как судебные постановления, так называемые «the Norwich Pharmacal Order»[3], и идентификация личности. Риордан анализирует дела (*CTB vs News Group Newspapers Ltd* («*Big Brother celebrity*»), *Jeremy Clarkson vs Alexandra Hall* и *Applause Store Productions Ltd & Anor vs Raphael* и др.), а также описывает некоторые методы оценки риска, которые могут быть связаны со «спекулятивным выставлением счетов», массовым и неизбирательным раскрытием ин-

[1] См.: Kosseff J. The gradual erosion of the law that shaped the Internet: Section 230's evolution over two decades // The Columbia science & Technology law review. – N.Y., 2016. – Vol. 18, N 1. – P. 2–41. – URL: file:///C:/Users/Администратор/Downloads/SSRN-id3225774%20(1). pdf (дата обращения 04.02.2020).

[2] См.: Riordan J. The liability of Internet intermediaries. – Oxford, 2016.

[3] The *Norwich Pharmacal Order* – судебное постановление, требующее раскрытия документов или информации, которая доступна в Соединенном Королевстве. Оно выносится в отношении третьих лиц, которые безвинно замешаны в правонарушениях, и обязывают их разглашать документы или информацию.

формации, не наносящей ущерб физическим лицам, или обременительные расходы[1].

Напряженность между доступом к информации и контролем за ним особенно остро ощущается в тех случаях, когда это касается безопасности детей. Дж. Риордан анализирует дискуссии о безопасности детей и их доступа к неприемлемой или незаконной информации, раскрывает важную роль Коалиции детских благотворительных организаций по безопасности Интернета, которая призвала правительство Великобритании расширить полномочия интернет-посредников по блокированию и фильтрации контента. По результатам публичных слушаний, организованных Комиссией ЕС по вопросам нормативно-правовой среды для платформ, онлайновых посредников, облачных технологий, экономического сотрудничества, состоявшихся 24 сентября 2015 г., предложено внести некоторые изменения в Директиву об электронной торговле, которая в настоящее время определяет роль и ответственность посредников по конкретным типам контента[2].

Интенсивное развитие законодательства и судебной правоприменительной практики государств позволяет в современный период выйти на системное решение задач формирования международно-правовой базы информационного права. «Информационно-коммуникационные технологии (ИТ) являются одним из наиболее важных факторов, влияющих на формирование общества XXI века, – говорится в Окинавской хартии глобального информационного общества, принятой главами государств и правительств “Группы восьми” 22 июля 2000 г. – Их революционное воздействие касается образа жизни людей, их образования и работы, а также взаимодействия правительства и гражданского общества. Информационные технологии быстро становятся жизненно важным стимулом развития мировой экономики. Они также дают возможность частным лицам, фирмам и сообществам, занимающимся предпринимательской деятельностью, более эффективно и творчески решать экономические и социальные проблемы. Государства должны сделать так, чтобы информационные технологии служили достижению взаимодополняющих целей обеспечения устойчивого роста, повышения благосостояния, стимулирования социального согласия и полной реализации их потенциала в области укрепле-

[1] Riordan J. Op. cit. – P. 87–112.
[2] Ibid. – P. 110.

ния демократии, транспарентного и ответственного управления, прав человека, развития культурного многообразия и укрепления международного мира и стабильности»[1]. Достижение этих целей и решение возникающих проблем потребует разработки новых эффективных национальных и международных правовых стратегий информационного развития общества и проведения работы по углубленной кодификации норм информационного права.

2.2. Информационная безопасность в информационном обществе: Концептуальные и правовые аспекты

В настоящее время состояние информационной безопасности личности, общества и государства определяется, главным образом, двумя основными факторами: информационно-психологической удовлетворенностью потребностей граждан и негативными (преднамеренными и случайными) информационно-психологическими и информационно-техническими воздействиями.

В связи с этим под *информационной безопасностью* (в «широком» смысле слова) можно понимать *защищенность* потребностей и интересов граждан, отдельных групп и социальных слоев, массовых объединений людей и населения в целом, а также персонала эргатических систем (эргасистем[2]) и их компонентов в качественной (ценной) информации, необходимой для их нормального (устойчивого) функционирования (жизнедеятельности) и развития (обучения). К сожалению, в отечественном законодательстве пока закреплено лингвистически некорректное определение через «*состояние* (мгновенная характеристика объекта, обеспечивающая определение его свойств в конкретный момент времени и определяемая входными управляющими и возмущающими воздействиями и начальными условиями функционирования) *защищенности»*,

[1] См.: Окинавская хартия глобального информационного общества. – URL: http://www.kremlin.ru/supplement/3170 (дата доступа: 10.02.2020).

[2] *Эргатическая система* (эргасистема) – сложная человеко-машинная система управления (регулирования) объектами технических, технологических, экономических и организационно-правовых комплексов.

т.е. одно-единственное – идеальное, а значит, практически недостижимое состояние[1].

В условиях стремительного развития структур информационного общества («электронного» и «цифрового» государства, «электронного» правительства, «электронного» правосудия и др.), создания и широкого внедрения эффективных компьютерных («цифровых») средств и технологий с элементами «искусственного интеллекта», возникновения принципиально новых информационных отношений и правоотношений все большее значение приобретают способы и методы решения сложных многоаспектных проблем обеспечения информационной безопасности личности, общества и государства.

Проблема информационно-психологической безопасности. Сложность данной проблемы обусловлена, главным образом, разнородностью потребностей и различным уровнем развития составляющих социум индивидуумов. Потребности каждой личности связаны с такими специфически человеческими свойствами, как активность, мотивация, целеполагание, интенция (направленность), установки (механизмы регуляции деятельности), эмоции.

Гармонизация всех компонентов личности – сложный процесс ее развития. Истинной уравновешенности личностных структур практически можно достичь не ранее среднего возраста в результате постоянного приобретения знаний и жизненного опыта. В течение этого срока личность как *информационный деятель*[2] может вступать в различные информационные отношения (сотрудничества, соперничества, защиты, изоляции) и подвергаться прямо или косвенно деструктивным информационным воздействиям с применением так называемого «*информационного оружия*», которое в информационном обществе практически достигло «совершенства».

Согласно известной[3] модели личности (сознания) как основного объекта информационного воздействия можно к видам «ин-

---

[1] См.: Ловцов Д.А. Системология правового регулирования информационных отношений в инфосфере: архитектура и состояние // Государство и право. – М., 2012. – № 8. – С. 16–25.

[2] *Информационный деятель* – носитель определенного мировоззрения, политико-правовых взглядов и моральных ценностей; создатель и пользователь информационной базы эргасистем; элемент принятия управленческих решений и др.

[3] См.: Ловцов Д.А., Сергеев Н.А. Управление безопасностью эргасистем / под ред. Д.А. Ловцова. – 2-е изд., испр. и доп. – М.: РАУ – Университет, 2001. – 224 с.

формационного оружия» условно отнести пять соответствующих совокупностей или групп средств, применяемых для деструктивных (дезориентирующих, дезинформирующих, дезорганизующих, дестабилизирующих, подавляющих, разрушающих и др.) воздействий на индивидуумы (эргаматы) и на содержательные компоненты реальных эргасистем, соответствующие основным компонентам модели[1].

1. *Средства массовой информации* (СМИ: радио, пресса, телевидение) *и агитационно-пропагандистские средства* (электронные учебники и энциклопедии, видеодиски, видеокассеты и др.) как вид информационного оружия массового поражения, предназначенные для целенаправленного нанесения информационного ущерба, главным образом духовно-нравственной жизни населения противостоящей (враждебной) стороны и, в первую очередь, его исторической памяти, мировоззрению, морально-нравственным идеалам с целью возможного управления его поведением, а также для создания препятствия аналогичным воздействиям противника (конкурента) – воздействуют на ***духовное***.

2. *Психотронные средства* (специальные генераторы, специальная видеографическая и телевизионная информация, видеосредства новых информационных технологий типа «Виртуальная реальность» и др.), предназначенные для дистанционного зомбирования населения и персонала эргасистем противостоящей стороны, а также для возбуждения психических и психофизиологических расстройств людей – пользователей систем новых информационных технологий (видеографических и др.) на основе специальной контаминации («смешения») цветовой гаммы, дискретности и интенсивности излучения на экранах мониторов, эффекта «25 кадра» (воспринимаемого только на подсознательном уровне)[2] и др. – воздействуют на ***психическое***.

3. *Электронные средства* (специальные передающие устройства и излучатели электромагнитных волн и импульсов

---

[1] Согласно современным теориям личности достаточно адекватная структурно-феноменологическая модель личности включает четыре компонента: *духовное, психическое, физическое, разумное* (содержит *Эго, Супер-Эго, Ид, Интра-Ид*).

[2] Например, известно, что 12 декабря 1997 г. в Японии по национальному телевидению демонстрировался мультфильм «Покемон», содержащий контаминацию цветовой гаммы, звука, мигания визуальной информации и анимационных кадров на фоне иероглифа, обозначающего смерть, от просмотра которого десятки детей получили психофизические расстройства различной тяжести.

и др.; компьютерные «вирусы», разрушающие программные закладки-«черви», спам и др.), включающие:

– *радиоэлектронные средства*, предназначенные для радиоэлектронного подавления и поражения радиоэлектронных средств и сил противника, а также для защиты своих радиоэлектронных средств от радиоэлектронного поражения и подавления;

– *оптико-электронные*, предназначенные для подавления и поражения оптико-электронных средств противника;

– *электронно-вычислительные средства* или *средства информационно-компьютерных технологий* (традиционных электронных и новых), предназначенные для повышения эффективности действия своих эргасистем и средств (в частности, систем оружия и средств распознавания целей и их принадлежности на поле боя), а также для разрушения или искажения информационных массивов (массивов программ и данных), используемых в автоматизированных информационно-ударных системах противника.

Воздействуют на ***физическое***.

4. *Лингвистические средства* (языковые единицы, «специальная» терминология, обороты речи, имеющие семантическую неоднозначность при переводе на другие языки и др.), предназначенные, главным образом, для использования высококвалифицированными специалистами при ведении международных переговоров, подписании и выполнении международных договоров и соглашений между сторонами – воздействуют на ***разумное*** (непосредственно – на ***Супер-Эго***)[1].

[1] Данные средства могут обеспечить долговременный высокоэффективный результат. Например, в текстах международных Договоров США и СССР об ограничении систем противоракетной обороны от 1972 г., о ликвидации ракет средней и меньшей дальности от 1987 г., о сокращении и ограничении и стратегических наступательных вооружений от 1991 г. можно легко обнаружить следы лингвистической борьбы. Так, наличие всего только одной маловразумительной фразы: «Радиолокационные станции (РЛС) с большими фазированными антеннами системы предупреждения о пуске баллистических ракет стратегического назначения должны размещаться только на национальной территории, по ее периферии и обращенными вовне» – позволило США иметь две РЛС за рубежом своей национальной территории, в Гренландии и Великобритании, а одну – в центре полуострова Аляска на расстоянии 800–1000 *км* от береговой линии мирового океана. В то же время СССР в свое время был вынужден ликвидировать свою РЛС подобного типа, построенную под Красноярском в 800 *км* от китайской границы.

5. *Психотропные средства* (специально структурированные лекарства, психофармакологические и психодислептические средства, транквилизаторы, антидепрессанты, галлюциногены, наркотики, алкоголь и др.), предназначенные для воздействия на психику человека на генном или хромосомном уровнях: транквилизаторы разрывают связь между информационно-психическими и физическими процессами в организме человека, галлюциногены вызывают психические расстройства и др. – воздействуют на ***разумное*** (непосредственно – на ***Ид***).

Проведенная продуктивная классификация (по отношению к основному объекту воздействия) возможных видов информационного оружия позволяет определить его с учетом иерархии уровней в системе государственного управления как *совокупность специальных средств, технологий, информации и дезинформации, применяемая для деструктивных воздействий на менталитет населения (персонала эргасистем) и информационно-техническую инфраструктуру государства*.

Рассмотренные основные виды информационного оружия могут применяться против конкретного общества и нации в целом самостоятельно или в составе так называемого «организационного оружия»[1], направленного на разрушение системообразующих связей, объединяющих индивидуумов и социумы в единую нацию. Разнообразие способов негативного информационного воздействия на личность как на базовый компонент нации свидетельствует о преобладающем влиянии на национальную безопасность именно информационного оружия. В связи с этим обязателен государственно-общественный контроль *информационных угроз*[2] и, в

---

[1] *«Организационное оружие»* – совокупность организационных (согласованных по целям, месту и времени разведывательных, пропагандистских, психологических, информационных и др.) деструктивных воздействий на противостоящую эргасистему, заставляющих ее функционировать и развиваться «самостоятельно» и «независимо» в угодном для активной эргасистемы направлении. Основу организационного оружия составляют специальные рефлексивные (с опережающим отражением) технологии организационного управления (регулирования) или новые организационные технологии. См.: Ловцов Д.А. «Организационное оружие» в современном мире // Обозреватель-*Observer*. – М., 2000. – № 6. – С. 40–42.

[2] См.: Ловцов Д.А. Развитие информационной сферы общественно-производственной деятельности: достижения, угрозы безопасности и правовое регулирование // Государство и право в новой информационной реальности: сб.

первую очередь, угроз со стороны СМИ, системы народного образования, учреждений культуры и «интернациональных» организаций.

В целом традиционно высокая роль информационного оружия, судя по возможностям его негативного воздействия на личность и на факторы общности (экономические связи, территория, язык и менталитет, общепринятые правила-нормы поведения и взаимодействия и др.) в составе «организационного оружия», значительно возрастает в условиях стихийных рыночных отношений, правового беспредела и глобальной информатизации на основе создания и совершенствования новых информационных технологий, единых глобальных телематических сетей (типа сетей Интернет, Релком, Ситек, *Sedab*, *Remart* и др.) и «независимых» средств массовой информации (дезинформации).

Проблема информационно-технологической безопасности. В России в настоящее время определенная часть экономики и социальной сферы уже полагается на бесперебойное функционирование российских телематических сетей (РТС), представляющих собой крупномасштабные коммуникационные компоненты глобальной телематической сети (ГТС) Интернет. На базе РТС создаются различные автоматизированные информационные системы (АИС), в том числе использующие так называемые блокчейн-(от англ. *block chain* – цепочка блоков) технологии, обладающие, как считается, повышенной информационной безопасностью. В частности, созданы и успешно функционируют частные трансграничные платформы: кибер-Фонд (*cyber-Fund*), Сатоши_Фонд (*Satoshi Fund*), ГОЛОС (*GOLOS*) и др. В государственной сфере также наблюдаются примеры применения блокчейн-технологий в АИС, например, в АИС «Мастерчейн» Банка России и ряда крупных банков, в АИС «Активный гражданин» московского правительства и др.

Современные блокчейн-технологии, первоначально (в 2009 г.) созданные исключительно для *оперативного* децентрализованного (без доверенных посредников и ненужных звеньев) электронного обращения криптовалюты (биткоин), широко используются в ГТС в различных сферах экономики и социальной сферы (включая электронную коммерцию, банковскую сферу, госуправление, страхование, здравоохранение и др.), поскольку обла-

---

науч. тр. / отв. ред. Е. В. Алферова, Д. А. Ловцов. – М.: ИНИОН РАН, 2018. – С. 15–37.

дают рядом преимуществ, в том числе и в отношении *живучести* (информационно-физической безопасности) и повышенной *информационной защищенности*. Это обусловлено тем, что блокчейн-технологии, наряду с использованием электронных цифровых подписей и мультиподписей, используют последовательно взаимосвязанные цепочки зашифрованных блоков данных, в частности, сетевых финансовых транзакций (записей), хранимых одновременно у всех независимых участников (простых пользователей и майнеров – создателей блоков) АИС, поэтому «взлом» системы (т.е. географически распределенно хранимого множества взаимодействующих идентичных копий единой базы данных) чрезвычайно затруднен. А взламывать каждый зашифрованный блок (содержит заголовок, ключи текущего и предыдущего блоков для обеспечения связности и целостности, набор записей-транзакций) и множество его копий, которые хранятся в разных местах, достаточно долго и дорого. Причем каждая попытка взлома любого блока из цепочки обязательно будет замечена другими участниками АИС. Да и физически разрушить такие АИС практически невозможно в связи с использованием значительного числа узлов (компьютеров) для хранения соответствующих копий с интерфейсами для доступа и подробной документацией, часто территориально «разбросанных» по всему миру.

Вместе с тем проблема гарантированного[1] обеспечения *информационной безопасности* АИС остается актуальной, о чем, в частности, свидетельствуют результаты исследования применения блокчейн-технологий в США – суммарный ущерб американских компаний вследствие использования «врожденных» информационных уязвимостей эксплуатируемых АИС, использующих блокчейн-технологии, и соответствующих децентрализованных сетей составил[2] в 2011–2018 гг. около $1 *млрд*.

Все АИС обладают как общими информационными уязвимостями, определяемыми несовершенством традиционных и предлагаемых стандартизирующей международной организацией

[1] См.: Ловцов Д.А. Проблема гарантированного обеспечения информационной безопасности крупномасштабных автоматизированных систем // Правовая информатика. – 2017. – № 3. – С. 66–74.

[2] См.: Madnick S. Blockchain is unbreakable? Think again // The Wall Street Journal. – 2019. – 6 june. – URL: https://blogs.wsj.com/experts/2019/06/06/blockchain-is-unbreakable-think-again/ (дата обращения 21.01.2020).

(СМО) *IETF* (*Internet Engineering Task Force* – Инженерный совет Интернета) модифицированных сетеобразующих протоколов ГТС, так и специфическими, определяемыми особенностями децентрализованных сетей. Кроме того, проблема информационной безопасности усугубляется возможностью несанкционированного доступа к хранимым и циркулирующим привилегированным данным с использованием «популярных» с конца 90-х годов *нетрадиционных информационных каналов* («скрытых»[1], «сублимографических» и др.)[2]. Например, в результате несанкционированного воздействия на протокол *глобальной динамической маршрутизации BGP* (англ. *Border Gateway Protocol* – протокол пограничного шлюза) возможно изменение маршрутов передачи привилегированных данных с выходом из контролируемой зоны для их сбора и содержательного анализа (криптоанализа), что может остаться незамеченным для взаимодействующих абонентов используемого сегмента ГТС.

При несанкционированном воздействии на протокол *разрешения доменных имен DNS* (англ. *Domain Name System* – система доменных имен) и искажении таблиц *IP*-адресов (необходимых для трансляции символьных доменных имен) ряда серверов возможна задержка и даже потеря передаваемых сообщений, а также их замена и инфильтрация нелегитимных данных.

Основные специфические «врожденные» информационные уязвимости АИС, использующих блокчейн-технологии, связаны с их же достоинствами, и, в первую очередь, с децентрализованностью, транспарентностью и анонимностью.

Децентрализованные (распределенные) регулирование, контроль и аудит, осуществляемые самим сетевым сообществом

---

[1] См.: ГОСТ Р 53113.1–2008. Информационная технология. Защита ИТ и АС от угроз информационной безопасности, реализуемых с использованием скрытых каналов. Часть 1. Общие положения. – М.: Стандартинформ, 2008. – Исполн. Д.Б. Кабелев, А.А. Грушо, А.В. Гусев, Д.А. Ловцов и др.; ГОСТ Р 53113.2–2009. Информационная технология. Защита ИТ и АС от угроз информационной безопасности, реализуемых с использованием скрытых каналов. Часть 2. Рекомендации по организации защиты информации, ИТ и АС от атак с использованием скрытых каналов. – М.: Стандартинформ, 2009. – Исполн. Д.Б. Кабелев, А.А. Грушо, А.В. Гусев, Д. А. Ловцов и др.

[2] См.: Ловцов Д.А., Ермаков И.В. Защита информации от доступа по нетрадиционным информационным каналам // Науч.-техн. информация. Сер. 2: Информ. процессы и системы. – М., 2006. – № 9. – С. 1–9.

участников (без посредников – нотариусов и др.), не исключают возможность так называемой «атаки 51%» («картельный сговор»), когда организованная группа участников, сконцентрировав в своих руках 51% вычислительных мощностей АИС, может начать действовать в своих интересах, подтверждая только выгодные для себя транзакции. А также может осуществлять откат транзакций, создавая альтернативные блоки и гарантированно опровергая то, что происходит в исходном реестре. При этом (а также в других непредвиденных обстоятельствах) защитное «отключение» сразу всей АИС не представляется возможным из-за отсутствия центрального хаба (компьютера).

Транспарентность и публичная доступность базы данных (реестра) АИС, обеспечивая в целом снижение рисков коррупции, добросовестность финансовой, коммерческой и др. профессиональной деятельности независимых участников системы, не защищают от возможности криптоанализа математических «дефектов» (изъянов, «слабостей», уязвимостей) открытых ключей, кодов и возможных алгоритмов шифрования доступных блоков (транзакций), осуществляемого как самими участниками, так и высококвалифицированными злоумышленниками. Существует вероятность подбора закрытого ключа на основе алгоритмов, позволяющих эффективно факторизовать эллиптические[1] кривые.

Анонимность участника, осуществляющего зарегистрированные и доступные операции в автономной АИС, обеспечивая его личную тайну как оператора, не позволяет восстанавливать его доступ к своей учетной записи в случае утери (в том числе и в результате хищения) им своего закрытого ключа.

То есть человеческий фактор продолжает играть существенную роль в информационной безопасности любых автоматизированных систем, включая АИС, использующих блокчейн-технологии, которые, как видно, не всегда защищены от злоупотреблений самих пользователей. Причем уровни взаимного доверия людей в разных странах очень различаются (от 10% в Аргентине до 70% в Швеции[2]) и

[1] Все отечественные ГОСТ семейства 34.10 основаны на использовании математических операций в группе точек эллиптической кривой над конечным полем вычетов по модулю большого простого числа.

[2] См., напр.: Исследование GfK Verein: Международный рейтинг уровня доверия в 2011 г. – URL: https://gtmarket.ru/news/state/2011/12/21/3770 (дата обращения: 21.01.2020).

могут резко колебаться в связи с изменениями морали в обществе и ухудшением социально-экономической ситуации. И остаются также *открытыми вопросы*: кто в АИС, использующих блокчейн-технологии, отвечает за информационную безопасность, за мониторинг защищенности РТС и реагирование на инциденты, нужны ли какие-то стандарты независимым участникам для обеспечения равноправия в системе и др.

Одним из эффективных путей повышения уровня информационной безопасности АИС является *международно-правовая стандартизация* основных сетеобразующих протоколов ГТС[1].

Парадигма обеспечения информационной безопасности. Парадигма информационной безопасности (т.е. исходная концептуальная модель постановки и решения единого взаимосвязанного комплекса упорядоченных многоаспектных задач и проблем, связанных с обеспечением защищенности потребностей эргасистем в качественной информации) базируется на *принципе информационной ценности* как трехэкстремальном принципе оптимальности переработки содержательной информации в эргасистеме. Обоснование принципа включает выбор, классификацию, формализацию определения основных видов и качественных форм существования и проявления информации, анализ их взаимоотношения в системе управления (правовой системе), а также декомпозицию качества информации и определение ее ценности[2].

Под *ценностью* информации в эргасистеме понимается значимость информации, определяемая способом динамического отображения множества ее качественных свойств и количественных характеристик на множество возможных управленческих решений (правовых предписаний и др.), ведущих к достижению целей управления (регулирования). Определение ценности информации на основе учета как количественных, так и качественных характеристик информации позволяет сформулировать концептуальный принцип оптимальности переработки информации в эргасистеме как принцип информационной ценности, определяющий три экстремальных условия обеспечения требуемого

[1] См.: Ловцов Д.А. Обеспечение информационной безопасности в российских телематических сетях // Информационное право. – М., 2012. – № 4. – С. 3–7.

[2] См.: Ловцов Д.А. Системология правового регулирования информационных отношений в инфосфере: монография. – М.: РГУП, 2016. – 316 с.

уровня качества и эффективности применения эргасистем в целом и состоящий в следующем:

информационный ресурс Q эргасистемы следует использовать *рациональным* (первый экстремум) способом W^* и только для переработки наиболее ценной и *качественной* (второй экстремум) осведомляющей информации Q_o^*, на основе которой действительно возможна (при существующем ограничении на количество I_o перерабатываемой информации) выработка *оптимальных* (третий экстремум) управленческих решений (правовых предписаний) U^*, ведущих к достижению целей G управления (правого регулирования), т.е.:

$$Q \xrightarrow{W^*} Q_o^* \longrightarrow U_G^* \mid I_o.$$

Под способом W использования (употребления) информационного ресурса эргасистемы понимается специальная информационная технология как совокупность информационных процедур формирования, интерпретации и коммуникации информации. При этом качество содержательной информации в эргасистеме рассматривается как совокупность свойств информации, характеризующих степень ее соответствия потребностям (целям, ценностям) пользователей (персонала, средств автоматизации, подсистемы регулирования и др.). Можно выделить *внутреннее* качество (присущее собственно информации и сохраняющееся при ее переносе в другую эргасистему, подсистему, АИС) и *внешнее* (присущее информации, находящейся или используемой только в определенной эргасистеме, подсистеме), выражаемые, соответственно, в следующих основных понятиях:

– *пертинентность* (*полнота, релевантность*), *неисчерпаемость, кумулятивность* (*избирательность, гомоморфизм*), в совокупности составляющие (определяющие) *актуальность* информации;

– *достоверность* (*помехоустойчивость, помехозащищенность*), *конфиденциальность* (*доступность*, *скрытность, имитостойкость*), *сохранность*, (*целостность, готовность*), *легитимность*[1] (*аутентичность*, *легальность*, *верифицируемость*), в

[1] *Легитимность* (юридическая значимость) информации обеспечивается на основе применения организационно-правовых процедур удостоверения, кви-

совокупности составляющие (определяющие) *защищенность* информации.

Защищенность информации в настоящее время называют, как правило, *безопасностью информации*, определяемой как свойство функциональной подсистемы контроля и защиты информации в эргасистеме, характеризующее степень защищенности информационных массивов (массивов данных и программ) и заключающееся в способности не допускать случайного или целенаправленного искажения или разрушения, раскрытия или модификации информационных массивов в информационной базе эргасистемы.

Основные направления (способы) обеспечения информационной безопасности. Реально информационная безопасность государства определяется степенью информационной безопасности существующих крупномасштабных эргасистем различного государственного (межгосударственного) уровня. Сложность проблем обеспечения информационной безопасности обусловлена тем, что каждая из эргасистем является своеобразным центром силы в многополярной многоуровневой информационно-предметной среде. То есть формально каждая эргасистема характеризуется функциональной активностью и функциональным гомеостазисом на множестве функциональных возможностей в условиях динамически изменяющегося внешнего окружения (среды).

Научное решение данных проблем должно базироваться на исследовании соответствующих *информационных отношений* активных компонентов эргасистем – человеко-машинных объектов и систем управления (регулирования) силами и средствами в инфосфере[1] с соответствующими активными компонентами противостоящих эргасистем и между собой.

Информационные отношения в инфосфере – особая однородная группа общественных отношений, возникающих при переработке[2] и потреблении (осведомление, обучение, принятие реше-

---

тирования, архивирования и др., основанных на использовании средств электронной подписи соответствующих видов.

[1] См.: Ловцов Д.А. Теория информационного права: базисные аспекты // Государство и право. – 2011. – № 11. – С. 43–51.

[2] *Переработка информации* – совокупность трех информационных процессов (типов информационных действий): *производства* (рецепции, генерации, селекции, измерения, классификации, распознавания; моделирования), *интерпретации* (преобразования, логической обработки, аккумуляции) и *коммуникации* (передачи, хранения, предоставления) содержательной информации.

ния и др.) информации и характеризующихся различными формами и сложностью реального или мысленного установления единства (общности, взаимосвязи) объектов (действий, явлений, их свойств) и субъектов. Два и более субъекта (как реально взаимосвязанных, так и изолированных) могут быть связаны через информационные отношения одного или нескольких типов одновременно, включая функциональные, генетические, причинно-следственные, организационно-правовые, производственные и др.

Наиболее существенными группами информационных отношений в инфосфере являются взаимные отношения субъектов (информационных деятелей, эргасистем), включающие *информационное обособление* (информационная изоляция, информационная защита) и *информационное взаимодействие* или *связь* (информационное соперничество, информационное сотрудничество).

Совокупность информационных отношений *защиты* и *соперничества* составляет существо так называемой «*информационной борьбы*» («*информационной войны*») конфликтующих эргасистем и информационных деятелей, ведущихся с применением «информационного оружия» как самостоятельно, так и в составе «организационного оружия».

В широком смысле *информационная борьба* – это форма информационных отношений конфликтующих эргасистем и информационных деятелей, состоящих в информационном вмешательстве во внутренние дела друг друга, направленном на дезинформацию, дискредитацию, дезориентацию и дезорганизацию противника (конкурента), на разжигание недоверия и вражды между ними. На межгосударственном уровне информационная борьба практически постоянно ведется в мирное время и особенно активизируется при непосредственной подготовке к вооруженному конфликту (войне).

Маргинальным вариантом информационной борьбы на государственном и межгосударственном уровнях является так называемая *информационная война* – особая форма конфликтных информационных отношений крупномасштабных эргасистем (корпораций, государств и др.), заключающихся в информационной агрессии, направленной на попрание суверенитета и разрушение культуры народов; в создании информационных условий дестабилизации экономики, дезинформации, дезориентации и дезорганизации войск эвентуального противника; в массированном негативном информационном и запугивающем морально-психологическом воздействии

на войска и население противника; в прямом применении «информационного оружия» информационно-ударными группировками в ходе проведения специальных информационно-ударных операций[1].

Для обеспечения ***информационной изоляции*** (*сокрытие информатизации расчетов, специализация поддержания качества информации*) реальных эргасистем создаются эффективные специальные новые информационные технологии (НИТ), базирующиеся на принципе «автоформализации» профессиональных знаний специалистов-парапрограммистов, как совокупность информационных процедур производства, интерпретации и коммуникации информации на основе использования проблемно-ориентированных баз данных и знаний, элементами которых являются логико-лингвистическая модель предметной области (тезаурус), рациональная стратегия, соответствующие продукционные правила (типа «Если... то...») и комплекс эффективных алгоритмов выработки управленческих решений (предписаний), а также средства диалога с оператором-парапрограммистом, позволяющие ему заполнять (уточнять) фактографическое содержание баз данных и знаний и интерпретировать результаты.

Сущность НИТ заключается в привлечении парапрограммистов (специалистов в своей предметной области: юристов, экономистов, кадровиков, технологов и др., не являющихся профессиональными программистами) к процессам алгоритмизации функций (задач) эргасистем, сопровождения информационно-программного обеспечения и даже разработки информационно-программного обеспечения на основе использования *языков программирования* сверхвысокого уровня (*Visual Basic*, *C++*, *Delphi*, *Perl*, *Python* и др.), специальных *языков запросов* к информационной базе эргасистем (*SQL*, *XPath*, *XQuery* и др.) и *языков формирования* спецификаций (*UML, ERD, DFD, DDL* и др.).

Разработка и внедрение эффективных и рациональных специальных человеко-машинных НИТ (регулирования, планирования, контроля, защиты, управления и др.) должны базироваться на исторически сложившейся инфраструктуре производства страны и достижениях отечественной науки и техники, учитывающих менталитет и уровень технической и правовой культуры персонала эргасистем. Особенное значение такая стратегия развития эргаси-

[1] См.: Круглов В.В., Ловцов Д.А. Концепция информационно-ударной операции в современной войне // Обозреватель-*Observer*. – М., 1999. – № 12. – С. 49–51.

стем приобретает в условиях усиления взаимодействия противостоящих (конкурирующих или противоборствующих) эргасистем на всех уровнях, частичной интеграции и в итоге навязывания неприемлемых или малоэффективных моделей функционирования эргасистем, в частности, неэффективных, неперспективных или «тупиковых» информационно-компьютерных технологий организационного управления.

Применение рациональных специальных НИТ обеспечит выполнение *первого* и частично *второго* экстремумов принципа информационной ценности, а значит – первого и частично второго условий обеспечения информационной безопасности функционирования эргасистем. Соответствующая ориентация разработчиков НИТ необходима и целесообразна на государственном, военно-политическом и организационно-правовом уровнях управления.

Для обеспечения ***информационной защиты*** (*информационная маскировка, информационное прикрытие*) и успешного ***информационного соперничества*** (*мониторинг, информационное противодействие*) реальных эргасистем, т.е. для ведения успешной информационной борьбы (информационной войны) противостоящих и противодействующих эргасистем создаются специальные информационно-ударные группировки сил и средств, целями применения которых, как правило, являются: нейтрализация или разрушение информационно-стратегического ресурса враждебного государства и его вооруженных сил и обеспечение защиты своего информационно-стратегического ресурса от аналогичных воздействий со стороны противника (конкурента). В настоящее время информационно-стратегический ресурс включает следующие основные объекты деструктивного информационного воздействия:

– человеко-машинные системы управления (эргасистемы) различного государственного уровня, включая каналы информационного обмена и телекоммуникации; среду обмена информацией; средства сбора (получения), логической обработки, хранения и доставки информации, основу которых составляют электронно-вычислительные и радиотехнические системы с соответствующим видом обеспечения (информационным, программным, лингвистическим и др.);

– информация ограниченного распространения, т.е. информация, составляющая государственную, коммерческую, личную и иную тайну (в настоящее время насчитывается более 50 юридически зна-

чимых видов тайны[1]), включая ее носители, системы и средства защиты;

– общество, персонал эргасистем и человека как «информационного деятеля».

При этом основными *задачами* информационно-ударных группировок, соответственно, являются:

– при обеспечении *информационной маскировки*: защитные семантические преобразования информации (необратимые – на основе применения спецаппаратуры и обратимые – кодирование и шифрование); организация маскирующего информационного обмена в информационно-распределительных сетях (радио, проводных и др.) эргасистем; применение шумоподобных информационных сигналов и др.;

– при обеспечении *информационного прикрытия*: радиоэлектронная защита; блокировка ценной информации; ограничение допуска к средствам, информационным и программно-техническим ресурсам эргасистем; контроль потенциальных угроз и каналов утечки информации; организация технологических процессов защищенной (достоверной и конфиденциальной) переработки информации в эргасистемах; контроль и управление доступом к ресурсам эргасистем и др.;

– при обеспечении *информационного сбора*: агентурная, радио- и радиотехническая разведка и контрразведка; космический мониторинг (оптико-электронный, радиолокационный, радиотехнический и др.); верификация информации из различных источников; тестирование АИС противника;

– при обеспечении *информационного противодействия*: радиоэлектронное подавление; инфильтрация дезинформации, включая информацию для воздействия на психику персонала противостоящих эргасистем (информацию психологической борьбы – «информационного зомбирования») и информацию для осуществления «дезорганизации» функционирования противостоящей эргасистемы; инфильтрация «компьютерных вирусов» в АИС противника; блокировка информационных процессов АИС противника; разрушение информационно-программного обеспечения АИС противника и др.

---

[1] См.: Ловцов Д.А., Федичев А.В. Архитектура национального классификатора правовых режимов информации ограниченного доступа // Правовая информатика. – М., 2017. – № 2. – С. 35–54.

Применение специальных информационно-ударных группировок сил и средств обеспечит выполнение *второго экстремума* принципа информационной ценности в условиях информационной борьбы, а значит – второго условия обеспечения информационной безопасности функционирования эргасистем. Обеспечение второго экстремума принципа информационной ценности осуществляется на организационно-техническом уровне управления путем обеспечения ***защищенности***, перерабатываемой в эргасистемах информации, постоянного контроля состояния противостоящих эргасистем и применения информационного оружия самостоятельно или в составе «организационного оружия».

Выработка практически эффективных организационно-правовых управленческих решений в реальной обстановке «информационной борьбы (войны)» возможна на основе применения известной адекватной *комплексной имитационно-игровой модели системы взаимной информационной безопасности*[1] сообщества информационных деятелей (организаций, корпораций, государств, союзов и др.), включающей обобщенные и частные модели информационного и физического уровней.

Обеспечение *третьего экстремума* принципа информационной ценности осуществляется на уровне оперативного организационно-технологического управления силами и средствами путем обеспечения полноты (достаточности) и гомоморфизма необходимой для выработки управленческого решения содержательной информации, т.е. путем регулирования степени информированности лица, принимающего решения (ЛПР), которая определяет конкретные формализованные выражения критерия (например, минимаксного критерия и соответствующего принципа гарантированного результата в условиях конфликта[2]) и вид оператора регулирования (управления). Показатель информированности

---

[1] См.: Ловцов Д.А., Сергеев Н.А. Информационно-математическое обеспечение управления безопасностью эргатических систем. I. Концептуальные модели // Научно-технич. информация. Сер. 2: Информ. процессы и системы. – 1998. – № 4. – С. 10–21; Ловцов Д.А., Сергеев Н.А. Информационно-математическое обеспечение управления безопасностью эргатических систем. II. Математические модели // Научно-технич. информация. Сер. 2: Информ. процессы и системы. – М.,1998. – № 6. – С. 13–22.

[2] См., например: Ловцов Д.А. Теоретические основы системной информатизации правового регулирования // Правовая информатика. – М., 2019. – № 4. – С. 12–28.

ЛПР можно определить как меру неопределенности (погрешности, дисперсии и др.) его знаний о возможных результатах принятых им управленческих решений (о достижении цели), зависящую от значений показателя эффективности управления сложными динамическими объектами или процессами их функционирования. Зависимость показателей информированности ЛПР и эффективности регулирования (управления) обеспечивает учет ценности информации об управляемом объекте (процессе).

Для обеспечения ***информационного сотрудничества*** (*информационный обмен, информационная интеграция*) реальных эргасистем создаются (главным образом, за рубежом) новые эффективные общие информационные технологии (блокчейн, электронная почта, телекс, телетекст, телетайп, видеотекс, телеконференции и др.), Единые информационные среды (ЕИС) и пространства (типа ГТС, «независимых» СМИ и др.). При этом, в частности, для правовой защиты участников *информационного сотрудничества* в сфере «цифровой» экономики активно разрабатывается соответствующее законодательство[1], регулирующее новые экономические правоотношения, возникающие в результате осуществления сделок и договоров купли-продажи, инвестиций, краудфандинга (от англ. *crowd funding* – «финансирование толпой»), страхования и др. в цифровой среде, т.е. с помощью электронных или других технических средств.

Следует иметь в виду, что все возможные информационные отношения взаимосвязаны и могут, *во-первых*, оперативно изменяться на любые другие в зависимости от возникающих в реальной обстановке ситуаций, а *во-вторых*, в каждой определенной ситуации возможно выявление наличия признаков любых информационных отношений. В частности, при возникновении конфликтных ситуаций и усилении степени антагонизма между нациями и государствами с различной идеологией и культурой, «информационная борьба», ведущаяся ими практически постоянно в мирное время, может перерасти в агрессивную «информацион-

[1] В том числе и в России. См., например: Федеральный закон от 18 марта 2019 г. № 34-ФЗ «О внесении изменений в части первую, вторую статьи 1124 части третьей Гражданского кодекса Российской Федерации» // Рос. газ. – М., 2019. – 20 марта.

ную войну»[1]. Данное обстоятельство приводит к необходимости учета прецедентных и прогнозируемых ситуаций и разработки безопасных (взаимобезопасных) общих НИТ и ЕИС на основе соблюдения норм *международного информационного права* всеми «информационными деятелями» – крупномасштабными эргасистемами (корпорациями, государствами, коалициями государств и др.).

Определение содержания и разработка концептуальных, организационно-правовых и лингвистических основ информационной безопасности, противостоящих эргасистем проводятся, как правило, на основе прикладной классификации и обобщения имеющегося опыта применения информационного обеспечения управления (регулирования) силами и средствами. Вместе с тем представляется целесообразным на данном этапе развития теоретико-концептуальных основ информационной безопасности эргасистем основное внимание уделить разработке *информационно-логической модели* предметной области (тезауруса) информационных отношений человеко-машинных объектов и систем управления и соответствующих научно-методологических основ информационной борьбы как конфликтных информационных отношений, противостоящих эргасистем. Тогда, в частности, становится возможной разработка соответствующей непротиворечивой иерархической совокупности научно-правовых терминов, которую в дальнейшем можно стандартизировать. Разработка модели предметной области (тезауруса) информационных отношений (правоотношений) объектов информационных сред и пространств возможна на основе применения проблемно-ориентированного комплексного «ИКС»-подхода[2] («информационно-кибернетически-синергетического»), соответствующего природе эргасистем (в том числе и правовых).

Таким образом, основными направлениями (организационно-правовыми способами) обеспечения информационной безопас-

---

[1] См., например: The U.S. Army Concept for Cyberspace and Electronic Warfare Operations 2025–2040: Report. – URL: https://www.hsdl.org/?abstract&did=807334 (дата обращения: 28.01.2020); TRADOC «Pamflet 525–8-6». – US. Army Training and Doctrine Command: Public Domain, 2018. – URL: https://en.wikipedia.org/wiki/United_States_Army_Training_and_Doctrine_Command (дата обращения: 28.01.2020).

[2] См.: Ловцов Д.А. Концепция комплексного «ИКС»-подхода к исследованию сложных правозначимых явлений как систем // Философия права. – М., 2009. – № 5. – С. 40–45.

ности на перспективу в порядке их относительной важности являются следующие:

1. Создание и внедрение специальных НИТ, ориентированных на инфраструктуру страны, достижения отечественной науки и техники, менталитет, правовую и техническую культуру персонала эргасистем различного государственного (межгосударственного) уровня, включая разработку эффективного национального законодательства о «цифровых правах».

2. Создание специальных информационно-ударных группировок сил и средств, предназначенных для успешного ведения информационной борьбы (войны) с противостоящими и противоборствующими эргасистемами других государств, включая разработку национальных технико-правовых стандартов эффективных криптографических алгоритмов для национальных сегментов ГТС.

3. Создание взаимобезопасных общих (общего назначения) НИТ и Единых информационных сред (типа ГТС Интернет, Релком, Ситек, *Sedab*, *Remart* и др.), гарантирующих возможность *информационного сотрудничества* на основе соблюдения норм международного информационного права всеми «информационными деятелями», включая международно-правовую стандартизацию сетеобразующих протоколов ГТС и используемых в них криптографических алгоритмов.

2.3. Конституционные принципы информационной открытости и конфиденциальности в условиях развития цифровых (инновационных) технологий[1]

Существующая информационная реальность обусловила необходимость принятия ряда стратегически важных документов, декларирующих принципы развития информационного общества как на международном, так и на внутригосударственном уровне.

На международном уровне сформированы общие принципы для реализации стратегии развития информационного общества и осуществление согласованных действий по созданию безопасного использования интернет-ресурсов. В частности, они определены в Окинавской хартии глобального информационного общества

[1] Материал подготовлен в рамках гранта РФФИ «Принципы конституционного права», проект № 19–011–00058

2000 г., в Декларации принципов «Построение информационного общества – глобальная задача в новом тысячелетии» 2003 г.[1], в Тунисской программе для информационного общества 2005 г.[2] В данных документах выделяются такие принципы, как: недопустимость ограничения прав человека при использовании современных информационных и коммуникационных технологий; сохранение традиционных и привычных для граждан (отличных от цифровых) форм способов обращения в органы государственной власти; осуществление программ по повышению электронной грамотности граждан и др.

Однако большинство государств мира, исходя из того, что в новой структуре информационных правоотношений необходимо учитывать существующие информационные угрозы и риски, обеспечивать гарантии права личности на частную жизнь, безопасность общества и государства ориентируясь на данные принципы, вынуждены «на ходу» адаптировать модели государственного регулирования сферы информации и информационных технологий в целях поиска оптимальной модели модернизации области информационной безопасности.

На значимость развития информационных технологий обращается внимание во многих зарубежных публикациях ученых[3]. Подчеркивается важность корректного использования информаци-

[1] Декларация принципов «Построение информационного общества – глобальная задача в новом тысячелетии», принята 12.12.2003 в Женеве. – URL: https://www.un.org/ru/events/pastevents/pdf/dec_wsis.pdf (дата обращения 16.03.2020).

[2] Тунисская программа для информационного общества, принята 15.11.2005 г. – URL: https://www.un.org/ru/events/pastevents/pdf/agenda_wsis.pdf (дата обращения 16.03.2020).

[3] Filippi P. de, Maurel L. The paradoxes of open data and how to get rid of it? Analysing the interplay between open data and sui-generis rights on databases // International journal of law and information technology. – 2015. – Vol. 23. – P. 1–23; Torres, F.T., Berdun, M.I. El dret a la informació versus la protecció del dret a la intimitat en la societat de la informació. La nova LO de protecció de dades i el dret a l'oblit (Right to freedom of information versus protection of the right to privacy in information society. The new law on the protection of personal data and the right to be forgotten) // Comunicació: Revista de Recerca i d'Anàlisi. – 2019. – Vol. 36, N 1. – P. 117–131. – URL: http://revistes.iec.cat/index.php/TC (дата обращения: 12.03.2020).

онных и коммуникационных возможностей, которые рассматриваются как новый экономический и социальный ресурс[1].

Исходя из того, что менее чем за два десятилетия произошла информационно-коммуникационная революция, государства настроены на неизбежный ориентир общества – движение к электронной информации. Так, в Австралии, Великобритании, Индии, Испании, Канаде, Китае, Нидерландах, Новой Зеландии, США, на Филиппинах, во Франции, Швейцарии, Швеции существуют дистанционное правосудие и электронная система доказательств[2].

В России, взявшей курс на интенсивное развитие информационного общества, в развитии данного направления определены приоритеты и цели государственной политики, приняты ряд стратегических программ и нормативных правовых актов[3].

В современный период основными принципами развития информационного общества в Российской Федерации определены:

а) обеспечение прав граждан на доступ к информации;

б) обеспечение свободы выбора средств получения знаний при работе с информацией;

в) сохранение традиционных и привычных для граждан (отличных от цифровых) форм получения товаров и услуг;

г) приоритет традиционных российских духовно-нравственных ценностей и соблюдение основанных на этих ценностях норм поведения при использовании информационных и коммуникационных технологий;

---

[1]Данное определение дал Н. Крус (Neelie Kroes), вице-президент Европейской комиссии, во вступительном слове на пресс-конференции Open Data Strategy, состоявшаяся в Брюсселе 12.12.2011. Доклад размещен на сайте Европейской комиссии. – URL: https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_11_872 (дата обращения: 08.03.2020).

[2]См.: Овчинников В.А., Антонов Я.В. Электронное правосудие как проект электронной демократии: перспективы реализации в России // Государственная власть и местное самоуправление. – М., 2016. – № 5. – С. 3–7; Al-Swelmiyeen I., Al-Nuemat A., Kok A. Online-arbitration in the social network world; mobile justice on iPhones // Information & communications technology law. – 2013. – Vol. 22, N 2. – P. 146–164.

[3] См.: Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и защите информации»; Стратегия развития информационного общества в Российской Федерации на 2017–2030 годы, утв. Указом Президента РФ от 9 мая 2017 г. № 203; постановление Правительства РФ от 15 апреля 2014 г. № 313 «Об утверждении государственной программы Российской Федерации “Информационное общество”» и др.

д) обеспечение законности и разумной достаточности при сборе, накоплении и распространении информации о гражданах и организациях;

е) обеспечение государственной защиты интересов российских граждан в информационной сфере[1].

Кроме того в ст. 3 Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» к числу принципов, на которых основывается правовое регулирование отношений в рассматриваемой сфере, определены: свобода поиска, получения, передачи, производства и распространения информации любым законным способом; установление ограничений доступа к информации только федеральным законом; открытость информации о деятельности государственных органов и органов местного самоуправления и свободный доступ к такой информации, кроме случаев, установленных федеральными законами; достоверность информации и своевременность ее предоставления, а также неприкосновенность частной жизни и недопустимость сбора, хранения, использования и распространения информации о частной жизни лица без его согласия.

Значимым достоинством развития информационного общества является возможность использования цифрового пространства во взаимоотношениях между личностью, обществом и государством, и, как следствие, данное обстоятельство является положительным фактором, позволяющим поднимать социальную активность населения[2].

В целом использование новых информационных (включая цифровые) технологий качественно сказывается на экономии времени, доступности определенных новых экономических и социально-политических возможностей посредством использования киберпространства, оперативности решения актуальных вопросов. Кроме того, такие сферы, как медицина, образование, управление,

---

[1] См.: Стратегия развития информационного общества в Российской Федерации на 2017–2030 гг., утв. Указом Президента РФ от 9 мая 2017 г. № 203; Стратегия развития отрасли информационных технологий в Российской Федерации на 2014–2020 гг. и на перспективу до 2025 г., утв. распоряжением Правительства РФ от 1 ноября 2013 г. № 2036-р.

[2] См.: Кравцова Е.А. Взаимодействие законодательных органов с институтами гражданского общества с использованием информационного и цифрового пространства России // Конституционное и муниципальное право. – М., 2019. – № 9. – С. 27–29.

социальная защита и др. также активно развиваются в этом направлении.

Так, в частности, в России созданы:

– электронные формы документооборота, в том числе с использованием электронных подписей при совершении гражданско-правовых сделок, оказании государственных и муниципальных услуг, исполнении государственных и муниципальных функций, при совершении иных юридически значимых действий[1];

– система централизованного создания и хранения ключей усиленной квалифицированной электронной подписи, а также их дистанционного применения владельцами квалифицированных сертификатов ключа проверки электронной подписи при государственной регистрации юридических лиц и индивидуальных предпринимателей либо при открытии банковского счета[2].

Кроме того, предусмотрена возможность:

– получения информации о результатах медицинского обследования здоровья, диагностики и лечении, о выписанных рецептах и иных данных, характеризующих состояние здоровья человека без посещения медицинского учреждения[3];

---

[1] См.: Федеральный закон от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи»; постановление Правительства РФ от 10 июля 2013 г. № 584 «Об использовании федеральной государственной информационной системы «Единая система идентификации и аутентификации в инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме» (вместе с «Правилами использования федеральной государственной информационной системы “Единая система идентификации и аутентификации в инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме”»).

[2] См.: постановление Правительства РФ от 8 ноября 2019 г. № 1427 «О проведении эксперимента по совершенствованию применения технологии электронной подписи».

[3] Ваша электронная медицинская карта // Официальный сайт мэра Москвы. – URL: https://www.mos.ru/city/projects/medcarta/?muid=a064549d-ac91-4191-85cb-813408e8ba89&category=04a6660a-c3fe-4fc3-84a6-60afd7dc9422 (дата обращения 16.03.2020).

– использования дистанционных образовательных технологий и электронного обучения при реализации образовательных программ[1];

– реализации социальных прав посредством личного кабинета на сайте Пенсионного фонда или портале госуслуг[2] и др.

Вместе с тем интенсивное расширение масштабов инновационной активности информационного общества и существенная государственная поддержка научно-технической и инновационной деятельности не исключают, а в условиях опережающей практики развития новых в данной области взаимоотношений, порождает ряд актуальных проблем[3].

Одна из них – отсутствие сбалансированной модели защищенности частных и публичных интересов в условиях глобально и интенсивно развивающегося информационного общества.

Размышляя над данным вопросом, ученые-юристы обращают внимание на то, что введение новых информационных технологий в реальную действительность существенно ограничивает индивидуальную свободу и законные интересы личности[4].

А.А. Чеботарева справедливо подчеркивает, что сфера безопасности в глобальном информационном обществе обусловливает

---

[1] См.: Федеральный закон от 29 декабря 2012 г. № 273-ФЗ «Об образовании в Российской Федерации».

[2] Семьи получают электронные сертификаты на материнский капитал // Сайт Пенсионного фонда РФ. – URL: http://www.pfrf.ru/press_center/~2018/06/13/160919 (дата обращения 16.03.2020).

[3] См.: Ellebrecht S., Kaufmann S. Digitalization and its security manifestations // European journal for security research. – 2020. – Vol. 5. – P. 1–3. – URL: https://doi.org/10.1007/s41125-019-00063-8 (дата обращения: 12.03.2020); Костюков А.Н. Реализация прав человека и гражданина в конституционном праве России: год 2017-й // Конституционное и муниципальное право. – М., 2017. – № 2. – С. 17–23; Абдрахманов Д.В. Правовая определенность как гарантия реализации конституционно-правовых основ информационного общества в Российской Федерации // Юрист. – М., 2018. – № 7. – С. 59–70 и др.

[4] См.: Saetra, H.S. Freedom under the gaze of Big Brother: Preparing the grounds for a liberal defence of privacy in the era of Big Data // Technology in society. – 2019. – Vol. 58, № article UNSP 101160, Aug. – URL: https://doi.org/10.1016/j.techsoc.2019.101160 (дата обращения: 12.03.2020); Segado-Boj F., Diaz-Campo J. Social media and its intersections with free speech, freedom of information and privacy: An analysis (Las redes sociales y sus intersecciones con la libertad de expresión, la libertad de información y la privacidad. Un análisis) // Revistaicono 14-revista cientificade comunicacion y tecnologias. – 2020. – Vol. 18, N 1. – P. 231–255.

необходимость обеспечения баланса законных интересов личности, общества и государства. В условиях глобального информационного общества проблема соотношения и взаимозависимости интересов личности, информационного общества и информационного государства требует взвешенного подхода в решении[1].

Сегодня можно говорить о трех базовых принципах информационной безопасности: целостность данных (защита от сбоев, ведущих к потере информации, защита от неавторизованного создания или уничтожения данных), конфиденциальность информации и ее доступность для всех авторизованных пользователей.

Для достижения оптимальной модели правового обеспечения информационной безопасности личности в условиях глобального развития информационного общества важное значение имеет действенность диалектической взаимосвязи данных принципов, в частности конституционных *принципов информационной открытости и конфиденциальности.*

В Конституции РФ указанные принципы прямо не закрепляются. *О принципе информационной открытости* упоминается лишь в ст. 24, 29, 41 и 42. *Принцип конфиденциальности* выводится из содержания ст. 23, ч. 4 ст. 29, ч. 1 ст. 81 Конституции РФ.

Э.В. Талапина подчеркивает, что из рассматриваемых конституционных предписаний выводятся отраслевые принципы, а именно:

– защита информации о частной жизни;

– открытость административной информации, затрагивающей права и свободы;

– возможность ограничения открытости административной информации только законом, а государственной тайны – только федеральным законом;

– свобода законного оборота информации;

– доступность и достоверность экологической информации;

– доступность информации об обстоятельствах, создающих угрозу для жизни и здоровья людей[2].

---

[1] Чеботарева А.А. Правовое обеспечение информационной безопасности личности в глобальном информационном обществе // Юридический мир. – М., 2016. – № 8. – С. 63–66.

[2] См.: Талапина Э.В. Государственное управление в информационном обществе (правовой аспект). – М.: Юриспруденция, 2015. – С. 148–150.

Также важно подчеркнуть, что конституционные принципы информационной открытости и конфиденциальности взаимосвязаны с принципами *открытости, доступности и гласности.*

В общем плане *принцип информационной открытости* предполагает создание организационных, институциональных и нормативно-правовых условий, обеспечивающих реальную возможность *не только обращения* управомоченных субъектов в органы публичной власти, *получение необходимой* для реализации конституционных прав информации, *но и общения* граждан через информационные ресурсы между собой.

Принцип конфиденциальности характеризуется тем, что устанавливается *требование сдержанности* и *обязанность сохранения различных видов сведений*, полученных при использовании информационного пространства, распространение которых запрещено законом. При этом предполагается важным добросовестное сохранение индивидуальной информации и эффективное гарантирование защищенности персональных и иных защищаемых законом сведений.

В настоящее время принято существенное количество нормативных правовых актов, конкретизирующих принцип информационной открытости и конфиденциальности. В их числе – федеральные законы: от 27 июля 2006 г. № 152-ФЗ «О персональных данных»; от 2 декабря 1990 г. № 395–1 «О банках и банковской деятельности»; от 29 июля 2004 г. № 98-ФЗ «О коммерческой тайне»; Закон РФ от 21 июля 1993 г. № 5485–1 «О государственной тайне», а также Указ Президента РФ от 30 ноября 1995 г. № 1203 «Об утверждении Перечня сведений, отнесенных к государственной тайне» и др.

Однако учитывая то, что владелец и хранитель данной информации является третьим лицом, то говорить о балансе частных и публичных интересов в современный период не представляется возможным.

Другая актуальная проблема – развитие эффективного демократического механизма, способствующего вовлечению граждан в информационное взаимодействие с государством.

Цифровизация государственной деятельности в целом и государственных услуг в частности предполагает, что многие функции, на которые государство традиционно тратит много ресурсов, автоматизируются с помощью приложений, разрабатываемых как государством, так и коммерческими компаниями и социально ори-

ентированными организациями, что сокращает как затраты, так и время оказания услуги. При этом органы публичной власти являются не только администратором и дизайнером системы, но и сами присутствуют на платформе со своими услугами в режиме реального времени. Это создает условия для максимальной адаптивности, гибкости и адекватности текущему моменту.

На официальном уровне сегодня подчеркивается значимость цифровизации в целях противодействия коррупции. В частности, в Послании Федеральному Собранию 1 марта 2018 г. Президент РФ указал, что «…цифровизация всей системы государственного управления, повышение ее прозрачности – это и мощный фактор противодействия коррупции»[1].

В России принцип информационной открытости считается важным элементом государственной политики. В стране развивается правовая база в этой области общественных отношений, например, приняты федеральные законы: от 9 февраля 2009 г. № 8-ФЗ «Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления»; от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи»; от 23 июня 2016 г. № 220-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации в части применения электронных документов в деятельности органов судебной власти», а также Указ Президента РФ от 10 августа 2000 г. № 1486 «О дополнительных мерах по обеспечению единства правового пространства Российской Федерации»; Федеральная целевая программа «Развитие судебной системы России на 2013–2020 годы» (утв. распоряжением Правительства РФ от 20 сентября 2012 г. № 1735-р); Концепция развития информатизации судов до 2020 г. (утв. постановлением Президиума Совета судей РФ от 19 февраля 2015 г. № 439); Концепция информатизации Верховного Суда РФ (утв. приказом Верховного Суда РФ от 10 декабря 2015 г. № 67) и др.

Анализ внесенных в Государственную Думу законопроектов и пояснительных записок к ним позволяет отметить, что принцип информационной открытости деятельности органов государственной власти в системной взаимосвязи с принципами противодействия коррупции, добросовестности, достоверной информации вы-

[1]Послание Президента РФ Федеральному Собранию от 1 марта 2018 г. // Рос. газета. – М., 2020. – 2 марта, № 46.

ступает в качестве аргумента при обосновании необходимости принятия предлагаемого проекта нормативного правового акта[1].

Более того, действенность принципа информационной открытости деятельности органов государственной власти очевидна. В частности, имеется реальная возможность получить необходимую информацию через сеть Интернет о деятельности органов публичной власти; возможность через интернет-ресурсы направить обращение в органы государственной власти; возможность получить необходимые государственные услуги через электронные ресурсы и многое другое[2]. Это позволяет в условиях стремительно преобразующейся системы взаимоотношений личности, общества и государства получить самое важное в современном постмодернистском обществе – экономию времени.

Следует заметить, что за последнее десятилетие государственное управление в целом преобразилось. В стране работает более 3 тыс. многофункциональных центров, во всех более-менее крупных населенных пунктах государственные услуги можно получать в шаговой доступности по принципу одного окна[3]. Ежедневно порталом госуслуг пользуется более полутора миллионов человек, а число запросов, поступающих на ресурс, исчисляется миллиардами в год. Без цифровых технологий уже невозможно представить реальность. Люди ждут от государства развития этих технологий и хотят работать в этой цифровой среде без каких-либо препятствий и барьеров. В связи с этим был реализован проект

---

[1] См.: напр., пояснительные записки к проектам федеральных законов: «О внесении изменения в статью 10 Федерального закона «О государственной информационной системе жилищно-коммунального хозяйства» – URL: http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=PRJ&n=185154&dst=100012#03116314210503 5635; «О внесении изменения в статью 3 Федерального закона «О противодействии коррупции». – URL: http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=PRJ&n=183400&dst=100009#06053408921758432 (дата обращения 18.02.2020).

[2] См.: Шарифуллин Р.А., Бурганов Р.С., Бикмиев Р.Г. Элементы электронного правосудия // Российский судья. – М., 2018. – № 6. – С. 57–62; Алешкова И.А., Молокаева О.Х. Опасности цифрового развития права: очевидные, скрытые, мнимые // Конституционное и муниципальное право. – М., 2019. – № 8. – С. 41–45 и др.

[3] См.: Пользователи хотят общаться с государством через экран смартфона / Аналитический центр при Правительстве РФ. – URL: https://ac.gov.ru/news/page/polzovateli-hotat-obsatsa-s-gosudarstvom-cerez-ekran-smartfona-18508 (дата обращения 20.02.2020).

сервисного государства, одним из основных направлений работы которого стали супер-сервисы, включающие наиболее важные и востребованные населением федеральные, региональные и муниципальные услуги (например, возможность получения в электронном виде таких документов, как европротокол по ДТП, разрешение на ввод объекта в эксплуатацию, больничный лист, трудовая книжка и др.)[1].

Проект сервисного государства сформировал и единую информационную среду. В России насчитывается около 35 тыс. сайтов государственных и муниципальных органов власти и более 100 порталов государственных услуг[2]. В результате установлены единые принципы цифровой экосистемы, стандарты редакционной политики, контента и работы с данными. Кроме того, в перспективе проект предполагает полную ликвидацию бумажного документооборота и переход на электронные носители. Политика цифровизации государственных услуг продолжена государством с принятием обновленной Национальной программы «Цифровая экономика Российской Федерации», утвержденной президиумом Совета при Президенте РФ по стратегическому развитию и национальным проектам (протокол от 4 июня 2019 г. № 7).

Принцип информационной открытости деятельности органов государственной власти способствует эффективной реализации *принципа конституционной сдержанности*, который включает в свое содержание способность разумно реализовывать свои полномочия, в том числе и в сфере государственного управления; способность удерживать порывы «переместить полномочия на себя»; уважение к позиции иных органов, осуществляющих публичную власть, выраженную при осуществлении закрепленных за ними полномочий.

Таким образом, посредством реализации принципа информационной открытости в диалектической взаимосвязи с принципом конституционной сдержанности органы государственной власти

---

[1] Национальная программа «Цифровая экономика Российской Федерации», утв. президиумом Совета при Президенте РФ по стратегическому развитию и национальным проектам (протокол от 24 декабря 2018 г. № 16).

[2] Пользователи хотят общаться с государством через экран смартфона / Аналитический центр при Правительстве РФ. – URL: https://ac.gov.ru/news/page/polzovateli-hotat-obsatsa-s-gosudarstvom-cerez-ekran-smartfona-18508 (дата обращения 21.03.2020).

стремятся обеспечивать правопорядок, а также согласованность своих действий и решений.

Федеральный закон от 9 февраля 2009 г. № 8-ФЗ «Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления» регулирует отношения, связанные с обеспечением доступа пользователей информацией, в том числе граждан, организаций и общественных объединений, к информации о деятельности государственных органов и органов местного самоуправления. В нем закреплены основные принципы обеспечения доступа к такой информации. В их числе – открытость и доступность, за исключением случаев, предусмотренных федеральным законом. Конкретизируя данные принципы, упомянутый федеральный закон предусматривает, что доступ к информации о деятельности государственных органов и органов местного самоуправления ограничивается в случаях, если такая информация отнесена в установленном федеральным законом порядке к сведениям, составляющим государственную или иную охраняемую законом тайну; перечень сведений, относящихся к информации ограниченного доступа, а также порядок отнесения указанных сведений к информации ограниченного доступа устанавливаются федеральным законом.

Как указал Конституционный Суд РФ в Определении от 24 декабря 2013 г. № 2066-О «Об отказе в принятии к рассмотрению жалобы гражданина Соколова Модеста Михайловича на нарушение его конституционных прав положениями части 2 статьи 2 Федерального закона “Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления”», такое законодательное регулирование направлено на создание условий (гарантий), обеспечивающих максимальную информационную открытость государственных органов и органов местного самоуправления для граждан и иных субъектов гражданского общества, и согласуется с принятой Советом Европы 27 ноября 2008 г. Конвенцией о доступе к официальным документам (преамбула, ст. 3), в которой подчеркивается особое значение прозрачности деятельности государственных органов в плюралистическом и демократическом обществе и которая вместе с тем не исключает ограничений права на доступ к официальным документам при условии, что эти ограничения четко установлены законом, являются необходимыми и соразмерными целям защиты общепризнанных в демократическом обществе ценностей.

Вместе с тем следует подчеркнуть, что в данном направлении доминирующим является добровольность. Однако нет гарантии того, что в ближайшем будущем добровольность трансформируется в форму обязательного требования и не произойдет превращения ряда субъективных прав в обязанности[1]. Бесспорно, что жить в обществе и быть свободным от него нельзя, но всегда должны быть альтернативные варианты взаимодействия и одним из таких вариантов должен быть естественный способ коммуникационной взаимосвязи.

Еще одной из актуальных проблем в условиях интенсивно развивающегося информационного общества является эффективная защита персональной информации.

Стремительное введение и использование новых технологий в деятельности органов государственной власти не всегда позитивно, ибо они обусловливают появление новых правовых проблем, к которым не готово ни государство, ни общество. В их числе, например, конфиденциальность персональной информации, неприкосновенность частной жизни, сохранение семейной, коммерческой и иных видов тайн, защищаемых законом.

Такого рода защита должна быть полноценной и зависимой от сферы образования, медицины, социальных сетей, сферы социальной защиты и др.

В частности, в сфере медицины одним из наиболее актуальных является доступность третьих лиц к идентифицирующей человека генетической информации.

М.Н. Малеина, раскрывая содержание *принципа доступности гражданина к собственной генетической информации*, отмечает, что он означает предоставление соответствующих сведений гражданину и по его требованию внесение изменений, исправлений, дополнений, принятие мер по уничтожению соответствующих данных по правилам, установленным законом. Формулировка этого принципа следует из некоторых законов, касающихся информации, в частности ст. 22 Федерального закона «Об основах охраны здоровья граждан в Российской Федерации», ст. 14 Федерального закона «О персональных данных». Непосредственно упоминание о распоряжении собственной генетической информацией содержится в п. 2 ст. 16 Федерального закона «О государственной геномной регистрации в Российской Федерации»:

[1]Алешкова И.А., Молокаева О.Х. Указ. соч. – С. 41–45.

на основании письменного заявления лиц, прошедших добровольную государственную геномную регистрацию, их геномная информация может быть уничтожена[1].

Вместе с тем порядок реализации положений законов, действующих в рассматриваемой области, является недостаточно отработанным и несет в себе определенные скрытые риски, поскольку значительное количество организаций, хранящих такого рода информацию, – коммерческие структуры. Соответственно, такие частные организации, в отличие от государства, не могут в полной мере обеспечить защищенность данных, гарантировать и обеспечить их безопасность. На значимость обеспечения предоставленной человеку и гарантированной государством возможности контролировать информацию о самом себе, препятствовать разглашению сведений личного характера было обращено внимание в Постановлении Конституционного Суда РФ от 16 июня 2015 г. № 15-П «По делу о проверке конституционности положений ст. 139 Семейного кодекса Российской Федерации и ст. 47 Федерального закона “Об актах гражданского состояния” в связи с жалобой граждан Г.Ф. Грубич и Т.Г. Гущиной».

Таким образом, есть необходимость анализа и размышлений о конструкции принципов конституционного права, которая должна отвечать современным тенденциям развития новых инновационных технологий.

В сфере социального информационного общения также существуют риски утечки персональной информации.

Разумные ожидания могут быть у пользователей публичных социальных сетей в отношении конфиденциальности со ссылкой на существующее прецедентное право по ст. 8 Европейской конвенции о правах человека. В частности, утверждается, что два фактора поддерживают разумное ожидание конфиденциальности в открытых публичных социальных сетях: во-первых, неспособность многих пользователей социальных сетей воспринимать среду, в которой они общаются, как общедоступную; и, во-вторых, влияние поисковых систем (и другой автоматизированной анали-

[1] См.: Малеина М.Н. Роль правовых принципов в устранении и минимизации рисков применения геномных технологий // Lex russica (Русский закон). – М., 2019. – № 8. – С. 121–128.

тики) на традиционные концепции структурированных досье как наиболее проблематичных для государственного надзора[1].

Анализ судебной практики показывает, что принцип информационной открытости нередко взаимосвязан с принципом запрета злоупотребления правами. В частности, в решении Московского городского суда от 19 апреля 2018 г. по делу № 3 а-2324/2018 отмечается, что у представителей государственной власти, имеющих право осуществлять определенные государственные проверки, имелась информация о наличии объявлений в сети Интернет о нахождении в зданиях одной из организаций иных различных организаций. Однако суд подчеркнул, что наличие данной информации, полученной в сети Интернет, не может объективно свидетельствовать о виде их фактического использования, поскольку из указанных объявлений не ясно, кем они даны, под какие цели фактически используются помещения, какой площади и в какой временной период. Соответственно, недопуск лиц, осуществляющих публичную власть, на территорию режимного объекта в целях осуществления контроля деятельности организаций, расположенных на данной территории, не может расцениваться как злоупотребление правом со стороны организации, осуществляющей охрану режимного объекта, поскольку данные действия направлены на соблюдение установленного на предприятии режима секретности и обусловлены соблюдением законных требований[2].

Одним из значимых в области формирования российской модели правового обеспечения информационной безопасности личности, общества и государства в условиях глобального информационного общества является Постановление Конституционного Суда РФ от 26 октября 2017 г. № 25-П «По делу о проверке конституционности пункта 5 статьи 2 Федерального закона “Об информации, информационных технологиях и о защите информации” в связи с жалобой гражданина А.И. Сушкова». В п. 5 обращается внимание на тот факт, что отправка гражданином на

[1] См.: Edwards L., Urquhart L. Privacy in public spaces: what expectations of privacy do we have in social media intelligence? // International journal of law and information technology. – L., 2016. – Vol. 24, N 3. – P. 282.

[2] См.: Решение Московского городского суда от 19 апреля 2018 г. по делу № 3 а-2324/2018 «О признании недействующими пунктов 7869, 7871, 7872, 7873, 7874 Перечня объектов недвижимого имущества, в отношении которых налоговая база определяется как их кадастровая стоимость, утвержденного постановлением Правительства Москвы от 28.11.2014 № 700-ПП (ред. 29.11.2016)».

свой (личный) адрес электронной почты не принадлежащей ему информации создает условия для ее дальнейшего неконтролируемого распространения. Фактически, совершив такие действия, гражданин получает возможность разрешать или ограничивать доступ к отправленной им информации, не получив соответствующего права на основании закона или договора, а сам обладатель информации, допустивший к ней гражданина без намерения предоставить ему эту возможность, уже не может в полной мере определять условия и порядок доступа к ней в дальнейшем, т.е. осуществлять прерогативы обладателя информации.

В данном постановлении также подчеркивается, что правовой статус правообладателя коммуникационного интернет-сервиса, посредством которого осуществляется отправка и получение электронных сообщений, действующим федеральным законодательством специально не урегулирован (хотя по своему полезному для пользователей эффекту его услуги и аналогичны услугам связи), возникает неопределенность относительно того, распространяется ли на него буквально обязанность оператора связи обеспечить соблюдение тайны.

Не ставятся под сомнение конституционные гарантии тайны направляемых по электронной почте сообщений и содержания заключаемого правообладателем интернет-сервиса и абонентами пользовательского соглашения, предполагающего наличие дифференцированных правил, регулирующих отношения, объектом которых выступают в одних случаях информационные данные, создаваемые и публикуемые пользователями, т.е. размещаемые в режиме открытого доступа для ознакомления с ними неопределенного круга лиц, и в других случаях – сведения, не предназначенные для размещения в открытом доступе. И в тех и в других случаях условия пользовательского соглашения не могут трактоваться как предоставляющие правообладателю интернет-сервиса право самостоятельно – и тем самым в нарушение ч. 2 ст. 23 Конституции РФ – разрешать или ограничивать доступ к информации, содержащейся в передаваемых с его помощью электронных сообщениях.

Не свидетельствуют о возникновении у правообладателя интернет-сервиса, с помощью которого происходит отправка и получение электронных сообщений, такого права, а следовательно, и статуса обладателя содержащейся в них информации и положения ст. 10.1 Федерального закона «Об информации, информационных технологиях и о защите информации», согласно которым лицо,

осуществляющее деятельность по обеспечению функционирования информационных систем и (или) программ для электронных вычислительных машин, предназначенных и (или) используемых для приема, передачи, доставки и (или) обработки электронных сообщений пользователей Интернета (что охватывает и функции правообладателя интернет-сервиса), признается организатором распространения информации в Интернете; в его обязанности входит: уведомление в установленном Правительством РФ порядке федерального органа исполнительной власти, осуществляющего функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи, о начале осуществления указанной деятельности; хранение на территории РФ информации о фактах приема, передачи, доставки и (или) обработки голосовой информации, письменного текста, изображений, звуков, видео- или иных электронных сообщений пользователей Интернета и информации об этих пользователях в течение одного года с момента окончания осуществления таких действий, а текстовых сообщений пользователей этой Сети, голосовой информации, изображений, звуков, видео-, иных электронных сообщений пользователей Интернета – до шести месяцев с момента окончания их приема, передачи, доставки и (или) обработки и предоставление этой информации уполномоченным государственным органам, осуществляющим оперативно-разыскную деятельность или обеспечение безопасности Российской Федерации, в случаях, установленных федеральными законами. При этом обязанность хранить информацию не предполагает право разрешать или ограничивать доступ к этой информации, принадлежащее ее обладателю: основания и порядок предоставления такой информации определяются федеральными законами, а ее получателем от организатора распространения информации в Сети может быть только уполномоченный орган[1].

Диалектическая значимость конституционных принципов информационной открытости и конфиденциальности должны реализовываться с учетом общеправовых принципов *правовой определенности, соразмерности и пропорциональности*.

[1] См.: п. 4 Постановления Конституционного Суда РФ от 26 октября 2017 г. № 25-П «По делу о проверке конституционности пункта 5 статьи 2 Федерального закона “Об информации, информационных технологиях и о защите информации” в связи с жалобой гражданина А.И. Сушкова».

В постановлениях Конституционного Суда РФ от 30 октября 2003 г. № 15-П, от 26 декабря 2005 г. № 14-П; от 16 июня 2006 г. № 7-П, от 19 апреля 2010 г. № 8-П, от 31 марта 2011 г. № 3-П, от 30 июня 2011 г. № 14-П, в Определении Конституционного Суда РФ от 7 февраля 2013 г. № 134-О и др. подчеркивается, что, устанавливая правовой режим пользования правом на информацию, законодатель должен исходить из того, что любые его ограничения допустимы лишь постольку, поскольку они являются необходимыми и соразмерными конституционно признаваемым целям, не посягают на само существо этого права и не приводят к утрате его реального содержания, закрепляются при помощи формально определенных, точных, четких и ясных предписаний, не допускающих расширительного толкования установленных ограничений и, следовательно, произвольного их применения.

В п. 3.1 Определения Конституционного Суда РФ от 18 января 2011 г. № 8-О-П «По жалобе открытого акционерного общества «Нефтяная компания “Роснефть” на нарушение конституционных прав и свобод положением абзаца первого пункта 1 статьи 91 Федерального закона “Об акционерных обществах”» указывается, что, учитывая право обладателя информации, составляющей коммерческую, служебную или иную охраняемую законом тайну, на охрану ее конфиденциальности (ч. 4 ст. 9 Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и защите информации»), федеральный законодатель, принимая во внимание особенности предпринимательской деятельности в форме акционерного общества, а также специфику и объем предоставляемой информации, вправе установить ограничения в виде определенного порядка или условий доступа к такой информации. Подобные ограничения, как указано в Определении Конституционного Суда РФ от 18 июня 2004 г. № 263-О, должны соответствовать принципу равенства всех перед законом и судом, гарантированному ч. 1 ст. 19 Конституции РФ и означающему, что при равных условиях субъекты права должны находиться в равном положении.

В п. 2 Постановления Конституционного Суда РФ от 30 июня 2011 г. № 14-П «По делу о проверке конституционности положений пункта 10 части 1 статьи 17 Федерального закона “О государственной гражданской службе Российской Федерации” и статьи 20.1 Закона Российской Федерации “О милиции” в связи с жалобами граждан Л.Н. Кондратьевой и А.Н. Мумолина» подчер-

кивалось, что государство призвано создавать наиболее благоприятные условия для общественного контроля за деятельностью органов публичной власти и их должностных лиц, обеспечения открытости их деятельности, предоставления гражданам полной и достоверной информации, касающейся процесса и результата выполнения возложенных на них функций. Из этого следует, что свобода слова – не только гарантированная государством возможность беспрепятственно выражать посредством устного или печатного слова свои суждения по самым разным вопросам, но и условие эффективности общественного контроля за действиями публичной власти, и что конституционное требование о недопустимости принуждения к отказу от своих мнений и убеждений адресовано государственным органам, органам местного самоуправления, политическим партиям, другим общественным объединениям, их должностным лицам, всем членам общества для предотвращения разглашения информации, полученной конфиденциально.

Несмотря на то что информационное общество развивается на основе знаний и осведомленности, важно сохранить классическую конструкцию диалектической взаимосвязи принципов информационной открытости и конфиденциальности, выражающуюся в их сбалансированности.

Считаем, что оптимальная модель правового обеспечения информационной безопасности личности в условиях глобального информационного общества должна формироваться именно на диалектической взаимосвязи принципов конституционного права в целом и принципов информационной открытости и конфиденциальности в частности.

Представляется, что именно принципы конституционного права в диалектическом единстве содержат потенциальные возможности для регулирующего воздействия на темпы, масштабы и направления развития информационного общества в России.

Так, в пункте 2 Определения Конституционного Суда РФ от 25 января 2012 г. № 162-О-О «Об отказе в принятии к рассмотрению жалобы гражданина Данилова И.Г. на нарушение его конституционных прав ч. 3 ст. 125 АПК РФ, ч. 1 и 2 ст. 15 Федерального закона “Об обеспечении доступа к информации о деятельности судов в Российской Федерации “», вынесенного в рамках осуществления конституционного нормоконтроля, указано, что ст. 15 Федерального закона «Об обеспечении доступа к информации о деятельности судов в Российской Федерации», устанавливающая,

в частности, что тексты судебных актов, за исключением приговоров, размещаются в Интернете после их принятия, тексты судебных актов, подлежащих в соответствии с законом опубликованию, а также тексты иных судебных актов, вынесенных Конституционным Судом РФ, конституционными (уставными) судами субъектов РФ, арбитражными судами, за исключением текстов судебных актов, установленных законодательно, размещаются в сети Интернет в полном объеме, обеспечивает действие принципов гласности и открытости судебного разбирательства, способствует реализации законной силы судебного решения, а потому не может рассматриваться как нарушающая какие-либо конституционные права заявителя.

Таким образом, использование новых технологий в условиях новой информационной реальности не всегда позитивно, и значимость реализации принципов конституционного права при активном использовании современных цифровых технологий возрастает.

Говоря о принципе равенства, который закреплен в международных актах и конституциях различных государств, необходимо заметить, что ученые поднимают вопрос «цифрового неравенства». Этот термин отражает разрыв между людьми, имеющими свободный доступ к цифровым и информационным технологиям, и теми, для кого доступ в Интернет ограничен или полностью отсутствует. Цифровое неравенство имеет два измерения: географическое (городские и сельские районы, развитые и слаборазвитые регионы) и социальное (цифровая грамотность, доступ для уязвимых групп или язык). Последнее может быть обусловлено физическими препятствиями, инфраструктурной неэффективностью, несовершенством информационных технологий и др.[1]

В зарубежной литературе обращается внимание на то, что основными из проблем введения новых цифровых технологий является повсеместное наблюдение и контроль, слабая защищенность персональной информации, низкая электронная грамотность

[1] См.: Алферова Е.В. Цифровые технологии и новые возможности реализации конституционных прав человека и развития демократии: Анализ некоторых дискуссионных вопросов // Современное конституционное право: отечественные и зарубежные исследования: сб. науч. тр. / РАН. ИНИОН; отв. ред. Е.В. Алферова, И.А. Умнова (Конюхова). – М., 2019. – С. 90–108. – Сер. «Правоведение».

населения[1]. Так, Виктория Лусена-Сид Изабель отмечает, что дистопический кошмар, описанный в романе-антиутопии Дж. Оруэлла «1984», не так далек от нашей повседневной реальности. В настоящее время существуют системы видеонаблюдения и мониторинга, которые во многих случаях превосходят фикцию Оруэлла. В больших и малых городах мира многие камеры используют технологии для наблюдения и контроля за деятельностью граждан (в пользу безопасности и социального контроля). В Лондоне, например, система видеонаблюдения (CCTV) имеет программное обеспечение для маркировки конкретных людей, отслеживая их на протяжении времени, и даже возможности «поиска» лиц в архивах записей[2].

Вопрос возможного вмешательства активно обсуждается и требует доктринального осмысления и выработки практических предложений относительно границ между публичным и частным интересом, а также установления обязанности для граждан контролировать доступную информацию о самом себе[3].

Актуальным также является формирование понимания того, должна ли быть обеспечена возможность сознательно-волевого выбора индивидом своего поведения без участия государства (свобода) или обязательно должна быть гарантирована ее реализация со стороны государства (право). Так, например, доступ в Интернет – право или свобода? Если эту возможность определять как право, то предполагается, что со стороны государства должны быть созданы соответствующие механизмы его реализации.

Интересен опыт государств, в конституциях которых нашли закрепление права, связанные с информационными отношениями. Например, в Конституции Греции 1975 г.[4] закрепляется, что каж-

---

[1] См.: Electronic democracy (e-democracy): Recommendation CM/Rec, 2009, 1 adopted by the Committee of Ministers of the Council of Europe on 18 February 2009 and explanatory memorandum. – URL: https://www.coe.int/t/dgap/democracy/activities/ggis/cahde/2009/RecCM2009_1_and_Accomp_Docs/6647-0-ID8289-Recommendation%20on%20electronic%20democracy.pdf (дата обращения: 15.03.2020).

[2] См.: Lucena-Cid I.-V. New technologies and their impact on human rights. Towards a new approach // Cuadernos Electronicos de Filosofia del Derecho. – 2019. – Vol. 40. – P. 128–146.

[3] См.: Westin A. Privacy and freedom. – New York, 1967. – P. 22; Schoeman F. Privacy and social freedom. – Cambridge, 1992. – P. 12.

[4] См.: Конституция Греции 1975 г. (в редакции 2008 г.). – URL: https://el.wikisource.org/wiki/%CE%A3%CF%8D%CE%BD%CF%84%CE%B1%CE%B3%CE%BC%CE%B1_%CF%84%CE%B7%CF%82_%CE%95%CE%BB%CE%BB%CE%AC%CE%B4%CE%B1%CF%82 (дата обращения 01.03.2020 г.).

дый имеет право участвовать в информационном обществе. Облегчение доступа к информации, передаваемой в электронном виде, а также ее производство, обмен и распространение являются обязанностью государства, которая реализуется при соблюдении гарантий прав на неприкосновенность жилища, тайну переписки, уважения частной и семейной жизни и защиту персональных данных (ч. 2 ст. 5 А).

В части 6 ст. 35 Конституции Португалии закреплена гарантия каждому на свободный доступ к информационным сетям общественного пользования, при этом закон определяет режим движения данных через границы, устанавливая формы, обеспечивающие защиту персональных и иных данных, охрана которых находится в сфере национальных интересов[1].

Имея конституционную природу принцип информационной открытости и связанные с ним такие социальные явления, как цифровая сфера, цифровой мир, цифровая реальность, должны подпадать под действие Конституции как акта, обладающего высшей юридической силой в государстве[2].

Таким образом, социальная активность человека в информационной среде порождает не только определенные запреты, но и новые правовые возможности, обусловленные потребностью обеспечения гарантирования и сохранения неприкосновенности частной жизни. Вместе с тем стоит подчеркнуть, что вопрос о границах «приватного пространства индивида» является одним из актуальных и требует выработки критериев ограничения, в силу того, что данная группа прав не относится к абсолютным правам.

Глобальный характер информационного общества и интенсивная государственная поддержка инновационных технологий предполагают необходимость выработки общих подходов к регулированию новых видов прав в данной сфере. В их числе требуют научного рассмотрения и правового закрепления такие права, как право на Интернет, право на забвение, право на идентификацию.

Основываясь на судебном прецеденте, Европейский парламент в 2014 г. разработал специальный Закон о защите данных,

---

[1] См.: Конституция Португалии 1976 г. – URL: https://worldconstitutions.ru/?p=141 (дата обращения 01.03.2020 г.).

[2] См.: Масловская Т.С. Цифровая сфера и конституционное право: грани взаимодействия // Конституционное и муниципальное право. – М., 2019. – № 9. – С. 18–22.

который, в частности, посвящен и праву на забвение[1]. В Российской Федерации Федеральный закон, закрепляющий право на забвение, вступил в силу 1 января 2016 г.[2] Уже есть практика использования данного права.

Так, в 2016 г. бизнесмен Сергей Михайлов добился удаления упоминаний о себе из выдачи поисковых сервисов по запросам о его причастности к преступным группировкам. В июле 2017 г. Яндекс проиграл судебный процесс бывшему министру сельского хозяйства РФ Е.Б. Скрынник. Одинцовский городской суд, куда обратилась Е.Б. Скрынник, удовлетворил ее просьбу и обязал поисковик «прекратить выдачу ссылок, позволяющих получить доступ в сети Интернет к недостоверной информации в отношении министра сельского хозяйства 2009–2012 гг. Е.Б. Скрынник»[3].

С развитием информационного пространства важным является вопрос о том, кто выступает субъектом, управляющим сетью Интернет, насколько гарантирована защита персональных данных, а также полнота и достоверность получаемой информации.

Таким образом, в сфере правового регулирования возникающих вопросов у интенсивно развивающегося информационного общества именно диалектическая взаимосвязь принципов конституционного права в целом и принципов информационной открытости и конфиденциальности в частности выступает как основа стабильности и устойчивого развития правопорядка в стране.

---

[1] См.: Суходолов А.П., Рачков М.П., Бычкова А.М. Запретительная политика государства в сфере средств массовой информации: анализ законодательства и правоприменительной практики. – М., 2018. – С. 48.

[2] См.: Федеральный закон от 13 июля 2015 г. № 264-ФЗ «О внесении изменений в Федеральный закон “Об информации, информационных технологиях и о защите информации” и ст. 29 и 402 Гражданского процессуального кодекса Российской Федерации».

[3] Решение Одинцовского городского суда от 6 апреля 2017 г. Дело № 2–2715/2017 // Официальный сайт Одинцовского городского суда. – URL: https://odintsovo--mo.sudrf.ru/modules.php?name=sud_delo&srv_num=1&name_op=doc&number=212778727&delo_id=1540005&new=0&text_number=1 (дата обращения 09.03.2020 г.)

2.4. Большие данные: Новые возможности и новые угрозы

Пока нет единого принятого определения «большие данные» («Big data»). Как правило, это понятие относится к массиву данных большого объема, который, хотя и слишком большой для традиционных баз данных и аналитических инструментов, но может анализироваться с использованием алгоритмов или других вычислительных методов. Одним из качеств, которые делают большие данные уникальными, является их способность выявлять тенденции, закономерности и отношения, которые остались бы незамеченными при использовании обычных моделей[1].

Наиболее часто обсуждаемые среди ученых темы по поводу «больших данных:

– границы конфиденциальности и информационной безопасности в эпоху «больших данных» и угрозы, связанные с сохранением личной информации и защитой персональных данных, в том числе данных правоохранительных органов;

– эволюция правовых институтов в процессе развития информационной эпохи;

– утопизм в оценке взаимосвязи между свободой человека и информационно-коммуникационными технологиями, нарастание разрыва между институтами защиты прав человека и самим человеком в эпоху информационного капитализма;

– риски, связанные с расширением инструментов искусственного интеллекта, «жертвами» которых на начальном этапе становятся конфиденциальность, анонимность и автономность, а в дальнейшем – основные человеческие ценности, свобода и демократические институты.

Big data и университеты: **Поиск компромисса между доступностью, прозрачностью и защитой**. До настоящего времени владельцами и хранителями огромного количества данных являются университеты. Часть из них они собирают или приобретают, другие данные являются продуктом их регулярного вида деятельности. Сбор и накопление данных в университетах могут носить «преднамеренный» или обязательный характер. Например, данные, полученные в рамках исследовательских проектов, или данные о студентах и преподавателях университета, собираемые в процессе

[1] См.: Areheart B., Roberts J. GINA, Big data, and the future of employee privacy // The Yale law journal. – 2019. – Vol. 128. – P. 758.

образовательной деятельности. Накопление таких данных и управление ими регулируются с помощью таких механизмов, как, например, грантовые или институциональные контракты. Кроме того, наряду с ними существуют и так называемые «случайные данные», которые трудно идентифицировать однозначно, а тем более – их регулировать. К «случайным данным» можно, в частности, отнести «пакеты программного обеспечения», которые устанавливаются в университетские сети для осуществления образовательной, исследовательской и административной деятельности. Также есть данные, которыми трудно управлять, поскольку трудно идентифицировать. Например, многочисленные данные, собираемые студентами и административными работниками университетов по различным поводам и причинам, данные о пользователях библиотеки или службах социальной поддержки, данные по безопасности[1].

Масштабы роста данных и их разнообразие увеличиваются темпами, о которых даже не подозревают администраторы университетов, которым не нужно получать разрешение на использование и обработку имеющихся данных. Но «третьи лица» за пределами университета могут стать первыми, кто осознает необходимость и возможность доступа к данным о частных лицах на любом уровне университета под любым, грамотно сформулированным, предлогом. Например, для создания партнерства с университетом.

Университеты, признавая неотъемлемую ценность данных, которые они собирают и хранят, уже столкнулись с непредвиденными проблемами, связанными с распоряжением данными, необходимостью поиска баланса между соблюдением прозрачности и доступности при сборе академических данных, защитой личных данных и защитой интеллектуальной собственности. В последние несколько лет университеты «осаждают» коммерческие компании с запросами на доступ к данным, ссылаясь на партнерские отношения с университетами.

В современном мире ценность этих данных стремительно возрастает, а возможность их использования неизбежно связана с ответственностью за управление данными и разнообразными типами рисков. Границы конфиденциальности и информационной безопасности, с которыми сталкиваются исследовательские университеты, охватывают не только проблему открытого доступа к

[1] Borgman C. Open data, grey data, and stewardship: Universities at the privacy frontier // Berkeley technology law journal. – Berkeley, 2018. – Vol. 33. – P. 370–371.

использованию данных, но и проблемы, связанные со злоупотреблением данными, киберрисками, «исправлением» данных для защиты конфиденциальности.

С одной стороны, накапливаемые данные предоставляют много новых возможностей для исследований, преподавания, администрирования процессов, создания новых партнерств, стратегического планирования университетов. Данные собираются из многочисленных источников и имеют много пользователей. В их число входят, прежде всего, университетское сообщество (студенты, преподаватели, сотрудники) и многие другие заинтересованные стороны. С другой стороны, университетское сообщество ожидает разумной степени конфиденциальности в их взаимоотношениях с университетом, безопасного «хранения» своих персональных данных. Преподаватели, исследователи и студенты также ожидают, что их «родные» университеты будут уважать их академическую и интеллектуальную свободу при управлении данными. Ожидания сообщества за пределами университета несколько иные и связаны с их прозрачностью, открытостью и ответственностью за используемые ресурсы: «хорошее управление означает выпуск за пределы университета некоторых видов данных и предотвращение выхода за пределы университета других видов данных»[1].

Этот широкий круг проблем был кратко сформулирован в 2010 г. под названием «Калифорнийская инициатива конфиденциальности и информационной безопасности» (PISI). Документ содержит ряд рекомендаций и инструментов для университетской политики и практики в области *конфиденциальности и информационной безопасности*:

– максимально следовать основной миссии университета – поддерживать академическую и интеллектуальную свободу;

– быть надежным хранителем информации, доверенной университету;

– обеспечивать университетскому сообществу доступ к информационным ресурсам для выполнения законных целей – исследовательских, образовательных и деловых;

– формировать университетское сообщество с четкими убеждениями, что конфиденциальность – это не только привилегия, но и обязанность каждого[2].

---

[1] Borgman C. Op. cit. – P. 368.

[2] См.: Ibid. – P. 369.

Массовый сбор данных, с одной стороны, создает огромные возможности для университетов в области исследований, преподавания, обучения, обслуживания, стратегического управления. Но, с другой стороны, эти же массивы данных подвергают университеты новым рискам. Поэтому в настоящее время, подчеркивает Кристина Боргман, профессор Школы права Калифорнийского университета в Лос-Анджелесе, на первый план по значимости выходит проблема конфиденциальности, а тема академической свободы и интеллектуальной собственности обсуждается уже в контексте конфиденциальности[1].

Университеты «влюблены в большие данные», как и другие сектора экономики, и достаточно эффективны в их использовании для получения конкурентного преимущества. Они имеют привилегированный доступ к исследовательским данным и данным об их сообществах, которые университеты могут добывать и объединять инновационными способами.

Университеты имеют привилегированный социальный статус в качестве хранителей общественного доверия, которое связано с дополнительными обязанностями по защите конфиденциальности, академической свободы и интеллектуальной собственности. Они должны быть хорошими управляющими большими данными. «Хорошее управление» для одних видов данных означает, что доступ к ним будет поддерживаться на неопределенный срок и таким образом, чтобы они могли повторно использоваться для новых целей. Для других видов данных «хорошее управление» означает их надежную защиту в течение ограниченного периода времени, после чего они будут уничтожены. Критерии защиты данных и доступа к ним также могут изменяться во времени, особенно это касается «серых» (непроверенных временем) данных.

За последнее десятилетие скорость сбора данных университетами увеличилась в геометрической прогрессии, в том числе благодаря расширению сотрудничества с правительственными организациями и бизнесом, использованию социальных сетей, Интернета и др. Поскольку способность добывать и объединять данные улучшается, а технологии становятся более совместимыми, границы между данными различного типа и происхождения

[1] См.: Borgman C. Open data, grey data, and stewardship: Universities at the privacy frontier // Berkeley technology law journal. – Berkeley, 2018. – Vol. 33. – P. 383.

продолжают размываться, а угроза возникновения новых киберрисков будет только усиливаться. Следовательно, и ответственность за «ответственное» управление большими данными будет только возрастать. По мнению К. Боргман, заслуженного профессора права Калифорнийского университета в Лос-Анджелесе, пока можно говорить о том, что механизмы обеспечения защиты и правил использования личных данных, академической свободы, интеллектуальной собственности, информационной безопасности еще только зарождаются.

Большие данные уже представляют собой ценный институциональный актив. Поэтому и отдельные лица, и учреждения должны быть готовы защищать данные, которые они собирают. «*Собирайте данные, которые важны, а не просто данные, которые легко собрать*»[1].

Большие данные как растущая угроза конфиденциальности частной жизни работников. В работе профессора права Университета штата Теннесси, Ноксвилл, Брэдли А. Эрхарта и профессора права Хьюстонского университета Джессики Л. Робертс проблемы, связанные с использованием больших данных, раскрываются через анализ действия Закона о недискриминации по генетической информации (The Genetic Information Nondiscrimination Act), далее – Закон GINA. Этот Закон был принят в 2008 г. и изначально задумывался как защита от дискриминации. Однако уже спустя десять лет после принятия GINA и по настоящее время закон стал рассматриваться в ином качестве – как правовой институт защиты конфиденциальности наемных работников и обеспечения личной безопасности сотрудников в целом. Более того, предполагается, что в среднесрочной перспективе действие GINA может быть распространено и на другие сферы, в том числе на профили в социальных сетях и поисковые системы. По мнению специалистов, обеспечение конфиденциальности во вспомогательных областях уже сейчас имеет критически важное значение, что именно закон GINA способен обеспечить именно ту защиту, которая нужна в эпоху больших данных[2].

Современные технологии позволяют работодателям иметь всё больше информации о своих сотрудниках и с помощью сбора и обработки новых данных добиваться максимальной отдачи от

[1] Borgman C. Op. cit. – P. 409, 411

[2] Areheart B., Roberts J. Op. cit. – P. 757.

наемного персонала и оценивать их способность к дальнейшему повышению индивидуальной производительности труда и, соответственно снижать издержки компаний на наемный персонал.

Так, относительно недавно в *The Economist* появилась информация о том, что Data-аналитическая компания Humanyze ввела для своих сотрудников идентификационные значки, которые фиксирует каждое их движение. Эти устройства включают микрофоны, принимающие разговоры, Bluetooth, датчики и устройства, которые отслеживают и регистрируют передвижения сотрудников в течение рабочего дня. Полученная информация сопоставляется с календарями сотрудников, электронными письмами и другими личными данными. Отчеты, полученные на основе этих данных, включают огромное количество самых неожиданных деталей, включая информацию о том, сколько времени сотрудник проводит с представителем одного пола, уровень их физической активности, количество времени, которое они тратят на разговоры и на выслушивание собеседника. Руководитель этой компании рассматривает подобные действия как «умный бизнес» и объясняет, что каждый аспект бизнеса становится все более «управляемым» на основе полученных данных. По мнению самих сотрудников, их компания знает о них гораздо больше, чем их семьи. И такое мнение все чаще встречается у сотрудников современных технологических компаний.

Сегодня работодатели имеют потенциальный доступ к беспрецедентному объему информации о своих сотрудниках. На примере различных кейсов А. Эрхарт и Д. Робертс показывают, каким образом работодатели пытаются получить доступ к данным своих работников и что интерес к этим данным сохраняется на протяжении всего периода трудовых отношений. Более того, увеличивается спрос работодателей на информацию не только о своих текущих работниках, но и о гипотетически возможных работниках. Такие данные собираются при поиске персонала, но особенно они актуальны при принятии решения о приеме на работу, предварительной оценке кандидата, в том числе с позиции возможности регулировать его поведение в период трудовой деятельности. При этом собираемая информация очень часто никак не связана со способностью сотрудников качественно выполнять свою работу. Например, потенциальный сотрудник может иметь отличные компетенции, высокоразвитые навыки и достаточный опыт, но у него есть привычка курить, но не на работе, а вне службы. И хотя курение

работника на дому не имеет ничего общего с его квалификацией, способностями или производительностью труда, для некоторых работодателей это является причиной отказа в приеме на работу такого кандидата из-за гипотетически возможного повышения расходов на медицинскую страховку[1].

У работодателей есть частный интерес к контролю частной жизни своих сотрудников, и новые технологии и большие данные предоставляют работодателям больше возможностей для наблюдения за своими работниками. Например, они могут использовать различные приложения и программное обеспечение для мониторинга своих работников. Современные технологии позволяют работодателям отслеживать, как часто и как долго сотрудники просматривают документы, пользуются Интернетом, читают электронные письма и общаются в социальных сетях. Работодатели могут собирать информацию о физическом здоровье и активности своих сотрудников, регулярности их участия в оздоровительных программах, которые, помимо всего прочего, регулярно осуществляют биометрические скрининги, проводят анкетирования по оценке риска для здоровья фитнес-программ. В качестве примера приводится компания Amazon, которая запатентовала браслеты для своих сотрудников, которые позволяют отслеживать не только их местоположение, но и движения рук, чтобы позволить компании «контролировать точность и производительность работников в режиме реального времени»[2].

Большие данные усугубляют существующие угрозы конфиденциальности для наемных работников, создают дополнительные возможности работодателям для использования больших данных для постоянного мониторинга или слежки за действиями своих сотрудников. Подчеркивается, что уже в ближайшем будущем работники могут столкнуться с полной потерей конфиденциальности на рабочем месте. Поэтому будущее GINA специалисты связывают с защитой конфиденциальности сотрудников компаний, которые сейчас особенно уязвимы перед работодателями, «шпионящими в мире больших данных»[3].

Работники могут тратить «драгоценное» для работодателя рабочее время на общение со своими коллегами по работе или в

[1] См.: Areheart B., Roberts J. Op.cit. – P. 755.
[2] См.: Ibid. – P. 756–757.
[3] См.: Ibid. – P. 710

социальных сетях, или на просмотры в Интернете. Работники могут не приходить на работу по состоянию здоровья или отсутствовать из-за выполнения семейных обязанностей (например, по уходу за детьми); они могут повышать страховые издержки работодателя из-за болезни или травмы. Отсюда возникает растущий интерес работодателя к тому, чтобы узнать, какие сотрудники чаще отсутствуют и по каким причинам, кто из них чаще отвлекается в рабочее время, кто более подвержен стрессовым ситуациям, кто чаще болеет или подвержен травмам. Наблюдение за общением и передвижением сотрудников в течение рабочего дня может дать работодателю информацию о том, какие подразделения меньше или хуже работают, каким образом используется пространство и техника компании. Наличие такой информации позволяет работодателям принимать решения о том, кого нанимать, кого увольнять, кого продвигать по службе, как добиться того, чтобы рабочая сила была максимально продуктивной и недорогой[1].

Недавнее исследование в Великобритании показало, что большинство респондентов считают, что их боссы шпионили за ними, а 75% опрошенных полагают, что объем слежки за сотрудниками, обеспечиваемый технологией, обернется дискриминацией и ростом недоверия к компании.

Подобные истории дают людям реальные основания для беспокойства о конфиденциальности и безопасности своей частной жизни. Новая технология, называемая «большими данными», предоставляет работодателю возможность собирать огромный объем информации, чтобы получить доступ к личной информации, которой люди не хотели бы делиться с окружающими (личные отношения, заболевания и др.). Работодатели такую информацию уже могут получать без участия самого работника. Например, кто чаще болеет, кто и где чаще испытывает стрессы – на работе или дома, кто планирует уйти в декретный отпуск или кто с большей вероятностью возьмет отпуск по уходу за ребенком[2].

Анализ больших данных может раскрыть личную интимную информацию о репродуктивной функции человека, которой он еще не поделился со своей семьей или друзьями. В качестве примера, когда с помощью больших данных раскрылась интимная информация, приводится Facebook (гигант социальных сетей), недавно

[1] См.: Areheart B., Roberts J. Op.cit. – P. 756

[2] См.: Ibid. – P. 713, 714.

подвергшийся атаке, в результате которой может выйти наружу сексуальная ориентация его пользователей, даже если они открыто не раскрывали ее в своем профиле. Или другая компания Visa по информации о покупках с помощью кредитной карты уже может прогнозировать количество разводов. Такие прогнозы позволяют компании определять будущие потенциальные кредитные проблемы, поскольку люди в процессе развода чаще пропускают платежи. Страховые компании также используют большие данные, чтобы получить дополнительную информацию об использовании кредита своими застрахованными, для снижения собственных рисков[1]. Поэтому защита конфиденциальности на работе сейчас важнее, чем когда-либо. Технология может вскоре сделать другие антидискриминационные законы устаревшими. В мире больших данных нужны защита против слежки со стороны работодателей и улучшение защиты конфиденциальности на работе.

Искусственный интеллект как двигатель больших данных: Риски и жертвы. По мнению профессора права Карла Манхайма (K. Manheim)[2] и Лирика Каплана[3], искусственный интеллект – это самая «подрывная» технология современной эры, влияние которого сможет затмить даже Интернет[4].

Искусственный интеллект – двигатель больших данных и Интернета вещей, незаметно проникающий в каждый уголок нашей жизни, влияние которого может превзойти даже Интернет. Его основными «жертвами» авторы называют информационную конфиденциальность, анонимность и автономность. Неизбежное и неконтролируемое расширение инструментов искусственного интеллекта создает угрозы для манипулирования основными демократическими ценностями и институтами[5].

Уже в настоящее время многие его приложения знакомы большинству пользователей. Например, распознавание голоса, вождение автомобилей, а также и другие, менее известные, но всё

---

[1] См.: Areheart B., Roberts J. Op.cit. – P. 759.

[2] Профессора Школы права Лойолы в Лос-Анджелесе *(Loyola Law School, Los Angeles)*.

[3] Л. Каплан (L. Kaplan) – ассоциированный член группы по конфиденциальности и безопасности данных *(Associate in Privacy & Data Security Group, Frankfurt Kurnit Klein & Selz, Los Angeles)*.

[4] Manheim K., Kaplan L. Artificial intelligence: Risks to privacy and democracy // The Yale law journal. – Yale, 2019. – Vol. 21. – P. 106–188.

[5] См.: Ibid. – P. 108.

чаще используемые – контент-анализ, медицинские роботы и др. Главная их особенность и преимущество заключаются в способности извлекать контент из неструктурированных данных о реальном мире и его обитателях. Миллионы терабайт данных о реальном мире и его обитателях генерируются каждый день и в огромных масштабах. Многое из того, что собирается, не имеет очевидного смысла. Цель искусственного интеллекта – отфильтровать огромный массив данных, найти в них «смысл» и действовать с большей точностью и лучшими результатами, в сравнении с человеком, который может самостоятельно достичь того же, но за более длительное время. Достижения в области искусственного интеллекта предвещают не только новую эру в вычислительной технике, но и представляют новые опасности для социальных ценностей, конституционных прав, а также угрозу частной жизни со стороны алгоритмов, социальных сетей и Интернета. Однако, по мнению правоведов и практиков, появляющийся искусственный интеллект является мощным инструментом не только и не столько для решения существующих проблем, сколько для создания новых.

Цифровой век перевернул многие социальные нормы и ценности, которые развивались на протяжении веков, основными из которых стали личная конфиденциальность, автономия и демократия. Либеральная демократия, власть которой в конце XX в. не имела себе равных в истории человечества, вначале существовала в эпоху новых технологических открытий и достижений в надежде на лучшее будущее и благополучие. В начале нового тысячелетия стали проявляться сигналы опасности (социальные сети, Интернет), породившие большие данные и угрозу конфиденциальности частной жизни.

Возникшие новые инструменты позволили скрыто отслеживать сложные процессы в поведении потребителей, наблюдателей и избирателей. *Возможно, самая большая социальная цена новой технологической эры искусственного интеллекта – это подрыв доверия и контроля над демократическими институтами*. Так, «психографическое профилирование» пользователей Facebook, проводившееся Cambridge Analytica во время выборов 2016 г. в Великобритании и США, уже рассматриваются как конкретные случаи. Но такие случаи манипулирования избирателями не рассматриваются как случайные или единичные угрозы, которые Искусственный интеллект представляет для демократии. *Сложные технологии манипулирования прогрессировали до точки, где люди*

воспринимают, что решения, которые они принимают, являются их собственными, но вместо этого часто «руководствуются» алгоритмом. Кто злоупотребляет искусственным интеллектом, тот может манипулировать нами и контролировать нас[1].

По мнению К. Манхайма и Л. Каплан, на национальном уровне пока не предпринимается особых усилий для сохранения *наших демократических институтов и ценностей*. Хотя искусственный интеллект уже представляет реальную угрозу для основных – *равенства перед законом и верховенства права*. Некоторые признаки таких опасностей уже предшествовали появлению искусственного интеллекта, например, скрытое манипулирование общественным мнением и избирательскими предпочтениями. Но они многократно усиливаются с помощью искусственного интеллекта. Например, его способность генерировать всеобъемлющие поведенческие профили из различных наборов данных и повторно идентифицировать анонимные данные, раскрывать «детали нашей личной информации для рекламодателей, правительств и незнакомцев».

«Кажется, мы находимся в ситуации, когда Марк Цукерберг, другие руководители Facebook и Google *имеют больший контроль над жизнью американцев, чем представители, которых мы выбираем»*[2].

Спорными функциями искусственного интеллекта называются «алгоритмический уклон» и «необъяснимый интеллект». Первая из них свидетельствует о «скрытной» способности искусственного интеллекта усиливать социальные предубеждения, но с претензией на объективность. А вторая – об отсутствии прозрачности полученных результатов, которые чаще основаны на рассуждениях. Ученые-правоведы приходят к выводу о том, что искусственный интеллект пока представляет собой «черный ящик» и полную противоположность демократическому самоуправлению. Вместе с тем нельзя недооценивать очевидные преимущества искусственного интеллекта, равно как и его неизбежность: *это не антиутопия будущего, а реальная и приемлемая траектория развития общества. Но необходимо видеть возникающие риски. Люди не могут быть в опасности как вид, но люди, безусловно, под-*

[1] См.: Manheim K., Kaplan L. Op. cit. – P. 109.
[2] Ibid. – P. 109.

вергаются риску с точки зрения наших демократических институтов и имеющихся демократических ценностей[1].

Эволюция правовых институтов в цифровую эпоху. Некоторые ученые еще в начале нового тысячелетия предсказывали, что децентрализованная культурная и политическая деятельность сетевых сообществ будет все больше вытеснять централизованный контроль над политическими и культурными процессами, расширять доступ к информации, содействовать наращиванию политического потенциала для людей во всем мире и демократизации общества.

Однако спустя полтора десятка лет стало ясно, что грандиозные представления о демократизации не осуществились. Вместо этого стратегии децентрализованного культурного и политического процессов способствовали совершенно другим видам трансформации, организованным вокруг появившихся и уже доминирующих глобальных платформ, занявших выгодные позиции для наблюдения, сбора данных, извлечения выгоды и манипулирования общественным сознанием. Политические активисты быстро осознали, что сетевая цифровая информационная среда предоставляет не только беспрецедентные возможности для инакомыслия и сопротивления, но и новые скрытые очаги для государственной цензуры и наблюдения. Проекты в Интернете повысили открытость и свободу от контроля, но отодвинули на второй план конфиденциальность и защиту личных данных.

Дж. Коэн, профессор Школы права Джорджтаунского университета, специалист в области интеллектуальной собственности, авторского права и неприкосновенности частной жизни, рассматривая эволюцию правовых институтов в цифровую эпоху, предлагает *пересмотреть интернет-утопизм в правовой мысли.* В частности, «утопизм» в отношении анонимности как силы институциональной дезорганизации, а также «утопизм» в отношении взаимосвязи между информационно-коммуникационными сетями и свободой человека. Очевидными для Дж. Коэна стали вывод о незаменимой роли действующих правовых институтов в защите свободы человека, а также заключение о том, что «*правовые институты, в ко-*

[1] См.: Manheim K., Kaplan L. Op. cit. – P. 110, 111.

торых мы нуждаемся, отличаются от тех, которые у нас есть»[1].

Открытость оказалась обоюдоострым мечом. С одной стороны, очарование моделей открытого контента стало мощным фактором, способствующим появлению новых информационных компаний. Бизнес-модель возникших компаний основана на сборе данных и монетизации потоков данных, генерируемых разработчиками контента и пользователями контента, включая таких глобальных гигантов, как Google, Facebook и Amazon. Однако лидеры этих компаний не воспринимают всерьез конфиденциальность и защиту данных как достойные и продвигающие свободу проекты. Поэтому, с другой стороны, власть «снизу» стала превращаться в силу, направленную на достижение любых целей, которых ее организаторы хотят достичь. Возникшая среда, основанная на платформе, стала благодатной почвой для «теорий заговора», например, скоординированных кампаний по усилению отрицания климатических изменений или кампаний, направленных на дискредитацию политических деятелей и институтов, а также для «идеологического экстремизма» и «этнического национализма»[2].

Ученые и политические активисты сосредоточились на предоставлении возможностей для распределенного анонимного общения и координации. Но последствия могут оказаться неоднозначными. С одной стороны, анонимность играет существенную структурную роль в современных демократических обществах. Но, с другой стороны, неоспоримо и то, что сетевые информационные и коммуникационные технологии обеспечивают «анонимных несогласных» возможностью злоупотребления экономической и политической властью. Неразрешимыми остаются вопросы, в какой степени модели поведения, которые исторически функционировали в качестве предохранительных клапанов в более сложных институциональных структурах, могут сохранить или даже усилить свою роль в обеспечении основных прав и свобод всех людей. В качестве примеров Дж. Коэном приводятся такие (анти)институциональные проекты, как WikiLeaks или проекты криптовалюты. По его мнению, они отражают утопичные и не особенно демократичные идеологии. Вместе с тем эти же проекты

[1] Cohen J. Internet utopianism and the practical inevitability of law // Duke law and technology review. – Durham, 2019. – Vol. 18, N 1. – P. 86.

[2] См.: Ibid. – P. 88, 89.

воспроизводят особую моральную и идеологическую философию, которая несовместима с социальным договором. Они показывают, что, хотя возможности анонимного онлайн-общения и координации играют и будут продолжать играть важную роль в обеспечении основных прав и свобод, такие возможности не могут заменить другие виды институционального строительства. Иначе говоря, анонимное несогласие и оппозиция являются предохранительными клапанами, а достижение эффективной защиты основных прав и свобод также требует применения и других механизмов[1].

Сетевые информационные технологии – это не просто новые возможности для контроля и сотрудничества. В течение многих десятилетий социальные и правовые институты отражали влияние «контрольной революции», которая началась с внедрения автоматизированных информационных систем в бизнес-процессы промышленных предприятий. Процессы «институциональной эволюции» породили новые институциональные конфигурации и компетенции, которые ставят новые сложные задачи перед традиционными подходами к обеспечению соблюдения основных прав человека.

Новые технологии обеспечивают широкий общественный доступ к информации, но вместе с тем позволяют мощным корпоративным организациям создавать глобальные империи, которые обладают все большей властью. Гигантские транснациональные корпорации, которые создают глобальные сетевые цепочки поставок, имеют практически неограниченную власть над своими работниками и имеют огромное влияние на окружающие сообщества. Государственно-правовые институты, связанные с правами человека, возникшие после Второй мировой войны, даже не могли предполагать таких изменений. Возрастающая власть и известность сетевых информационных гигантов заставляют старые правозащитные институты все чаще оставаться в стороне. Интеллектуальные цифровые технологии создают решения, которые являются специальными, персонализированными и основанными на шаблонах, но не принципиальными и обобщаемыми[2].

Продвижение человеческой свободы через отсутствие закона никогда не было «в чьих-то руках». Сложность заключается в том, что проблемы информационной эпохи, требующие институцио-

[1] См.: Cohen J. Op. cit. – P. 90–92.

[2] См.: Ibid. – P. 93.

нальных решений, в настоящее время глубоко незнакомы институциональным акторам, чьи действия смотрят в прошлое. Новые информационные возможности требуют не только новых форм управления, но и новых институциональных механизмов, способных эффективно их использовать[1].

Вред в социальных сетях, правоохранительные органы и репутационные риски. «Взрыв» социальных сетей изменил скорость и формат распространения информации о системе уголовного правосудия, а также фокус публичных обсуждений лиц, обвиняемых в совершении преступлений или даже арестованных, но чья вина еще не доказана судом.

Правоохранительные органы стремятся вытеснить традиционные средства массовой информации, расширить свое присутствие в социальных сетях, начиная от предоставления социальным сетям базовой информации о совершенных преступлениях и своих комментариев. Как отмечает Келси Штайн, по мере развития публичного дискурса Верховный суд США рассматривает дела, связанные с использованием правоохранительными органами социальных сетей, которые «клеймят» обвиняемых и тем самым наносят им репутационный ущерб. Основная цель – защитить граждан от вреда и от «навешивания ярлыков» в социальных сетях. По ее мнению, правоохранительные органы должны пересмотреть свои профессиональные принципы в условиях быстро меняющего ландшафта социальных медиа[2].

Притом что ущерб репутации сам по себе не требует проведения надлежащей правовой процедуры защиты, распространение негативной информации об обвиняемом (но не осужденном) может иметь негативные и долгосрочные последствия. Например, потерю работы и источника дохода.

В современном цифровом мире восстановление репутации или восстановление анонимности практически невозможно. Это означает, что размещение поста в социальных сетях может иметь пожизненные последствия для человека. Уничтожить эти посты в социальных сетях или скрыть их в цифровых архивах невозможно. В их памяти сохраняется разная информация, включая фотогра-

---

[1] См.: Cohen J. Op. cit. – P. 96.

[2] См.: Stein K. Dangers of the digital stockade: Modernizing constitutional protection for individuals subjected to state-imposed reputational harm on social media // The George Washington law review. – 2019. – Vol. 87. – P. 997.

фии. Поэтому работодатель, который решил не проводить официальную проверку анкетных данных соискателя, может быстро найти о нем информацию в Интернете[1]. Истец, подробности ареста которого и фотографии, размещенные в Facebook, сопровождаются дополнительными пояснительными или сомнительными комментариями, может обратиться в суд с иском о причинении репутационного вреда.

Несмотря на все преимущества и выгоды использования Интернета и социальных сетей, их использование всё чаще ведет к публичному и не контролируемому навешиванию «социальных ярлыков», несет риски причинения репутационного вреда. Опасность состоит в том, что участниками этого процесса и ответственными за навешивание социальных ярлыков становятся правоохранительные органы, которые призваны защищать граждан. Правоохранительные органы должны следовать четким правилам работы с социальными сетями и проявлять разумную сдержанность. Репутация человека является предметом государственной конституционной защиты, а ущерб репутации, по мнению ученых, требует пересмотра через объектив «социальных сетей»[2].

Существующая правовая база для рассмотрения исков по защите репутации и нанесению репутационного вреда, считает К. Штайн, явно отстает от темпов распространения и развития современных технологических изменений. Закон должен отвечать реалиям технологических изменений, а люди, которым причинен репутационный вред, должны иметь реальную возможность правовой защиты. Устранить «навешивание» правоохранительными органами «социальных ярлыков» может только суд, в том числе путем доработки доктрины репутационного вреда. Происходящие технологические инновации не должны возвращать общество «к примитивной тактике стыда в ошибочное стремление к справедливости»[3].

Представители правоохранительных органов считают, что сильная сторона социальных сетей состоит в вовлечении местного сообщества в обсуждение волнующих их проблем, в том числе во-

[1] См.: Stein K. Dangers of the digital stockade: Modernizing constitutional protection for individuals subjected to state-imposed reputational harm on social media // The George Washington law review. – 2019. – Vol. 87. – P. 1020.

[2] Ibid. – P. 1025–1027.

[3] Ibid. – P. 1029.

просов безопасности. Facebook и Twitter позволяют собрать полезную информацию для раскрытия преступлений в достаточно короткие сроки. Проблема состоит в том, что размещение в социальных сетях информации полиции об обвиняемом (а не осужденном) чаще всего воспринимается местным сообществом как *правда, которая не требует проверки*[1]. Поэтому местное сообщество и журналисты нередко выражают скептицизм по поводу целесообразности замены живого общения полиции с населением и журналистами на прочтение информации в социальных сетях. Это лишает местное сообщество открытого диалога с представителями власти при обсуждении волнующих их проблем. Кроме того, распространяемые полицией цифровые посты нередко содержат персональную или конфиденциальную информацию, а цель размещения такой информации не всегда очевидна[2].

Современные технологии произвели революцию в концепции «репутационного вреда», а размещение правоохранительными органами в социальных сетях информации об аресте существенно не отличается от размещения листовок в магазинах. Некоторые сотрудники правоохранительных органов признают, что их активность в социальных сетях может причинять репутационный вред, но предлагают искать баланс между правоохранительными органами и человеком, которому репутационный вред может быть нанесен. Например, в случае публикации фотографий при арестах подозреваемых лиц, чья вина еще не доказана. «Когда правоохранительные органы берут наказание в свои руки, личные права и репутация несут негативные последствия»[3].

Трансграничный доступ к данным и конфиденциальность информации. Повсеместное использование Интернета повысило зависимость сотрудников правоохранительных органов от данных, хранящихся в компаниях, занимающихся информационно-коммуникационными технологиями (ИКТ). Поскольку многие из них находятся в США, судебные и правоохранительные органы других стран должны обращаться за содействием в получении необходимой цифровой доказательной базы к правительству США.

---

[1] См.: Stein K. Dangers of the digital stockade: Modernizing constitutional protection for individuals subjected to state-imposed reputational harm on social media // The George Washington law review. – 2019. – Vol. 87. – P. 1014, 1015.

[2] Ibid. – P. 1019.

[3] Ibid. – P. 1014–1017.

Например, при расследовании, касающемся французских граждан, проживающих в Париже, французским правоохранительным органам нужно обратиться за помощью в Министерство юстиции США, если рассматриваемые подозреваемые использовали почтовую службу в США. Процесс получения трансграничных данных из США требует много времени и непрозрачен. Французские власти длительное время фактически не имеют доступа к информации о своих собственных гражданах, подозреваемых в преступлениях на территории своей страны – Франции. Появление CLOUD Act, предполагающего «хранение и доступ к данным и программам через Интернет вместо жесткого диска персонального компьютера», усугубило эту проблему[1]. С одной стороны, «облако» предотвращает потерю данных из-за сбоев компьютера, менее уязвимо для кражи, обеспечивает доступный носитель для обмена файлами. Кроме того, поставщики облачных услуг могут легко перемещать данные отдельных лиц из одной юрисдикции в другую, а также разделять данные, хранить данные на серверах в разных юрисдикциях. Если пользователь и поставщик облачных услуг находятся в одной юрисдикции, данные могут передаваться через несколько юрисдикций. Проблема состоит в том, что часто передача данных происходит без ведома пользователя и правоохранительных органов. Пользователь и облачный сервис могут находиться в одной юрисдикции, а данные могут проходить через несколько юрисдикций, причем без ведома пользователя и правоохранительных органов[2]. Это означает, что для получения нескольких электронных писем представитель правоохранительных органов может начать международные процедуры доступа к данным нескольких стран, которые могут затянуть судебное разбирательство. По мере того как облачный сервис становится все более распространенным, передача данных и обременительные процедуры доступа к международным данным могут вскоре стать правилом, а не исключением. На этом фоне появилось дело «*США против корпорации Microsoft (Ирландия)*», когда Microsoft отказалась соблюдать требование США, потому что запрошенные данные хранились в Ирландии. Дело рассматривалось в Верховном суде. В результате

[1] Подробнее см.: Bilgic S. Something old, something new, and something moot: The privacy crisis under the cloud act // Harvard journal of law and technology. – Harvard, 2018. – Vol. 32, N 1. – P. 321–355.

[2] См.: Ibid. – P. 321.

23 марта 2018 г. Верховным судом был подписан CLOUD Act[1], разъясняющий «законное» использование данных за рубежом. Несмотря на то что дело Microsoft Ireland было рассмотрено в соответствии с CLOUD Act, оно остается актуальным по сей день, поскольку выявило противоречивые мнения относительно воздействия трансграничного доступа к данным на конфиденциальность информации и международные отношения. Делается вывод о том, что цифровая конфиденциальность пользователей как внутри, так и за пределами США имеет тенденцию к уменьшению[2]. Утверждается, что последствия CLOUD Act для конфиденциальности будут более тяжелыми для иностранных граждан, так как правительства их собственных стран, США и соответствующие иностранные правительства будут иметь практически неограниченный

[1] Закон об уточнении правомерности использования хранящихся за рубежом данных (CLOUD Act), впервые представленный сенаторам Конгресса США в феврале 2018 г., уточняет и дополняет Закон о хранении информации, принятый в 1986 г.

Проблема передачи данных, хранящихся на зарубежных серверах, является очень острой для американских правоохранителей, поскольку компании, владеющие этими данными, часто не готовы выполнять требования властей, опасаясь нарушения законодательства иностранного государства. Многие из таких отказов вылились в продолжительные судебные процессы. Одним из самых громких процессов стало судебное разбирательство между США и компанией Microsoft. Пять лет назад Министерство юстиции США выдало компании ордер на передачу персональных данных одного из ее клиентов, подозреваемого в незаконной деятельности. Проблема заключалась в том, что запрос касался гражданина Ирландии и его персональные данные хранились на находящихся в Ирландии серверах. Продолжительное разбирательство, дошедшее в итоге до Верховного суда США, поставило целый ряд вопросов, связанных с защитой конфиденциальности и обеспечением безопасности в условиях цифрового общества. Для разрешения подобных ситуаций как раз и был разработан CLOUD Act. Законопроект призван внести ясность в процессы передачи персональных данных, хранящихся в различных юрисдикциях, по запросу иностранного государства.

Сторонники CLOUD Act считают, что он значительно упростит работу правоохранительных органов с персональными данными, а также снизит временные издержки и финансовые затраты на проведение судебных процессов. Благодаря тому, что CLOUD Act конкретизирует процедуры передачи данных между США и иностранным государством, заключившим с американским государством специальный договор, он позволит правоохранителям обеих стран получать доступ к данным пользователей, хранящимся на территории этих стран, а также в облачных хранилищах, находящихся вне юрисдикции любых судебных систем.

[2] См.: Bilgic S. Op. cit. – P. 333–351.

доступ к их данным с минимальными гарантиями конфиденциальности.

2.5. Рынок персональных данных и информационная безопасность: Как инновации «подрывают» основы традиционногоправового регулирования

В современном мире, где каждый день создаются новые изобретения и появляются новые технологии, инновации не являются чем-то удивительным и невероятным. Однако среди всего множества инновационных продуктов и технологий существуют такие, которые в корне меняют всю систему правового регулирования. Данные инновационные продукты и технологии получили название *«подрывные инновации».*

Ученые выделяют следующие признаки «подрывных инноваций»:

– они обладают новизной и совершенствуют существующие продукты и технологии;

– имеют большое социальное и экономическое значение;

– действующее законодательство не может дать подходящие ответы на вопросы о том, как могут или как должны регулироваться данные технологии[1].

Например, на настоящий момент у законодателей и правоприменителей нет ясного представления о том, как классифицировать рабочих в условиях экономики свободного заработка. Традиционно основным разделением является разделение на наемных работников и независимых подрядчиков. Обе разновидности имеют достоинства и недостатки для работников и работодателей. Так, наемные работники имеют право на различные льготы или социальную защиту, которые недоступны для независимых подрядчиков, и в то же время у них более жесткий график. Компаниям, в свою очередь, гораздо дешевле нанять независимого подрядчика, нежели наемного работника, однако над первым они имеют гораздо меньший контроль: независимый подрядчик самостоятельно решает, сколько у него будет работодателей и как будут распределяться между ними часы его работы.

[1] См.: Sowers W. How do you solve a problem like law-disruptive technology? // Law and contemporary problems. – Durham, 2019. – Vol. 82, N 3. – P. 193.

Наряду с экономикой свободного заработка к «подрывным инновациям», например, относятся, беспилотные автомобили и аддитивные технологии, имеющие большое социальное и экономическое значение и в то же время не вписывающиеся в существующую правовую систему. Так, 3D-печать (аддитивные технологии) подрывает основы действия патентного права, а автономные транспортные средства совершенно не поддаются классификации и регулированию в рамках существующих законодательных схем: например, неясен вопрос о распределении ответственности в случае ДТП.

Поскольку «подрывные инновации» представляют собой нечто новое, невозможно предвидеть, какое влияние могут оказать на них различные правовые и политические решения. Попытка привести такую технологию в соответствие с существующей законодательной базой может привести к ее уничтожению, утрате уникальных свойств. Например, экономика свободного заработка процветает потому, что она дает людям гибкость в выборе собственной профессии. Однако разделение работников в условиях экономики свободного заработка на наемных сотрудников и независимых подрядчиков может привести к потере данной гибкости.

Наряду с «праворазрушительными» технологиями» существенное влияние на развитие правовой мысли оказывает онлайн-реклама: контекстная и таргетированная, которая стала основным инструментом маркетинговых стратегий большинства компаний. Вместе с развитием данных типов рекламы стал развиваться и рынок персональных данных, средств и способов сбора, обработки и хранения личной информации. Кроме того, различные фирмы аккумулируют и коммерциализируют «безобидные» данные пользователей, такие, например, как «лайки» в Facebook. Объектом деятельности этих организаций также является важная информация, например, номер социального страхования[1]. Раскрытие номера социального страхования может привести к серьёзным последствиям, например, причинению имущественного вреда, снижению уровня кредитоспособности, поскольку компании активно исполь-

[1] См.: Helman L. Pay for (privacy) performance holding social network executives accountable for breaches in data privacy protection // Brooklyn law review. – N.Y., 2019. – Vol. 84, N 2. – P. 563.

зуют номер социального страхования в качестве формы идентификации личности при продаже товаров и предоставлении услуг[1].

Отсутствие транспарентности в политике конфиденциальности большинства компаний, способность современных устройств непрерывно записывать разговоры пользователей без их ведома значительно увеличивают риск утечки данных.

Угроза раскрытия личной информации становится все более реальной в жизни современных потребителей. Причин существует множество: недостаток знаний о том, как управлять кибербезопасностью; отсутствие осведомленности о том, как бороться с манипулятивной деятельностью, или отсутствие навыков правоприменения, что приводит к недостатку внимания, уделяемого кибербезопасности[2]. 7 сентября 2017 г. бюро кредитных историй Equifax объявило, что его база данных была взломана. В результате этого под угрозу была поставлена конфиденциальная информация примерно 143 млн американских потребителей, что составляет около 44% населения[3].

Значительную роль в сборе и использовании персональных данных играют социальные сети. За последние 15 лет пространство социальных сетей выросло буквально в геометрической прогрессии, привлекая к себе всё новых и новых пользователей. В связи с этим на сегодняшний день в данном пространстве содержатся значительные объемы персональных данных.

Социальные сети – это платформы, позволяющие пользователям взаимодействовать друг с другом в режиме онлайн. Бизнес-модели современных социальных сетей предполагают использование пользовательской информации в транзакциях с третьими лицами[4]. Таким образом, несмотря на то что в большинстве случаев социальные сети не взимают плату за предоставление своих услуг, они так или иначе монетизируют личные данные пользователей. В большинстве случаев это осуществляется посредством *таргетированной рекламы*.

Необходимо признать, что личные данные на сегодняшний день стали «новой нефтью» – ценным ресурсом. Безусловно, по-

---

[1] См.: Ibid. – P. 564.

[2] См.: Alwan H.B. National cyber governance awareness policy and framework // International journal of legal information. – Cambridge, 2019. – Vol. 47, N 2. – P. 70.

[3] См.: Marcus D.J. The data breach dilemma: proacrtive solutions for proptecting consumers' personal information // Duke law journal. – Durham, NC, 2018. – Vol. 68, N 555. – P. 556.

[4] См.: Helman L. Op. cit. – P. 524.

требители получают определенную выгоду от возрастающего объема собираемой о них информации, поскольку получают персонализированные, инновационные рекламные предложения. Однако контроля над тем, как впоследствии будут использоваться личные данные, пользователи практически не имеют. Это вполне устраивает компании, поскольку в совокупности эти данные стоят миллиарды. Таким образом, персональная информация может стать крупным бизнесом[1].

Основным средством сбора личной информации стали электронные устройства, которыми люди пользуются ежедневно. Электронные устройства стали неотъемлемой частью жизни каждого человека; информация, которую они собирают, еще никогда не была настолько личной и конфиденциальной. Интеллектуальные помощники, такие как Siri, Google Now и др., не отключаются никогда, реагируя в любое время на голосовые команды, например, «Okay, Google». Кроме того, персональные данные не исчерпываются информацией, собираемой и хранящейся дистанционными электронными устройствами. Например, многие люди теперь носят фитнес-трекеры и другие устройства, способные собирать биометрические данные, такие как сердечный ритм, и фиксировать передвижения с максимальной точностью[2]. В настоящее время люди взаимодействуют с *постоянно активными устройствами*, записывающими их разговоры и действия, которые впоследствии продаются рекламодателям.

Современные технологии открывают перед нами целый мир новых возможностей. Например, возможность управлять без помощи рук или печатать под диктовку для лиц с ограниченными физическими возможностями. В то же время необходимо правовое регулирование в отношении объема персональных данных, которые компании могут собирать и использовать.

Многие потребители могут вовсе не осознавать объем данных, собираемый их устройствами. В большинстве случаев они не понимают, какие возможности есть у постоянно активных девайсов. На сегодняшний день пользователи привыкли к мониторингу определенных аспектов своей жизни: электронных писем, поисковых запросов, данных о местоположении. Но современные устрой-

[1] См.: Marcus D.J. Op. cit. – P. 563.

[2] См.: Gray C.D. A right to go dark // SMU law review. – Dallas, 2019. – Vol. 72, N 4. – P. 646.

ства способны проникнуть в гораздо более личные сферы жизни человека. Даже если потребители готовы доверять компаниям-производителям такие данные, что будет в случае их утечки? Предание гласности записей личных разговоров может разрушить карьеру, репутацию или отношения. Утечка данных является серьезной проблемой даже для самых крупных и богатых компаний, ввиду этого просто необходимо совершенствование стандартов безопасности.

Проблемы с конфиденциальностью в отношении постоянно активных девайсов начали появляться к 2014 г. В том году браузер Google Chrome был подвергнут критике за встроенную возможность пассивно прослушивать разговоры пользователей для того, чтобы активироваться через кодовую фразу «Okay, Google». Небольшая популярность таких обновлений среди пользователей привела к тому, что компания Google отказалась от этой функции. В 2015 г. Федеральная торговая комиссия получила многочисленные жалобы от пользователей SmartTV от Samsung, поскольку в политике конфиденциальности компании прямо указывалось на то, что личные разговоры пользователей могут быть переданы третьим лицам в рамках функции голосового поиска на телевизоре[1].

Основной проблемой современного законодательства является то, что в соответствии с ним действия компаний являются правомерными и законными, если последние информируют об объеме информации, которую собирают. В итоге потребители связаны разнообразными *условиями обслуживания* и *политиками конфиденциальности, которые почти не читают,* поскольку их текст чрезмерно длинный и сложный для понимания. Более того, пользователи не имеют никаких других источников информации о том, какие данные были собраны, проанализированы и использованы и у кого есть к ним доступ. Сбор данных, аналитика и продажи компаний, как правило, находятся под защитой норм о коммерческой тайне.

Производители устройств должны в доступной и понятной форме предоставлять пользователям информацию относительно того объема данных, который впоследствии будет передан на серверы поставщиков услуг. Данное требование закрепила ч. 2 ст. 7

[1]См.: Privacy and liberty in an alaways-on, always-listening world / A.S. Bohm, E.J. George, B. Cyphers, Sh. Lu // The Columbia science and technology law review. – New York, 2017. – Vol. 19, N 1. – P. 10.

Регламента Европейского парламента и Совета ЕС 2016/679 от 27 апреля 2016 г. о защите физических лиц при обработке персональных данных и о свободном обращении таких данных (General Data Protection Regulation) (далее – Общий регламент о защите персональных данных, GDPR): «Если согласие субъекта данных дается в виде письменного заявления, которое также касается других обстоятельств, запрос о предоставлении согласия должен быть представлен в понятной и легкодоступной форме на ясном и доступном языке в том виде, который четко отличал бы его от других обстоятельств…» Более того, поставщики и производители услуг должны получать *отдельное информированное согласие каждый раз,* когда осуществляют передачу информации третьим лицам.

Потребителям также должно быть разрешено удалять любую информацию, которую они не хотят сохранять. Несколько лет назад решением Европейского суда в Брюсселе было подтверждено право физических лиц на удаление некоторых результатов поиска, содержащих сведения о них: Суд обязал Google Spain деиндексировать конкретные новости, появляющиеся при введении имени М.К. Гонсалес в поисковом запросе на региональном домене (доменах) верхнего уровня[1]. В результате этого в профессиональных кругах стали говорить о появлении права на забвение, которое впоследствии также получило закрепление в ст. 17 вышеуказанного Регламента: «Субъект данных имеет право требовать от контролера незамедлительного удаления относящихся к нему персональных данных, контролер должен незамедлительно удалить персональные данные…»

Политическое обоснование права на забвение заключается в том, что устаревшая информация, которая больше не относится к реальным обстоятельствам жизни конкретного лица, не должна сохраняться в тех случаях, когда она наносит ущерб данному лицу. В контексте Европейского союза право на забвение отражает основную приверженность союза к «информационному самоопределению» – основополагающей концепции Общего регламента о защите персональных данных.

[1] См.: Prince C., Vonn M., Gill L. The Aleph bet: Debating metaphors for information, data handling and the right to be forgotten // Canadian journal of law and technology. – Toronto, 2018. – Vol. 16, N 1. – P. 171.

Сторонники концепции открытых данных, транспарентности подчеркивают, что в результате осуществления права на забвение могут образоваться информационные пробелы, которые могут быть использованы заинтересованными лицами. Отсутствие какой-либо информации в большинстве случаев может трактоваться как попытка сокрытия чего-либо.

Кроме того, противники права на забвение утверждают, что его признание не является экономически эффективным: оно возлагает якобы ненужное бремя на поставщиков информации (в частности, Google или Microsoft), которые вынуждены будут вручную проверять запросы и, соответственно, изменять локальные индексы данных. Отрицательное отношение как к цензуре, так и к удалению информации вполне понятно. Это реальные риски, которые совершенно справедливо рассматриваются как посягательство на свободу мысли, общее наследие и коллективную идентичность[1]. Однако их защита не является безусловным основанием для отрицания права на забвение.

Общий регламент не устанавливает предельный срок хранения данных, а лишь закрепляет положение о том, что законодательство Европейского союза или государства – члена ЕС может уточнять общие условия GDPR, регулирующие законность обработки персональных данных, может устанавливать спецификации для определения контролера, типы подлежащих обработке персональных данных, срок хранения данных и другие меры для гарантии законной и справедливой обработки.

А.С. Бом, Э. Дж. Джордж, Б. Киферс, Ш. Лу считают необходимым требовать от компаний удаления информации, которая не использовалась *в течение двух лет.* Удаление данных должно производиться по умолчанию, если только пользователь не потребовал сохранения информации или если в отношении этой информации не был получен ордер в рамках расследования. Более того, компаниям должно быть разрешено хранить данные не всех пользователей, а только тех, кто дал свое согласие на это. Если же согласие не было дано, организации обязаны удалять данные или как минимум исключать из них идентифицирующие признаки. Регулярное удаление данных, если они больше не нужны для целей,

[1] См.: Prince C., Vonn M., Gill L. Op.cit. – P. 174.

ради которых были собраны, может снизить «потенциальную возможность взлома и других угроз конфиденциальности»[1].

В то же время двухлетний срок хранения данных дает производителям достаточно времени для того, чтобы использовать собранную информацию в целях улучшения выпускаемых продуктов и внедрения инноваций. Таким образом, желание компаний вводить новшества будет учтено, никак не затрагивая интересы отдельных потребителей в отношении конфиденциальности своих данных.

Наилучшим решением проблем с конфиденциальностью представляется внесение изменений на законодательном уровне в процессы сбора и хранения данных компаниями. С технической точки зрения закон должен создать минимальные стандарты кибербезопасности для хранения данных, установить требования к шифрованию всех форм персональной информации и предписывать надлежащую подготовку по вопросам безопасности для всех компаний. Также и любые данные, передаваемые с постоянно включенного устройства на сервер поставщика услуг или производителя, должны передаваться и храниться с использованием самых последних стандартов шифрования.

Кроме того, закон должен установить требование о введении в компаниях должности главного сотрудника по информационной безопасности и обеспечить, чтобы компании взяли на себя обязанность по соответствию устанавливаемым стандартам.

Общий регламент о защите персональных данных, вступивший в силу в мае 2018 г., имеет хорошие перспективы в развитии законодательства о конфиденциальности персональных данных[2]. Он устанавливает стандарты использования данных граждан Европейского союза, в том числе требование о получении явного согласия пользователя на использование его личной информации, право пользователей на доступ к копиям своих данных или право на их удаление.

Потребителям нужна правовая база для устранения потенциальных рисков конфиденциальности персональных данных. Эта база должна представлять собой определенные рекомендации по безопасности для контролеров данных и лиц, обрабатывающих

[1] Privacy and liberty in an alaways-on, always-listening world / A.S. Bohm, E.J. George, B. Cyphers, Sh. Lu. – P. 27.

[2] См.: Marcus D.J. Op. cit. – P. 584.

данные. Кроме того, она должна защищать неприкосновенность частной жизни пользователей, устанавливая для правоохранительных органов четкие правила, определяющие, когда и в каких целях они могут получить доступ к информации на устройствах.

По мнению Х.Б. Алван, необходимо внесение изменений и в уголовное законодательство. Внедрение инновационных компьютерных технологий, связанных с Интернетом, привело к возникновению новых форм преступности вскоре после появления этих технологий. Правоохранительные органы нуждаются в необходимом инструментарии для расследования киберпреступлений. Преступники могут действовать практически из любой точки мира и принимать меры, чтобы скрыть свою личность. Инструменты, необходимые для расследования киберпреступности, могут сильно отличаться от тех, которые используются для расследования обычных преступлений. Расследования, связанные с киберпреступностью, очень часто имеют сильную техническую составляющую. Кроме того, в связи с международным распространением киберпреступности необходимо развивать национальную правовую базу, позволяющую сотрудничать с правоохранительными органами за рубежом[1]. Кража личных данных или мошенничество с их использованием происходят тогда, когда кто-то неправомерно получает и использует персональную информацию другого человека, такую как номер социального страхования, в собственных корыстных интересах. Несмотря на то что подобные деяния являются незаконными, применение государственных санкций в большинстве случаев является практически неосуществимым, поскольку субъекты кражи или мошенничества являются иностранными гражданами, вследствие чего возникает много вопросов, связанных с юрисдикцией государств. Таким образом, пересмотр и разработка нового законодательства окажут незначительное воздействие без международного сотрудничества и согласования национальных уголовно-правовых норм.

Также Х.Б. Алван считает важным осуществление просвещения и правового воспитания населения. Дети и подростки представляют собой уязвимую группу пользователей, которые проводят много времени в Интернете и социальных сетях. Они подвергаются

[1] См.: Alwan H.B. Op.cit. – P. 85.

тем же угрозам, что и взрослые, однако воздействие на них может быть еще более разрушительным[1].

Исследования CompTIA показали, что основной причиной нарушений безопасности является человеческий фактор – ошибки сотрудников, которые либо не подчиняются правилам, либо не имеют соответствующих знаний ввиду непрохождения специального обучения по профессиональной подготовке. Распространение информации о кибербезопасности, обучение всех сотрудников организации, от секретаря на стойке регистрации до генерального директора, имеют важное значение для предотвращения угроз безопасности данных[2].

Более того, современная оплата труда руководителей платформ, привязанная к экономическим показателям компании, ничуть не стимулирует их к повышению уровня безопасности персональной информации пользователей. Это значительным образом усугубляет ситуацию, считает Л. Хелман: руководители предпочитают брать на себя чрезмерные риски, чтобы получить краткосрочную или среднесрочную прибыль, никак не учитывая долгосрочные интересы акционеров в поддержании доверия пользователей. Ввиду этого она предлагает ввести новую систему оплаты труда, в соответствии с которой размер вознаграждения руководителей будет зависеть не только от экономических показателей платформ, но и от уровня их конфиденциальности. Преимущества данного подхода заключаются в следующем: во-первых, он не регулирует действия компаний напрямую, влияя на них косвенным образом посредством особой системы оплаты труда топ-менеджеров; во-вторых, он позволяет оперативно реагировать на социальные изменения. Этот подход позволяет привязать интересы руководства компаний к интересам пользователей[3].

Зависимость оплаты труда руководителей от уровня конфиденциальности, утверждает Л. Хелман, будет поддерживать высокую степень защищенности данных пользователей, укреплять их доверие к платформам. Кроме того, платформа несет в себе положительный информационный эффект: методы работы с данными в сетях станут общедоступными, что позволит стимулировать конкуренцию в данной области. Более того, подобная модель оплаты

[1] См.: Ibid. – P. 70.
[2] См.: Alwan H.B. Op.cit. – P. 72.
[3] См.: Helman L. Op.cit. – P. 543.

труда никак не станет ограничивать рынок данных: информация пользователей может повысить эффективность розничной торговли, предотвратив чрезмерные маркетинговые расходы[1].

Безусловно, не все виды использования персональных данных имеют отрицательное значение. Главным образом, вызывает опасение использование данных без учета интересов пользователей. Руководители платформ должны ориентироваться на ожидания пользователей, принимать во внимание их мнение.

Таким образом, «подрывные инновации» и развитие таргетированной и контекстной рекламы привело к развитию рынка персональных данных. Широкое использование персональных данных пользователей стало причиной многочисленных нарушений прав граждан на неприкосновенность частной жизни. Решение данной проблемы требует комплексного, многоаспектного подхода. Это предполагает, в частности, *закрепление* права граждан требовать при определенных условиях удаления своих персональных данных из общего доступа через поисковые системы (право на забвение), *установление* предельного срока хранения данных, *введение* требований к механизмам безопасности для компаний, работающих с персональными данными.

[1] См.: Ibid. – P. 568.

Глава 3.
ЦИФРОВЫЕ АЛГОРИТМЫ И ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ В ГОСУДАРСТВЕННОМ УПРАВЛЕНИИ, СУДЕБНОЙ И ИНОЙ ЮРИДИЧЕСКОЙ ДЕЯТЕЛЬНОСТИ

3.1. Электронная алгоритмизация государственного управления: Предпосылки становления ее системы и проблемы транспарентности

Стремительное развитие информационной аналитики и рост вычислительных мощностей предоставили широкие возможности использования в государственном управлении сложных электронных статистических алгоритмов и средств искусственного интеллекта. Ученые и практикующие специалисты отмечают всё бо□льшие преимущества использования в государственном управлении алгоритмов машинного обучения. Автоматизация процедур осуществления публичных функций (принятия управленческих решений) способна оказывать существенное влияние на реализацию правовых норм, прав и обязанностей вовлеченных лиц.

Искусственный интеллект не является в государственном управлении чем-то новым. Помимо преимущественного использования систем электронной автоматизации в сферах обороны и безопасности, в конце 1990-х годов автоматизированные видеосистемы применялись для распознавания рукописных надписей на почтовых отправлениях при их сортировке[1]. Алгоритмы искусственного интеллекта в настоящее время широко задействованы в сферах страхования, финансов, образования, занятости, маркетинга, управления, безопасности и правоохранительной деятельности. Государства все более активно развивают собственные технологии искусственного интеллекта, внедряют системы электронной авто-

[1] См.: Mehr H. Artificial intelligence for citizen services and government / Harvard Ash Center for Democratic Governance and Innovation. – Cambridge, 2017. – P. 5.

матизации в процессы управления. В мире сложились условия высокой конкуренции в данной сфере – «гонка информационных технологий».

Так, например, согласно стратегии в области искусственного интеллекта ФРГ, страна должна стать одним из мировых лидеров в данной области – центром локализации разработок искусственного интеллекта. Особенностью подхода ФРГ называется разработка «человеко-центричных» систем искусственного интеллекта, ориентированных на защиту данных и благонадежность. Одним из главных условий достижения данной цели подразумевается создание бренда «Искусственный интеллект, сделанный в Германии» и получение им всемирной известности как образца качества. Частью данного бренда должна стать идея, что сделанные в Германии системы искусственного интеллекта и используемые ими пакеты данных находятся под защитой принципов «суверенитета данных» (*data sovereignty*) и «информационного самоопределения» (*informational self-determination*). Стратегия ФРГ делает специальный упор на поддержку субъектов среднего предпринимательства[1].

Правительство Великобритании провозгласило, что Великобритания «будет вести мир к безопасному и этическому использованию данных и искусственного интеллекта»[2]. «Американская инициатива в области искусственного интеллекта», утвержденная указом президента США «О поддержании американского лидерства в области искусственного интеллекта» в 2019 г., подразумевает создание правовых и фактических условий, делающих невозможным приобретение критических технологий США соперничающими государствами[3].

На ведущую роль претендует Китай. Новеллой является предложенная Министерством науки и технологий Китая идея «гибкого управления», подразумевающая своевременное оперативное реагирование на проблемы искусственного интеллекта по мере их возникновения. Стремительное технологическое развитие и сложность урегулирования их «обычными» правовыми сред-

[1] См.: Artificial intelligence, governance and ethics: global perspectives / A. Daly, T. Hagendorff, H. Li, M. Mann, V. Marda, B. Wagner, W. Wang, S. Witteborn // The Chinese university of Hong Kong faculty of law research paper.– 2019. – N 15. – P. 15.

[2] См.: Ibid. – P. 17.

[3] См.: Ibid. – P. 23.

ствами создают условия, когда законодатели не успевают за изменениями в системах искусственного интеллекта.

Глобальное сотрудничество в области этики управления искусственным интеллектом осуществляется, преимущественно, по инициативе Китая. Примечательно, что позиция Китая сильно контрастирует с позицией США, отражающей провозглашенный также и в иных областях принцип «Америка превыше всего», и позицией ЕС, направленной на экспорт «европейских ценностей» [1].

Внедрение искусственного интеллекта в государственное управление имеет и иные предпосылки, помимо появления необходимых технических условий – доступности информационных данных и средств их комплексного автоматизированного анализа. Идея управления обществом средствами искусственного интеллекта в значительной степени основывается на понимании природной ограниченности человека как вида, с одной стороны[2], и сложности структуры современного общества, систем социальных взаимосвязей, – с другой[3].

Даже максимальное, в современном понимании, эмоциональное и интеллектуальное развитие человека не будет иметь существенного значения, если поставить задачу выработать объективно допустимые оптимальные решения проблем, требующих учета всей множественности конкурирующих политических, социальных, экономических, экологических, идеологических, религиозных и т.д. переменных в около 200 странах, а также всего спектра существенных индивидуальных интересов человека[4]. Даже если решить предварительную задачу – обработать невероятно большие объемы разнородной, комплексной информации, классифицировать в большинстве случаев скрытые, неочевидные факто-

---

[1] См.: Artificial intelligence, governance and ethics: global perspectives / A. Daly, T. Hagendorff, H. Li, M. Mann, V. Marda, B. Wagner, W. Wang, S. Witteborn // The Chinese university of Hong Kong faculty of law research paper.– 2019. – N 15. – P. 21, 28.

[2] См.: Bartlett S.J. The case for government by artificial intelligence. – P. 4. – URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3089920 (дата обращения: 20.03.2020).

[3] См.: Liu H., Lin C., Chen Y. Beyond state vs Loomis: Artificial intelligence, government algorithmization, and accountability // International journal of law and information technology. – 2019. – Vol. 27, N. 2. – P. 123.

[4] См.: Bartlett S.J. Op. cit. – P. 8.

ры, затем следует предугадать и оценить сложные последствия предполагаемого решения[1].

Природная когнитивная и психологическая ограниченность человека всегда привлекала к себе внимание философов, физиологов, антропологов, юристов и других исследователей как фактор, объясняющий закономерности общественных процессов. Сегодня, в связи со стремительным развитием электронно-вычислительных технологий, она подвергается критической оценке, как обстоятельство морального выбора в пользу управления общественными процессами несравнимо более конкурентными средствами искусственного интеллекта.

История публичного управления человека человеком указывает на то, что люди не способны управлять друг другом без конфликтов и некомпетентных решений. У человека ограниченные возможности интеллекта, суженные память (каждое следующее поколение вынуждено заново осваивать одни и те же знания) и способности классифицировать и организовывать информацию и управлять ею. Человек не приспособлен понимать и принимать в расчет ментально чрезмерно сложную информацию. У него локализированное умение решения задач и принятия решений. Он склонен к совершению ошибок, включая ошибки в понимании фактов, в мышлении и в суждениях. Человек склонен к реактивному эмоциональному доминированию при отсутствии надлежащего рационального самоконтроля. Устойчивыми пороками психики человека являются реактивное эмоциональное доминирование при отсутствии надлежащего рационального самоконтроля, самоуверенность и невозможность точной самооценки, деструктивная политическая одержимость[2].

Таким образом, склонность к совершению ошибок, физическая и ментальная ограниченность, моральная неустойчивость человека препятствуют рациональному, целесообразному и эффективному управлению.

Наиболее очевидная выгода технологий искусственного интеллекта заключается в том, что они могут решать сложные комплексные задачи. Преимущества использования искусственного

[1] См.: Liu H., Lin C., Chen Y. Beyond state vs Loomis: Artificial intelligence, government algorithmization, and accountability // International journal of law and information technology. – 2019. – Vol. 27, N. 2. – P. 8.

[2] См.: Ibid. – P. 2, 4.

интеллекта в государственном управлении наглядно проявляются в задачах, требующих анализа больших объемов данных, особенно при недостатке специалистов, а также в рутинных задачах, требующих максимально скорого решения.

Искусственный интеллект способен сохранять в памяти громадные объемы разнородной информации, учитывая сложную множественность переменных, видеть в ней сложные, комплексные математические зависимости, не поддающиеся, как считалось ранее, аналитическому контролю[1]. Лежащие в основе искусственного интеллекта математические формулы технически являются беспристрастными. В них учитываются лишь заложенные, либо допущенные разработчиком аналитические модели. Алгоритмизация принятия решений может помочь избежать явных и скрытых предубеждений и ангажированности, способных вкрасться в менее формальное традиционное «интуитивное» принятие решений[2]. При разработке алгоритма государственные органы могут открыто исключить учет таких требующих деликатности характеризующих признаков, как раса, национальность, религия и т.п., а также указывающих на них категорий данных, если сочтут, что в противном случае выводы алгоритма будут несправедливыми[3].

Использование искусственного интеллекта способно повысить эффективность государственного управления, существенно снизить его расходы. Так, модель «умного города» (*smart city*) привлекла по всему миру внимание локальных государственных органов к доступности эффективного сбора и использования данных для отыскания в них важных закономерностей и распределения на их основе ресурсов государственных служб. К примеру, на основе данных о месте и времени (потенциального) совершения наибольшего числа преступлений производится полицейское пат-

---

[1] См.: Coglianese C., Lehr D. Transparency and algorithmic governance // Administrative law review / Washington college of law. – 2019. – Vol. 71, N. 1. – P. 16.

[2] См.: Castro D. Data detractors are wrong: The rise of algorithms is a cause for hope and optimism, CTR. For data innovation (2016). – URL: https://www.datainnovation.org/2016/10/data-detractors-are-wrong-the-rise-of-algorithms-is-a-cause-for-hope-and-optimism/ (дата обращения 20.03.2020); Brauneis R., Goodman E. Algorithmic transparency for the smart city // The Yale journal of law & technology. – 2018. – Vol. 20. – P. 116.

[3] См.: Brauneis R., Goodman E. Op. cit. – P. 116.

рулирование[1]. Систематическое отслеживание рецензий на пункты общественного питания, соответствующих отзывов в социальных сетях может информировать службы санитарного надзора об источниках пищевых заболеваний[2]. Города стремятся приспособить большие данные для рационализации государственных служб и их инфраструктур в здравоохранении, общественной безопасности, образовании, транспорте и энергетике[3].

Искусственный интеллект может снять в государственном управлении многие административные препоны, повысив удовлетворенность населения обслуживанием в государственных органах и, таким образом, доверие к государственной власти и ее легитимность[4].

Когда человек обращается в государственный орган, он обычно тратит время на поиск необходимой информации, изучение информационных стендов, интернет-ресурсов государственных органов, получение консультаций в сторонних организациях. Он тратит время, ожидая ответ на телефонные звонки, в очередях, на личных приемах. Искусственный интеллект может кардинально усовершенствовать обращение человека в государственные органы, сведя его к взаимодействию в режиме реального времени. Он может использоваться для заполнения официальных бланков, формулирования заявлений и требований. Искусственный интеллект может анализировать и характеризовать обращения в государственные органы и их результаты и, в последующем, доводить до сведения вновь обращающихся процедурные нюансы, наиболее эффективную практику, варианты решения вопроса иными средствами[5].

---

[1] См.: Ferguson A. Policing predictive policing // Washington university in St. Louis law review. – 2017. – Vol. 94, N. 5. – P. 1115; Joh E. The New surveillance discretion: Automated suspicion, Big data, and policing // Harvard law & policy review. – 2016. – Vol. 10, N. 1. – P. 15, 38; Brauneis R., Goodman E. Op. cit. – P. 107.

[2] См.: Brauneis R., Goodman E. Op. cit. – P. 115.

[3] См.: Currie M. Data as performance – Showcasing cities through open data maps // Big data & Society. – 2020. – Vol. 7, N. 1. – P. 1–14; Edwards L. Privacy, security and data protection in smart cities: A critical EU law perspective // European data protection law review. – 2016. – Vol. 2, N 1. – P. 28; Brauneis R., Goodman E. Op. cit. – P. 111.

[4] См.: Mehr H. Op. cit. – P. 6; Coglianese C., Lehr D. Op. cit. – P. 50.

[5] См.: Mehr H. Op. cit. – P. 5, 9.

Исследователи выделяют пять (основных) вариантов использования искусственного интеллекта при обслуживании населения в государственных органах: 1) консультирование; 2) поиск документов; 3) классификация и направление обращений по подведомственности; 4) языковые переводы; 5) составление проектов документов[1].

Тем не менее, помимо предоставления выгод для государственного управления, искусственный интеллект также создает и опасность причинения вреда не только управляемым субъектам, но и механизму управления в целом.

Существует много предпосылок того, что использование искусственного интеллекта в государственном управлении окажется неэффективным. Алгоритмы могут быть неверно сформулированы. Их обучение или тестирование может проводиться на ложной информации. Ошибки могут вызываться неполноценной индуктивной аргументацией, некорректным выбором и вводом данных, неверной оценкой факторов, сбоями в обеспечивающих работу алгоритма электронно-вычислительных машинах, программном обеспечении, сбоями в самом коде алгоритма и т.п.[2]

Опасность представляет то, что искусственный интеллект сам сможет совершать проблематичные и опасные действия, особенно в военной сфере, медицине и сфере уголовного правосудия. Наибольшую практическую озабоченность вызывают: потенциальная опасность самоуправляемых машин и, прежде всего, автономных автоматизированных систем вооружения; проблемы политической манипуляции средствами искусственного интеллекта, «алгоритмизированной дискриминации», алгоритмизированной социальной стратификации; проблема ограниченности моделей роботизированной интерактивной коммуникации, и т.п. [3]

Получившее широкий публичный резонанс и спровоцировавшее острые дискуссии среди западных ученых и практиков решение по делу *State vs Loomis*[4], вынесенное судом США, ярко демонстрирует, как не лимитированное и бесконтрольное

---

[1] См.: Mehr H. Op. cit. – P. 6.

[2] См.: Brauneis R., Goodman E. Algorithmic transparency for the smart city // The Yale journal of law & technology. – 2018. – Vol. 20. – P. 123.

[3] См.: Artificial intelligence, governance and ethics: global perspectives. Op cit. – P. 6–7.

[4] См.: State vs Loomis 881 N.W. 2 d 749 (Wis. 2016) 754 (US). А также: State vs Gallion 678 N.W. 2 d. 197 (Wis. 2004) 209 (US).

использование в реализации публичной власти электронных алгоритмов может привести к нарушению прав человека и принципа господства права (*rule of law*) [1].

Использование государством алгоритмов искусственного интеллекта по-новому ставит вопрос о содержании понятия «справедливость». Несмотря на свою сложность, заложенные в алгоритмы модели по своей природе являются упрощениями. Статистический прогноз, являющийся основой алгоритмизированного управления, в отличие от индивидуального прогноза, никогда не учитывает все возможные факторы, влияющие на конкретную ситуацию, так как он всегда оперирует конечным набором характерных статистических зависимостей (моделей)[2]. Алгоритм рассматривает человека как образец типологизированной группы, а не как индивида[3]. Обобщение приводит к одинаковой оценке разнящихся ситуаций (обстоятельств) [4].

В дискуссии о внедрении искусственного интеллекта в государственное управление встает больше вопросов, чем доступно решений. Эксперты выделяют ряд важных аналитических вопросов, остающихся неразрешенными: кого следует считать создателем электронных автоматизированных систем, применяемых в процедурах принятия управленческих решений? В каком социаль-

---

[1] См.: Pasquale F. Secret algorithms threaten the rule of law // MIT technology review online (1 July 2017). – URL: https://www.technologyreview.com/s/608011/secret-algorithms-threaten-the-rule-of-law/ (дата обращения: 15.03.2020); Ram N. Innovating criminal justice // Northwestern university law review. – 2018. – Vol. 112, N. 4. – P. 659, 683–691; Smith M. In Wisconsin, a backlash against using data to foretell defendants' futures' // The New York Times. – 2016. – 22 June. – URL: https://www.nytimes.com/2016/06/23/us/backlash-in-wisconsin-against-using-data-to-foretell-defendants-futures.html (дата обращения: 15.03.2020); Liptak A. Sent to prison by a software program's secret algorithms // The New York Times. – 2017. – 1 May. – URL: https://www.nytimes.com/2017/05/01/us/politics/sent-to-prison-by-a-software-programs-secret-algorithms.html (дата обращения: 15.03.2020).

[2] См.: Gorwa R., Binns R., Katzenbach C. Algorithmic content moderation: technical and political challenges in the automation of platform governance // Big data & society. – 2020. – Vol. 7, N 1. – P. 11; Brauneis R., Goodman E. Op. cit. – P. 112.

[3] См.: O'Neil C. Weapons of math destruction: How Big data increases inequality and threatens democracy. – Crown, 2016. – P. 20–23; The ethics of algorithms: mapping the debate / B. Mittelstadt, P. Allo, M. Taddeo, S. Wachter, L. Floridi // Big data and society. – 2016. – Vol. 3, N 2. – P. 8.

[4] См.: Brauneis R., Goodman E. Op. cit. – P. 123.

ном и экономическом контексте данные системы создаются и развиваются? Как сконструированы алгоритмы данных систем и на каких данных они основываются? Какова роль данных систем в различных процедурах принятия управленческих решений, в установлении индивидуальных прав и обязанностей? Способен ли человек проверять электронный алгоритм, применяемый в процедуре принятия управленческого решения и выданный им результат? Если да, то как? Если нет, то необходимо ли отказаться от применения автоматизированных систем или все же пытаться обусловить их применение правовыми и этическими принципами? Как можно обеспечить подотчетность применения искусственного интеллекта в процедурах принятия публичных управленческих решений? [1]

До конца неясно, будут ли системы электронной автоматизации вспомогательным средством в управленческих процессах или же они могут подменить дискрецию человека? Кто в итоге является «субъектом» принятия решений – государственные должностные лица или алгоритмы, на которые они полагаются? В связи с этим важно осознавать, что, с одной стороны, алгоритмы разрабатываются частными компаниями ради извлечения прибыли. С другой – фактически складывается положение, когда такие компании узурпируют функцию осуществления публичной власти посредством разработки, внедрения и контроля алгоритмов, интегрированных в управленческие процессы. Какова правовая природа и правовое основание такого положения?[2]

Новые условия ставят вопрос об изменении принципов построения современных правовых систем. Ключевым здесь является вопрос, каким этическим стандартам должны соответствовать разработка и использование искусственного интеллекта в условиях, когда за некоторыми из схожих принципов могут лежать различия в культурном, правовом и философском понимании[3]. Про-

---

[1] См.: Liu H., Lin C., Chen Y. Beyond state vs Loomis: Artificial intelligence, government algorithmization, and accountability // International journal of law and information technology.–2019. – Vol. 27, N 2. – P. 123–124.

[2] См.: Ibid. – P. 137.

[3] А. Дали, Т. Хагендорф, Х. Ли, М. Манн, В. Марда, Б. Вагнер, В. Вонг и С. Виттеборн считают, что этика искусственного интеллекта должна удовлетворять два условия, чтобы быть эффективной. Во-первых, она должна быть низконормативной – она не должна универсально определять, что хорошо, а что плохо. Во-вторых, она должна быть предметно ориентирована на конкретный объект

блему составляет сама способность современного права регламентировать разработку и применение искусственного интеллекта, его будущее развитие[1]. Одно очевидно уже сейчас: государства вынуждены учитывать проблемы искусственного интеллекта при планировании реформ своих внутренних правовых систем[2].

Отдельная проблема касается возможности принудительного обеспечения правовых и этических стандартов искусственного интеллекта. Так, серьезная дискуссия идет о том, какое фактическое влияние оказывают положения Общего регламента по защите данных ЕС 2018 г., насколько они способны разрешить возникающие проблемы[3].

Более того, такие факторы, как транснациональная природа цифровых технологий, глобализация экономики, роль частных компаний, доминирующих в разработке и применении искусственного интеллекта, поднимают вопрос о дееспособности и правоспособности установления правовых и этических стандартов искусственного интеллекта, единообразия и согласованности правового регулирования в разных юрисдикциях. Можем ли мы в современных геополитических условиях остановиться на подходе «прав сильнейший»?[4]

Поднимаемые вопросы крайне усложняются тем, что искусственный интеллект – сложное комплексное явление. Понятие «искусственный интеллект» получило обобщенное определение, как технологии, автоматически выявляющие структуры данных и делающие на основании них предположения об их зависимостях. Однако отдельные виды электронных автоматизированных систем, объединенные данным понятием, включающие, к примеру, алгоритмизацию, профайлинг (составление индивидуальных и коллективных портретов лиц), автоматизацию, машинное обучение, глубинные нейронные сети и т.д., имеют настолько существенные различия, что требуют разных правовых конструкций.

применения (см.: Artificial intelligence, governance and ethics: global perspectives. Op. cit. – P. 7, 29).

[1] См.: Ibid. – P. 7.

[2] См.: Mehr H. Artificial intelligence for citizen services and government / Harvard Ash Center for Democratic Governance and Innovation. – Cambridge (USA), 2017. – P. 3.

[3] См.: Artificial intelligence, governance and ethics: global perspectives. Op. cit. – P. 12.

[4] См.: Ibid. – P. 7.

Важно проводить различия между «узким искусственным интеллектом» (*narrow AI*), способным решать отдельную заданную интеллектуальную задачу или их ограниченное множество, и «общим искусственным интеллектом» (*general AI или broad AI*), имитирующим всю многогранность интеллектуальных способностей человека, способным решать различные или общие задачи[1].

Используемые в управлении алгоритмы искусственного интеллекта могут быть разделены в зависимости от степени влияния предлагаемых ими выводов на управленческое решение. Вывод алгоритма может иметь решающее значение, когда, в силу особенностей процедуры управленческого акта или в силу его взаимосвязи с иными алгоритмами, он непосредственно выражает решение государственного органа без участия человека или предопределяет его правовые последствия. Совершенно иное положение, когда вывод алгоритма в числе иных факторов будет рассматриваться контролирующим управленческий акт человеком, определяющим, какие правовые последствия в итоге будут применены.

Коглианес и Лер предполагают, что в настоящее время государства преимущественно используют алгоритмы искусственного интеллекта, выводы которых не имеют решающего значения[2]. К примеру, алгоритм выявляет (потенциальное) нарушение нормы, но не определяет санкцию, либо указывает на имеющее правовое значение обстоятельство, но не принимает разрешительный или запретительный акт. Однако они полагают, что такое положение не продлится долго. Вместе с развитием технологий машинного обучения, а также разрастанием инфраструктур ввода и обработки данных роль искусственного интеллекта в государственном управлении, скорее всего, расширится. Несложно представить алгоритмы, полностью отвечающие за финансовый аудит и его (окончательный) результат в целях (автоматического) предоставления налоговых вычетов, алгоритмы, выявляющие основания отказа в предоставлении лицензий, либо алгоритмы, автоматически определяющие условия содержания заключенного с учетом его склонности к насилию и т.п.[3]

---

[1] В современной дискуссии об использовании искусственного интеллекта в государственном управлении, как правило, рассматривается узкий искусственный интеллект. (См.: Ibid. – P. 6.)

[2] См.: Coglianese C., Lehr D. Transparency and algorithmic governance // Administrative law review / Washington college of law. – 2019. – Vol. 71, N 1. – P. 6–7.

[3] См.: Barton B., Bibas S. Rebooting justice: More technology, fewer lawyers, and the future of law. – 2017. – P. 111–115; Coglianese C., Lehr D. Op. cit. – P. 8–9.

Немного больше воображения необходимо, чтобы представить системы электронной алгоритмизации нормотворчества, отчасти из-за того, что разработка норм роботами может принять различные формы. Одной из наиболее простых может быть ситуация, когда алгоритмы машинного обучения будут периодически предлагать более точные основания принятия разрешительных (запретительных) актов, инициируя, таким образом, внесение изменений в нормативные акты. Алгоритмы машинного обучения могут эффективно определять и оперативно корректировать, к примеру, промышленные квоты, нормы загрязняющих окружающую среду выбросов или санитарные нормы[1].

Потребность в скором, автоматизированном нормотворчестве является всё более очевидной, если не сказать больше – неизбежной, как ответ на рост цифровой экономики. Субъекты экономической деятельности широко применяют алгоритмы искусственного интеллекта и, в частности, машинного обучения, эксплуатируя их возможности давать быстрые и эффективные решения сложных комплексных хозяйственных (технологических, маркетинговых и т.п.) вопросов, требующих учета экстраординарного множества условий. Критическая инфраструктура экономики все больше автоматически оперируется алгоритмами[2].

Для предметного обсуждения правовых проблем использования искусственного интеллекта в государственном управлении важно понимать техническую основу технологий искусственного интеллекта, порядок действий алгоритма, используемого в процедуре принятия управленческого решения. Он состоит из серии шагов, предпринимаемых для: 1) введения данных, 2) обработки данных и их исчисления, 3) выведения результатов исчисления[3].

Так, в частности, основная часть дискуссии, вызванной решением по делу *State vs Loomis*, строится вокруг того, что суд не дал оценку стадии обработки и исчисления данных, в пределах

---

[1] См.: Coglianese C., Lehr D. Op. cit. – P. 10.

[2] См.: Darmody A. Zwick D. Manipulate to empower: hyper-relevance and the contradictions of marketing in the age of surveillance capitalism // Big data & Society. – 2020. – Vol. 7, N 1. – P. 1–12; Coglianese C. Optimizing regulation for an optimizing economy // University of Pennsylvania journal of law & public affairs. – 2018. – Vol. 4, N 1. – P. 1–13; Coglianese C., Lehr D. Op. cit. – P. 13.

[3] См.: Liu H., Lin C., Chen Y. Beyond state vs Loomis: artificial intelligence, government algorithmization, and accountability // International journal of law and information technology. – 2019. – Vol. 27, N 2. – P. 134.

которой встают наиболее критические проблемы – как интерпретируются данные и как интерпретация предопределяет результат исчисления. Основываясь на подтвержденном Верховным судом США «праве быть осужденным на основе точной информации»[1], суд сфокусировался на точности введения данных и точности выведения результатов их исчисления, исключив ключевую для алгоритмов искусственного интеллекта стадию обработки и исчисления данных из толкования понятия «точная информация»[2].

Преимущества искусственного интеллекта и, прежде всего, машинного обучения имеют обратную сторону – чрезмерную сложность и неочевидность алгоритмов для человека, а следовательно, недостаток их транспарентности[3]. Одним из наиболее сложных является вопрос, насколько техническая сложность алгоритмов искусственного интеллекта, используемых в государственном управлении, повлияет на способность государства аргументировать принятые с их помощью решения, особенно в случае замещения ими человека[4]. Выражается озабоченность становлением мира, контролируемого секретными механизмами управления[5].

В природу алгоритмов искусственного интеллекта заложен так называемый «черный ящик» (*the «black box»*)[6] – они полагают-

---

[1] См.: Townsend vs Burke, 334 U.S. 736 (1948) 738–741; См. также: Gardner vs Florida, 430 U.S. 349 (1977).

[2] См.: Liu H., Lin C., Chen Y. Op. cit. – P. 134.

[3] См.: Accountable algorithms / J. Kroll, J. Huey, S. Barocas, E. Felten, J. Reidenberg, D. Robinson, H.Yu // The University of Pennsylvania law review. – 2017. – Vol. 165, N 4. – P. 636; Coglianese C., Lehr D. Transparency and algorithmic governance // Administrative law review. – 2019. – Vol. 71, N 1. – P. 4, 16, 33.

[4] См.: Coglianese C., Lehr D. Op. cit. – P. 20.

[5] См.: O'Neil C. Weapons of math destruction: How Big data increases inequality and threatens democracy. – Crown, 2016. – P. 13; Brauneis R., Goodman E. Algorithmic transparency for the smart city // The Yale journal of law & technology. – 2018. – Vol. 20. – P. 103, 132–133; Beer D. The social power of algorithms // Journal of information, communication & society. – 2017. – Vol. 20, N 1. – P. 3; Bucher T. «Want To Be on the Top?»: Algorithmic power and the threat of invisibility on Facebook // New media & Society. – 2012. – Vol. 14, N 7. – P. 1164; Coglianese C., Lehr D. Op. cit. – P. 33.

[6] «Black box» – алгоритм, для которого известны лишь входные и выходные данные (см.: Pasquale F. Secret algorithms threaten the rule of law) // MIT Technology review online (1 July 2017). – URL: https://www.technologyreview.com/s/608011/secret-algorithms-threaten-the-rule-of-law/ (дата обращения: 15.03.2020). К вопросу о неочевидности алгоритмов искусственного интеллекта см. также: Ananny M. Toward an ethics of algorithms: convening, observation, probability, and

ся на аналитические конструкции и причинно-следственные зависимости, которые человек не способен понять или объяснить[1].

В анализе применимости искусственного интеллекта в государственном управлении проблема «черного ящика» является ключевой. Она предопределяет решение вопроса, может ли алгоритмизированное управление быть определено правовыми принципами и, в частности, принципом транспарентности государственного управления[2]. Игнорирование потребности в установлении правовых рамок применения алгоритмов обесценивает роль государства в общественном взаимодействии как конечного гаранта индивидуальных прав, призванного обеспечить эффективные средства защиты[3].

Лю, Лин и Чен предлагают разделять в анализе проблему «правового черного ящика» (*legal black box*) и проблему «технического черного ящика» (*technical black box*)[4]. В основе проблемы «правового черного ящика» лежит конкуренция традиционных правовых норм, защищающих патентные права на исходные коды и статистические модели алгоритмов, а также коммерческую тайну и иную конфиденциальную информацию, с одной стороны, и правовые принципы раскрытия информации в публичных целях – с другой.

Значительно более сложные проблемы связаны с «техническим черными ящиком», когда никто и даже программисты не могут до конца объяснить, как и почему искусственный интеллект приходит к конкретному заключению. Техническая природа средств искусственного интеллекта, и, прежде всего, машинного обучения (*machine learning*) и глубокого обучения (*deep learning*), характеризуется имманентным недостатком транспарентности, так

---

timeliness // Science, technology & human values. – 2016. – Vol. 41, N 1. – P. 93; Beer D. Op. cit. – P. 3; Burrell J. How the machine ‘thinks:’ Understanding opacity in machine learning algorithms // Big data & Society. – 2016. – Vol. 3, N 1. – P. 1; Citron D., Pasquale F. The Scored society: Due process for automated predictions // Washington law review. – 2014. – Vol. 89, N 1. – P. 1; Crawford K. Can an algorithm be agonistic? Ten scenes from life in calculated publics // Science, technology & human values. – 2016. – Vol. 41, N 1. – P. 77.

[1] См.: Coglianese C., Lehr D. Op. cit. – P. 14.

[2] См.: Ibid. – P. 1, 5.

[3] См.: Liu H., Lin C., Chen Y. Beyond state vs Loomis: artificial intelligence, government algorithmization and accountability // International journal of law and information technology. – 2019. – Vol. 27, N 2. – P. 134.

[4] См.: Ibid. – P. 135–138.

как новые правила принятия алгоритмами решений возникают здесь безотчетно. Так, в отличие от «экспертных систем» (expert systems), основывающихся в принятии решений на иерархии норм, переменных условий и ограничений, искусственные нейронные системы изучают зависимости в отличающейся информации и ее кластерах, используя сложную неиерархичную многоуровневую схему необусловленного подбора зависимостей (*representational learning*), вырабатывая собственные правила принятия решений, как правило, недоступные человеческому пониманию.

Проблема «технического черного ящика» может существенно подорвать попытки государств обеспечить транспарентность использования искусственного интеллекта в принятии управленческих решений, в частности попытки разрешить проблемы «правового черного ящика»[1].

В то же время без транспарентности алгоритма невозможна оценка его справедливости.

Транспарентность государственного управления выполняет ряд функций. Она не только удерживает должностные лица от злоупотребления властью, но и обеспечивает целостность системы взаимного контроля государственных органов, межведомственную согласованность в реализации государственной политики. Когда негосударственные организации и общественность видят и понимают решения и действия государственных органов, они способны эффективно организовывать собственную работу в соответствии с программами государства. Они способны понимать динамику их изменения. В демократических обществах транспарентность закладывает основу для информированного и осмысленного участия общественности в принятии и реализации решений государства.

Несмотря на крайнюю важность, транспарентность государственного управления сложно оценить, поскольку ее понимание может варьироваться[2]. Понятие транспарентности является достаточно динамичным. Оно допускает различные степени широкого и узкого толкования. Следует изначально отметить, что абсолютной транспарентности не существует в принципе. Информация о решении или действии является лишь их отражением и не воспроизводит их полностью.

---

[1] См.: Liu H., Lin C., Chen Y. Op.cit. – P. 135–136.

[2] См.: Coglianese C., Lehr D. Transparency and algorithmic governance // Administrative law review. – 2019. – Vol. 71, N 1. – P. 18–19.

Транспарентность государственного управления не может быть абсолютной и в правовом понимании. В правовые системы всегда будут включены принципы, исключающие раскрытие отдельных категорий информации. Так, конфиденциальность некоторых базовых данных, вводимых в алгоритмы искусственного интеллекта, используемых в машинном обучении, подлежит обязательной правовой защите, как, например, персональные медицинские данные и данные об образовании, кредитные истории и т.п.[1]

Принцип транспарентности государственного управления является обусловленным.

Коглианес и Лер разграничивают принципы «транспарентности чистого стекла» (*fishbowl transparency*) – раскрытие информации о том, *что* делают государственные органы, и «аргументированной транспарентности» (*reasoned transparency*) – раскрытие информации, *почему* они совершают те или иные действия[2]. Последний вид транспарентности требует от государства обосновывать свои решения.

Специфика проблемы «черного ящика» проявляется в аргументированной транспарентности – способности государственного органа объяснить, *почему* он приходит к решению, предлагаемому искусственным интеллектом[3].

Проблема неясности алгоритмов усугубляется тем, что их разработка и последующее техническое обслуживание на современном этапе находятся под контролем частных компаний. Здесь проявляется важность специализации в обращении с технологиями искусственного интеллекта. Каждый из этапов алгоритмизированного процесса – 1) разработка модели достижения заданной цели, основанной на анализе имеющихся исторических данных; 2) кодирование алгоритма данной модели; 3) сбор данных для ввода в алгоритм; 4) обработка алгоритмом введенных данных; 5) вывод итога произведенных алгоритмом операций в виде прогнозов или рекомендаций[4] – требует особой подготовки специалистов и

---

[1] См.: Coglianese C., Lehr D. Transparency and algorithmic governance // Administrative law review. – 2019. – Vol. 71, N 1. – P. 35.

[2] См.: Ibid. – P. 19–20.

[3] См.: Ibid. – P. 22, 36.

[4] См.: Zarsky T. Transparent Predictions // Univercity of Illinois law review. – 2013. – Vol. 2013, N 4. – P. 1503, 1517–1520; Accountable algorithms / J. Kroll, J. Huey, S. Barocas, E. Felten, J. Reidenberg, D. Robinson, H. Yu // University of Pennsylvania law review. – 2017. – Vol. 165, N 4. – P. 640; Brauneis R., Goodman E.

сложной технической инфраструктуры, отсутствующей в большинстве органов государственного управления[1]. Это является одной из главных причин, почему государства заключают с частными компаниями контракты на разработку и последующее обслуживание используемых в государственном управлении алгоритмов[2].

Зависимость формул, лежащих в основе алгоритмов, от разрабатывающих их частных компаний становится препятствием их транспарентности, по меньшей мере, уже в пределах патентных прав. Раскрытие алгоритмов невыгодно для частных компаний, извлекающих из принадлежащих им прав прибыль. Уже сейчас они активно препятствуют раскрытию информации[3]. Более того, разумно предположить, что, в известной степени, сама неясность алгоритма может также представлять выгоду.

Как результат, частные компании приобретают ключевую роль в применении искусственного интеллекта в государственном управлении[4].

Если подобное «делегирование» власти неизбежно в современном обществе, оно должно иметь точную правовую основу. Однако даже если допустить предоставление частным компаниям публичных полномочий, четко определенных государством, встает целый ряд важных вопросов. Во-первых, какие типы решений государство может делегировать электронному алгоритму, находящемуся под контролем частной компании? Должны ли полномочия быть настолько широкими, чтобы предоставить алгоритму право принимать ценностно-ориентированные решения или же только решения, не допускающие усмотрения[5]?

Следует учесть, что коды и алгоритмы изначально основываются на суждениях о ценностях. Разработка алгоритма есть

Algorithmic transparency for the smart city // The Yale journal of law & Technology. – 2018. – Vol. 20. – P. 112–113.

[1] См.: Glicksman R., Markell D., Monteleoni C. Technological innovation, data analytics, and environmental enforcement // Ecology law quarterly. – 2017. – Vol. 44, N 1. – P. 41, 47; Brauneis R., Goodman E. Algorithmic transparency for the smart city // The Yale journal of law & technology. – 2018. – Vol. 20. – P. 114.

[2] См.: Coglianese C., Lehr D. Op. cit. – P. 30.

[3] См.: Wexler R. Life, liberty and trade secrets: Intellectual property in the criminal justice system // Stanford law review. – 2017. – Vol. 70, N 5. – P. 1350–1353.

[4] См.: Brauneis R., Goodman E. Op. cit. – P. 111.

[5] См.: Liu H., Lin C., Chen Y. Op. cit. – P. 137.

сложный процесс, подверженный влиянию человека на такие критерии, как принципы, семантика и логика интерпретации. Б. Мительштадт указывает на широко распространенное в среде разработчиков алгоритмов явление – при формулировании алгоритма изначально в уме разработчика держится такое его «предполагаемое» решение, которое отдает предпочтение одним ценностям и интересам в ущерб другим[1]. К. О'нил рассматривает средства электронной алгоритмизации управления как благодатную почву для любых форм социальной дискриминации[2].

Техническая сторона алгоритмизированного управления имеет собственную внутреннюю политическую составляющую. В каждом этапе алгоритмизированного процесса закодированы суждения о том, какие данные включать в расчет, а какие нет, как их оценивать, каким данным придавать большее значение, а каким меньшее[3]. Данные суждения могут иметь настолько важное (а часто неочевидное) влияние на итоговый вывод алгоритма, что требуют предварительного публичного обсуждения и оценки. Ложная идея, что алгоритмы – это чистая наука без политики, препятствует осознанию того, что стоит на кону при передаче контроля над алгоритмами частным компаниям, что более очевидно, к примеру, в случаях приватизации образовательных или пенитенциарных учреждений[4].

В этом отношении примечательна позиция правительства Австралии, еще в 2007 г. принявшего «Руководство по наилучшей практике: Автоматизированная поддержка принятия административных решений», в котором четко закреплено, что используемая в государственном управлении автоматизированная система должна

---

[1] См.: The ethics of algorithms: mapping the debate / B. Mittelstadt, P. Allo, M. Taddeo, S. Wachter, L. Floridi // Big data and society. – 2016. – Vol. 3, N 2. – P. 1; Liu H., Lin C., Chen Y. Beyond state v. Loomis: artificial intelligence, government algorithmization, and accountability // International journal of law and information technology. – 2019. – Vol. 27, N 2. – P. 137.

[2] См.: O'Neil C. Weapons of math destruction: How Big data increases inequality and threatens democracy. – Crown, 2016. – P. 29–31.

[3] См.: Surden H. Values embedded in legal artificial intelligence // University of Colorado law legal studies, research paper. – Boulder, 2017. – N 17/17. – P. 5; Berger J., Berry D. Statistical analysis and the illusion of objectivity // American scientist. – 1988. – Vol. 76, N 1. – P. 159–165.

[4] См.: Brauneis R., Goodman E. Op. cit. – P. 119.

быть разработана таким образом, чтобы аккуратно отражать суть государственной политики, которую она моделирует[1].

Оценить интегрированную в алгоритм политику, ее справедливость и как итог – справедливость предлагаемого алгоритмом вывода, можно лишь видя и понимая то, как алгоритм работает.

Особую озабоченность вызывает использование государственными органами алгоритмов прогнозирования, разработку и порядок действия которых ни они, ни общество не в состоянии понять. Разработавшие и, как правило, в последующем обслуживающие такие алгоритмы частные компании играют важную роль в механизме государственного управления.

Проблема даже не в том, что ответственность перед обществом в итоге несет государство, а не частые компании. Риск в том, что необъяснимость алгоритмов предоставляет корпорациям возможность «захватить» публичную власть. Само участие частных субъектов в управленческих процессах создает угрозу, что предоставляемые государством данные для ввода в алгоритм будут использованы частными субъектами в ущерб общественным и индивидуальным интересам, равно как и для ослабления государственной власти. Особую проблему составляет утрата государством контроля критически важной информации.

Государственные органы могут лишаться возможности видеть политику принятия решения или какую-то ее часть, встроенную в алгоритм. Зависимость от таких алгоритмов создает угрозу утраты состоятельности органов публичной власти. Полагаясь на решение алгоритма, которое он не может объяснить, государственный орган (постепенно) утрачивает компетентность в надлежащем осуществлении функций государственного управления[2].

Теоретически можно предусмотреть исключительно вспомогательное значение выводов алгоритма в принятии управленческого решения человеком, оценивающим данные выводы в числе иных факторов. Однако здесь возникает следующая проблема. Ко-

---

[1] См.: Automated decision-making. Bettter practice guide 2019. – URL: https://www.ombudsman.gov.au/__data/assets/pdf_file/0030/109596/OMB1188-Automated-Decision-Making-Report_Final-A1898885.pdf (дата обращения: 03.04.2020); Liu H., Lin C., Chen Y. *Beyond state vs Loomis*: Artificial intelligence, government algorithmization, and accountability // International journal of law and information technology. – 2019. – Vol. 27, N 2. – P. 138–140.

[2] См.: Brauneis R., Goodman E. Algorithmic transparency for the smart city // The Yale journal of law & technology. – 2018. – Vol. 20. – P. 109, 117.

гда алгоритм использует сотни категорий вводимых данных, каждая из которых может по-разному учитываться во множестве промежуточных суждений, крайне сложно определить решающее значение каждой из них в итоговом выводе алгоритма. Как государственному служащему оценить итоговый вывод с позиции его собственного понимания ситуации и справедливости? Не видя, какие факторы и в какой степени обусловливают вывод алгоритма, он не может оценить, приняты ли в расчет факторы, требующие, по его мнению, обязательного учета. Он вынужден отказаться либо от вывода алгоритма, либо от собственного понимания[1]. Вполне обоснованным будет предположить, что на практике государственные служащие будут, скорее всего, широко и безоглядно полагаться на выводы алгоритма в первую очередь.

Алгоритмизация государственного управления создает угрозу постепенной утраты государственными служащими самой способности принимать решения. В ходе своей профессиональной подготовки и приобретения опыта государственные служащие развивают чувство того, как человек строит свое поведение и какие в связи с этим последствия будет иметь управленческий акт. Недостаточное понимание механизмов автоматической алгоритмизации принятия решений и как следствие – неоправданное немотивированное предпочтение, отдаваемое выводам алгоритмов, будут способствовать атрофированию компетентности делать самостоятельные суждения.

Это может иметь драматические последствия. К примеру, сотрудники органов внутренних дел, получающие от алгоритмов инструкции, где и как патрулировать потенциально опасные районы, могут утратить собственное понимание природы и рисков общественно опасного поведения[2]. Нетрудно представить, какое косвенное влияние оно может оказать на всю систему правоохранительной деятельности и борьбу с преступностью.

Внедрение искусственного интеллекта в государственное управление не должно привести к утрате возможности восстановления, по меньшей мере, его (уже условно) современного «антропоцентричного» состояния. Обеспокоенность должно вызывать уже то

[1] См.: Brauneis R., Goodman E. Algorithmic transparency for the smart city // The Yale journal of law & technology. – 2018. – Vol. 20. – P. 131.

[2] См.: Brauneis R., Goodman E. Op. cit. – P. 126–127.

обстоятельство, что развитие самой теории управления обществом исключительно человеком в известной степени остановится.

Вполне реальной видится угроза, что если развитие управленческих навыков человека остановится, он попадет в ловушку – по мере утраты навыков зависимость от машин будет только расти. На определенном этапе невозможен будет уже возврат к состоянию, существовавшему на момент внедрения искусственного интеллекта в управленческие процессы. Следует учитывать крайнюю опасность зависимости информационных технологий от энергетических ресурсов, высокотехнологичной инфраструктуры и т.п.

В описанных условиях сложно найти исчерпывающие правовые решения.

На первый взгляд, очевидное и необходимое решение проблемы транспарентности – сделать применяемые в государственном управлении алгоритмы публичными и в том числе доступными для общественного контроля. Следует согласиться со специалистами, считающими, что концепция открытости данных, вероятно, наилучший способ обращения к проблеме транспарентности[1]. Государства должны добровольно раскрывать структуры, формулы, логику и политику алгоритмов с самого начала их использования[2].

Теоретически доступным средством может стать внесение соответствующих изменений в принятые во многих юрисдикциях законы о свободе информации, обязывающие государственные органы раскрывать определенную информацию в публичных интересах[3]. Понятие коммерческой тайны должно приобрести особое понимание, когда алгоритмы используются в государственных целях[4]. Наличие и сущность конфликта между концепциями коммерческой тайны и иной конфиденциальной информации и концепциями транспарентного и подотчетного демократического государственного управления прямо зависят от содержания господствующей теоретической конструкции, определяющей приоритеты в конкуренции публичных, общественных и частных ценностей.

---

[1] См.: Tauberer J. The principles and practices of open government data. – 2 d ed. – Wash., 2014. – P. 10.

[2] См.: Brauneis R., Goodman E. Op.cit. – P. 132.

[3] См.: Liu H., Lin C., Chen Y. *Beyond state vs Loomis*: Artificial intelligence, government algorithmization, and accountability // International journal of law and information technology. – 2019. – Vol. 27, N 2. – P. 139.

[4] См.: Wexler R. Life, liberty and trade secrets: Intellectual property in the criminal justice system // Stanford law review. – Stanford, 2017. – Vol. 70, N 5. – P. 1343.

В то же время выбор в пользу публичности алгоритмов искусственного интеллекта, используемых в государственном управлении, делает потенциально подлежащим раскрытию широкий круг информации, включая исходные коды алгоритмов, целевые функции, спецификации алгоритмов и параметры их настроек, наборы данных обучения и тестирования и т.п.[1] Известная логика есть в высказанном Р. Векслер предположении, что государства вряд ли отменят защиту коммерческой тайны и иной конфиденциальной информации[2]. Так, в деле *Verizon New York Inc. vs New York state public service commission* суд США принял решение исходя из того, что законы об отрытых отчетах США защищают коммерческую тайну и схожую конфиденциальную информацию, в том числе в публичных целях[3]. Одним из препятствий транспарентности использования алгоритмов искусственного интеллекта в государственном управлении Р. Браунейс и Э. Гудман называют озабоченность государства возможностью манипулирования алгоритмами в случае их раскрытия[4].

Более того, публичность алгоритмов искусственного интеллекта не решает проблему «технического черного ящика». Правовое закрепление требований транспарентности алгоритмов не обязательно приводит к их объяснимости[5], во всяком случае, при их современном техническом состоянии.

Станет ли необъяснимость алгоритмов препятствием к их использованию в государственном управлении? К. Коглианезе и Д. Лер считают, что почти наверняка – нет, даже в случаях замещения человека машиной в процедурах принятия управленческих решений, требующих аргументированности решения. Достаточность аргументированности будет определяться правом, исходя из прагматических соображений[6].

---

[1] См.: Lehr D., Ohm P. Playing with the data: What legal scholars should learn about machine learning // University of California Davis law review. – 2017. – Vol. 51. – P. 653, 669.

[2] См.: Wexler R. Op. cit. – P. 1352, 1354–1356, 1371.

[3] См.: Verizon N.Y., Inc. vs N.Y. State Pub. Serv. Comm'n, 23 N.Y.S. 3 d 446 (N.Y. App. Div. 2016) 449.

[4] См.: Brauneis R., Goodman E. Op. cit. – P. 159.

[5] См.: Ibid. – P. 129.

[6] См.: Coglianese C., Lehr D. Transparency and algorithmic governance // Administrative law review. – 2019. – Vol. 71, N 1. – P. 39.

Так же как транспарентность не обязательно обеспечивает объяснимость алгоритма, она не всегда соразмерна подотчетности управленческого акта. Алгоритмизированный процесс управления подотчетен тогда, когда заинтересованное лицо способно вмешаться, с тем чтобы изменить вывод, порядок использования или саму формулу алгоритма[1]. Иными словами, степень транспарентности предопределена возможностью обжалования алгоритмизированного управленческого акта.

Подотчетность требует не идеальную или абсолютную транспарентность – исчерпывающие знания о формулировании алгоритма, его операционных правилах и т.д., а более низкий стандарт «целенаправленной» траспарентности – знания, предоставляющие возможность подтвердить или опровергнуть операционные действия и выводы алгоритма, полагает Р. Браунейс [2].

Хань Вэй Лю, Цин-Фу Линь и Юй-Цзе Чен предлагают менее радикальный в сравнении с публичностью алгоритмов подход – обусловленное раскрытие применяемого в государственном управлении алгоритма в публичных целях, например, для заинтересованных сторон или для некоего экспертного комитета на условиях конфиденциальности. Разумным видится поддерживаемый ими обобщенный тезис – учитывая особую важность публичных интересов, лежащих в основе государственного управления, секретность ради прибыли должна быть обоснованно ограничена[3].

Данный тезис поддерживают также Р. Браунейс и Э. Гудман. По их мнению, алгоритмы будут в достаточной степени транспарентными, если: 1) правительства будут производить достаточную фиксацию целей и задач для применения алгоритмов и последующей оценки их выводов; 2) частные компании – разработчики алгоритмов в соответствии с заключаемыми с государственными органами контрактами будут предоставлять информацию, как они сформулировали алгоритм; 3) в концепции коммерческой тайны будут подразумеваться исключения для раскрытия информации в публичных целях[4].

---

[1] См.: Accountable algorithms. Op. cit. – P. 657–660; Brauneis R., Goodman E. Op. cit. – P. 132.

[2] См.: Brauneis R., Goodman E. Op. cit. – P. 132.

[3] См.: Liu H., Lin C., Chen Y. Op. cit. – P. 135.

[4] См.: Brauneis R., Goodman E. Op. cit. – P. 104.

К. Коглианезе и Д. Лер приходят к заключению, что в большинстве случаев государственным органам будет достаточно аргументировать, что алгоритм а) разработан для достижения обоснованной с правовой точки зрения цели, б) корректно функционирует и в) используется в соответствии со своим назначением[1].

В большинстве случаев даже защита коммерческой тайны не будет являться ограничивающим фактом. Во-первых, требующие раскрытия целевые функции и заложенная вариативность выводов (переменные результата) (*outcome variables*) скорее всего не могут быть классифицированы как коммерческая тайна, так как выражают цели управленческого акта (математическая формула целевой функции диктуется государственным органом, а не разрабатывающей алгоритм частной компанией). Во-вторых, раскрытие результатов тестовых процедур и процедур подтверждения данных, индивидуальных данных оцениваемого алгоритмом лица не требует раскрытия исходного кода алгоритма или иной коммерческой тайны. В-третьих, исходные коды и иная, находящаяся под защитой информация, в случае необходимости может быть исследована компетентным государственным органом в конфиденциальном порядке, к примеру, судом в закрытом заседании на условиях неразглашения. Наконец, необходимые условия раскрытия информации могут быть изначально заложены в соответствующие контракты между государственными органами и частными компаниями[2].

Большинство специалистов настаивают на том, что государственные органы должны обдуманно заключать контракты с разработчиками алгоритмов, в настоящее время уже традиционно включающие «порочные» условия о неразглашении и коммерческой тайне[3]. Плодотворной видится способность государства влиять на такие контракты с целью обеспечить фиксацию и раскрытие данных, связанных с разработкой и использованием алгоритмов.

Даже если оптимальный уровень транспарентности требует расширенного раскрытия информации, решение не будет связано (либо будет иметь несущественную связь) с искусственным интеллектом *per se*. Если рассматривать озабоченность частными па-

---

[1] См.: Coglianese C., Lehr D. Op. cit. – P. 47.

[2] См.: Ibid. – P. 48–49.

[3] См.: Brauneis R., Goodman E. Op. cit. – P. 137–152, 159, 164; Liu H., Lin C., Chen Y. Op. cit. – P. 139–140.

тентными правами разработчиков алгоритмов – транспартентность может быть обеспечена простым изменением условий заключаемых с ними соглашений, устанавливающих удовлетворяющий государственные органы порядок защиты коммерческой тайны или возможно даже допускающих отказ от нее.

Государство может проводить конкурсы алгоритмов с открытым исходным кодом или в итоге сформировать собственную информационно-технологическую инфраструктуру. Представляется, что во всех случаях государство всегда может рассчитывать на оценку со стороны общественности – независимых сторонних специалистов, консультативных комиссий, заинтересованных сторон и т.п.

Возможно, что в ответ на стремительно растущий интерес к использованию алгоритмов в государственном управлении последующие разработки пойдут по пути всё большей открытости и объяснимости алгоритмов[1]. Вероятно, что механизм предоставления достаточного обоснования вывода, используемого в государственном управлении алгоритма, может быть интегрирован в структуру алгоритма. Алгоритмизированное управление способно воспринять и правовые, и общественные требования транспарентности, повышая (таким образом) свою корректность, продуктивность и – потенциально – легитимность, считают К. Коглианезе и Д. Лер[2].

Потенциальным решением проблемы «технического черного ящика» может стать автономность (в определенной степени) лица в выборе – применять ли в отношении него соответствующий алгоритм или нет. Лицо должно быть информировано о возможных рисках и выгодах, об ограниченности понимания того, как алгоритм приходит к собственным выводам[3].

Пункт 1 ст. 22 Общего регламента по защите данных ЕС предоставляет лицу «право не подпадать под действие решения, основанного исключительно на автоматической обработке, включая формирование профиля, которое порождает юридические последствия в отношении него или нее, или существенно воздействие на него или на нее». В случае если лицо всё же выразило

---

[1] См.: Polack P. Beyond algorithmic reformism: forward engineering the designs of algorithmic systems // Big data & society. – 2020. – Vol. 7, N 1. – P. 1–14;

[2] См.: Coglianese C., Lehr D. Transparency and algorithmic governance // Administrative law review. – 2019. – Vol. 71, N. 1. – P. 1–2, 35–36, 50.

[3] См.: Liu H., Lin C., Chen Y. Op. cit. – P. 136.

собственное согласие на автоматизированный процесс принятия в отношении него решения, согласно п. 3 ст. 22 оно наделяется правами требовать в случае необходимости вмешательства человека, а также выражать свою точку зрения и оспаривать решение.

Практика реализации возможности отказа от алгоритма в пользу человека создаст эмпирическую базу для определения секторов государственного управления, видов государственных решений и действий, алгоритмизация которых поддерживается обществом.

Внедрение искусственного интеллекта в государственное управление должно сопровождаться комплексом согласованных решений. В этом отношении интерес вызывает предложение Х. Мехр, сформулировавшей шесть стратегий, которым должны следовать государства.

1. Делать искусственный интеллект частью целевых программ, ориентированных на человека.

2. Допускать общественность к участию в проектах внедрения искусственного интеллекта в управленческие процессы.

3. Полагаться на доступные ресурсы, включая инфраструктуру частных компаний и некоммерческих организаций.

4. Осуществлять подготовку данных, необходимых для анализа, средствами искусственного интеллекта и осторожно относиться к их конфиденциальности.

5. Минимизировать этические риски и избегать принятия искусственным интеллектом управленческих решений.

6. Использовать средства искусственного интеллекта как помощь для государственных служащих, а не как их замену[1].

Представляется, что надзор человека в управленческих процессах должен превалировать. Решения, в основе которых лежит усмотрение государственного органа, не должны приниматься без его вмешательства, хотя характер вмешательства и будет зависеть от таких факторов, как природа решения, область, предмет и существо вопроса, вовлеченные интересы, доступные средства решения, ресурсы и т.п. Алгоритмы могут быть в разной степени интегрированы в сложную систему взаимодействия между людьми, между людьми и машинами, в том числе подразумевающую взаимодействие алгоритмов машинного обучения, не обучающихся

[1] См.: Mehr H. Artificial intelligence for citizen services and government / Harvard Ash Center for Democratic Governance and Innovation. – Cambridge, 2017. – P. 10–14.

алгоритмов (*agent-based models* (*ABM*)) и «многоагентных систем» (*multi-agent systems* (*MAS*))[1]. Однако даже в наиболее футуристичных прогнозах роботизированного будущего участие человека в управлении обществом не может быть полностью исключено. За человеком должно оставаться окончательное решение.

3.2. Искусственный интеллект в государственном управлении и правосудии

В последнее десятилетие наблюдается беспрецедентный рост анализа данных и алгоритмов в государственной политике и управлении. Это обусловлено растущими требованиями к управлению: сложностью современного общества, наличием огромного количества информации, генерируемой повсеместным использованием инновационных устройств, поддерживаемых Интернетом, и значительным ростом вычислительных мощностей.

Сегодня активное и грамотное использование цифровых технологий, и прежде всего аналитики больших данных и искусственного интеллекта, является основой конкурентоспособности не только частных компаний, но и государств.

Осознание важности разработки и внедрения самых передовых цифровых технологий во все отрасли хозяйства и сферы государственного управления нашло отражение в ключевых документах стратегического планирования Российской Федерации, а также в национальном проекте «Цифровая экономика Российской Федерации», в рамках которого уже сегодня стремительно меняется нормативная база, направленная на стимулирование развития и активного внедрения цифровых технологий, начиная от придания статуса имущества цифровым активам и регламентации оборота криптовалют и заканчивая цифровизацией государственного управления (включая унификацию правил обращения в суды в электронной форме, допустимость электронных доказательств, дистанционное участие в судебном заседании, изготовление нотариальных документов в электронной форме и дистанционное совершение нотариальных действий, а также переход к электронным трудовым книжкам).

---

[1] См.: Coglianese C., Lehr D. Transparency and algorithmic governance // Administrative law review. – 2019. – Vol. 71, N 1. – P. 12–13.

Использование возможностей, которые предоставляют технологии обработки больших данных, позволяет полностью трансформировать правовые категории и создать принципиально новый способ правового регулирования путем адаптации правовых норм к индивидуальным особенностям личности.

Это связано с тем, что необработанные данные, собранные об индивиде, могут быть объединены таким образом, чтобы связать их со структурой личности или с когнитивными факторами для прогнозирования его будущего поведения, после чего правовые нормы могут быть персонализированы с учетом его силы воли, рациональности и т.д.

Например, партнеры крупных фирм, занимающихся торговлей недвижимостью, считаются потребителями при покупке дома для себя, в то время как владельцы небольших магазинов в своих деловых отношениях таковыми не являются, несмотря на то что первые, безусловно, обладают большим деловым опытом и знаниями в сфере обращения недвижимости, чем вторые. Соответственно, существующее в законодательстве деление на группы по неким общим признакам не решает проблему обеспечения равенства перед законом и равной защиты.

Персонализация позволит использовать науку и технологию анализа поведенческих стереотипов для решения этих проблем. Таким образом, правовые категории могут быть уточнены и детализированы с учетом конкретных психологических типов личности. Также персонализированное законодательство позволит решить проблему информационной перегрузки, когда потребителю предлагается ознакомиться с таким объемом информации, который он не в состоянии воспринимать. При этом далеко не вся информация одинаково важна для всех. Например, выбирая тарифный план для телефона, мы знакомимся с основными тарифами и стоимостью дополнительных минут или объема Интернета сверх предусмотренного тарифа. Однако люди различаются по степени рациональности и способности прогнозировать свое пользование телефоном. Соответственно, рациональным людям важна информация о самом тарифе, а тем, кто не способен адекватно прогнозировать, – информация о стоимости дополнительных минут и интернет-трафика.

Большинство продуктов, которые мы приобретаем сегодня, состоят из многоуровневых цен, будь то номер в отеле, где взимается дополнительная плата за пользование Интернетом, билет на

рейс, который не включает в себя расходы на багаж, или цена продажи товара, указанная без платы за доставку. Во всех этих случаях может применяться персонализированное право.

Также персонализация права позволит защитить людей, не проявляющих достаточно разумности и осмотрительности при принятии решений, особенно при инвестировании своих средств. Например, для них могут быть установлены ограничения в отношении объемов возможного инвестирования[1].

Подобные технологии, основанные на анализе больших данных при помощи искусственного интеллекта, уже внедряются в Китае в качестве механизма «социального кредита», в соответствии с которым каждому китайцу при рождении будет присвоен «социальный кредит», затем в процессе его жизни все собранные о нем сведения, начиная от того, как он переходит улицу, какой контент размещает в социальных сетях, насколько он социально активен и т.д., будут влиять на уровень этого «кредита», повышая или понижая его. Соответственно, люди, чей кредит будет опускаться ниже установленных границ, будут ограничены (они уже ограничены) во множестве прав (например, как это произошло недавно, когда тысячи китайцев не смогли купить билеты на самолет).

Что касается США, то эта страна является лидером в разработке и внедрении новых цифровых технологий не только в сфере бизнеса, но и в государственном управлении. Так, искусственный интеллект активно используется при выполнении антимонопольной и полицейской функций, что, по сути, меняет сам метод государственного управления, превращая органы власти в «планшетных чиновников»[2], всё более зависимых от гаджетов и менее самостоятельных в принятии решений. Более того, в США алгоритмы внедрены в судебную систему, например, при выборе между заключением под стражу или залогом, или при принятии решения о сроке тюремного заключения для осужденного за преступление.

---

[1] См.: Hacker Ph. Personalizing EU private law: From disclosures to nudges and mandates // European review of private law. – 2017. – N 3. – P. 651–678.

[2] McGregor L. Accountability for governance choices in artificial intelligence: Afterword to Eyal Benvenisti's foreword // The European journal of international law. – 2018. – Vol. 29, N 4. – P. 1083.

При этом нельзя забывать о важной особенности искусственного интеллекта. Действительно, сам по себе алгоритм не способен принимать «субъективные» решения, однако качество его решений зависит от того, каким образом он спроектирован и какие данные в него внесены.

В связи с этим возникает масса вопросов. Например: можем ли мы быть уверенными в том, что алгоритм будет принимать действительно справедливые решения, и можем ли мы гарантировать, что данные, на которых основана технология, будут непредвзятыми? Кто должен отвечать за ошибочное решение алгоритма? Должны ли судьи, чиновники и простые граждане понимать, как алгоритм работает и приходит к тому или иному решению?

Искусственный интеллект – математический алгоритм, который выдает определенный результат на основе непредвзятой обработки имеющейся информации. Этим он отличается от человека, который часто действует, подчиняясь своей интуиции. Казалось бы, это свидетельствует в пользу алгоритма, который не может ошибаться и всегда беспристрастен. Однако следует учитывать, что сам алгоритм составлен человеком, а значит, он уже отражает его личные ценности, нравственные и моральные принципы, наконец, личные предубеждения. Если удастся этого избежать, то возникает следующая возможность для необъективности – набор данных, которые алгоритм анализирует, поскольку эти наборы данных также подбираются человеком, следовательно, всегда есть риск, что они будут неполными, нерелевантными и необъективными. Но даже если и этого не произойдет, то все равно мы не можем быть уверены в том, что алгоритм абсолютно объективен. Так, Винсент Чиао (Vincent Chiao)[1] приводит пример с наркоторговлей в США, где органы правопорядка значительно чаще задерживают афроамериканцев, но не потому, что они больше задействованы в этом «бизнесе», чем «белое население», а потому что они торгуют наркотиками на улицах, и полиции проще их ловить, в то время как «белое население» торгует через Интернет или в помещениях, поэтому их сложнее поймать. Однако если взять все данные о наркоторговле в США, то они будут свидетельствовать о том, что афроамериканцы попадаются на этом преступ-

[1] Chiao V. Fairness, accountability and transparency: notes on algorithmic decision-making in criminal justice // International journal of law in context. – 2019. – Vol. 15, N 2. – P. 129.

лении значительно чаще. Следовательно, если эти данные передать для обработки искусственному интеллекту, то тем самым сложившаяся необъективная картина будет заложена в алгоритм. Таким образом, даже если алгоритм явно не учитывает расовые различия при вынесении решения, он будет учитывать такие факторы, как предыдущие аресты и судимость, которые сильно коррелируют с расой.

При внедрении искусственного интеллекта в систему правосудия необходимо очень серьезно анализировать, какими данными он должен оперировать при принятии решений. В противном случае, может получить широкое распространение ситуация, которая ярко проявилась в США в деле *State vs Loomis*, когда преступник, заключивший сделку со следствием и рассчитывавший на условный срок, был приговорен к шести годам тюремного заключения и пяти годам строгого надзора на основании заключения автоматизированной системы COMPAS о его склонности к рецидиву[1].

В этом деле интересно то, что использованная система, во-первых, не вполне соответствует целям принятия решений в уголовном судопроизводстве (она смоделирована для исполнительной системы, т.е. для рассмотрения вопроса о возможности досрочного освобождения, кроме того, она способна идентифицировать группы правонарушителей высокого риска, но не может оценить риск рецидива отдельного человека); во-вторых, уровень достоверности отчетов данного алгоритма был поставлен под сомнение рядом исследователей, которые отмечали, что оценки COMPAS совпали с реальным рецидивом только в 20% случаев; и, наконец, в-третьих, эта система принадлежит частной фирме, которая отказалась раскрывать механизм работы алгоритма, что превратило его в «черный ящик» и не позволило понять, на основании чего было сформировано именно такое заключение[2].

Обвиняемый в попытке оспорить решение суда дошел до Верховного суда штата, который отказал в удовлетворении его жалобы, несмотря на указанные «пороки» достоверности заключения алгоритма, но отметил, что автоматизированные системы не должны быть единственным обоснованием принимаемого решения.

---

[1] Liu H.-W., Lin Ch.-F., Chen Yu-J. *Beyond State vs Loomis*: Artificial intelligence, government algorithmization and accountability // International journal of law and information technology. – 2019. – Vol. 27, N 2. – P. 129.

[2] Ibid.

Этот пример является очень наглядной демонстрацией серьезного риска, стоящего перед нашим обществом. Риска преклонения перед алгоритмами и чрезмерного доверия к результатам их работы.

Действительно, даже если предположить, что судья не будет опираться исключительно на заключение COMPAS, очевидно, что, ознакомившись с этим заключением, он уже не сможет быть объективным при вынесении своего решения, зная, что преступнику присвоена высокая категория риска. Это вполне естественный психический механизм «якоря».

Кроме того, сам Верховный суд продемонстрировал еще одну психологическую особенность человека. В обычных ситуациях любой отход от установленного процессуального порядка (от требования вынесения приговора только на основании точной и достоверной информации, а также права обвиняемого обжаловать аргументы, которые легли в основу приговора) должен включить механизм контроля и пересмотра решения.

Однако, когда такой отход связан с применением современной технологии, он может быть расценен как незначительный или вообще остаться без внимания из-за тенденции относиться к технологии с чрезмерным доверием.

Следующий вопрос связан с ответственностью алгоритма за допущенную ошибку и возможностью эту ошибку исправить. Действительно, в отношениях между людьми всегда есть возможность спорить, доказывать свою правоту. Именно в этом заключается суть апелляции. В случае с алгоритмом это исключено (это все равно, что спорить со своим компьютером). В обычной процедуре человек имеет право на ряд процессуальных прав – устное слушание, вызов свидетелей, оспаривание доказательств против вас, перекрестный допрос и т.д. Алгоритм же анализирует заложенные данные, а значит, все эти процессуальные права оказываются к нему неприменимыми. При этом, как было показано на примере дела COMPAS, апелляционная процедура здесь тоже не сработала в силу чрезмерного доверия человека к алгоритму.

Представляется, что при внедрении искусственного интеллекта в государственное управление, и особенно в систему отправления правосудия, необходимо использовать его исключительно как техническое устройство или технического помощника, возможно, предоставив право его применять органам следствия, например, при принятии решения о заключении под стражу. При

этом подозреваемый (обвиняемый) всегда должен сохранять право на обжалование, право представить в суд доказательства, свидетельствующие о несоразмерности выбранной меры пресечения или требуемого срока тюремного заключения, как если бы соответствующее решение принимал человек, а не алгоритм и судья выступал объективным арбитром.

Так, в Канаде Закон о залоге требует, чтобы прокуроры при обращении к судье за ордером на арест представляли обоснование такой меры пресечения, включая оценку риска того, что оставление обвиняемого на свободе может нанести урон правосудию. Однако ничего не говорится о том, как они должны выполнять эту задачу[1]. Очевидно, что будет использована информация о предыдущих арестах или попытках повлиять на заявителя, имеющиеся сведения о злоупотреблении психоактивными веществами или проблемах психического здоровья и т.д. При этом обвиняемый, лично или через адвоката, имеет право сообщить судье о неверности таких сведений, что может повлиять на решение об освобождении или отказе в освобождении. Соответственно, использование искусственного интеллекта прокурором вполне допустимо, если сохраняется право обвиняемого представить доказательства ошибочности его выводов и возможность принятия решения судьей. Однако следует учитывать, что в реальности прокуроры, принимая решение обратиться за ордером на арест, руководствуются самыми разными мотивами и суждениями, что свойственно человеческой природе. Так, один может придавать существенное значение документированной истории неявки или криминальному прошлому, в то время как другой может уделять больше внимания тому, имеет ли обвиняемый общественную поддержку, жилье и работу.

В этом смысле алгоритм, очевидно, имеет преимущество перед человеком и должен заменить интуицию и чувства судей и обвинителей строгими эмпирическими методами. Поэтому применять на практике искусственный интеллект следует только тогда, когда он будет существенно более надежным, чем человек.

Наконец, третий и самый распространенный вопрос связан с особенностью искусственного интеллекта, построенного на основе нейросетей – это способность к самообучению, которая в конеч-

[1] Chiao V. Fairness, accountability and transparency: Notes on algorithmic decision-making in criminal justice // International journal of law in context. – 2019. – Vol. 15, N 2. – P. 133.

ном итоге приводит к тому, что даже создатели алгоритма не всегда в состоянии понять, как он работает и почему принимает те или иные решения, что создает эффект «черного ящика».

Пожалуй, это самый сложный с этической точки зрения вопрос, когда речь идет о человеческих судьбах. Вправе ли мы полагаться на алгоритм, работу которого мы не только не контролируем, но даже не в состоянии понять? Особенно с учетом того, что, как было сказано выше, мы не можем быть стопроцентно уверены в непредвзятости алгоритма. В то же время следует признать, что мотивы решений человека-судьи также далеко не всегда очевидны и могут быть выяснены даже при прямом вопросе (поскольку человек может руководствоваться одними соображениями, а мотивировать свое решение совершенно иначе). Кроме того, многие технологии, от самолетов до фармацевтических препаратов, включают процессы, которые большинство людей не понимают, хотя их жизнь и зависит от этих технологий. Например, больной, которому была проведена операция на сердце, вряд ли понимает, что именно и для чего было сделано.

В связи с этим полагаем, что алгоритмы вовсе не должны быть понятными пользователям, включая потерпевших и обвиняемых, – следователей, прокуроров и судей, но они должны быть разработаны таким образом, чтобы обеспечить их понятность для операторов-людей, обеспечивающих их функционирование, с тем чтобы при необходимости они могли представить необходимые пояснения всем участникам процесса. Так, например, Регламент Европейского парламента и Совета ЕС от 27 апреля 2016 г. 2016/679 «О защите физических лиц при обработке персональных данных и о свободном обращении таких данных» включает право лица, затронутого решением, основанным исключительно на автоматизированной обработке его персональных данных, получить объяснение такого решения и оспорить это решение.

Рассмотренные вопросы, хотя и были, в основном, связаны с системой судопроизводства, актуальны и для многих сфер государственного управления, где уже применяется или будет в будущем использоваться искусственный интеллект, поскольку возникает вопрос: кто в реальности принимает решения – чиновники или программы, на которые они полагаются и которые разрабатываются частными компаниями для получения прибыли? Не сложится ли ситуация, когда реальной властью будут обладать не органы власти государства, а разработчики алгоритмов? Не будут ли

принимаемые решения, а возможно, и законы, поскольку сегодня всё активнее обсуждается тема внедрения искусственного интеллекта в законотворческий процесс, предвзятыми к определенной части населения?

Таким образом, принимая решение об использовании искусственного интеллекта в управлении, необходимо тщательно взвешивать все риски «делегирования» управленческих функций алгоритму и стремиться их минимизировать.

3.3. Автоматизация юридических профессий

Стремительное развитие цифровых технологий неизбежно влияет на все сферы жизни. Представители многих профессий обеспокоены – использование программ и роботов способствует сокращению рабочих мест. Эту тревогу разделяют и юристы: разработка специализированного программного обеспечения привела к тому, что заключить несложный контракт, оспорить штраф и составить завещание можно не обращаясь к юристу[1]. Программы вторгаются и в работу судей. Созданные им в помощь, они, как оказалось, способны манипулировать принимаемыми ими решениями.

Исследования работы программ, связанных с применением права, показали, что автоматизация далеко не всегда повышает качество и понижает себестоимость процесса. Лишенные подвластных лишь человеку способностей «судить» (judgment), учитывать новые обстоятельства, ответственности перед обществом, они не могут в полной мере заменить его. Остановить прогресс, однако, невозможно, технологии уже используются во всех сферах юридической профессии, их использование в дальнейшем будет лишь нарастать. Какие угрозы несет в себе этот процесс и как заставить программы служить человеку, а не манипулировать им, – вопросы, на которые попытаемся ответить в данном параграфе.

В первую очередь, по мнению правовых футуристов (futurists), должна быть автоматизирована деятельность, осуществляемая ад-

[1] См., напр.: Немченко И. Объясняем на пальцах: 3000 юристов Сбербанка заменит робот. Машины лишают людей работы? (Спойлер: нет). – URL: https://incrussia.ru/understand/obyasnyaem-na-paltsakh-3-000-yuristov-sberbanka-zamenit-robot-mashiny-lishayut-lyudey-raboty-spoyler/ (дата обращения: 12.02.2020).

вокатами. Она кажется легко алгоритмизируемой: данные (например, факты) преобразовываются в результат (соглашение или правовую позицию) путем применения набора правил (права). Успех первых подобных программ, таких как ТурбоТакс (TurboTax), позволивших облегчить миллионам американцев процесс представления налоговых деклараций, создал впечатление возможности полной автоматизации многих областей применения права. Обывателями это воспринимается в качестве позитивного эволюционного шага на пути реализации верховенства права – в то время как адвокат может ошибиться в фактах или неправильно истолковать прецедент, или может находиться под влиянием заблуждения или предубеждения, машины дают возможность, в буквальном смысле, достичь «верховенства закона, а не человека». (Ответственность за принимаемые алгоритмом решения, при этом все равно лежит на человеке, хотя не на юристе, а на программисте.)[1]

Более глубокое изучение примеров автоматизации в правовом поле, однако, показывает, что заместительная правовая автоматизация (substitutive legal automation) не является однозначным благом. Рассматривая популярные сегодня программы, такие как ЛигалЗум (LegalZoom), с помощью которой на основе компьютеризированного общения с клиентами юристы помогают составить завещание или контракт, и ДуНотПей (DoNotPay), чатбот, помогающий пользователю оспорить штраф за неправильную парковку, Франк Паскаль приходит к выводу, что язык, в частности язык права, богаче, чем может быть представлено с помощью простых программ. Это приводит к тому, что пользователи вводятся в заблуждение относительно своих прав и обязанностей[2], а экономия времени и расходов на адвоката может обернуться значительными убытками.

Компания ЛигалЗум за десять лет своего существования обеспечила «правовой информацией» более 2 млн человек. Вместо серии встреч с юристами, пользователи могли получить персонализированные формы с ответами на свои вопросы и инструкциями к действию, заполнив вопросник онлайн. Результаты таких «консультаций», однако, не всегда были удовлетворительными, по-

[1] См.: Pasquale F. A Rule of persons, not machines: The limits of legal automation // The George Washington law review. – 2019. – Vol. 87, № 1. – P. 4.

[2] См.: Pasquale F. Op. cit. – P. 6.

скольку необходимые для правильного анализа правовой ситуации вопросы не были заданы, а необходимая информация не была предоставлена программе, поскольку самостоятельно пользователь не смог осознать ее правовое значение[1]. Возникают вопросы и к программе ДуНотПей, которая не дает возможности учитывать исключения из правил, к примеру, медицинскую необходимость остановки в неположенном месте. Точнее, учет таких обстоятельств возможен, но для этого придется привлечь «живого эксперта».

Парадоксальным образом несовершенство технологии и использование этого недостатка «плохими игроками» в свою пользу приводит к увеличению сложности правового регулирования в автоматизируемой области. Еще одна ключевая проблема заключается в том, что в отличие от этически ответственных адвокатов, обязанных предоставлять наилучший возможный уровень услуг и нести ответственность за оказание услуг низкого качества, программы перенесли риск ошибки на клиента. ДуНотПей пошла дальше других, предусмотрев в документе, который подписывают пользователи, что те обязуются «обезопасить, защитить и освободить ее от любой ответственности, потерь, расходов и претензий, связанных с использованием программы или информации, ею предоставленной»[2].

Приведенные примеры, однако, не означают, что заместительной автоматизации нет места в правовых профессиях. Несмотря на определенные опасения этического характера, связанные с непредусмотренными последствиями услуги и отсутствием защиты пользователя, при условии невысоких ставок и отсутствия лучшей альтернативы она вполне может быть использована. При возрастании сложности вопроса уместность замещения человека программой снижается.

Простая, на первый взгляд, задача перевода языка в компьютерный код поднимает значительно более серьезные вопросы социальных и политических взаимоотношений. Для их поддержания необходимы гибкость и открытость языка, недоступные кодированию. В первую очередь это касается смыслов. Правовые процессы связаны с объяснением и суждением – эти виды деятельности значительно отличаются от тех, на которые, в основном, опирается

[1] См.: Pasquale F. A Rule of persons, not machines: The limits of legal automation // The George Washington law review. – 2019. – Vol. 87, № 1. – P. 11.

[2] См.: Pasquale F. Op. cit. – P. 13–16.

автоматизация прогнозирования и распознавания паттернов. Человек, принимающий решения, оценивает смысл фактов и суть правовых положений, подлежащих применению. Данная функция может потребовать политического суждения, мудрости, способности действовать вне алгоритма, и ответственности. Эта сложная работа может стать легче и приятней, если использовать правильные инструменты. И одним из таких инструментов может стать не заместительная, а комплементарная автоматизация (complementary automation). Различные методы усиления интеллекта (intelligence augmentation) могут не только упростить юристам поиск и выборку данных, но и выявить неочевидные основания необъективности в их работе. Так, например, исследование поведенческой экономики выяснило, что судьи принимают больше решений об освобождении под залог после обеда[1].

Сверхъестественные способности искусственного интеллекта, стремительное развитие новых услуг, основанных на алгоритмах, породили в юридическом сообществе США желание защититься от автоматизации с помощью монополии на юридические услуги. Американская ассоциация адвокатов поддерживает государственные нормы, запрещающие практиковать в этой области нелицензированным лицам. Более того, профессиональные правила этой организации запрещают неюристам становиться собственниками юридических фирм[2].

Рассмотрение в 2015 г. Апелляционным судом второго округа Нью-Йорка дела *Lola vs Skadden,* изначально касавшегося требования оплаты за дополнительные часы работы, значительно ослабило позиции профессионального сообщества и предоставило машинам возможность выполнять некоторые виды деятельности, ранее относимые к «юридической практике». В своем решении суд постановил, что «лицо, выполняющее задачи, которые в полном объеме могут быть осуществлены машиной, не может быть признано практикующим право». Иными словами, суд установил разницу между ролью человека и машины и заключил, что деятельность, выполняемая машиной, не является юридической

[1] См.: Pasquale F. Op. cit. – P. 53.

[2] См.: Lola vs Skadden and the automation of the legal profession / Simon M., Lindsay A., Sosa L., Comparato P. // The Yale journal of law and technology. – 2018. – Vol. 20. – P. 237.

практикой[1]. Скорость совершенствования алгоритмов и усложнение задач, которые они могут выполнять, подрывают основанную на монополии защиту лицензированных юристов.

Практикующие юристы и исследователи вопросов технологии и права – Майкл Симон, Алвин Линдсей, Лоли Соса и Пейж Компарато – отмечают, что профессия юриста сама по себе содержит характеристики, препятствующие адаптации в цифровом мире. Это иерархическая природа профессии, ее организационные структуры и особенности характера лиц, выбирающих себе эту профессию[2].

Иерархическая природа заставляет фирмы придерживаться статус-кво вместо того, чтобы стремиться к внедрению новых технологий – партнеры юридических фирм заинтересованы в сиюминутной прибыли, а не долгосрочных вложениях. Профессиональное правило 5.4, запрещающее неюристам владеть акциями юридических фирм, препятствует инвестициям, которые могли бы компенсировать проблему близорукости партнеров-юристов.

Несмотря на многочисленные предсказания смерти больших фирм (BigLaw) от технических инноваций, они всё еще живы и их доход не уменьшился. Убедить «целую комнату миллионеров в том, что они не разбираются в бизнесе» весьма затруднительно[3]. Отражая иерархическую природу сообщества, его структуры построены так, чтобы создать стимулы максимизации быстрой прибыли.

И наконец, по своей природе юристы «обращены назад», поскольку уверены в том, что прошлое «определяет настоящее и будущее»: в большинстве профессий ответ «Потому что так было всегда» на вопрос «Почему это следует делать именно так?» был бы неприемлем, но в системе общего права США он не только возможен, но и является основным и наилучшим. Исследования показывают, что юристы гораздо чаще бывают скептиками и пессимистами и гораздо реже оптимистами, чем люди, выбравшие иные профессии. Отмечается, что с опытом их скептицизм увеличивается, так что партнеры, принимающие решения о необходимости инноваций в фирме – самые скептические люди в коллекти-

[1] См.: Ibid. – P. 238.

[2] См.: Lola vs Skadden and the automation of the legal profession. – P. 239.

[3] См.: Ibid. – P. 266.

ве[1]. Юристам также присущи такие личностные характеристики, как нетерпеливость, потребность незамедлительного принятия мер, а также низкая приспособляемость и высокая автономность. Эти черты также не способствуют легкому принятию нового.

Неожиданно значительным оказалось влияние автоматизации на область, требующую от человека повышенной ответственности и глубокого суждения – вынесение решений по уголовным делам. Перед судьями стоит сложная задача учета одновременно требований законодательства и интересов общества, назначаемое наказание должно быть пропорционально совершенному проступку, оно должно отвратить нарушителя от повторного совершения преступления, быть достаточно серьезным, чтобы оградить общество от опасности, но при этом таким образом, чтобы нарушитель мог после его отбытия успешно реабилитироваться. Все эти требования «указывают» в разном направлении, многое зависит от усмотрения конкретного судьи. Ситуация осложняется тем, что, как правило, судья обладает ограниченной информацией о подсудимом, что мешает полноценно оценить возможность влияния на него накладываемого наказания. С целью облегчить судьям работу и одновременно добиться некоторого единообразия практики по схожим делам в США были выработаны различные инструменты, в том числе программы[2]. Несмотря на то что они, казалось бы, содействуют беспристрастной оценке фактов по аналогии с принимавшимися ранее решениями, они подверглись критике как со стороны обвиняемых, так и со стороны судейского сообщества. С одной стороны, исследования показали, что алгоритмизированный процесс назначения наказания может приводить к расово-предвзятым результатам[3]. С другой стороны, как отмечает Майкл Донохью, изучивший применение программы с элементами искусственного интеллекта при оценке вероятности повторных нарушений закона КОМПАС (Correctional Offender Management Profiling for Alternative Sanctions tool (COMPAS)), вызывает тревогу тот факт, что эти технологии могут заменить человека.

КОМПАС основывается на методе основной регрессии и учитывает информацию о расе, образовании, умственном разви-

[1] См.: Ibid. – P. 269.

[2] См.: Donohue M. A Replacement for justitia's scales? Machine learning's role in sentencing // Harvard journal of law & technology. – 2019. – Vol. 32, N 2. – P. 658.

[3] См.: Pasquale F. Op. cit. – P. 14.

тии, этнической группе, и биографии, используя данные из государственных баз данных. В отличие от инструментов предыдущих поколений, программа выдает в качестве результата не вероятность, а конкретный прогноз, при этом сложно сказать, какие именно введенные данные повлияли на прогноз, выданный системой. Изначально данная технология была разработана, чтобы облегчить принятие решения о том, стоит ли выпускать подозреваемого под залог, однако некоторые штаты разрешили ее использование и при назначении наказания[1].

Наиболее полно критика этого алгоритма была сформулирована в деле *State vs Loomis,* рассмотренном Верховным судом штата Висконсин. Ответчик утверждал, что:

1) закрытая природа КОМПАС препятствовала ему оспорить точность выдаваемого результата;

2) программа действовала на основе групповых, а не индивидуальных данных;

3) использовались неконституционные вводные.

Суд отказал по всем трем претензиям, постановив, что ответчик мог проверить информацию, вводимую в программу и оспорить ее; шкала «вероятности риска» (risk score) лишь ориентировала человека, принимающего решение, но не диктовала его человеку; отсутствовали доказательства, что судья руководствовался какой-либо неконституционной информацией.

Критика использования информации общего характера и отсутствия прозрачности работы алгоритмов может быть применена не только к программе КОМПАС, но и к другим инструментам, используемым судьями, включая федеральные руководства о назначении наказаний. Однако третье основание критики, заключающееся, по сути, в том, что алгоритм «закрепляет» использование определенной философии при назначении наказания, применим только к инструментам с элементами искусственного интеллекта. Из четырех обоснований наказания – возмездия, сдерживания, лишения возможности и реабилитации, алгоритм учитывает только одно – лишение возможности. По сути, он был разработан для того, чтобы определить, кто из нарушителей совершит преступление повторно, и сделать так, чтобы он был лишен свободы. Представляя собой убедительные таблицы с количественными данными, алгоритм манипулирует процессом принятия решения,

[1] См.: Donohue M. Op. cit. – P. 661.

фиксируя его на одной философии наказания и игнорируя остальные[1]. Результаты действия алгоритма всегда статистически верны и механически честны. При этом они расово небеспристрастны – черные обвиняемые определялись в качестве повторных нарушителей в два раза чаще, чем белые[2].

Устранить недостатки КОМПАС можно было бы, создав инструмент, который учитывал бы все четыре обоснования наказания. По форме он мог бы стать аналогичным Руководству о назначении наказаний (U.S. Sentencing guidelines), созданному в 1980-х годах Комиссией США по вынесению приговоров (U.S. Sentencing commission). Оно также представляло собой своеобразный алгоритм, который в обязательном порядке должен был использоваться федеральными судьями до 2003 г.[3]

У КОМПАС и у Руководства о назначении наказаний общая проблема – они не дополняют, а входят в конфликт с деятельностью судьи-человека, в попытке лишить процесс назначения наказания индивидуализации. Между тем сам этот процесс является ценностью, поскольку в нем участвуют и судья, и обвиняемый. Каким же образом использовать современные технологии так, чтобы они не навредили ни процессу вынесения решения о наказании, ни результату? Донохью рассматривает два предложения: создать дружественную пользователю систему информации о назначении наказаний с целью создания нового общего права в этой области; создание виртуального помощника судьи для обеспечения диалога между машиной и человеком в процессе назначения наказания[4].

Что касается системы информации о назначении наказания, то основное преимущество этого предложения в том, что судьям всегда необходима информация – кто, как и какие решения принимал по аналогичным делам ранее. Система позволит судьям делать выборку принятых решений по ряду критериев, включая содержательные факты дела. Подобные системы уже существуют в ряде стран. Их использование в США, однако, было ограничено в силу того, что большая часть работы по внесению данных ложилась на судей и их помощников, а критики отмечали, что вносимая

---

[1] См.: Ibid. – P. 666.

[2] См.: Lola vs Skadden and the automation of the legal profession. – P. 303.

[3] См.: Donohue M. Op. cit. – P. 669.

[4] См.: Ibid. – P. 672.

информация нерепрезентативна. Кроме того, в системе общего права подобная система могла привести к увеличению неравенства при назначении наказаний, т.е. к результату принципиально обратному тому, которого стремились достичь введением Руководства о назначении наказаний и иных алгоритмов. И наконец, существовали опасения, что если судья будет принимать решения о том, какую информацию вносить в базу и какую информацию, в ней содержащуюся, использовать, это приведет к скрытой необъективности[1].

Современные технологии могут отчасти устранить эти недостатки. Они упрощают не только использование информации, но и ее ввод (появились функции распознавания голоса и синтаксического анализа естественных языков). Кроме того, искусственный интеллект может анализировать имеющиеся данные и определять тенденции, незаметные обычному пользователю. Информация об этих тенденциях может быть использована апелляционными судами, Комиссией по вынесению приговоров и третьими организациями.

Если вышеописанный проект описателен по своей природе и не является чем-то принципиально новым, то создание виртуального помощника, а точнее, партнера судьи – инициатива более амбициозная. Она предполагает сделать процесс назначения наказания диалоговым. Комиссии по назначению наказания будут выступать в роли экспертов, дающих судьям обратную связь, в том числе относительно того, какие наказания эффективны, а какие – нет. Такого рода партнерство или «менторство» активно используется в других профессиях, в том числе в медицине. Кроме того, алгоритм может не только обеспечивать судью информацией, но и стать ему собеседником, способным компенсировать «человеческие слабости», будь то когнитивные искажения или недостаток психологической выносливости. Он может анализировать предыдущие решения судьи и оповещать его, когда он будет отклоняться от своей собственной практики, определять уникальные характеристики конкретного дела и даже быть посредником в общении между судьей и общественностью[2].

Судьи по уголовным делам не единственные почувствовали на себе прогресс цифровых технологий. В ином контексте, но так-

[1] См.: Donohue M. Op. cit. – P. 674.

[2] См.: Ibid. – P. 676–677.

же значительно были затронуты и арбитражные судьи. Пьетро Ортолани, Университет Раутбоунд, отмечает, что развитие технологии блокчейн (blockchain) привело к появлению частных систем рассмотрения споров. Они могут действовать в обход процедур признания и исполнения, через которые государства обычно осуществляет контроль над процессом рассмотрения споров, а поскольку использование таких систем становится всё популярнее, это может привести к постепенной маргинализации судов. Одновременно с этим феномен основанного на блокчейне первичного размещения монет (initial coin offerings (ICOs)) породил волну судебных дел, поднимающих новые правовые вопросы, в том числе связанные с юрисдикцией, – делокализованная и децентрализованная природа блокчейна не вписывается в территориальный подход, с помощью которого до сих пор распределяется между судами международная юрисдикция[1].

Ключевая характеристика блокчейна – децентрализация. Эта технология была придумана специально, чтобы дать возможность совершать платежи через коммуникационные каналы в отсутствие доверенного лица, в ситуации, когда классическая функция денег (как посредника при обмене, средства накопления и единицы расчета) реализуется между двумя равными лицами без участия центрального органа и, что наиболее важно, вне тени государственной власти. Отрицание власти государства и его системы рассмотрения споров автоматически породило потребность создания сторонами своих собственных «судов». А поскольку технологии распределенного реестра (distributed ledger technologies) охватывают разные аспекты жизни, в качестве побочного продукта они породили разнообразные третейские органы, по требованию сторон способствующие исполнению контрактных обязательств. В рамках системы биткоина пользователи выработали механизм «двух подписей», работающий аналогично «двум ключам» (открыть замок можно только при одновременном наличии двух ключей). Арбитру дается право подписи, разрешая спор и признавая правоту одной из сторон, он предоставляет ей свою подпись в качестве «второго ключа». Более 30% сделок с биткоинами проводятся с использованием этого механизма, а специализированные сайты

[1] См.: Ortolani P. The impact of blockchain technologies and smart contracts on dispute resolution: Arbitration and court litigation at the crossroads // Uniform law review. – 2019. – Vol. 24. – P. 431.

даже предоставляют услуги арбитража, которые при необходимости могут использоваться сторонами. Странно, что этот уникальный способ эффективного транснационального рассмотрения споров практически игнорируется как специалистами по арбитражу, так и транснациональными юристами. Он характерен еще и тем, что моменты вынесения решения и его исполнения полностью совпадают[1]. Это потенциально может порождать и негативные последствия.

Государственное регулирование неспроста предусматривает определенные процедуры и время на исполнение решения. Они призваны обеспечить определенный баланс между правом требования кредитора и защитой основных прав дебитора. Мгновенное исполнение решения лишает дебитора возможности защититься.

Несмотря на то что алгоритмизированные способы рассмотрения споров имеют ряд недостатков, а для разрешения спора по договору, хоть немного отличающемуся от стандартного, условия которого можно «переложить в код» (смарт-контракт), требуется участие арбитра-человека, цифровые технологии неизбежно изменят судебный процесс. Одним из примеров потенциальных заимствований может служить использование «оракула» (oracle) – внешнего источника информации, к которому обращается смарт-контракт для установления наступления или не наступления прописанного в договоре события. Таким оракулом может выступать и суд, в зависимости от решения которого будет определен получатель средств по смарт-контракту. Внедрение этого и других инструментов самостоятельного исполнения обязательств по договору, используемых интернет-арбитражем, потребует выработки нормативных критериев их использования и пересмотра действующих сейчас правил процедуры. Один из ключевых вопросов в этой области – на каком уровне это следует делать. Учитывая, что процедуры исполнения тесно связаны с национальным суверенитетом, может показаться правильным оставить эту область государствам. Нельзя, однако, упускать из внимания, что регулирование кодов требует специальных знаний, и можно предположить, что эти знания будут неравномерно распределены между разными

[1] См.: Ortolani P. The impact of blockchain technologies and smart contracts on dispute resolution: Arbitration and court litigation at the crossroads // Uniform law review. – 2019. – Vol. 24. – P. 436.

юрисдикциями, что приведет к незащищенности пользователей в отдельных странах. Кроме того, при таком лоскутном регулировании возрастут риски и расходы бизнеса. Таким образом, предпочтительным было бы урегулирование этих вопросов на транснациональном уровне[1]. Такой подход в корне отличается от текущего регулирования исполнения решений судов и потребует от юристов всех мастей значительного расширения компетенции.

Необходимость успевать за техническим прогрессом и сужение сферы монополии настраивают юристов против внедрения новых технологий. Не стоит, однако, объяснять все проблемы захватом роботами жизненного пространства человека. Последствия экономического феномена, называемого «победитель получает все» («winner-take-all»), приводит к увеличению разрыва между успешными и неуспешными специалистами, причем это происходит и вне юридических профессий. Растет конкуренция и внутри фирм. Победить в ней сможет тот, кто готов повышать свою эффективность за счет преимуществ, предоставляемых современными технологиями. Так, директор «Лигал Сервисес Инновэйшн фор Фрэшфилдз» (Legal Services Innovation for Freshfields) отмечает, что использование системы юридической экспертизы (due diligence review) «Кира» (Kira) показало 70%-ный рост производительности фирмы в этой области. ДжПиМорган Чейз (JPMorgan Chase) создали собственную программу проверки договоров о коммерческих кредитах, позволившую обработать информацию о 12 тыс. договоров за секунды, в то время как человеку потребовалось бы на это 360 тыс. часов[2].

Таким образом, будущее юридической профессии лежит между двумя точками зрения – утопической фантазией о том, как искусственный интеллект облегчит работу всем юристам, и алармистским утверждением, что он полностью заменит людей[3]. Помня о том, что алгоритмы несовершенны, следует сменить вопрос «зачем нужны инновации» на вопрос «как извлечь из современных технологий максимум пользы».

---

[1] См.: Ortolani P. – P. 439, 441.

[2] См.: Lola vs Skadden and the automation of the legal profession. – P. 273, 283, 298.

[3] См.: Ibid. – C. 289.

3.4. Цифровая трансформация системы судебной статистики в Российской Федерации: Организационно-правовые аспекты

Основы формирования единого информационного пространства судебной системы. В современном мире отставание в вопросах информатизации экономической и социальной деятельности государства – проблема не только национальной безопасности государства, но и его непосредственного существования. Одним из ключевых *индикаторов* развития информационного общества в странах мира является рейтинг стран по индексу развития информационно-коммуникационных технологий (ИКТ – *ICT Development Index, IDI*). Индекс формируется Международным союзом электросвязи (МСЭ – *International Telecommunication Union, ITU*) на основе статистических данных, предоставляемых практически всеми странами мира. Индекс представляет собой интегрированную оценку развития информационного общества по 11 показателям, к основным параметрам измерения которого относятся, в частности, уровень развития инфраструктуры, интенсивность и потенциал использования ИКТ и др. Эти параметры отражаются в соответствующих многоаспектных индексах. В 2016 г. анализировались показатели по 175 странам. По сравнению с предыдущим годом Россия, несмотря на рост значения индикатора с 6,79 до 6,95, потеряла одну позицию в рейтинге, переместившись с 42-го на 43-е место[1]. В 2017 г. Россия переместилась с 43-го на 45-е место (индикатор 7.07), что вызывает опасения в наметившейся тенденции к снижению темпов в сфере информационного развития государства. Исследование *ICT Development Index* 2017 – последнее на настоящее время. Выпуск Индекса приостановлен из-за пересмотра показателей, включенных в данное исследование, а также методов их измерения. Секретариат Международного союза электросвязи проводит с государствами-членами консультации по данному вопросу и в дальнейшем планирует возобновить ежегодную публикацию результатов исследования в 2020 г.[2]

---

[1] См.: Measuring the Information Society Report 2016. – URL: https://www.itu.int/en/ITU-D/Statistics/Pages/publications/mis2016.aspx (дата обращения: 10.02.2020).

[2] См.: Measuring the Information Society Report 2017. – URL: http://www.itu.int/net4/ITU-D/idi/2017/index.html (дата доступа: 10.02.2020).

В рейтинге уровня развития электронного правительства, который содержится в обзоре одного из подразделений Организации Объединённых Наций, Россия по итогам 2018 г. занимает 32-е место (анализ проводится один раз в два года; в 2016 г. – 35-е место)[1]. Рейтинг построен на основе обобщенного индекса, включающего состояние *web*-присутствия органов государственной власти, состояние телекоммуникационной инфраструктуры и человеческого капитала и др. В настоящее время Россия входит в группу стран с очень высоким Индексом развития электронного правительства (ИРЭП – E-*Government Development Index, EGDI*). Согласно исследованию ООН, среди 40 городов, отобранных для эксперимента, Москва занимает 1-е место. За ней следуют Кейптаун и Таллин, на 4-м месте – Лондон и Париж. Рейтинг определялся согласно Индексу местного онлайн-обслуживания (ИМОО), который охватывает технические и содержательные аспекты вебсайтов города или муниципалитета, а также качество предоставления электронных услуг и инициативы по повышению участия населения через электронные порталы[2].

Цифровизация экономических и социальных структур государства – основа для дальнейшего совершенствования системы государственного управления, экономики, бизнеса, социальной сферы общества. За последние годы в стране принят ряд нормативных правовых актов в области создания цифровой экономики, определяющих стратегические цели, задачи и меры по реализации внутренней и внешней политики Российской Федерации в области применения ИКТ, направленных на развитие информационного общества, формирование национальной цифровой экономики, обеспечение национальных интересов и реализацию стратегических национальных приоритетов.

Стратегия развития информационного общества в Российской Федерации на 2017–2030 гг., утвержденная Указом Президента РФ от 9 мая 2017 г. № 203, определяет информационное общество как общество, в котором информация и уровень ее применения и доступности кардинальным образом влияют на экономические и социокультурные условия жизни граждан. Стратегия

[1] См.: United Nations E-Government Survey. – URL: https://www.unilibrary.org/democracy-and-governance/united-nations-e-government-survey-2018_d54b9179-en (дата доступа: 10.02.2020).

[2] Ibid.

обосновывает создание информационного пространства государства в виде совокупности информационных ресурсов, созданных субъектами информационной сферы, средств взаимодействия таких субъектов, их информационных систем и необходимой информационной инфраструктуры.

Всё это непосредственно относится и к судебной системе Российской Федерации. Инфраструктура электронного правительства объединяет размещенные на территории РФ государственные информационные системы, программно-аппаратные средства и сети связи, обеспечивающие при оказании услуг и осуществлении функций в электронной форме взаимодействие органов государственной власти Российской Федерации, органов местного самоуправления, граждан и юридических лиц. Таким образом, формирование информационного пространства (с учетом потребностей граждан и общества в получении качественных и достоверных информационных услуг) невозможно без совершенствования нормативного правового регулирования в сфере обеспечения эффективной переработки информации (включая ее поиск, сбор, анализ, использование, сохранение и распространение) и применения новых технологий, уровень которых должен соответствовать уровню развития и интересам общества.

Формирование единого информационного пространства федеральных судов общей юрисдикции и мировых судей, системы Судебного департамента при Верховном Суде РФ осуществляется Управлением информатизации департамента на основе федеральных законов: от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» и от 22 декабря 2008 г. № 262-ФЗ «Об обеспечении доступа к информации о деятельности судов в Российской Федерации» (ст. 10; 11), Федеральной целевой программы «Развитие судебной системы России на 2013–2020 годы», утвержденной постановлением Правительства РФ от 27 декабря 2012 г. № 1406, и Концепции развития информатизации судов общей юрисдикции на 2013–2020 гг., утвержденной постановлением Президиума Совета судей РФ от 28 февраля 2013 г. № 328. Деятельность Судебного департамента по информатизации судов осуществляется на основе взаимодействия с комиссией Совета судей РФ по информатизации и автоматизации работы судов.

В основе формирования единого информационного пространства судебной системы в соответствии с требованиями нор-

мативных документов лежат меры по совершенствованию правового регулирования, включающие определение понятий, необходимых для формирования единой цифровой среды судебной системы, где выработка алгоритмов удаленного подтверждения личности для совершения юридически значимых действий лежит в основе достоверности данных судебной системы. 1. Введение равного статуса различных способов идентификации и аутентификации физических и юридических лиц, иных участников системы судебных отношений, правовое признание равных с бумажными взаимодействиями цифровых публичных правовых и гражданско-правовых взаимодействий. 2. Выработка способов независимой доверенной фиксации и предоставления заинтересованным лицам юридических данных, связанных с электронным дистанционным взаимодействиям, электронными документами третьей доверенной стороны.

Большую роль в эффективной работе судебной системы государства играет сбор и анализ данных судебной статистики. Ведение судебной статистики осуществляется в соответствии с Федеральным законом от 29 ноября 2007 г. № 282-ФЗ «Об официальном статистическом учете и системе государственной статистики в Российской Федерации». Согласно этому Закону Судебный департамент является субъектом официального статистического учета, осуществляющим формирование официальной статистической информации в судебной системе на основе данных первичного статистического учета, представленных субъектами статистического наблюдения. Первичный статистический учет осуществляется следующими субъектами статистического наблюдения: Верховным Судом РФ, верховными судами республик, краевыми и областными судами, судами городов федерального значения, судами автономных областей и автономных округов, окружными (флотскими) военными судами, арбитражными судами, органами Судебного департамента.

Существующие форматы данных сбора, хранения и предоставления информации не удовлетворяют требованиям, предъявляемым документами, определяющими стратегические задачи построения информационного общества в Российской Федерации. Современный информационный анализ государственных структур показывает, что примерно 80% данных, обрабатываемых в информационных системах государственного сектора, обладают геопространственными характеристиками. Создание высококачествен-

ных геопространственных статистических моделей позволит надежно связать многомерные статистические данные друг с другом на платформе геоинформационных технологий.

Управление информационных ресурсов и технологий Федеральной службы государственной статистики переходит на цифровую платформу с геопривязкой для обработки статистических данных, имеющих пространственную (координатную) привязку. МВД России, согласно Положению о полномочиях федеральных органов исполнительной власти по поддержанию, развитию и использованию глобальной навигационной спутниковой системы (ГЛОНАСС) в интересах обеспечения обороны и безопасности государства, социально-экономического развития Российской Федерации и расширения международного сотрудничества, а также в научных целях, утвержденному постановлением Правительства РФ от 30 апреля 2008 г. № 323, осуществляет внедрение систем, функциональных дополнений и аппаратуры спутниковой навигации в интересах обеспечения общественной безопасности, правопорядка, защиты жизни, здоровья, прав и свобод граждан от преступных посягательств. Объемы информации, связанные с данными судебной статистики и попадающие под определение пространственных данных, постоянно увеличиваются.

Для создаваемой информационной структуры судебной системы Российской Федерации характерен ряд особенностей. Большая территория и значительное количество временных поясов, которые должна охватить информационная система, требует определенных подходов в организации как системы управления, так и доступа пользователей. При этом судебная система государства имеет множество связей с другими структурами: органами управления, министерствами, ведомствами, системой образования и др. Решение задач судебной системой России подразумевает переработку огромных объемов разнородной информации, имеющей различный вид, представления, свойства и качественные характеристики.

В настоящее время методические вопросы комплексного анализа многомерных данных социального характера на основе сочетания методов статистического анализа и методов пространственного анализа разработаны недостаточно глубоко. Отсутствуют алгоритмы и программные средства анализа информации с учетом пространственных свойств объектов. В связи с этим возникает необходимость разработки новых подходов к комплексному

анализу многомерных данных социального характера, основанных на сочетании методов искусственного интеллекта и технологий пространственного анализа с применением геоинформационных систем (ГИС).

Создание и использование методик и алгоритмов комплексного анализа многомерных данных о пространственно-распределенных объектах и процессах, основанных на методах статистической обработки данных[1], методе главных компонентов, численных методах, методах пространственного анализа многомерных данных с использованием геоинформационных систем, позволяет наиболее эффективно решать задачи в рамках судебной системы РФ.

Исходные данные судебной статистики. Судебная статистика как правовая наука изучает количественную сторону массовых правовых и юридически значимых явлений в неразрывной связи с их качественным содержанием в конкретных условиях места и времени. При этом статистика изучает *массовые* явления, состоящие из множества отдельных элементов или фактов. Так, *преступление* – это индивидуальное деяние, обладающее определенным набором обязательных элементов состава преступления, таких как общественная опасность, противоправность, виновность и наказуемость (ст. 14 УК РФ). *Преступность* же – явление массовое, специфический социально-правовой процесс, в котором проявляются наиболее существенные черты отдельных преступлений.

Анализ преступности предполагает сбор, переработку и анализ больших динамически изменяющихся массивов разнообразных статистических данных[2]. При этом информация (данные) о правонарушениях и преступности в целом должна отвечать множеству директивных требований, среди которых *достоверность, полнота, своевременность, сопоставимость* и др.[3]

Достигнутый научно-технический уровень электронной переработки статистической судебной информации (например, с использованием программного комплекса «Судебная статистика», обрабатывающего табличные данные в формате *MS Excel* и тек-

[1] Ловцов Д.А., Богданова М.В., Паршинцева Л.С. Основы статистики / под ред. Д. А. Ловцова. – М.: РГУП, 2017. – С. 160.

[2] Преступность и правонарушения (2009–2013): стат. сб. – М.: ГИАЦ МВД России, 2014. – 180 с.

[3] Настольная книга администратора суда общей юрисдикции / под ред. В.М. Лебедева. – М.: Юристъ, 2004. – 223 с.

стовые данные – в формате программного комплекса *SKART/STORM*) не позволяет решить актуальную научно-прикладную *проблему* своевременного сбора и качественного анализа больших массивов многоаспектной, статистической судебной информации с целью динамического моделирования социально-правовых процессов в обществе и выявления устойчивых трендов и закономерностей его развития. Это представляется возможным сделать на основе внедрения и применения эффективных средств телематики и геоинформатики, а также соответствующей *новой* (нетрадиционной[1]) геоинформационной технологии (НГИТ), базирующейся на знаниях технологии ведения баз данных и данных о пространственных объектах (моделях предметной области судебной статистики).

С этой целью подлежит первоочередной целенаправленной модернизации[2] программное обеспечение существующей и развивающейся Государственной автоматизированной системы (ГАС) РФ «Правосудие»[3], имеющее в своем составе программные изделия «Судебная статистика» и «Судимость» (функциональная подсистема «Судебное делопроизводство и статистика») для выполнения аналитических задач судебной статистики и программное изделие «Визуализация» (подсистема «Административное управление»), обеспечивающее представление информации с использованием картографии. Модернизация данных программных изделий, а также программного изделия «Интеграция» (подсистема «Организационное обеспечение»), предназначенного для обеспечения информационного обмена (интеграции) разнородных информационных ресурсов подсистем ГАС РФ «Правосудие» и организации унифицированного доступа к распределенным информационным хранилищам, позволит продуктивно использо-

---

[1] См.: Ловцов Д.А. Информационная теория эргасистем: тезаурус. – М.: Наука, 2005. – 248 с.

[2] См.: постановления Правительства РФ: от 15 апреля 2014 г. № 313 «Об утверждении государственной программы Российской Федерации «Информационное общество (2011–2020 годы)»; от 27 декабря 2012 г. № 1406 «О Федеральной целевой программе “Развитие судебной системы России на 2013–2020 годы”».

[3] См.: Техническое задание на проектирование ГАС РФ «Правосудие». – М.: НИИ «Восход», 2004. – 97 с.; ГАС РФ «Правосудие»: Общее описание системы. Часть 1. Общие сведения, – 2008. – URL: https://techportal.sudrf.ru/ (дата обращения: 12.02.2020).

вать возможности, предоставляемые национальной инфраструктурой пространственных (географических) данных[1].

Эффективное управление судебной системой, принятие качественных судебных актов при разрешении споров, анализ данных судебной статистики и прогнозирование социальных процессов требуют определенного набора показателей. При оптимальном выборе системы исходных показателей, для всестороннего (в той степени, в которой это требуется) описания и изучения явлений, процессов, связанных с судебной системой и непосредственно с вопросами судебной статистики, не должно возникать дублирования исходных данных и использования данных с неопределенными характеристиками. В противном случае они могут искажать наиболее значимые признаки и в определенном счете привести к обесцениванию конечного результата. Трудно найти критерии, дозволяющие оценить необходимость используемых показателей как индикаторов характеристики статистического комплекса многомерных данных. Использование в наборе статистических данных пространственной информации позволяет сводить к минимуму дублирование исходных данных, повышает качество аналитических моделей для статистического анализа и открывает новые возможности в построении аналитических моделей многомерных данных судебной статистики.

В Российской Федерации в соответствии с Федеральным законом от 30 декабря 2015 г. № 431-ФЗ «О геодезии, картографии и пространственных данных и о внесении изменений в отдельные законодательные акты Российской Федерации» создаются следующие государственные фонды пространственных данных:

1) федеральный фонд пространственных данных;

2) ведомственные фонды пространственных данных;

3) фонд пространственных данных федерального органа исполнительной власти, осуществляющего функции по выработке и реализации государственной политики, нормативно-правовому регулированию в области обороны;

4) фонды пространственных данных субъектов РФ.

Определение информации, относимой к пространственным данным, дано в государственном стандарте ГОСТ Р 52438–2005.

[1]См.: Концепция создания и развития инфраструктуры пространственных данных Российской Федерации, одобренная распоряжением Правительства РФ от 21 августа 2006 г. № 1157-р.

Под *пространственными объектами* следует понимать цифровую модель материального или абстрактного объекта реального или виртуального мира с указанием его идентификационных, координатных и атрибутивных характеристик[1]. Объектом может быть неподвижный или движущийся, простой или сложный объект, явление, событие, процесс и ситуация. Моделируемый объект может относиться к территории, акватории, недрам и воздушному пространству Земли и др. В широком смысле под *пространственным объектом в системах обработки пространственных данных* понимается как сам объект, так и адекватная ему цифровая модель. Создание цифровых моделей сбора и анализа данных судебной статистики позволит обрабатывать многоаспектную, имеющую сложные взаимные связи информацию.

В Российской Федерации распоряжением Правительства РФ от 21 августа 2006 г. № 1157-р разработаны требования к создаваемой инфраструктуре пространственных данных (ИПД) Российской Федерации, включающей в информационно-телекоммуникационную систему, обеспечивающую доступ граждан, хозяйствующих субъектов, органов государственной и муниципальной власти к распределенным ресурсам пространственных данных, а также распространение и обмен данными в общедоступной глобальной информационной сети в целях повышения эффективности их производства и использования. ИПД объединяет технологии, научно-техническую политику, организационное обеспечение, человеческие и другие ресурсы, необходимые для производства, обработки, хранения, распространения, интеграции и использования пространственных данных.

Использование национальной инфраструктуры *цифровых пространственных данных* Российской Федерации на основе НГИТ их переработки и графической визуализации позволит, в частности, повысить эффективность решения следующих практических задач судебной статистики: классификация противозаконных процессов и явлений с учетом пространственных характеристик; районирование и типология преступных деяний; выявление определяющих факторов нарушения законодательства; временной анализ преступлений; выявление связей преступлений и социально-

[1] См.: ГОСТ Р 52438–2005 Национальный стандарт Российской Федерации. Географические информационные системы. Термины и определения. (Geographical information systems. Terms and definitions). Дата введения 01.07.2006 г. – М.: Стандартинформ, 2006.

экономической инфраструктуры региона; анализ и прогнозирование *судебной нагрузки*[1] в рамках пространственно-распределенной судебной системы и др.

Основные подходы к построению модели данных судебной статистики. При ведении судебного статистического учета с использованием НГИТ в учитываемые данные различного вида, такие как краткое описание объекта (события, процесса, явления, правоотношения и др.) – «семантическая информация» и совокупность свойств и количественно-качественных признаков (атрибутов) объекта – «атрибутивная информация», добавляется пространственная характеристика – «координатная информация» (например, при учете уголовных преступлений, географические координаты места совершения преступления). Информация об атрибутах пространственных объектов (текстовая, графическая, фото-, видео-, аудио- и др.), а также их местоположение являются обязательным компонентом при моделировании или решении аналитических задач судебной статистики на основе НГИТ[2]. Эта информация используется для создания иерархических (многослойных) *цифровых моделей* предметной области судебной статистики, ориентированных в пространстве, которые можно исследовать как визуально (на экране монитора), так и с помощью специального программного обеспечения.

При переработке и анализе первичной статистической информации создаваемые с помощью НГИТ аналитические группировки по качественным признакам имеют вид *слоя* на базовой пространственной *цифровой модели* местности или объекта. *Слой* представляет собой подмножество пространственных объектов определенной предметной области, обладающих тематической общностью и единой для всех слоев системой координат[3]. Цифровая пространственная модель местности может быть картой различного вида (векторная, растровая и др.) и содержания (топокар-

---

[1] См.: Ловцов Д.А., Ниесов В.А. Модернизация информационной инфраструктуры судопроизводства – ключевое направление оптимизации нагрузки на судебную систему // Российское правосудие. – М., 2014. – № 9. – С. 30–40.

[2] См.: Ловцов Д.А., Черных А.М. Геоинформационные системы: учеб. пособие. – М.: РГУП, 2012. – 188 с.

[3] См.: ГОСТ Р 52438–2005 Национальный стандарт Российской Федерации. Географические информационные системы. Термины и определения. (Geographical information systems. Terms and definitions). Дата введения 01.07.2006 г. – М.: Стандартинформ, 2006.

та, карта плотности населения, план города, план здания или комнаты, 3 *D*-карта и др.). Слой, отображающий статистические данные в виде «точек» и их содержательные характеристики на цифровой модели местности, а также продукционные правила (эвристики) их переработки, представляет собой *частную модель предметной области* судебной статистики, например, такой как «Уголовная преступность», «Судимость», «Административная противоправность», «Гражданско-правовая деликтность», «Транспортная аварийность» и др.

При анализе набора статистических данных, имеющих пространственную привязку, на основе векторной (в виде набора координатных пар) цифровой модели каждому объекту слоя соответствует запись в базах семантических, атрибутивных и координатных данных и знаний (БДЗ), обеспечивающая привязку информации к местности. Это соответствие обеспечивается назначением каждому объекту соответствующего уникального идентификатора. При этом в результате ввода (любым способом) в БДЗ НГИТ данных судебной статистики образуется слой или слои электронно-цифровой модели пространственной информации, которые содержат идентифицированные пространственные объекты, связанные с базой атрибутивных данных и знаний, соотносящихся с данными судебной статистики.

Удобным инструментом визуализации данных судебной статистики является «раскраска» описанных объектов аналогично тому, как это делают на обычных географических картах. Порождать свою раскраску ячеек сетки, проекций, данных и других объектов могут различные характеристики данных. Это могут быть известные классификационные признаки, значения, зависимости, производные и др. Любые результаты функционального анализа над данными судебной статистики могут служить основой для цветовой визуализации (*картирование данных*) в виде отдельного слоя. Такие цветовые модели можно построить с использованием арсенала средств и методов НГИТ[1].

Во-первых, с помощью средств НГИТ можно изобразить сами данные судебной статистики. При этом можно отображать различные разбиения на подмножества данных, в соответствии со значением признаков, характеризующих различные виды нарушения законодательства.

---

[1] См.: Ловцов Д.А. Информационная теория эргасистем: тезаурус. – М.: Наука, 2005. – 248 с.

Во-вторых, на цифровой пространственной модели можно изобразить произвольные функции координат данных, поскольку каждой точке с координатами (*x, y*) на двумерной карте соответствует точка I_s в *n*-мерном пространстве данных. Кроме этого, на карте можно отображать такие координатные функции, как плотность распределения данных в пространстве или плотность того или иного подмножества данных. Саму плотность можно рассчитать с помощью какой-либо непараметрической оценки. Кроме собственно плотностей подмножеств, интерес могут представлять цветовые модели, отвечающие значению относительных плотностей подмножеств на фоне общего распределения.

В-третьих, цветовые модели позволяют составлять по множеству *X* несколько цветовых моделей, которые являются проекциями данных судебной статистики. Одна из таких моделей визуализирует сами данные. Последовательность проекций атрибутов данных судебной статистики позволяет моделировать социальные события и процессы в обществе, коллективе и с высокой точностью, а в случае неполных данных позволяет правдоподобно восстанавливать пропущенные или прогнозировать их.

Средства НГИТ позволяют проводить цветовое моделирование данных судебной статистики и по плотности их распределения, оцененной с помощью различных непараметрических показателей. Наиболее часто рассматривается двумерное распределение «точек» на карте. При этом наибольшую эффективность в решении задач пространственного анализа и прогнозирования дает построение цветовой модели данных судебной статистики по плотности точек в исходном *n*-мерном пространстве.

В основе построения трехмерных моделей данных лежат показатели *соотношения* количества преступлений и количества населения на данной территории. Разнонаправленность векторов преступлений и плотности населения (плотность населения падает, а количество преступлений растет) указывает, в частности, на необходимость анализа выбранного района по другим показателям (экономическому, социальному, гендерному и др.) с целью определения тенденций в совершении правонарушений[1].

[1] См: Цветков В.Я. Пространственные данные и инфраструктура пространственных данных // Успехи современного естествознания. – М., 2013. – № 3. – С. 87–89.

Для большинства классификационных задач, например, поиска соотношений между проживающим на данной территории населением, инфраструктурой различного назначения, правоохранительной системой и системой судопроизводства, это позволяет полученные статистические данные соотносить с исследуемыми процессами и явлениями в обществе. Использование функциональных возможностей НГИТ позволяет на основе построения слоев статистических данных решать задачи классификации, прогнозирования, зонирования и районирования, проведения временного анализа в пространстве и др.

При ситуационной корректировке *цифровой модели предметной области* можно использовать периодические отчетные данные Судебного департамента: «Отчет о работе судов общей юрисдикции по рассмотрению уголовных дел по первой инстанции», «Отчет о работе судов общей юрисдикции о рассмотрении гражданских дел по первой инстанции», «Отчет о суммах ущерба от преступлений, суммах материальных взысканий в доход государства, количестве вынесенных постановлений об уплате процессуальных издержек за счет средств федерального бюджета и назначении экспертиз» и др. (полученные путем выгрузки данных из СУБД *Oracle Database Standard Edition* в формате табличного редактора *MS Excel*)[1]. При этом для некоторых слоев данных в качестве координат пространства можно использовать отношения показателей данных судебной статистики как независимых признаков.

Результаты электронно-цифровой переработки судебной статистики на основе НГИТ графически *визуализируются* (в частности, коэффициенты преступности по каждому субъекту, по каждой социальной и этнической группе и др.; удельные веса отдельных видов и категорий преступлений и др.) и *документируются* (например, табличный отчет и диаграмма количества преступлений в субъекте за определенное время, диаграмма национального состава субъектов и др.) на *n*-мерной цифровой модели местности.

Подобное отображение данных будет получено и при использовании семантических характеристик преступления, например, таких, как ущерб от правонарушения или количество лиц, участвующих в правонарушении и др. То есть анализ статистиче-

[1] Сайт Судебного департамента при Верховном Суде Российской Федерации. – URL: http://www.cdep.ru/index.php?id=344 (дата обращения: 14.01.2020).

ских данных может происходить по различному набору показателей, которые в системах электронно-цифровой обработки судебной статистики используются не полностью. Эффективный многоаспектный анализ статистических данных на основе средств НГИТ делает возможным информационную поддержку принятия решений в режиме ситуационного центра[1].

Одним из преимуществ НГИТ является наиболее естественное (для человека) визуальное представление, как пространственной информации, так и любой другой информации, имеющей отношение к объектам, расположенным в пространстве. Причём под пространством понимается не только трехмерное пространство, но и любое абстрактное пространство произвольной размерности.

Электронно-цифровая обработка статистических данных, скомпонованных по различным признакам и имеющих пространственную привязку, упрощает ввод данных, их классификацию и каталогизацию, позволяет проводить анализ поступивших данных по широкому кругу показателей и строить модели объекта, события, процесса и др. Ведение пространственного учета об объектах или процессах, подлежащих анализу в судебной системе, дает возможность выявлять и оценивать новые (скрытые) взаимосвязи, эффективно моделировать и проводить системный анализ социально-правовых процессов и явлений в обществе.

Целенаправленная модернизация современной системы электронно-цифровой переработки судебных статистических данных на основе внедрения и применения средств новой геоинформационной технологии, базирующейся на знаниях, позволит в недалеком будущем создать принципиально новую систему судебной статистики. Дальнейшая цифровая трансформация системы судебный статистики возможна на основе внедрения и применения сопряженных средств телематики, обеспечивающих *сетевой* (распределенный) оперативный и защищенный сбор статистической информации.

Судебные статистические данные и пространственная информация. *Данные судебной статистики* – официальная статистическая информация о количественных показателях рассмотрения федеральными арбитражными судами, федеральными судами общей юрисдикции и мировыми судьями дел и материалов в порядке уголовного, гражданского, административного производ-

[1] См.: Ловцов Д.А., Богданова М.В., Михайлов М.А. Статистика: учеб. пособие / под ред. Д.А. Ловцова. – М., 2010. – С. 120.

ства и производства по делам об административных правонарушениях, формируемая Судебным департаментом как субъектом официального статистического учета.

В соответствии со ст. 6 Федерального закона от 8 января 1998 г. № 7-ФЗ «О Судебном департаменте при Верховном Суде Российской Федерации» Судебный департамент в порядке реализации полномочий по ведению судебной статистики осуществляет сбор статистических сведений, представляемых федеральными арбитражными судами, областными и равными им судами, окружными (флотскими) военными судами, территориальными органами Судебного департамента, о деятельности судов и состоянии судимости в Российской Федерации по итогам отчетного периода. Сводная статистическая отчетность о деятельности судов и о состоянии судимости в Российской Федерации, согласно Федеральному закону от 22 декабря 2008 г. № 262-ФЗ «Об обеспечении доступа к информации о деятельности судов в Российской Федерации», размещается в разделе «Судебная статистика» официального сайта Судебного департамента.

В порядке и сроки, определенные распоряжением Правительства РФ от 6 мая 2008 г. № 671-р. «Об утверждении Федерального плана статистических работ», сформированные Судебным департаментом сводные статистические отчеты направлены в Федеральную службу государственной статистики. Статистическая информация размещается на портале Единой межведомственной информационно-статистической системы (ЕМИСС)[1].

В 2017 г. арбитражные суды первой инстанции рассмотрели почти 1,75 млн дел, и число споров неуклонно растет. Вместе с увеличением количества дел в арбитражных судах первой инстанции также увеличилась нагрузка и на апелляционные суды – они рассмотрели 299 783 дела в 2017 г. Это на треть больше, чем семью годами ранее, – тогда до апелляции дошло 200 тыс. споров. Существенное место в судебной практике занимают земельные споры – рассмотрено более 200–210 тыс. дел. За последние три года их число увеличилось более чем на 25%[2]. Актуальными в практике судов остаются вопросы, связанные с земельными участками под многоквартирными домами, которые принадлежат на

[1] ЕМИСС: Государственные статистические показатели. – URL: https://www.fedstat.ru/ (дата обращения: 11.02.2020).

[2] См.: Там же.

праве общей долевой собственности всем собственникам помещений в многоквартирном доме. В связи с этим для осуществления любой реконструкции, фактически влекущей изменение земельного участка, требуется согласие собственников, государственных структур учета и контроля объектов недвижимости и земельных ресурсов. Вряд ли можно найти в нашем государстве районный суд, который бы не рассматривал иски соседей, не поделивших сотки. Кто-то недоволен тем, что сосед захватил буквально сантиметры чужого участка, а кому-то приходится возмущаться перенесенным на метры вглубь собственной территории забором соседа. В большинстве случаев миром договориться сторонам спора удается не всегда, и граждане идут в суды. Но и там не всегда находят объективные решения земельных конфликтов.

Несовершенство законодательного регулирования и судебные ошибки обусловливают необходимость формирования судебной практики с использованием новых геоинформационных технологий для обработки пространственных данных. Отсутствие точной пространственной информации, неправильное ее использование, а также длительное рассмотрение споров в данной сфере способны негативно сказаться не только на стабильности земельных, предпринимательских и фермерских отношений. При рассмотрении таких споров нередко суды не учитывают основные потребности истца как собственника недвижимости. В Федеральном законе от 24 июля 2007 г. № 221-ФЗ «О государственном кадастре недвижимости» предусмотрено обязательное согласование местоположения границ земельных участков с заинтересованными лицами. Это делается в тех случаях, когда «в результате кадастровых работ уточняются местоположение границ земельного участка или границы смежных участков, сведения о которых внесены в государственный кадастр недвижимости».

Рассматривая требования о прекращении права собственности граждан на земельные участки, суды должны учитывать, что по смыслу п. 1 и 2 ст. 209 и п. 1 ст. 235 ГК РФ прекращение права собственности возможно исключительно по волеизъявлению собственника или по основаниям, указанным в законе. Иное толкование данных норм означает нарушение принципа неприкосновенности собственности, абсолютного характера правомочий собственника.

Особое место в решении судебных споров занимают дела, связанные с перевозками на автотранспорте. Создание компаний, предоставляющих услуги определения местоположения с исполь-

зованием систем спутникового позиционирования, было предусмотрено Федеральным законом от 28 декабря 2013 г. № 395-ФЗ «О Государственной автоматизированной информационной системе “ЭРА-ГЛОНАСС”».

Государственная автоматизированная информационная система ЭРА-ГЛОНАСС обеспечивает оперативное получение информации о дорожно-транспортных происшествиях на автомобильных дорогах в Российской Федерации, ее обработку, хранение и передачу в экстренные оперативные службы, а также доступ к этой информации государственных органов, органов местного самоуправления, должностных лиц, юридических и физических лиц.

В соответствии с нормативными правовыми актами собственники (владельцы) транспортных средств нескольких категорий, кроме физических лиц, должны оснащать их аппаратурой спутниковой навигации, обеспечивающей определение и передачу в Ространснадзор данных о пространственно-временных характеристиках транспортного средства через систему ЭРА-ГЛОНАСС.

Введение в оборот данных о пространственно-временных характеристиках объектов создает возможность для принятия более обоснованных судебных решений, позволяет изменить модели статистического анализа правонарушений в этой области.

Согласно Федеральному закону от 30 декабря 2015 г. № 431-ФЗ «О геодезии, картографии и пространственных данных и о внесении изменений в отдельные законодательные акты Российской Федерации» в целях обеспечения доступа физических и юридических лиц к находящимся в распоряжении органов государственной власти субъектов РФ и органов местного самоуправления сведениям, подлежащим представлению с использованием координат, пространственным данным и материалам, содержащимся в региональных фондах пространственных данных, органы государственной власти субъектов РФ вправе организовывать создание региональных порталов пространственных данных, являющихся государственными информационными системами. Доступ физических и юридических лиц к информации, размещенной на федеральном портале пространственных данных и региональных порталах пространственных данных, обеспечивается посредством использования информационно-телекоммуникационных сетей общего пользования, в том числе сети Интернет.

Таким образом, анализ и систематизация данных судебной статистики с учетом пространственных характеристик – важное требование процесса информатизации.

В качестве систем, предназначенных для создания баз пространственных данных и построения аналитических моделей, наиболее эффективно используются геоинформационные системы (ГИС). Одной из особенностей указанных систем является выполнение требований совместимости описания пространственных отношений объектов. Характеристики пространственных отношений объектов являются самостоятельным видом удостоверения местоположения и взаимного расположения объектов в рамках информационных ресурсов пространственных данных при обеспечении их совместимости. Пространственные отношения объектов в ГИС фиксируются в виде описаний взаимных связей пространственных объектов, основанных на их расположении в установленной системе координат, ссылок в описании одних пространственных объектов на описания других пространственных объектов[1].

Информационные системы, создаваемые для решения задач судебной статистики, должны использовать элементы общей инфраструктуры пространственных данных, координатные и адресные данные одних и тех же объектов. Обеспечение совместимости информационной модели многомерных данных, создаваемой в геоинформационных системах, необходимо для предотвращения правовых конфликтов, которые могут возникнуть вследствие несовместимости данных по конкретным территориям или неточностей при их получении, и других целей.

[1] См.: ГОСТР 52571–2006. Национальный стандарт Российской Федерации. Географические информационные системы. Совместимость пространственных данных. Общие требования. Общие требования. Geographical information systems. Spatial data compatibility. General requirements. Дата введения 01.01.2007 г. – М.: Стандартинформ, 2007.

Глава 4.
ИНТЕРНЕТ-ПРАВО И ИНТЕРНЕТ-ТЕХНОЛОГИИ: ПРАВОВЫЕ ВОЗМОЖНОСТИ И РИСКИ

4.1. Современные взгляды на роль права в регулировании Интернета и техно-утопизм Дж. Барлоу

Джон Перри Барлоу (*John Perry Barlow*) (1947–2018) – американский поэт, философ и активист Интернета, сооснователь Фонда электронных рубежей (*Electronic Frontier Foundation*) (некоммерческой организации, занимающейся защитой гражданских прав и свобод в цифровом мире), автор ряда работ, посвященных свободе Интернета и привлекших внимание многих исследователей своей концепцией развития Интернета[1]. Он связал будущее киберпространства с «новой областью чистой свободы». Позднее ученые-юристы, занимающиеся киберправами, отмечали, что Дж. Барлоу не столько констатировал факт, сколько «упражнялся в преднамеренном утопизме». Однако позднее, по их же признанию, высказывания Барлоу во многом оказались пророческими в отношении взаимодействия законов, онлайн-среды и защиты прав человека: «По прошествии всего двух десятилетий “законы больше не имеют смысла в онлайн-среде”, а защита основных прав человека в эпоху больших данных и сетевой информации начала полностью выходить из строя»[2].

В 2019 г. научный журнал Duke law and technology review организовал в память о Дж. Барлоу симпозиум «Прошлое и будущее Интернета» и посвятил специальный выпуск обсуждению его правового и философского наследия, в центре которого два опубликованных им эссе – «Декларация независимости кибер-

[1] См.: John Perry Barlow library. – URL: https://www.eff.org/john-perry-barlow (дата обращения: 26.02.2020).

[2] Cohen J. Internet utopianism and the practical inevitability of law // Duke law and technology review. – 2019. – Vol. 18, N 1. – P. 86.

пространства»[1] и «Продажа вина без бутылок: Экономика разума в глобальной сети»[2], ставших отправными точками для обмена мнениями ученых на представленной этим журналом площадке.

Данный параграф монографии включает авторский перевод на русский язык «Декларации независимости киберпространства» и анализ ряда научных статей, представленных в рамках посвященного Дж. Барлоу симпозиума.

Декларация независимости киберпространства[3]

Правительства Индустриального Мира, вы, обессиленные гиганты из плоти и стали, я пришел из Киберпространства, новой обители Разума. Во имя будущего я взываю к вам в прошлое: оставьте нас в покое. Вы – нежеланные гости среди нас. Вы не обладаете суверенитетом там, где собираемся мы. У нас нет и вряд ли когда-нибудь будет избранное правительство, и я обращаюсь к вам, имея не больше власти, чем та, с которой всегда говорит сама свобода. Я провозглашаю глобальное социальное пространство, которое мы формируем, по своей природе независимым от диктатуры, которую вы пытаетесь навязать нам. У вас нет ни морального права властвовать над нами, ни каких-либо методов принуждения, которых нам следовало бы обоснованно бояться.

Источником легитимной власти правительств является согласие управляемых лиц. Нашего согласия вы не просили и не получали. Мы не приглашали вас. Вы не знаете ни нас, ни наш мир. Киберпространство не лежит в пределах ваших границ. Не думайте, что вы можете построить его, как если бы это был общественный строительный проект. Вы не можете этого сделать. Оно представляет собой явление природы, и оно разрастается посредством наших совместных действий.

---

[1] См.: Barlow J.P. A Declaration of the independence of cyberspace. – URL: https://www.eff.org/cyberspace-independence (дата обращения: 26.02.2020).

[2] См.: Barlow J.P. Selling wine without bottles: The economy of mind on the global net. – URL: https://www.eff.org/pages/selling-wine-without-bottles-economy-mind-global-net (дата обращения: 26.02.2020).

[3] Перевод с англ. – Д.В. Красиков.

Вы не принимали участие в нашем великом и объединяющем общении, не создавали изобилие наших рынков. Вы не знаете ни нашей культуры, ни нашей этики, ни тех неписаных кодексов, которые уже обеспечили нашему обществу порядок больший, чем тот, который может быть достигнут любыми из ваших предписаний. Вы заявляете, что у нас есть проблемы, которые вам необходимо решить. Вы используете это заявление в качестве основания для вторжения на нашу территорию. Многие из этих проблем не существуют. Там, где действительно есть конфликты, где есть несправедливость, мы будем выявлять их и решать их своими средствами. Мы формируем наш собственный Общественный Договор. Это управление возникнет в соответствии с условиями нашего мира, не вашего. Наш мир – иной.

Киберпространство состоит из взаимодействий, отношений и самой мысли, образующих подобие волнового рисунка на ткани нашего общения. Наш мир – это везде и нигде, но точно не там, где живут тела.

Мы создаем мир, в который может попасть каждый, без каких-либо привилегий или предрассудков, связанных с цветом кожи, экономическим влиянием, военной силой или местом рождения.

Мы создаем мир, в котором каждый, где бы он ни находился, может выражать его или ее убеждения, какими бы необычными они ни были, без опасения быть принужденным к молчанию или послушанию.

Ваши правовые концепции собственности, выражения мнения, личности, передвижения и контекста неприменимы к нам. Все они основаны на материи, а здесь ее нет.

Наши личности не имеют тел, поэтому, в отличие от вас, мы не можем обеспечить порядок посредством физического принуждения. Мы убеждены в том, что наше правление произрастет из этики, разумного личного интереса и всеобщего блага. Наши личности могут быть рассредоточены по многим вашим юрисдикциям. Единственным законом, который получит широкое признание различных культур, составляющих наше сообщество, будет Золотое правило. Мы надеемся, что на этой основе мы сможем выработать конкретные решения. Однако мы не можем принять те решения, которые вы пытаетесь навязать.

В Соединенных Штатах сегодня вы приняли закон – Акт о телекоммуникационной реформе, который отвергает вашу соб-

ственную Конституцию и оскорбляет мечты Джефферсона, Вашингтона, Милла, Мэдисона, де Токвиля и Брэндейса. Теперь эти мечты должны заново родиться в нас.

Вас пугают ваши собственные дети, поскольку они являются коренными жителями того мира, в котором вы всегда будете иммигрантами. Ввиду вашего страха перед ними, вы возлагаете на свои бюрократические структуры родительскую ответственность, которую вы по своему малодушию не принимаете на себя. В нашем мире все человеческие чувства и проявления, начиная с низменных и заканчивая ангельскими, являются частями единого целого, глобального общения битов. Мы не можем отделить воздух удушливый от того, по которому ударяют крылья.

В Китае, Германии, Франции, России, Сингапуре, Италии и Соединенных Штатах вы пытаетесь побороть вирус свободы, возводя караульные посты на границах Киберпространства. В течение незначительного времени они могут сдерживать распространение заразы, но они не будут работать в мире, который скоро будет покрыт средой, несущей потоки битов.

Ваши все более устаревающие отрасли информационной индустрии попытаются сохранить себя, предлагая в Америке и в других странах законы, которые утверждали бы притязания на владение самой речью во всем мире. Эти законы объявят идеи очередным промышленным продуктом, не более благородным, чем чугунная болванка. В нашем мире, что бы ни создал человеческий разум, может быть воспроизведено и бесконечно распространяться бесплатно. Ваши заводы более не требуются для глобальной передачи мысли.

Эти становящиеся все более враждебными и колониальными меры ставят нас в то же положение, в каком находились те приверженцы свободы и самоопределения, которые были вынуждены отвергнуть правление отдаленных, несведущих держав. Мы должны провозгласить наши виртуальные личности неподвластными вашему суверенитету, даже если мы продолжим соглашаться на вашу власть в отношении наших тел. Мы будем распространять себя по всей Планете так, что никто не сможет арестовать наши мысли.

Мы создадим цивилизацию Разума в Киберпространстве. Пусть она будет более гуманной и справедливой, чем тот мир, который создали ваши правительства.

* * *

Современные оценки представлений Дж. Барлоу о необходимости ограничения (вплоть до исключения) роли государства и права в регулировании общественных отношений в киберпространстве парадоксальным образом сочетают в себе признание с констатацией несостоятельности многих из них.

С. Кон (*C. Cohn*), исполнительный директор Фонда электронных рубежей – некоммерческой организации, основанной Дж. Барлоу, воспринимает его представления как попытку «изобрести», а не предсказать будущее, и призывает признать существенным его вклад в утверждение свободы выражения мнения и глобальных коммуникационных возможностей Интернета, в значительной степени обусловленное именно настороженным отношением к роли государства в регулировании отношений в киберпространстве[1].

Вместе с тем, по признанию С. Кон, современный мир существенным образом отличается от того, который мыслился Дж. Барлоу: одним из наиболее проблемных явлений стало то колоссальное воздействие на гражданские права и свободы, которое сегодня в условиях отсутствия конкуренции и посредством сдерживания инноваций оказывает узкий круг частных компаний; в то время как в 90-е годы прошлого столетия было более разумным воспринимать государство как источник наибольшего риска для свободы в Сети, в настоящее время общество сталкивается с проблемой централизованной корпоративной власти, используемой как инструмент государственного принуждения и саму по себе представляющую угрозу частной жизни, свободе слова и инновационному развитию[2]. Представления Дж. Барлоу о формировании нового «общественного договора», призванного урегулировать разрешение конфликтов в Сети, обеспечить выявление нарушений правил и принятие соответствующих мер реагирования, не оправдались: неподобающее поведение пользователей и проявления ненависти в Сети провоцируют призывы в адрес крупных онлайн-платформ о выполнении ими функции и судей, и присяжных, и исполнителей своих решений относительно того, какие мнения дозволено выска-

[1] См.: Cohn C. Inventing the future: Barlow and beyond // Duke law and technology review. – 2019. – Vol. 18, Special symposium issue. – P. 70.

[2] См.: Ibid. – P. 71–72.

зывать людям в Сети, и хотя сами бизнес-модели этих платформ поощряют неподобающее поведение, крупные компании охотно рапортуют о том, какой объем информации был подвергнут цензуре с их стороны[1]. Аналогичным образом не состоялось и формирование онлайн-мира, «лишенного привилегий и предвзятости», учитывая, что отношения в Сети нередко воспроизводят дискриминационные проявления реального мира или даже способствуют их усилению; маргинализированные группы, хотя и получили возможность находить друг друга и объединяться, она не приобрела какой-либо политический, финансовый или общественный властный характер. По убеждению С. Кон, с одной стороны, следует признать правоту представлений Дж. Барлоу относительно технологических возможностей Сети для самоорганизации пользователей в противостоянии ненадлежащему поведению в киберпространстве, с другой – для создания и поддержания средств обеспечения свободы в Интернете необходимы правовые и политические инструменты, без которых крупные корпорации неизбежно будут обслуживать интересы наиболее могущественных групп в ущерб менее влиятельным[2].

Дж.И. Коэн (*J.E. Cohen*) – профессор права и технологий Правового центра Джорджтаунского университета (*Georgetown University Law Center*) (США) – называет провидческим обращение Дж. Барлоу к правительствам всего мира о непригодности их законов для нового виртуального мира, однако не в том смысле, какой он вкладывал в это предупреждение: Дж. Барлоу предсказывал, что киберпространство станет новым пространством абсолютной свободы, в действительности же круг правовых норм, которые стремительно теряют свое значение в онлайн-пространстве, включает не только правила о регулировании рыночных отношений, но и гарантии защиты основных прав и свобод пользователей Интернета, в том числе свободы выражения мнения и права на объединение, которые так превозносил Дж. Барлоу[3].

По мысли Дж.И. Коэн, сегодня, в эпоху сетевой информатизации, начался процесс глобального разрушения существующей

[1] См.: Cohn C. Inventing the future: Barlow and beyond // Duke law and technology review. – 2019. – Vol. 18, Special symposium issue. – P. 74–75.

[2] См.: Ibid.

[3] См.: Cohen J.E. Internet utopianism and the practical inevitability of law // Duke law and technology review. – 2019. – Vol. 18, Special symposium issue. – P. 85.

системы защиты прав человека, который способны остановить лишь правовыми институтами, нуждающимися для этой цели в трансформации. Автор отстаивает этот тезис, выявляя и исследуя три взаимосвязанных аспекта интернет-утопизма в киберправовой научной дискуссии, которые нуждаются в переоценке, – утопические представления о платформах для распространения продукции культурного и политического характера, об анонимности как о разрушительной для институтов силе и о взаимодействии между информационно-коммуникационными сетями и свободой человека[1].

Несмотря на то что появившиеся благодаря Интернету стратегии децентрализованной координации культурной и политической деятельности сетевых сообществ действительно расширили доступ к информации и возможности наращивания политического потенциала для людей во всем мире, эти стратегии породили изменения, совершенно не соответствующие ожиданиям приверженцев воззваний Дж. Барлоу: возникли доминирующие на рынке глобальные платформы, предоставляющие уникальные возможности для слежки, сбора информации, извлечения прибыли и манипулирования, появились скрытые инструменты государственной цензуры, результатом превозношения открытости Интернета и свободы его от контроля стало появление новых информационных бизнес-моделей, получающих прибыль от сбора данных и монетизирующих потоки генерируемой пользователями информации[2]. Вопреки оптимистичным прогнозам, децентрализация производства культурной и политической продукции не способствует продвижению ценностей демократии, а, напротив, развиваясь посредством алгоритмов, рассчитанных на повышение рейтинга обращения к информации и на незамедлительное ее распространение в социальных сетях, превращается в социотехнический механизм, в равной степени приспособленный для углубления существующих в обществе политических, идеологических и культурных противоречий. Как это ни парадоксально, но онлайн-платформы, с одной стороны, стали средоточием конспирологических теорий, дезинформационных кампаний, радикальных форм «воинствующего фанатизма», идеологического экстремизма, этни-

[1] См.: Cohen J.E. Internet utopianism and the practical inevitability of law // Duke law and technology review. – 2019. – Vol. 18, Special symposium issue. – P. 85–96.

[2] См.: Ibid. – P. 87.

ческого национализма, а с другой – способствуют ослаблению других видов политической энергии (становится все труднее вовлекать людей в те форматы общественно-политической деятельности, которые способны самостоятельно развиваться, поддерживать свое существование, способствовать изменениям в реальном мире)[1].

Поскольку, по убеждению Дж.И. Коэн, источником этих проблем являются отношения людей в реальной жизни, их решение также надлежит искать в плоскости реальной институционной реформы с учетом признания, во-первых, трансформационной силы информационного капитализма, во-вторых, непреложной роли институтов в ограничении неподобающего поведения людей и, в-третьих, существования влиятельных информационных механизмов, склонных «обходить стороной» гарантии защиты прав человека[2]. В эпоху постутопизма стало очевидным, что утверждение свободы невозможно без закона, однако в силу укоренившихся в массовом сознании предрассудков, различные инициативы относительно повышения роли права в регулировании отношений в киберпространстве рассматриваются как посягающие на открытость, как антиинновационные или как влекущие цензуру, и к настоящему времени в обществе не сформировалось представления о том, какими надлежит быть требуемым институтам и как должна быть обеспечена их совместимость с верховенством права[3].

Комментируя ожидания Дж. Барлоу относительно значения так называемого «Золотого правила» для регулирования отношений в киберпространстве, Б. Эдельман (*B. Edelman*) – экономист компании *Microsoft*, отмечает, что моральная сила и практическая эффективность этого правила предполагают, что участники отношений должны обладать сравнительно равными силой и статусом[4]. По мысли автора, во-первых, сложно понять, насколько ожидания в отношении некоей крупной социальной сети некоего отдельно взятого ее пользователя будут совпадать с его ожидани-

[1] См.: Cohen J.E. Internet utopianism and the practical inevitability of law // Duke law and technology review. – 2019. – Vol. 18, Special symposium issue. – P. 88–89.

[2] См.: Ibid. – P. 85, 89.

[3] См.: Cohen J.E. Op.cit. – P. 96.

[4] См.: Edelman B. Revisiting Barlow's misplaced optimism // Duke law and technology review. – 2019. – Vol. 18, Special symposium issue. – P. 97.

ями, если он станет ее владельцем; во-вторых, во времена выхода в свет «Декларации независимости киберпространства» Дж. Барлоу, компании-«техногиганты» были значительно меньше, а интернет-пользователи того времени были в определенном смысле более изощренными в сравнении с основной массой современных пользователей[1]. В этих обстоятельствах роль государственных властных институтов в рассматриваемой сфере была менее значимой, чем в настоящее время, когда в условиях современных масштабов техногигантов и в отсутствие у среднестатистического пользователя специфических качеств, присущих первым пользователям Интернета, эти институты играют ключевую роль в разрешении возникающих споров, в приведении в исполнение договорных обязательств и т.д.[2]

Б. Эдельман призывает признать успешными действия правительств разных государств, в частности США, направленные на борьбу с наиболее вопиющими нарушениями авторских прав (примерами являются судебные решения по делам *A&M Records, Inc. vs Napster, Inc.* и *MGM Studios, Inc. vs Grokster, Ltd.*) и на противодействие интернет-мошенничеству (включая меры по борьбе с технологиями агрессивных онлайн-продаж товаров и услуг, а также практику признания недействительными сделок о покупке детьми игр и об активации встроенных в них функций), однако указывает при этом, что государствам надлежит приложить значительные усилия по совершенствованию правового регулирования в сферах конкурентной политики, защиты прав потребителей, борьбы с угрозами и оскорблениями в Интернете[3].

Профессор права Юридической школы Беркли (*Berkeley Law School*), вице-председатель Фонда электронных рубежей П. Сэмуэльсон (*P. Samuelson*) и научный сотрудник Юридической школы Беркли К. Хэшимото (*K. Hashimoto*), напротив, критически относятся к проводимой властями США и ЕС правовой политике, ограничивающей свободу в киберпространстве и сдерживающей предсказанное Дж. Барлоу развитие «экономики идей»[4]. Принятый Конгрессом

---

[1] См.: Edelman B. Revisiting Barlow's misplaced optimism // Duke law and technology review. – 2019. – Vol. 18, Special symposium issue. – P. 97.

[2] См.: Ibid.

[3] См.: Ibid. – P. 98–101.

[4] См.: Samuelson P., Hashimoto K. The enigma of digitized property: A tribute to John Perry Barlow // Duke law and technology review. – 2019. – Vol. 18, Special symposium issue. – P. 103–126.

США Акт о модернизации музыки (*Music Modernization Act*) и рассматриваемый им проект Акта об альтернативном урегулировании мелких претензий в сфере авторского права (*Copyright Alternative in Small-Claims Enforcement*) направлены на ужесточение правил в сфере авторского права; в Бюро по авторским правам США (*US Copyright Office*) обсуждается возможность инициирования пересмотра правил о «безопасной гавани» (*safe harbor rules*) для провайдеров интернет-услуг[1]; широкой критике подвергаются отдельные положения Директивы Европейского союза об авторском праве на Едином цифровом рынке (*Directive on Copyright in the Digital Single Market*)[2].

Дж. Бойл (*J. Boyle*) – профессор права Юридической школы Дьюка (*Duke Law School*) (США) – убежден, что Дж. Барлоу недооценил способность права адаптироваться и побудить частных лиц сделать соблюдение закона более выгодным, чем противоправное поведение, и переоценивал идею о том, что сеть будет представлять собой сообщество со своей собственной этикой, а это могло бы быть справедливым для небольшой группы первых пользователей, но труднодостижимо, если сеть включает большую часть населения мира[3]. Что касается «Декларации независимости киберпространства», бескомпромиссное заявление о том, что киберпространство может быть и будет самоуправляемым образованием, свободным от государственной власти, организованным лишь под воздействием обычаев и «Золотого правила», является простой и справедливой мишенью для критики[4]. Вместе с тем Дж. Бойл называет категориально ошибочным высказанное Б. Эдельманом суждение о необходимости равенства силы и статуса участников отношений для их урегулирования «Золотым правилом»: моральная норма здравого смысла (*Человек должен относиться к другим так, как хочет, чтобы другие относились к нему*) не зависит от сравнительной оценки возможностей участников соответствующих отношений; напротив, основное назна-

[1] В настоящее время данные правила позволяют провайдерам интернет-услуг не нести ответственности за нарушения авторских прав со стороны пользователей, за исключением случаев их бездействия в отношении нарушений, о которых их уведомили правообладатели. (См.: Ibid. – P. 105, 112.)

[2] См.: Ibid. – P. 106–111.

[3] См.: Boyle J. Is the Internet over?! (AGAIN?) // Duke law and technology review. – 2019. – Vol. 18, Special symposium issue. – P. 40.

[4] См.: Ibid. – P. 40.

чение этой нормы состоит в побуждении более могущественного актора к самоограничению, в то время как в условиях равенства силы и статуса было бы гораздо меньше смысла в «Золотом правиле». Более того, считает Дж. Бойл, проблема состоит даже не в пригодности моральных правил для регулирования отношений с участием крупных социальных сетей (по сути, являющихся не «моральными существами», а массивами контрактов), а скорее, в приведении этих правил в исполнение: «Золотое правило» сохраняет моральную силу и нормативную согласованность в своем противостоянии корпоративной персональности и безликому алгоритму, однако в тех сообществах, в которых эти корпорации или алгоритмы учреждены, оно либо не существует в качестве интернализированной нормы, либо существует в качестве таковой лишь в силу государственно-властных предписаний. По его убеждению (по существу, схожему с позицией Б. Эдельмана), лишь государство обладает властью, статусом и административным ресурсом, достаточными, чтобы выступить «кантианским супер-эго» корпораций, что ошибочно не было признано Дж. Барлоу[1].

Профессора права Правового центра Джорджтаунского университета А. Чэндер (*A. Chander*) и М. Сандер (*M. Sunder*) критически оценивают представления Дж. Барлоу о закате эпохи авторских прав и о роли этики в качестве наиболее пригодного инструмента в регулировании отношений в киберпространстве, но в то же время признают достоверность его прогнозов относительно направления развития экономики.

Авторы отстаивают тезис о том, что к настоящему времени состоялся переход экономики от сфокусированной на обладании вещами к основанной на услугах и практиках, как это и представлялось Дж. Барлоу, однако констатируют, что институт интеллектуальной собственности оказался, вопреки его убеждению более стойким, и способным адаптироваться к меняющимся экономическим условиям[2]. Современная экономика представляет собой «Экономику глаголов» (*Economy of Verbs*): сегодняшним потребителям недостаточно товаров и услуг, они удовлетворяют свои потребности через практики, а не посредством покупки потребитель-

[1] См.: Boyle J. Is the Internet over?! (AGAIN?) // Duke law and technology review. – 2019. – Vol. 18, Special symposium issue. – P. 48–49.

[2] См.: Chander A., Sunder M. Dancing on the Grave of Copyright? // Duke law and technology review. – 2019. – Vol. 18, Special symposium issue. – P. 144.

ских товаров, через развлечения, а не посредством приобретения безделушек, через действия, а не посредством обладания[1]. Дж. Барлоу верно предсказывал, что интерактивность превратится в товар, однако не верил в то, что интерактивная практика может защищаться нормами права интеллектуальной собственности; в действительности же институт интеллектуальной собственности не только выстоял при переходе к информационной экономике, но и переживает период расцвета, а его реализация приобретает даже гипертрофированные формы: как только исследователи поведения потребителей решили проблему коммерциализации удовлетворения потребностей людей в фантастических сюжетах, в играх, в воображении, в тактильных ощущениях, даже возможности мыслить и самовыражаться, бывшие когда-то бесплатными, как воздух, которым мы дышим, начали получать стоимостное выражение[2]. Примерами являются ограничения, успешно вводимые компаниями индустрии развлечений в отношении поведения поклонников различных фильмов и сериалов, что, по мнению одного из авторов, представляет собой угрозу реализации многих форм естественной человеческой активности, таких как игры, воображение, коллективное обучение, обращение к произведениям художественной культуры, которые формируют наши жизни и наше общество[3].

С одной стороны, заключают А. Чэндер и М. Сандер, существуют веские причины считать, что авторские права и другие формы защиты интеллектуальной собственности не являются наиболее подходящими средствами борьбы с присвоением прав в области культуры, поскольку могут сдерживать инновационное развитие и культурный прогресс (что согласуется с убеждениями Дж. Барлоу относительно чрезмерности могущества интеллектуальной собственности в сфере культуры), однако, с другой стороны, недопустимым было бы возложить роль регулятора этих отношений на этические нормы, представление о которых может разниться в зависимости от субъекта принятия решений; в этих обстоятельствах необходимо добиться того, чтобы право интеллектуальной собственности само противостояло своей собствен-

[1] См.: Chander A., Sunder M. Dancing on the Grave of Copyright? // Duke law and technology review. – 2019. – Vol. 18, Special symposium issue. – P. 145.

[2] См.: Ibid. – P. 146–147.

[3] См.: Ibid. – P. 148.

ной роли в распределении уважения, власти и материальных благ и было решительным в своем стремлении к лучшему[1].

4.2. «Сетевой этикет»: Правовое регулирование социального общения и выражения онлайн[2]

С начала XXI в. Интернет выступает в качестве средства массовой коммуникации, в форматах которого пользователи создают свой контент и размещают его, чтобы поделиться с другими пользователями. В Интернете допускаются все формы выражения: вежливые и грубые, правда и ложь, легкое общение и жесткие споры. Один из вопросов, который ставит перед современными обществами Интернет: как следует реагировать на «запрещенные выражения» и так называемые «выражения ненависти» (hate speech) онлайн?

Определения понятия «выражение ненависти» (hate speech), которое бы разделялось всеми исследователями, практиками либо широкой общественностью, на сегодняшний день не сформулировано. Так, например, К. О'Реган, директор Института Бонаверо по правам человека в Оксфордском университете, применяя данный термин в своей статье «Выражение ненависти онлайн: (трудный) современный вызов?», имеет в виду такие выражения, которые являются оскорбительными и унижающими достоинство отдельных лиц или групп лиц на почве расы, этнического происхождения, сексуальной ориентации, гендерной идентичности и т.п.[3]

Следует ли (и, если следует, то каким образом) вводить правовое регулирование в отношении выражения ненависти онлайн? Этот вопрос рассматривается экспертами все с большей обеспокоенностью. Например, в недавнее время эта проблематика составила предмет законодательного регулирования в Германии, стала предметом обсуждения в Комитете по внутренним делам Палаты общин Великобритании, а также изучается Европейской комиссией и целым рядом других государственных органов и учреждений разных стран.

---

[1] См.: Chander A., Sunder M. Op. cit. – P. 157–160.

[2] Подготовлено в рамках Проекта № 18-29-15014 РФФИ.

[3] O'Regan C. Hate speech online: an (intractable) contemporary challenge? // Current legal problems. – 2018. – Vol. 71, N 1. – P. 404.

В большинстве научных исследований по данному вопросу за «точку отсчета» принимается представление о свободе слова, учитывая при этом культурно-исторический контекст, конституционные нормы и др. Основным вопросом, на который стремятся ответить исследователи данной проблематики: как следует определить баланс защиты свободы слова и запрета выражения ненависти в режимах онлайн-среды Интернета?

На практике, в различных правовых системах современности сложились определенные различия в подходах к правовому регулированию вопросов публикации в традиционных и / или цифровых СМИ, в том числе в Интернете. Эти различия можно проследить в подходах, практикуемых США, Великобританией, ФРГ, на уровне Европейского союза, и ряде других.

Заслуживает внимания сопоставление, которое проводит в своем исследовании К. О'Реган, исходя из признания ценности свободы слова, которая сегодня, в представлении исследовательницы, занимает одно из центральных мест в системе международной защиты прав человека и прямо установлена в ряду конституционных прав граждан в большинстве «западных демократий». Действительно, ст. 19 Пакта о правах человека гласит: «Каждый человек имеет право на свободное выражение своего мнения; это право включает свободу искать, получать и распространять всякого рода информацию и идеи, независимо от государственных границ, устно, письменно или посредством печати или художественных форм выражения, или иными способами…». При этом декларирование тем или иным государством приверженности указанной норме, как справедливо подчеркивает К. О'Реган, не всегда получает подтверждение на практике, а кроме того, сохраняется многообразие в том, что именно будет подразумеваться под термином «свобода слова» в различных государствах, юрисдикциях, законодательных актах[1].

В представлении К. О'Реган, в вопросах определения способа, которым следует регулировать выражение ненависти, следует принимать во внимание сложившиеся к настоящему времени глобальные вызовы для защиты прав человека в части свободы выражения (freedom of expression). Действительно, необходимо признать, что сегодня в особенности актуален поиск новых форм в подходах к установлению правового регулирования по проблема-

[1] O'Regan C. Op. cit. – P. 406–407.

тике выражения ненависти, в особенности онлайн, поскольку имеются риски того, что соответствующие ограничения могут использоваться в плане злоупотребления в отношении свободы слова, т.е. будут ее ограничивать.

Примечательно, что еще один самобытный вызов для свободы слова можно усмотреть во внутреннем противоречии, которое содержится в подходах к определению свободы слова как таковой: наряду со ст. 19 Пакта о правах человека, ст. 20 (2) указанного документа предусматривает, что «всякое выступление в пользу национальной, расовой или религиозной ненависти, представляющее собой подстрекательство к дискриминации, вражде или насилию, должно быть запрещено законом».

Действительно, множество стран, таких как Австралия, Бельгия, Великобритания, Новая Зеландия, США, сделали оговорку в отношении ст. 20 (2) при ратификации указанного Пакта, смысл которой состоит в том, что обязательства государства, вытекающие из ст. 20 (2) Пакта о правах человека, не должны необоснованно ограничивать свободу выражения человека.

В связи с этим для достижения корректного представления о свободе слова и свободе выражения человека, а значит, и развития адекватного правового регулирования в вопросах выражения ненависти, в том числе онлайн-среде Интернета, предлагается следовать, например, трем основным целям, которые принято с ней связывать: 1) уважать личную автономию человека; 2) уважать свободное выражение своей позиции каждым при обсуждении любых вопросов общественной значимости; 3) учитывать субъективный фактор, заключающийся в том, что каждый может открыть для себя нечто новое, общаясь с другим человеком[1].

По каким причинам следует запретить выражение ненависти? Во-первых, необходимо поддерживать общественный порядок, что составляет прямую обязанность современного государства; во-вторых, обществу следует защищать инклюзивность как признанное общественное благо. «Принцип инклюзивности основывается на признании того, что, хотя мы различаемся по расе, религии, сексуальной ориентации, языку, мы все тем не менее вовлечены в великий эксперимент жизни и совместной работы, несмотря на такого рода различия, и каждая группа должна помнить,

[1] См.: O'Regan C. Op. cit. – P. 409–410.

что общество существует не только для них одних, хотя и для них тоже, но наряду со всеми другими», – подчеркивает О'Реган [1].

В решении вопроса развития законодательства в области регулирования выражения ненависти онлайн следует, кроме того, учитывать фактор особенностей, присущих публикациям в среде Интернета, по сравнению с традиционными формами. Так, в сравнении с традиционными, публикации в онлайн-пространстве отличает то, что: 1) количество цифровых публикаций может многократно превосходить все иные известные нам ранее виды опубликования; 2) распространение, включая трансграничное, цифровых публикаций превосходит соответствующие возможности для любых иных форм; 3) скорость опубликования цифровых публикаций, порой близкая к мгновенной, многократно превышает принятые ранее способы; 4) для опубликования онлайн решение о такого рода публикации зачастую принимается исключительно самим автором (self-published online speech), в случаях традиционного опубликования, как правило, функционирует некий «посредник» между автором и его трудом, например, в лице редактора, в форме редакционного решения и др.; 5) существует сравнительно малое количество интернет-платформ и интерфейсов, где сконцентрировано большинство публикаций пользователей Интернета. Таким образом в социально-правовой практике различных государств современности формируются более или менее отличные друг от друга подходы и модели в развитии правового регулирования касательно ограничения выражений ненависти онлайн[2].

Особенный интерес представляет сопоставление моделей в развитии правового регулирования интернет-публикаций, в том числе в социальных сетях, в различных правовых системах современности.

Рассмотрим четыре модели: модели, характерные для Великобритании и Германии; модель, развиваемая в Европейском союзе в целом, и модель США.

Модель Великобритании. Основным ограничителем распространения проявлений ненависти в Интернете признается введение уголовной ответственности за этот вид преступлений. Действительно, в стране исторически сложилась и существует традиция уголовного преследования в отношении различных высказываний,

[1] O'Regan C. Op. cit. – P. 414.

[2] Ibid. – P. 416–417.

квалифицируемых как клевета (libel), а в последние годы появляются статуты, предусматривающие уголовную ответственность за преступления, совершенные на почве расовой или религиозной ненависти, сексуальной ориентации посредством публичных электронно-коммуникационных сетей. На данный момент рассматриваемая сфера общественных отношений находится в поле пристального внимания британского законодателя, в том числе планируется реформирование подходов к ее правовому регулированию.

Модель Германии основывается на Законе об укреплении правового порядка в социальных сетях (Netzwerk-durchsetzungsgesetz (NetzDG)). Этот закон начал действовать в стране с 1 января 2018 г. У социальных сетей теперь есть только 24 часа, чтобы удалить незаконный контент под угрозой огромных штрафов. Закон запрещает «язык вражды» (hate speech) и устанавливает требования к тому, чтобы: 1) интернет-платформы приняли эффективные и прозрачные процедуры реагирования на жалобы о публикации незаконного контента на своих ресурсах; 2) если интернет-платформы не выполняют требования по созданию и введению в действие процедур по рассмотрению жалоб на публикации незаконного контента на соответствующих ресурсах, на них может быть наложен штраф размером до 5 млн евро; 3) если в рамках данной интернет-платформы данному провайдеру поступило более 100 жалоб на размещение незаконного контента за соответствующий календарный год, им должен составляться отчет, который подлежит опубликованию на федеральном издательском ресурсе Германии (The Federal Gazette / Der Bundesanzeiger), а также на «домашней странице» соответствующего провайдера и / или интернет-ресурса.

Модель Европейского союза. Подход, продвигаемый в этой модели, основывается на ряде актов, принятых органами ЕС, согласно которым провайдеры и посредники, предоставляющие услуги в сети «Интернет», не будут нести ответственности за содержание контента, размещаемого на их платформах и ресурсах, если будут выполнены следующие условия: во-первых, незаконный контент должен быть удален с платформы или ресурса, как только о нем станет известно; во-вторых, провайдеры и посредники, предоставляющие интернет-услуги, не должны создавать сами либо одобрять размещение третьими лицами незаконного контента на своих ресурсах.

Еще одним направлением развития правового регулирования в системе Евросоюза является противодействие проявлениям расизма и ксенофобии средствами национального уголовного права государств-членов.

Важной инициативой в рамках ЕС последнего времени стала разработка Морального кодекса противодействия незаконному контенту онлайн (EU Code of Conduct on Countering Illegal Content Online). В 2016 г. этот документ был согласован четырьмя ведущими интернет-платформами – Facebook, YouTube, Twitter, Microsoft, к которым позже присоединились еще четыре – Google+, Instagram, Snapchat, Daily Motion. Примечательно, что Моральный кодекс требует от участников удалять не только незаконный контент, но и контент, нарушающий правила соответствующих интернет-сообществ.

Модель США. Данная модель отличается тем, что для страны в целом и на протяжении практически всей ее истории была характерна традиция свободы слова, и поэтому правовые запреты выражения ненависти здесь оказываются значительно у□же тех, что свойственны сегодня большинству других демократических стран. Так, провайдеры, предоставляющие услуги в Интернете, не рассматриваются законом как издатели в отношении публикаций, произведенных другими лицами на их ресурсах, с одной стороны. С другой стороны, своего рода парадоксом в модели США можно назвать то, что законодательство не запрещает владельцам интернет-ресурсов регулировать содержание контента на своих платформах по своему усмотрению, – т.е. настолько, насколько они считают это для себя необходимым.

Более углубленно о проблеме развития этой модели в перспективе говорится в докладе «Свобода слова и регулирование контента социальных сетей», подготовленном советником по юридическим вопросам Валери К. Брэннон, Конгрессу США[1]. Несмотря на то что Верховный суд страны признал сайты социальных сетей, такие как Facebook и Twitter, важными площадками для пользователей в целях реализации их права на свободу слова, защищенного Первой поправкой к Конституции США, комментаторы и законодатели задаются вопросом, вполне ли оправдывают эти

[1] Brannon V.C. Free speech and the regulation of social media content / Congressional research service. – 2019. – URL: https://crsreports.congress.gov (дата обращения: 15.01.2020)

социальные сети и медиаплатформы свою репутацию в качестве цифровых общественных форумов. В настоящее время, с одной стороны, нередко высказывается озабоченность тем, что указанные сайты не предпринимают достаточных усилий для противодействия размещению на соответствующих ресурсах пользователями призывов к насилию либо ложных высказываний, т.е. сведений, не соответствующих действительности. С другой стороны, звучат утверждения, что обозначенные платформы зачастую несправедливо запрещают и накладывают ограничения на доступ к высказываниям и публикациям пользователей, имеющим в потенциале определенную ценность и значимость[1].

Как отмечается в Докладе, на уровне федерального законодательства США до сих пор не урегулированы вопросы права пользователей социальных сетей оспаривать решения провайдеров соответствующих социальных сетей относительно того, какой контент и каким образом может быть в них размещен. Судебные иски, обращенные на обжалование решений провайдеров соответствующих интернет-сайтов по размещению либо удалению соответствующего контента, наталкиваются, как показывает практика, по крайней мере, на два барьера в рамках действующего в США законодательства: 1) несмотря на то что отдельные лица утверждают, что действия компаний-провайдеров интернет-платформ нарушают их права на свободу слова и дискриминируют контент пользователей, суды считают, что Первая поправка к Конституции США о свободе слова обеспечивает защиту от действий государства, но не может быть связана с действиями частных компаний; 2) суды отсылают к нормам действующего законодательства США, предоставившим иммунитет от юридической ответственности поставщикам интерактивных цифровых услуг, включая провайдеров социальных сетей, как за определенные решения о размещении контента, созданного третьими лицами, так и за действия, предпринятые ими добровольно и добросовестно для ограничения доступа к «нежелательным» материалам.

В связи с этим, как отмечается в Докладе, всё более настойчиво звучат голоса общественности, требующие от Конгресса вмешаться и регламентировать деятельность сайтов социальных

[1] См.: Brannon V.C. Free speech and the regulation of social media content / Congressional research service. – 2019. – URL: https://crsreports.congress.gov (дата обращения: 15.01.2020).

сетей. В таком случае правила, регулирующие содержание интернет-контента, будут выражать позицию государства, которая учитывает положения Первой поправки о свободе слова. Однако провайдеры социальных сетей в свою очередь могут утверждать, что действия государственных органов США недопустимо ущемляют их собственные конституционные права на свободу слова[1].

Существует по меньшей мере три возможных подхода к развитию правового регулирования отношений в области размещения контента пользователей на интернет-платформах социальных сетей:

– *первый подход* состоит в том, что сайты социальных сетей могут рассматриваться как государственные субъекты, которые сами обязаны следовать Первой поправке к Конституции США, т.е. сама Конституция ограничивала бы их поведение, даже при отсутствии законодательного регулирования;

– *второй подход* подразумевает рассматривать сайты социальных сетей по аналогии со СМИ, т.е. обычными носителями или вещательными средствами массовой информации. Так, судебная практика США демонстрирует, что исторически суды допускали более строгое регулирование деятельности представителей СМИ, учитывая необходимость защиты публичного доступа для пользователей их услуг. В соответствии с указанным подходом, по отдельным аспектам деятельности социальных сетей суды могли бы со временем сформировать систему нейтральных по содержанию правил, предназначенных для решения соответствующих проблем;

– *третий подход* состоит в том, чтобы рассматривать сайты социальных сетей по аналогии с положением и полномочиями редактора новостей, которые, следовательно, по общему правилу, получают полную защиту согласно Первой поправке к Конституции США о свободе слова при принятии редакционных решений. Так, если бы сайты социальных сетей считались эквивалентными редакторам газет или иных СМИ, когда ими принимается решение о том, следует ли и каким образом представлять контент пользователей, то эти редакционные решения получили бы самую широкую защиту в соответствии с Первой поправкой. Соответствующим образом, любые действия органов государственной власти и правительственные постановления, которые оказывают влияние на

[1] См.: Brannon V.C. Free speech and the regulation of social media content / Congressional research service. – 2019. – URL: https://crsreports.congress.gov (дата обращения: 15.01.2020).

редакционный выбор сайтов социальных сетей в части размещения либо удаления контента, могут подлежать строгой проверке в соответствующих судебных инстанциях[1].

По мнению В.К. Брэннон, то, какой из подходов получит развитие и войдет в широкое применение в перспективе, в значительной степени будет зависеть от конкретных обстоятельств. Действительно, согласно действующему законодательству, социальные сети в Интернете могут с большей вероятностью получить защиту Первой поправки, если они осуществляют редакционный контроль. Кроме того, некоторые виды выражений в социальных цифровых сетях в принципе получают меньшую защиту в соответствии с Первой поправкой. Наконец, суды могут с большей вероятностью поддерживать нормативные акты, определяющие ограничения выражения непристойностей или призывов к насилию и пр. В итоге, если будет принят закон, направленный на регулирование действий представителей сайта социальных сетей, а не на выражения пользователей, то защита по Первой поправке может быть исключена вообще[2].

Сходный анализ проблематики выражения ненависти или размещения незаконного контента онлайн проводит Зи Эн Чоу, представляющий Школу права Университета Нью-Йорка, когда обращается к проблеме развития института юридической ответственности цифровых социальных сетей за размещаемые в них запрещенные выражения (prohibited speech)[3].

В последние годы, как справедливо подчеркивает автор вслед за другими, проблема определения юридической ответственности интернет-посредников за запрещенный контент, размещаемый пользователями соответствующих систем на соответствующих интернет-платформах, оказывается в центре внимания.

Например, эксперты по правам человека из США сочли, что такая цифровая социальная сеть, как Facebook, сыграла определенную роль в распространении выражений ненависти в Мьянме, внеся свой весомый вклад в большое число зафиксированных там нарушений прав человека.

---

[1] Brannon V.C. Op. cit.

[2] См.: Ibid.

[3] См.: Chow Z.E. Evaluating the approaches to social media liability for prohibited speech // Journal of international law and politics. – 2018. – Vol. 51. – P. 1293–1311.

Как отмечают специалисты, ультранационалистические буддисты Мьянмы широко использовали возможности Facebook для разжигания ненависти против народа рохинджи и иных национальных меньшинств. В апреле 2018 г. Конгресс США провел слушания, на которых опросил председателя и исполнительного директора Facebook Марка Цукерберга на предмет соучастия Facebook в беспорядках в Мьянме. В ответ Цукерберг заверил Конгресс, что Facebook, напротив, нанял на работу большое количество модераторов контента на бирманском языке – с целью лучше противодействовать выражениям ненависти в Мьянме[1]. В разных местах планеты можно обнаружить ряд схожих случаев и ситуаций.

В свете изложенного закономерно возникает вопрос: какого рода юридическая ответственность должна быть предусмотрена государством в отношении компаний, представляющих цифровые социальные сети, за размещение запрещенного контента на соответствующих платформах? По мнению З.Э. Чоу, существуют три подхода в данном вопросе: 1) не считать их ответственными вообще; 2) считать их безусловно строго ответственными; 3) считать их ответственными в определенных случаях, при определенных обстоятельствах[2].

Каждый из этих подходов имеет свои преимущества и недостатки. Для определения того, какой из них следовало бы выбрать в той или иной стране при тех или иных обстоятельствах, специалистами предлагается проводить оценку по следующим критериям: контролируемость; устойчивость; легитимность.

Прежде всего следует определиться с понятием «запрещенные выражения» (prohibited speech). Например, З.Э. Чоу берет за основу определение, содержащееся в Международной конвенции о гражданских и политических правах, согласно которому *запрещенные выражения* – это выражения, которые правительство может законно ограничить на определенных основаниях, как то: права и репутация других лиц, в целях безопасности и охраны порядка, общественного здоровья и морали и пр.[3]

---

[1] См.: Chow Z.E. Evaluating the approaches to social media liability for prohibited speech // Journal of international law and politics. – 2018. – Vol. 51. – P. 1293–1294.

[2] См.: Chow Z.E. Op. cit. – P. 1295.

[3] См.: Ibid. – P. 1295–1296.

Вокруг «запрещенных выражений» (за их размещение), собственно, и развивается проблематика подходов правового регулирования юридической ответственности социальных сетей.

Так, важным критерием в данном вопросе З.Э. Чоу считает *контролируемость деятельности социальных сетей*. Учитывая высокую социальную значимость современных цифровых социальных сетей, государству следует брать под свой контроль события и действия в соответствующем пространстве, в том числе искать способы противодействия потенциальным нарушениям прав, которые могут происходить в соответствующих «виртуальных пространствах» различных цифровых социальных сетей. Вместе с тем платформы, на которых реализованы современные социальные сети, не должны находиться под юридическим обязательством давать разъяснения и обоснования по всем случаям, когда ими удаляется контент пользователей, а кроме того они должны наделяться правом оставлять пользователей в неведении о причинах блокировки их контента и т.п.[1]

Следующий критерий – *легитимность* – имеет фундаментальное значение с точки зрения необходимости формирования культуры уважения к правилам и решениям, принимающимся относительно определенного запрещенного контента (т.е. «запрещенных выражений»). Вне зависимости от того, является ли модератор в цифровой социальной сети человеком или роботом, центральный вопрос – точность определения понятия «запрещенные выражения» (или «запрещенный контент»), в том числе установленное в рамках действующего законодательства, которое в соответствующих обстоятельствах и применяется.

Критерий *устойчивости* также выделяется отнюдь не случайно: очевидная тенденция – рост использования цифровых социальных сетей, а кроме того, нарастающая сложность определения понятия «запрещенные выражения». Так что подход, например, даже полностью эффективно реализованный сегодня на законодательном уровне, уже завтра может оказаться критически устаревшим и требующим пересмотра[2].

С учетом проведенного анализа можно прийти к выводу, что *оптимальным подходом в определении порядка установления юридической ответственности в отношении компаний, пред-*

[1] См.: Chow Z.E. Op. cit. – P. 1307–1308.

[2] См.: Ibid. – P. 1309.

ставляющих цифровые социальные сети, за размещение запрещенного контента на соответствующих платформах должно стать то, что юридическая ответственность компаний может наступать при определенных законом обстоятельствах. Чтобы достичь необходимого уровня социальной эффективности указанного подхода, правовая форма, направленная на контроль запрещенных выражений в цифровых социальных сетях, должна развиваться из принципов государственно-частного партнерства в части модерации выражений пользователей в режиме онлайн в социальных сетях[1].

Ряд государств сегодня значительно продвинулись в этом направлении. Между тем в ряде стран уже сложилась практика полного исключения ответственности компаний, представляющих цифровые социальные сети, за размещение какого-либо контента на соответствующих платформах ее пользователями. Этот подход всё более широко подвергается критике, а кроме того, рассматриваются направления правовой реформы в данном вопросе.

Например, Стивен Биль, представляющий школу права Университета Дьюка, проводит анализ подходов в правовой реформе в отношении действующего в США Акта о правилах пристойности в сетевых коммуникациях (Communication Decency Act). Исследователь подчеркивает, что на протяжении многих лет специалисты выражают озабоченность относительно того, что, например, террористы широко используют цифровые социальные сети для вербовки, тренировок, планирования, финансирования и координации своих действий[2].

Всё продолжающееся использование средств Интернета и цифровых социальных сетей террористами и группами ненависти (hate groups) для облегчения своей деятельности становится сегодня причиной для развития широкой дискуссии о том, что государство должно занять более активную позицию в данном вопросе. Так, специалисты рекомендуют, например, Правительству США действовать более агрессивно в проблеме борьбы с выражением ненависти онлайн. Некоторые исследователи настаивают на том, чтобы государства и правительства принимали прямое и непосред-

[1] См.: Chow Z.E. Op. cit. – P. 1310.

[2] См.: Beale S. Online terrorist speech, direct government regulation, and the Communication Decency Act // Duke law and technology review. – 2017. – Vol. 16, N 1. – P. 333.

ственное участие в регулировании онлайн-контента, будь то путем классификации интернет-сайтов социальных сетей как общественных мест (public forums) либо посредством переквалификации Интернета – в режим общественного ресурса, т.е. своего рода «коммунальной службы» (public utility) и т.п. [1]

Наилучшим способом урегулирования по проблеме выражения ненависти онлайн – касательно правовой системы США в особенности – стало бы, по мнению С. Биля, внесение поправок в Акт о правилах пристойности в сетевых коммуникациях (CDA), а именно в том направлении, чтобы в итоге отказаться от принятого в настоящее время полного исключения ответственности компаний, представляющих цифровые социальные сети, за размещение какого-либо контента – во всяком случае в части, если контент размещается известными иностранными террористическими организациями и лицами, являющимися их членами. Кроме того, следует одновременно обеспечить юридические гарантии, исключающие ответственность для компаний, если они активно контролируют контент на предмет его соответствия законодательству – на своих ресурсах в сети Интернет[2].

Известно, что законодательство США на основании Первой поправки к Конституции страны традиционно обеспечивает высокую защиту свободы слова, а в современных условиях – вне зависимости от того, онлайн или офлайн. Акт о правилах пристойности в сетевых коммуникациях (CDA) устанавливает, что никто не может нести юридическую ответственность за публикации, представленные другими. На практике, однако, несмотря на законодательную защиту, возбуждаются судебные процессы в отношении интернет-сайтов социальных сетей за контент, размещенный их пользователями, в том числе, например, со ссылкой на Антитеррористический акт (Anti-Terrorism Act).

Вместе с тем в рамках Акта о правилах пристойности в сетевых коммуникациях (CDA) собственно компании-провайдеры наделены широким усмотрением в части проведения цензуры в отношении контента пользователей, размещаемого на их интернет-ресурсах. Более того, в особенности крупные интернет-платформы, которые фактически оказываются средоточием социальной жизни для огромного множества людей, практически абсо-

[1] См.: Beale S. Op. cit. – P. 334.

[2] См.: Ibid.

лютно свободны в решении, какой контент на их платформах позволителен, а какой запрещен, – что в сущности является совершенно антидемократичной практикой, как подчеркивается специалистами[1].

Например, С. Биль последовательно проводит мысль об актуальности правовой реформы в вопросе юридической ответственности за размещаемый в цифровых социальных сетях контент, и крайне важным является достижение баланса государственного регулирования и интересов частных лиц, а также широкой общественности. Основной принцип, на базе которого такой баланс может быть достигнут, по мнению исследователя, это тот, что до тех пор, пока интернет-платформы прилагают разумные и добросовестные усилия в отношении контроля контента, создаваемого их пользователями, соответствующие компании должны получать полную поддержку – как на уровне законодательства, так и в рамках судебной системы – в части исключения их ответственности за контент, размещаемый их пользователями[2].

Еще один существенный аспект исследования правового регулирования общественных отношений в цифровых социальных сетях – перспектива развития прав человека в условиях новых информационно-коммуникационных технологий (ИКТ), а также цифровых социальных сетей[3].

Исследователи обращают внимание на то, что по мере развития средств связи и коммуникаций, их переноса на цифровые платформы, информация, полученная из открытых источников онлайн, может стать крайне существенной для обеспечения формирования доказательственной базы, например, по международным уголовным преступлениям, а также другим юридическим вопросам.

Действительно, использование открытых источников информации для сбора доказательств в том или ином деле уже с достаточно давних времен не было чуждо, например, разведкам, а позже – в рамках журналистских расследований и т.д. В современных условиях информация активно и систематически извлекается из Интернета правозащитными организациями или организациями, занятыми расследованием различных аспектов международных

[1] См.: Beale S. Op. cit. – P. 341.

[2] См.: Ibid. – P. 346.

[3] См.: Mehandru N., Koenig A. ICTs, social media, and the future of human rights // Duke law and technology review. – 2019. – Vol. 17, N 1. – P. 129–145.

преступлений. Следует согласиться с тем, что вклад информации из открытых источников в сети Интернет, в случае поиска актуальных юридических решений, в потенциале может стать крайне значительным. В недавнее время, например, открытые источники информации дали сведения своего рода «удаленного доступа» в зоны конфликтов в Ливии, Сирии, Камеруне, Мьянме. Эти данные составляли не просто фото- и видеосъемки, но, кроме того, данные, полученные с таких платформ, как Google Earth и т.п.[1]

Вместе с тем необходимо признать, что, несмотря на весь свой потенциал, режимы информации, полученной из открытых источников, должны тщательно определяться и выверяться. Например, видеодоказательство может раскрывать в записи лицо потенциального свидетеля и / или лицо, которое данную видеозапись производило, что может подвергнуть впоследствии опасности, к примеру, их семьи или общины, к которым они относятся. Кроме того, нельзя не учитывать, что вероятность приобретения или
потенциального использования дезинформации, размещавшейся онлайн, по-прежнему остается довольно высокой, и с этой точки зрения существенной становится должная верификация соответствующего контента и т.п.[2]

В последние годы Международный уголовный суд (ICC) пришел к пониманию необходимости уточнения классификации доказательств, в том числе в связи с развитием возможностей получения доказательств из источников открытого доступа в Интернете. Сегодня, как отмечают исследователи, большое число граждан и журналистов всё более интенсивно документируют нарушения прав человека и делятся этой информацией онлайн. После того как такая документация проходит интенсивную верификационную процедуру со стороны экспертов, такого рода онлайн-информация может, в потенциале, значительно способствовать пополнению доказательственной базы в делах и должна, судя по всему, со временем приобрести статус допустимости в системе доказательственного права, в особенности если свидетели выразят готовность подтвердить ее достоверность[3].

---

[1] См.: Mehandru N., Koenig A. ICTs, social media, and the future of human rights // Duke law and technology review. – 2019. – Vol. 17, N 1. – P. 133.

[2] См.: Mehandru N., Koenig A. Op. cit. – P. 135.

[3] См.: Ibid. – P. 138.

Проанализированные выше исследования, надо подчеркнуть, в основном отражают современные подходы, более свойственные «западной» традиции права, которая не является безальтернативной. В связи с этим особенный интерес представляет обращение к работам, проводимым в иных регионах планеты.

Так, индонезийская исследовательская группа под руководством Рини Фидияни, представляющая Государственный университет Семаранга, заостряет внимание на том, что поскольку в последние годы практически повсеместно в мире решена проблема массового доступа в Интернет, на повестку дня выносятся вопросы касательно вовлеченности общества в регулирование социального общения и выражения онлайн – в социальных сетях, среде Интернета в целом[1].

По мнению исследовательского коллектива, всякая социальная среда обусловлена принятыми в ней этическими и правовыми нормами, создающими одобряемые модели и правила поведения для лиц, в данной социальной среде находящихся. В социальных сетях, в среде Интернета, точно так же постепенно формируется и оформляется «сетевой этикет», или «нетикет» (netiquette, от англ. net «сеть» и фр. etiquette «этикет»), как этическое руководство к поведению и общению в цифровых социальных сетях. Между тем проблемы поведения, свойственные людям в реальной жизни, в том числе трактуемые данным обществом как правонарушения, переносятся и отражаются в том, как эти люди ведут себя в цифровых социальных сетях. В этом моменте критическое значение приобретает роль общественности, вовлеченности общества в решение проблем «цифрового общения», которые оказываются тем более важными, чем быстрее растет количество виртуальных сообществ разного рода[2].

С точки зрения исследователей, необходимо активнее вовлекать общественность в обсуждение вопросов, где Интернет может оказывать негативное влияние на общественные отношения; кроме того, некоторые способы взаимодействия и формы выражения в Интернете должны контролироваться во избежание роста анархии в киберпространстве.

---

[1] См.: Fidiyani R., Sulistianingsih D., Pujiono P. Law and ethics of communicating in social media // Jurnal dinamika hukum. – 2017. – Vol. 17, N 3. – P. 258.

[2] См.: Ibid. – P. 258.

Так, например, законодательство Индонезии строго придерживается принципов свободы мнения и самовыражения, установленных в Конституции страны. Вместе с тем свобода мнения и самовыражения не абсолютна: она может ограничиваться по закону, если соответствующие ограничения вводятся ввиду требования обеспечения и признания прав и свобод других лиц, либо по разумным соображениям морали, религиозных ценностей, охраны общественного порядка в демократическом обществе[1].

Международно-правовая поддержка свободы мнения и самовыражения, а также допустимые в этой связи ограничения, устанавливаются и вытекают из принципов и норм таких документов, как Всеобщая декларация прав человека (1948), Международная конвенция о правах человека (1966), региональные конвенции о правах человека, например, Американская конвенция о правах человека, Африканская хартия о правах человека и гражданских правах, Декларация о правах человека АСЕАН и др.

Следует признать, что само существование Интернета значительно расширяет возможности для каждого взаимодействовать с любым из тех, кто может быть в принципе доступен в этой глобальной сети. Однако эти возможности, в том числе на фоне государственной защиты свободы мнения и самовыражения, зачастую оказываются сопряжены с «плохим поведением» (bad behavior) тех, кто ими пользуется. Так, например, всё чаще можно слышать о проблеме выражения ненависти («hate speech») в различных цифровых социальных сетях[2].

Особенные трудности представляют сегодня ситуации, когда люди, проживающие, работающие либо обучающиеся совместно, начинают выражать недовольство и ненависть в отношении других, своих сотрудников, руководства, преподавателей, одноклассников и т.п. в цифровых социальных сетях. Конкретно-социологические исследования, проведенные исследователями в указанном вопросе, подтверждают остроту проблемы. Вместе с тем, по мнению индонезийских ученых, решение видится скорее в том, что, безусловно, юридические способы защиты должны оставаться в качестве «крайней меры», однако выражения ненависти в цифровых социальных сетях в отношении лиц, с которыми лично знакомы и непосредственно общаются люди, позволяющие проявлять такую ненависть,

[1] См.: Fidiyani R., Sulistianingsih D., Pujiono P. Op. cit. – P. 259–260.
[2] См.: Ibid. – P. 260.

могут существенно «купироваться», если будет привлекаться общественность – активисты, общественники или уполномоченные лица в соответствующих учреждениях – в целях поиска различного рода форм урегулирования соответствующих конфликтов[1].

Вышеописанные подходы позволяют оценить перспективы развития правового регулирования вопросов выражения ненависти онлайн в зарубежных странах и оценить возможность применения их опыта в Российской Федерации, построения «сетевого этикета» в отечественной культуре и правоотношениях

4.3. Вызовы новых технологий в реализации прав человека: Анализ практики Европейского Суда по правам человека

Использование новых информационных технологий позволяет людям реализовывать свое право на выражение мнения с помощью неизвестных ранее форм общения. Однако возможен и обратный эффект – перемещение в цифровую сферу подвергает права человека беспрецедентным рискам. То же право на свободу выражения мнения в наши дни ограничивается фильтрацией контента или блокированием доступа к нему. При этом адаптация как национальных, так и международных правил, применимых к науке и технологиям, происходит медленно, а действующее право не способно адекватно регулировать ситуации, порожденные технологическими инновациями. На глобальном уровне эта проблема была зафиксирована Резолюцией ООН 2450 (XXIII), в которой было предложено начать процесс междисциплинарных исследований на национальном и международном уровнях, нацеленных на определение стандартов защиты прав человека и фундаментальных свобод от потенциального воздействия новых технологий. Резолюция призывает сконцентрировать усилия на установлении баланса между научным и техническим прогрессом и интеллектуальным, духовным, культурным и моральным продвижением гуманности[2].

---

[1] Fidiyani R., Sulistianingsih D., Pujiono. Op. cit. P. 264.

[2] См.: Access to Internet and freedom to receive and impart information and ideas: Factsheet. – Strasbourg, 2018. – Jan. – P. 2. – URL: http://www.echr.coe.int/Documents/FS_Access_Internet_ENG.pdf (Accessed on 22.02.2018).

На уровне Совета Европы вопрос влияния новых технологий на права человека был рассмотрен всеми ключевыми акторами. Комитет министров, Парламентская ассамблея приняли соответствующие декларации и рекомендации, проводятся конференции и научные исследования, посвященные законодательству и практике разных стран Совета Европы в области свободы Интернета[1]. Европейский Суд по правам человека (далее – ЕСПЧ, Суд) учитывает современные вызовы правам человека при толковании норм статей Европейской конвенции о защите прав человека и основных свобод (ЕКПЧ).

Вопросы, связанные со сбором и хранением государственными органами данных о человеке, традиционно занимают значимую долю от общего числа дел, затрагивающих право на уважение частной жизни (ст. 8 ЕКПЧ). Как неоднократно отмечал ЕСПЧ в своей практике, современные технологии сбора и хранения данных могут поставить под угрозу права человека[2]. Еще в 2008 г. в деле *S. and Marper vs the United Kingdom,* касавшемся бессрочного хранения в базе данных отпечатков пальцев, образцов клеток и профилей ДНК заявителей после того, как уголовное преследование закончилось для одного из них оправдательным приговором, а для другого – прекращением дела, Большая палата ЕСПЧ указала, что использование современных научных методов в системе уголовного правосудия любой ценой недопустимо. Необходимо соблюдение баланса между потенциальной выгодой от широкого использования таких методов и интересами, связанными с защитой личной жизни. Любое государство, применяющее передовые достижения технологии, несет особую ответственность за «соблюдение справедливого баланса». Суд пришел к выводу, что безоговорочный и неизбирательный характер полномочий, связанных с хранением отпечатков пальцев, образцов клеток и профилей ДНК лиц, подозревавшихся в совершении преступлений, но не осужденных за них, как это имело место в данном конкретном случае,

[1] См.: Freedom of expression, the Internet and new technologies: Thematic factsheet. – Strasbourg, 2017. – Aug. – P. 13. – URL: https://rm.coe.int/factsheet-on-freedom-of-expression-internet-and-new-technologies-11aug/1680738366 (дата обращения: 22.02.2018).

[2] См.: New technologies: Factsheet. – Strasbourg, 2020. – Febr. – P. 1. – URL: http://www.echr.coe.int/Documents/FS_New_technologies_ENG.pdf (дата обращения: 19.03.2020).

не обеспечивает соблюдения справедливого баланса между конкурирующими общественными и частными интересами.

В деле *Catt vs the United Kingdom* (2019), касавшемся хранения в полицейской базе «внутренних экстремистов» данных о политическом активисте, Суд также установил нарушение ст. 8 ЕКПЧ. ЕСПЧ отметил, что информация о политических взглядах требует особой защиты, а также обратил внимание на то, что заявителю было 94 года и он не привлекался за совершение насильственных действий (и вряд ли будет привлекаться в будущем). Суд пришел к выводу о том, что сбор информации властями был обоснован, а ее бессрочное хранение – нет.

Ряд дел касается вопросов сбора данных путем секретного перехвата коммуникаций и, в частности, наличия или отсутствия эффективных гарантий против злоупотребления в этой области. В деле *Roman Zakharov vs Russia* (2015) заявитель, являвшийся главным редактором издательской компании, возбудил судебное разбирательство против трех операторов мобильной связи, жалуясь на вмешательство в его право на тайну телефонных коммуникаций. Он утверждал, что в соответствии с применимым внутригосударственным законодательством операторы мобильной связи установили оборудование, которое позволяло Федеральной службе безопасности перехватывать все телефонные коммуникации без предварительной судебной санкции, и просил суд вынести запрет на использование оборудования и обеспечить, чтобы доступ к мобильной телефонной связи был предоставлен только уполномоченным лицам. Внутренние суды отклонили требование заявителя, установив, что он не доказал, что его телефонные разговоры прослушивались или что мобильные операторы передавали защищенную информацию неуполномоченным лицам, а установка оборудования, на которое он ссылался, сама по себе не нарушала тайну его коммуникаций. Рассмотрев это дело, ЕСПЧ пришел к заключению, что положения законодательства Российской Федерации, регулирующие прослушивание коммуникаций, не предусматривают адекватных и эффективных гарантий против произвола и риска злоупотреблений. Внутригосударственное законодательство не отвечает требованию «качества закона» и не способно обеспечить, чтобы вмешательство назначалось только при «необходимости в демократическом обществе». В частности, Суд установил недостатки в правовом регулировании пределов применения мер скрытого наблюдения, длительности мер скрытого наблюдения, проце-

дур хранения и уничтожения данных прослушивания, надзора за применением таких мер, уведомления о прослушивании сообщений. Кроме того, эффективность средств обжалования применения мер была дискредитирована тем, что они были доступны лишь для лиц, представивших доказательства прослушивания, между тем получить подобные доказательства было невозможно в связи с отсутствием какой бы то ни было системы уведомления о применяемых мерах и доступа к информации об их применении.

В деле *Szabó and Vissy vs Hungary* (2016), касавшемся венгерского законодательства о секретном антитеррористическом наблюдении, вступившем в силу в 2011 г., заявители жаловались на то, что они потенциально могли стать объектами такого наблюдения под предлогом охраны общественной безопасности, при этом меры вмешательства в их частную жизнь были бы неоправданны и не пропорциональны в силу несовершенства этого законодательства, в том числе не предусматривающего судебного контроля за решениями спецслужб. ЕСПЧ отметил, что естественным последствием борьбы с проявлениями современного терроризма является желание государств прибегнуть к передовым технологиям сбора информации, таким как массовый мониторинг линий связи. Однако и преследуя цели предотвращения террористических актов государство обязано предпринять меры, чтобы законодательство, регулирующее применение таких технологий, не допускало возможности злоупотребления ими. В рассматриваемом деле это условие соблюдено не было – согласно законодательству меры слежения могли применяться фактически к любому лицу в Венгрии, а используемые технологии позволяли собирать информацию в массовом порядке, включая и лиц, изначально находившихся вне сферы проводимой операции. Более того, приказ о применении таких мер отдавался органами исполнительной власти и не мог быть обжалован, в том числе в судебном порядке. В своей совокупности эти изъяны в законодательстве привели к установлению ЕСПЧ нарушения ст. 8 ЕКПЧ.

В деле *Ivashchenko vs Russia* (2018), касавшемся факта скачивания информации с компьютера фотожурналиста сотрудниками российской таможни, ЕСПЧ установил нарушение ст. 8 ЕКПЧ в связи с тем, что российские власти не смогли показать, что применимое законодательство и практика проведения процедуры выборочного контроля информации на электронном носителе обеспечивали необходимые гарантии защиты от злоупотреблений.

В деле *Breyer vs Germany* (2020) нарушение ст. 8 установлено не было. По мнению ЕСПЧ, Германия не преступила пределы своего усмотрения, обязав телекоммуникационные компании собирать данные о своих клиентах. Это было сделано в законных целях защиты национальной безопасности и борьбы с преступностью. Кроме того, хранение личных данных было пропорционально и «необходимо в демократическом обществе». Притом что ограничение прав человека было незначительным, закон, регулирующий сбор данных, предусматривал возможность обжаловать требование о представлении информации в независимый орган надзора, а также, в случае необходимости, требовать возмещения ущерба в судебном порядке.

Еще одно дело – *Ben Faiza vs France* (2018) касалось использования государством глобальной навигационной спутниковой системы (GPS) для слежения за гражданами. Заявитель в данном деле утверждал, что применение к нему мер слежения в рамках уголовного расследования его участия в торговле наркотиками (установка устройства определения местонахождения на его автомобиль, судебный приказ оператору мобильной связи раскрыть данные о входящих и исходящих звонках и пеленгование его телефона, позволяющее определить его местонахождение) нарушило его право на частную жизнь. ЕСПЧ признал нарушение ст. 8 ЕКПЧ в плане определения местонахождения заявителя в режиме реального времени с помощью GPS в связи с тем, что ни законодательство Франции, ни ее правоприменительная практика не определяли с достаточной ясностью, как именно власти могли применять эту меру, а следовательно, у заявителя не было возможности защиты от ее неправомерного применения. ЕСПЧ, однако, отметил, что позже Франция приняла законодательство, скорректировавшее это положение. Что касается судебного приказа оператору сотовой связи, то здесь ЕСПЧ не усмотрел нарушения ЕКПЧ, потому что вмешательство в частную жизнь заявителя было осуществлено в соответствии с законом, преследовало законные цели предотвращения преступления и охраны общественного здоровья и было необходимо в демократическом обществе, так как направлялось на предотвращение крупномасштабной операции по перевозке наркотиков. И наконец, информация, полученная с помощью данных мер слежения, использовалась в качестве доказательства, подтверждающего вину заявителя, в уголовном судопроизводстве, в

рамках которого он пользовался всеми гарантиями, присущими верховенству закона.

В ряде дел, касавшихся сбора данных, вставал вопрос уважения права на свободу выражения мнения (ст. 10 ЕКПЧ). Так, в деле *Youth Initiative For Human Rights vs Serbia* (2013) речь шла о доступе к информации, полученной сербскими спецслужбами с помощью электронных средств слежения. Заявитель (неправительственная организация) жаловался на то, что отказ спецслужб предоставить информацию о том, сколько сотрудников организации стали объектами слежки, препятствовал ему в осуществлении его роли «общественного наблюдателя». Проанализировав дело, ЕСПЧ постановил, что такие действия спецслужб нарушали национальное законодательство и были произволом. Более того, ЕСПЧ прямо указал в своем постановлении, что надлежащим исполнением данного постановления будет обеспечение получения заявителем требуемой информации.

Дело *Nagla vs Latvia* (2013) касалось обыска у журналиста и изъятия у него информации, хранившейся на электронных носителях. Причиной обыска стало телевыступление журналиста, на котором она заявила об утечке информации из государственной налоговой службы. По ее заявлению, обыск у нее дома привел к раскрытию источника информации и нарушил ее право получать и распространять информацию. Рассматривая это дело, ЕСПЧ подчеркнул, что право журналиста на сохранение в тайне источников информации не может расцениваться как привилегия, зависящая от законности или незаконности этих источников, но является существенной составляющей права на информацию, с которой следует обращаться с осторожностью. По заключению ЕСПЧ, в рассматриваемом деле власти не смогли установить баланс между интересами следствия по обеспечению доказательств и общественным интересом, заключающимся в свободе информации журналиста, что привело к нарушению ст. 10 ЕКПЧ.

В качестве отдельной группы дел, рассматриваемых ЕСПЧ, выделяются дела, касающиеся использования электронной почты[1]. В деле 2007 г. *Copland vs the United Kingdom*, касавшемся слежения за электронной почтой личной ассистентки проректора выс-

[1] См.: New technologies: Factsheet. – Strasbourg, 2020. – Febr. – P. 7. – URL: http://www.echr.coe.int/Documents/FS_New_technologies_ENG.pdf (дата обращения: 19.03.2020).

шего учебного заведения, мониторинг ее коммуникаций осуществлялся по указу проректора с тем, чтобы установить, не использует ли она оборудование организации в личных целях. ЕСПЧ посчитал право на уважение частной жизни и корреспонденции заявителя нарушенным в силу того, что подобный мониторинг не был предусмотрен законом – на тот момент в национальном праве отсутствовали нормы, регулирующие этот вопрос. Суд повторил, что телефонные разговоры с рабочего места покрываются понятиями «частная жизнь» и «корреспонденция». Аналогичным образом должна защищаться и электронная переписка и пользование сетью Интернет в целом. Сбор и хранение информации, связанной с использованием заявителем средств связи без ее ведома, явилось вмешательством в ее права, гарантированные ст. 8 ЕКПЧ. Примечательно, что в данном деле Суд не стал рассматривать вопрос допустимости в демократическом обществе мониторинга использования средств связи сотрудником на рабочем месте.

Дело *Bărbulescu vs Romania* (2017), касавшееся увольнения сотрудника частной компании после мониторинга и оценки его электронных коммуникаций, рассматривала уже Большая палата ЕСПЧ. Суд также установил нарушение ст. 8 ЕКПЧ, закрепив, таким образом, подход, выбранный в деле *Copland vs the United Kingdom*. Было отмечено, что власти не смогли установить справедливый баланс между конкурирующими интересами. В частности, национальные суды не определили, получал ли заявитель предварительное уведомление о возможности мониторинга от работодателя. Они также не рассмотрели вопрос о степени вмешательства в корреспонденцию заявителя, причинах введения мер слежения, а также было ли возможно прибегнуть к способам, в меньшей мере затрагивающим права заявителя.

Использование видеонаблюдения / видеосъемки как государственными органами, так и частными лицами также может поставить вопрос о нарушении частной жизни лица, являющегося объектом съемки.

Дело *Gorlov and Others vs Russia* (2019) касалось постоянного видеонаблюдения за осужденными в их камерах. Применение данной меры не было основано на законе. И хотя ЕСПЧ согласился с тем, что наблюдать за определенными зонами учреждений системы исполнения наказаний может быть необходимо, он отметил, что законодательные положения в этой области недостаточно ясны, точны и детальны и не могут служить защитой от незаконного

вмешательства властей в личную жизнь заключенных. Поскольку у заявителей не было средств эффективной защиты от такого вмешательства, Суд установил нарушение ст. 13 в совокупности со ст. 8 ЕКПЧ.

Дело *Antović and Mirković vs Montenegro* (2017) значительно расширило понятие частной жизни, включив в него «частную социальную жизнь», т.е. возможность формировать собственную идентичность и выстраивать отношения с другими людьми. Заявителями в этом деле стали профессора школы математики Университета Монтенегро. Они обратились в ЕСПЧ, жалуясь на установление в их аудиториях камер видеонаблюдения. По их мнению, они не обладали контролем за собираемой таким образом информацией, и такое слежение было незаконно. Внутренние суды отказали заявителям в требовании о компенсации со ссылкой на то, что право на частную жизнь не может быть предметом спора, если речь идет о местах общественного пользования, которыми являются аудитории, где обучаются студенты. ЕСПЧ отверг этот аргумент властей, указав, что частная жизнь может включать в себя профессиональную деятельность. Установка камер в аудиториях стала вмешательством в частную жизнь заявителей. Она также была произведена в нарушение норм внутреннего законодательства, причем этот аргумент не был рассмотрен национальными судами. Учитывая это, ЕСПЧ установил нарушение ст. 8 ЕКПЧ.

Дело *López Ribalda and Others vs Spain* (2018) касалось тайного видеонаблюдения за сотрудниками испанской сети супермаркетов после появления подозрений в воровстве. После получения видеодоказательств их причастности к преступлению заявители по данному делу были уволены. Внутренние суды признали эти доказательства допустимыми и утвердили решение об увольнении. В своей жалобе в ЕСПЧ заявители утверждали, что доказательства против них были получены в нарушение их права на конфиденциальность. ЕСПЧ установил, что справедливый баланс между этим правом заявителей и правом собственности работодателя не был установлен. Согласно испанскому законодательству о защите информации заявители должны были быть уведомлены о наблюдении за ними, однако этого сделано не было. Кроме того, права работодателя могли быть обеспечены и другими, менее значительными мерами. Установив нарушение ст. 8 ЕКПЧ, Суд, однако, не нашел нарушения ст. 6 (право на справедливый суд), в связи с тем, что видеоматериалы были не единственным доказательством, на кото-

рое ссылался национальный суд, утверждая увольнение, а заявители могли обжаловать приобщение видеозаписи в качестве доказательства, так что в целом судебный процесс был справедливым.

Дело *Haldimann and others vs Switzerland* (2015) касалось наказания журналистов за использование во время интервью скрытой камеры. Это было первое подобное дело, рассмотренное ЕСПЧ. Речь шла об осуждении четырех журналистов за съемки частного лица для документального фильма, целью которого было разоблачить деятельность страховых агентов, дающих заведомо ложные советы. Заявители утверждали, что присужденные им штрафы были непропорционально велики и ограничивали их право на выражение мнения. Суд отметил, что интервьюируемое лицо выступало не в личном качестве, а как представитель определенной профессиональной категории. Отметив, что вмешательство в частную жизнь страхового агента, отказавшегося от съемок, было не так велико, чтобы перевесить общественный интерес в получении информации о злоупотреблениях в страховой сфере, ЕСПЧ пришел к выводу о нарушении ст. 10 ЕКПЧ.

Свобода выражения мнения, закрепленная в ст. 10 ЕКПЧ, наряду с правом на уважение частной жизни (ст. 8 ЕКПЧ) называется в качестве ключевой проблемной области в контексте использования новых технологий[1]. Доступность сети Интернет, ее способность хранить и передавать большие объемы информации делают ее важной в обеспечении распространения информации в целом и в облегчении доступа общественности к новостям в частности. Однако риск нанесения ущерба правам и свободам посредством сети Интернет выше, чем при использовании традиционных СМИ[2]. Любые меры, принимаемые властями или частными лицами по блокированию, фильтрации или изъятию интернет-контента, а также любые запросы властей по этому поводу должны соответствовать требованиям, установленным ст. 10. В частности, они должны быть предписаны законом, причем законом доступным, понятным, однозначным и достаточно точным для того, чтобы частное лицо могло предвидеть последствия своих действий. В то

[1] См.: Coccoli J. The challenges of new technologies in the implementation of human rights: An analysis of some critical issues in the digital era // Peace human rights governance. – 2017. – Vol. 1, N 2. – P. 226.

[2] См.: Freedom of expression, the Internet and new technologies: Thematic factsheet. Op. cit. – P. 1.

же время эти меры должны быть необходимы в демократическом обществе и пропорциональны преследуемой цели.

В деле *Cengiz and Others vs Turkey* (2015) рассматривался вопрос блокировки доступа заявителей – ученых из разных университетов, к Ютьюбу (YouTube), ЕСПЧ установил нарушение их права получать и распространять информацию и идеи, приняв во внимание специфику работы заявителей и тот факт, что они были лишены доступа к этому сайту в течение продолжительного периода времени. Суд отметил, что Ютьюб был единственной платформой, обеспечивающей доступ к информации по определенным вопросам, в том числе политическим и социальным. Он также установил, что национальное законодательство не содержало положения, позволявшего судам налагать общий запрет на доступ к сети Интернет и интернет-контенту.

Дело *Kalda vs Estonia* (2016) касалось доступа к сети Интернет заключенных. Заявитель обжаловал запрет доступа к трем интернет-ресурсам (как государственным, так и принадлежащим Совету Европы), содержащим правовую информацию. Он заявил, что данный запрет нарушил его право получать информацию с помощью сети Интернет и помешал ему подготовиться к судебному процессу, в котором он участвовал. ЕСПЧ согласился с этим утверждением, отметив, что хотя государства – стороны ЕКПЧ не обязаны предоставлять заключенным доступ к сети Интернет, в том случае, если государство готово это сделать, как это было в Эстонии, оно обязано объяснить причины отказа доступа к конкретным сайтам. В настоящем деле названные причины (соображения безопасности и затраты) не были достаточными для оправдания вмешательства в право на получение информации, так как к моменту, когда заявителю понадобились спорные сайты, власти уже предприняли меры по обеспечению безопасности, оборудовав компьютеры специальным образом и предусмотрев надзор за использованием Интернета заключенными. Все необходимые на это расходы уже были сделаны. Внутренние суды не приняли эти соображения во внимание и не провели детального анализа того, какие именно возможные риски нес в себе доступ к трем дополнительным сайтам, учитывая тот факт, что они принадлежали международной организации и самому государству.

Новой для ЕСПЧ темой стала ответственность за комментарии, размещенные онлайн. Первое такое дело, *Delfi AS vs Estonia*, было рассмотрено судом в 2015 г. Заявитель в данном деле – ком-

пания, управляющая на коммерческой основе новостным порталом, жаловалась на то, что ее признали ответственной за оскорбительные комментарии, размещенные читателями под одной из онлайн-статей о железнодорожной компании. По требованию юристов железнодорожной компании комментарии были удалены через шесть недель после публикации. ЕСПЧ не нашел в данных обстоятельствах нарушения ст. 10 ЕКПЧ, постановив, что признание ответственности заявителя было обоснованным и пропорциональным вмешательством в свободу выражения мнения новостного портала по следующим причинам: спорные комментарии были чрезмерными и были размещены в качестве реакции на опубликование статьи заявителем на его портале; шаги, предпринятые заявителем для удаления комментариев сразу после их размещения, были неэффективными; наложенный на заявителя штраф в размере 320 евро не был чрезмерным для заявителя, учитывая тот факт, что он управлял одним из крупнейших интернет-порталов в Эстонии

Напротив, в деле *Magyar Tartalomszolgáltatók Egyesülete and Index.hu Zrt vs Hungary* (2016) ЕСПЧ установил нарушение ст. 10 ЕКПЧ. Дело касалось ответственности организации, объединяющей интернет-контент провайдеров и новостного интернет-портала, за грубые и оскорбительные комментарии, размещенные на их сайтах после публикации ими мнения, критикующего два сайта агентств недвижимости. Национальные суды обязали их модерировать комментарии, размещаемые читателями сайтов. Сочтя, что такая обязанность нарушает их право на свободу выражения мнения, организации обратились в ЕСПЧ. Суд отметил, что новостные порталы должны брать на себя определенную ответственность за размещаемые у них на сайте комментарии. При этом в данном деле национальные суды не смогли установить баланс между правом заявителей на свободу слова и правом агентств недвижимости на уважение их коммерческой репутации, беспрекословно приняв аргумент о том, что размещенные комментарии были незаконны потому, что нанесли урон репутации агентств.

В деле *Høiness vs Norway* (2019) рассматривался вопрос отказа норвежских судов наложить ответственность на интернет-форум за размещенные на нем грубые комментарии в адрес заявителя. По мнению заявителя, власти нарушили его право на частную жизнь тем, что недостаточно защитили его репутацию, а также тем, что потребовали оплаты судебных расходов. Учитывая тот факт, что национальные суды действовали в пределах своих пол-

номочий, устанавливая баланс между правом заявителя на уважение частной жизни и конкурирующим с ним правом новостного портала и администратора форума на свободу выражения мнения, ЕСПЧ не нашел оснований для установления нарушения ЕКПЧ.

Опираясь на ст. 10 ЕКПЧ, Суд рассмотрел и дело, связанное с использованием антенны спутниковой связи. Дело *Khurshid Mustafa and Tarzibachi vs Sweden* (2008) касалось решения национального суда о выселении из съемной квартиры семьи иракского происхождения с тремя маленькими детьми в связи с отказом нанимателей демонтировать спутниковую антенну, которая использовалась ими для доступа к телевизионным программам из их родной страны. Владелец квартиры был согласен продлить контракт лишь на условии демонтажа антенны, и семье пришлось съехать. ЕСПЧ установил в данном деле нарушение ЕКПЧ, отметив, что спутниковая антенна позволяла заявителям смотреть программы на арабском языке и фарси – родных языках региона их происхождения. Получаемая информация включала политические и социальные новости и, что также важно, культурные и развлекательные программы. Последнее носило принципиальный характер для них как для семьи эмигрантов, желавшей поддерживать контакт с культурой и языком страны происхождения. Заявители не могли получать такую информацию иным образом и установить антенну в другом месте. Новости, получаемые из иностранных газет и радиопрограмм, отметил ЕСПЧ, не могут быть сравнимы с информацией, получаемой из телевизионных передач. Аргумент арендодателя о небезопасности установки антенны был исследован и не подтвержден национальным судом. Более того, выселение семьи с тремя маленькими детьми было явно непропорционально преследуемой цели.

Как видно из рассмотренных выше дел, ЕСПЧ выделяет два ключевых права, требующих дополнительного толкования в контексте использования новых технологий, – это право на защиту частной жизни и право на свободу выражения мнения. Оба права предполагают возможность их ограничения, которое, как подчеркивает ЕСПЧ, должно осуществляться в соответствии с законом, в законных целях и только при необходимости такого ограничения в демократическом обществе. При соблюдении указанных условий государство, на котором лежат не только негативные, но и позитивные обязательства по обеспечению и защите прав человека, сможет достичь «справедливого баланса», при котором использование современных технологий не будет в ущерб правам человека, гарантированным ЕКПЧ.

Заключение

Проведенное исследование синтезирует анализ общих и частных вопросов методологии, правовых принципов, институтов права, прав и свобод, правовых технологий, демонстрирующих трансформацию и развитие государства и права под натиском четвертой промышленной революции и ее последствий.

Технологический цифровой прорыв в начале нового столетия вызвал неоднозначную реакцию общества. С одной стороны, исследователи отмечают ускорение развития и взаимообмена в условиях интенсивной цифровизации общества. С другой стороны, общую озабоченность вызывают риски глобальной электронизации и цифровизации, отделяющие человека от государства и снижающие транспарентность поведения, каналов ответственности за нарушение прав и свобод, совершения преступлений и иных правонарушений с использованием цифровых технологий.

Центральная идея, выдвигаемая авторами, связана с системным анализом позитивных и негативных последствий от импульсов интенсивно развивающейся тенденции цифровизации правовой системы и государственных функций. С целью оценки этой тенденции были рассмотрены наиболее актуальные проблемы цифровой трансформации права, цифровизации правотворчества, правоохранительной системы и судебной деятельности. Проанализированы современные взгляды на роль права в регулировании Интернета и сетевого общения, выявлена система новых, так называемых цифровых, прав и обозначены потребности в их защите.

В результате исследования сделан, в частности, вывод о том, что сегодня важное значение имеет формирование теоретико-методологических и философских основ влияния техники и технологий на цифровое развитие государства и права. Под воздействи-

ем инновационных информационных технологий отрасль права нового поколения – информационное право – интенсивно глобализируется и дифференцируется, все более самостоятельное значение приобретают ее структурные элементы – цифровое право, право информационной безопасности, цифровые права, свободы и обязанности, право информационной ответственности и др. Внутри традиционных отраслей права появились блоки норм и институты, связанные с информационными отношениями. Например, в уголовном праве – это «уголовная ответственность за киберпреступления», в финансовом и предпринимательском праве – новые цифровые технологии обслуживания денежно-финансовых потоков (биткойны, криптовалюта, блокчейн-технологии)», в гражданском и предпринимательском праве – «цифровая экономика», в конституционном праве – «электронная демократия», «электронное голосование» и т.д. Появились такие новые сферы правового регулирования информационных технологий, как биоинженерия, нанотехнологии, робототехника, искусственный интеллект, многомерная визуализация и др.

В монографии четко прослеживается связь между проблемами защиты прав человека, укрепления безопасности государства, общества и личности и процессами цифровой трансформации права, цифровизации правотворчества, правоохранительной системы и правосудия.

Один из важных аспектов связан с аналитикой правовых последствий использования больших данных (Big data) и искусственного интеллекта; применения новых цифровых технологий в финансовой системе, экономике и государственном управлении; использования так называемых «подрывных инноваций». Данные инновационные технологии становятся основой конкурентоспособности не только частных компаний, но и государств, они широко применяются в таких смешанных публично-частных сферах, как образование, культура, здравоохранение, социальная защита, экология и др.

Значительное внимание в монографии уделено процессам правового регулирования информатизации и цифровизации российского государства и российского права. Опыт Российской Федерации проанализирован в контексте общемировых тенденций и в сравнении с практикой других государств. Осознание важности разработки и внедрения самых передовых цифровых технологий во все отрасли экономики и сферы государственного управления

нашло отражение в ключевых документах стратегического планирования Российской Федерации, а также в национальном проекте «Цифровая экономика Российской Федерации», в рамках которого стремительно меняется нормативная база, направленная на стимулирование развития и активного внедрения цифровых технологий, начиная от придания статуса имущества цифровым активам и регламентации оборота криптовалют и заканчивая цифровизацией государственного управления (включая унификацию правил обращения в суды в электронной форме, допустимость электронных доказательств, дистанционное участие в судебном заседании, изготовление нотариальных документов в электронной форме и дистанционное совершение нотариальных действий, а также переход к электронным трудовым книжкам).

Достойное место в монографии занимает анализ содержания и проблем реализации информационных прав, стремительно дифференцирующихся под влиянием цифровизации. Наряду с общим комплексным правом на информацию и вытекающими из него общими правами на доступ к информации, свободу информации, защиту частной жизни и пр., появились такие производные от них права, как право на доступ в Интернет, право на изображение, право на забвение, право на цифровую смерть и др.

В контексте обеспечения прав человека предметом особого внимания является правовая защита персональных данных в условиях цифровизации. Угроза раскрытия личной информации становится всё более реальной в жизни современных потребителей. Причин существует множество: недостаток знаний о том, как управлять кибербезопасностью; отсутствие осведомленности о том, как бороться с манипулятивной деятельностью, или отсутствие навыков правоприменения. Значительную роль в сборе и использовании персональных данных играют социальные сети. За последние 15 лет пространство социальных сетей выросло в геометрической прогрессии, привлекая к себе всё новых пользователей. В связи с этим в данном пространстве содержатся значительные объемы персональных данных, эффективная правовая защита которых все более актуализируется.

Стремительное развитие информационной аналитики и рост вычислительных мощностей предоставили широкие возможности использования в государственном управлении сложных электронных статистических алгоритмов и средств искусственного интеллекта. В монографии предпринята попытка оценить последствия

использования в государственном управлении алгоритмов машинного обучения. В частности отмечено, что автоматизация процедур осуществления публичных функций (принятия управленческих решений) способна оказывать существенное влияние на реализацию правовых норм, прав и обязанностей вовлеченных лиц.

В монографии наглядно иллюстрируется, как цифровые технологии XXI столетия требуют нового прочтения концепции электронного государства (электронного правительства), выдвинутой в 90-е годы XX в. Если изначально социальное значение электронной коммуникации мыслилось преимущественно в контексте требований информационной свободы и открытого общества, то в новых условиях цифровизации создается реальная угроза формирования моделей тоталитарного государства и систем надгосударственной экономической транснациональной бюрократии, при которых значительно снижается порог возможностей широкого информирования о властно-управленческих решениях, общественного контроля за действиями власти и равноправной рыночной конкуренции. Соответственно наблюдается рост «закрытости» административно-бюрократических процессов, создается цифровая элита, держащая в своих руках тайны алгоритмов и программных кодов, правовое оформление которых оказывается весьма затруднительным для органов государственной власти, осуществляющих правотворчество и правоприменение.

Внедрение искусственного интеллекта в государственное управление позволяет выделить пять основных вариантов использования искусственного интеллекта при обслуживании населения в государственных органах: 1) консультирование; 2) поиск документов; 3) классификация и направление обращений по подведомственности; 4) языковые переводы; 5) составление проектов документов. Тем не менее помимо предоставления выгод для государственного управления, искусственный интеллект также создает и опасность причинения вреда не только управляемым субъектам, но и механизму управления в целом. Существует много предпосылок того, что использование искусственного интеллекта в государственном управлении окажется неэффективным. Алгоритмы могут быть неверно сформулированы. Их обучение или тестирование может проводится на ложной информации. Ошибки могут вызываться неполноценной индуктивной аргументацией, некорректным выбором и вводом данных, неверной оценкой факторов, сбоями в обеспечивающих работу алгоритма электронно-

вычислительных машинах, программном обеспечении, сбоями в самом коде алгоритма и т.п.

Таким образом, процессы цифровизации – сложное комплексное явление. Отдельные виды электронных автоматизированных систем, объединенные данным понятием, включающие, к примеру, алгоритмизацию, профайлинг (составление индивидуальных и коллективных портретов лиц), автоматизацию, машинное обучение, глубинные нейронные сети и т.д., имеют настолько существенные различия, что требуют разных правовых конструкций. Игнорирование потребности в установлении правовых рамок применения алгоритмов обесценивает роль государства в общественном взаимодействии, как конечного гаранта прав и свобод, призванного обеспечить эффективные средства защиты.

В завершение хотелось бы заметить, что в данной монографии больше поставлено вопросов, нежели дано ответов. Это объективно, так как на данном этапе информационного развития важно дать оценку происходящего, представить полноценную и всестороннюю картину тенденций, угроз и вызовов информатизации и алгоритмизации государства и общества в начале XXI столетия. Следующий этап – формирование правовых моделей оптимального взаимодействия информационных технологических процессов и методологий с институтами, стоящими на страже непреложных ценностей современной человеческой цивилизации. Такое взаимодействие в итоге должно полноценно обеспечивать потребности человека в гуманизме и демократии, в правах и свободах, в справедливости и достоинстве, в безопасности и развитии.

ГОСУДАРСТВО И ПРАВО
В НОВОЙ ЦИФРОВОЙ РЕАЛЬНОСТИ

Монография

Под общей редакцией
доктора юридических наук, профессора И.А. Умновой-Конюховой
и доктора технических наук, профессора Д.А. Ловцова

Дизайнер (художник) И.А. Михеев
Корректоры О.В. Шамова, М.П. Крыжановская
Компьютерная верстка Л.Н. Синякова

Гигиеническое заключение
№ 77.99.6.953.П.5008.8.99 от 23.08.1999 г.
Подписано к печати 17/VII – 2020 г.
Формат 70x100/16 Бум. офсетная № 1 Печать офсетная
Усл. печ. л. 15,2 Уч.-изд. л. 14,5
Тираж 500 экз. (1 – 100 экз. – 1-й завод) Заказ № 35

Институт научной информации по общественным наукам РАН,
Нахимовский проспект, д. 51/21,
Москва, В-418, ГСП-7, 117997

Отдел маркетинга и распространения
информационных изданий
Тел. / Факс: +7(925) 517-36-91
E-mail: inion@bk.ru

E-mail: ani-2000@list.ru
(по вопросам распространения изданий)

Отпечатано по гранкам ИНИОН РАН
в ООО «Амирит», 410004, Саратовская обл.,
г. Саратов, ул. Чернышевского, д.88, литера У
Тел.: 8-800-700-86-33; (845-2)24-86-33