WWW.IGZAKON.RU

МАРТ 2022
Выходит с 1992 года

# ЗАКОН

Самый лукавый налог

К цивилистической теории смарт-контрактов

Новое законодательство КНР в области персональных данных: приватность «с китайской спецификой»

## Алексей МУНТЯН: «Мы вступили в эпоху цифрового огораживания и национализации персональных данных»

ТЕМА НОМЕРА: Персональные данные

ISSN 0869-4400
9 770869 440002 22003

первая социальная сеть для юристов

Реклама

# zakon ru одобрен с первого чтения

**Читайте**

@zakon_news

facebook.com/zakon.ru

vk.com/zakon_news

**Вступайте**

Более **67 900** пользователей

**15 000** юристов

**3200** студентов

**1900** компаний

**Высказывайтесь**

***Арина Ворожевич***

*преподаватель юридического факультета МГУ им. М.В. Ломоносова*

*«Масштабные экономические санкции — серьезный вызов для системы интеллектуальных прав»*

# ОТ РЕДАКЦИИ

Когда вы будете читать этот номер — неважно, через несколько дней или десятилетий после его выхода в свет, — имейте в виду: все материалы в нем, кроме этого вступительного слова, были написаны еще до того, как наш мир бесповоротно изменился. Любые изменения в праве — это не изменения в текстах правовых актов, это изменения в нашем с вами сознании. Теперь не только авторам статей, вошедших в номер, но и многим другим стало очевидно, что персональные данные — не просто записи в чьих-то базах данных, а наше право участия. Без них невозможны многие, если не все блага современного мира: от развлекательных компьютерных игр до базовых потребностей в коммуникациях и государственных услугах. Наши данные — не только возможность быть частью общего для человечества киберпространства, но и наше право участвовать в выработке правил для него. Иначе несправедливо: несправедливо не только по отношению к нашим данным, но и к нам самим.

В материалах этого номера показано, как развитие технологий убирает барьеры: законодатели разных стран уже не изолированы друг от друга, данные из всевозможных источников доступны для извлечения и слияния, коммуникационные системы конвергентны как никогда. Некоторые из этих барьеров, как выясняется, были естественными ограничителями для злоупотреблений. Долгое время частная жизнь была неприкосновенна просто потому, что не было доступных технологий для массового вторжения в нее, но сейчас такие технологии стали частью повседневности. Теперь задача права заключается в том, чтобы устранить несправедливость, заменив часть физических, технологических, организационных, экономических ограничений логическими границами, препятствующими произволу. Над выбором и созданием новых правил, как видно из вошедших в номер исследований, работают лучшие юристы по всему миру. Предлагаю вам присоединиться к этому большому процессу, поскольку он только начался. Пока мы не сочтем новые ограничения справедливыми, они не будут работать, какими бы логичными ни казались их создателям.

**Николай Дмитрик,**

кандидат юридических наук, заведующий лабораторией правовой информатики и кибернетики юридического факультета МГУ имени М.В. Ломоносова, доцент факультета права Национального исследовательского университета «Высшая школа экономики»

АЛЕКСЕЙ МУНТЯН

СОУЧРЕДИТЕЛЬ И ЧЛЕН ПРАВЛЕНИЯ
*RUSSIAN PRIVACY PROFESSIONALS ASSOCIATION*

**ИНТЕРВЬЮ НОМЕРА**

# МЫ ВСТУПИЛИ В ЭПОХУ ЦИФРОВОГО ОГОРАЖИВАНИЯ И НАЦИОНАЛИЗАЦИИ ПЕРСОНАЛЬНЫХ ДАННЫХ

“Зная о проблеме обработки персональных данных, люди станут внимательнее относиться к ним и соблюдать так называемую информационную гигиену”


**Оформить подписку на электронные и печатные версии журнала «Закон»**

*1. Online*
**https://zakon.ru/**
**https://igzakon.ru/**
**https://podpiska.pochta.ru/**

*2. E-mail*
**post@igzakon.ru**

*3. Телефон*
**+7 (495) 927-01-62**

*4. Почта России*
**П7299 в каталоге Почта России**
**39001 по каталогу агентства «Урал-пресс»**

читайте
в номере

# ЗАКОН

## ТЕМА НОМЕРА:
## Персональные данные

Среди авторов номера:

**А.С. Филяшин**

Уголовно-процессуальная политика *Crime Control* в США, ее контекст и идеология

*Роль политического и научно-исследовательского контекста при формировании доктрины экономического анализа права.*

**В.В. Архипов**

Персонажи (аватары) в многопользовательских компьютерных играх: вопросы правовой квалификации в свете междисциплинарных исследований

*Можно ли отнести персонажей компьютерных игр (аватары) и виртуальных миров к категории персональных данных?*

**Е.И. Дискин**

Фейковые новости как политико-правовой феномен

*Анализ термина «фейковые новости» и стремительный переход его из области политической борьбы в юридическую плоскость.*

Консультант номера:

**Н.А. Дмитрик**

кандидат юридических наук, заведующий лабораторией правовой информатики и кибернетики юридического факультета МГУ имени М.В. Ломоносова, доцент факультета права Национального исследовательского университета «Высшая школа экономики»

ЗАКОН
ИЗДАТЕЛЬСКАЯ ГРУППА

**Журнал «ЗАКОН» награжден Высшей юридической премией «ФЕМИДА» за 2007 год.**

**Журнал «ЗАКОН» включен в Перечень ведущих рецензируемых научных журналов и изданий, в которых должны быть опубликованы основные научные результаты диссертаций на соискание ученой степени доктора и кандидата юридических наук**

# содержание / contents

От редакции 1

Introduction

## ИНТЕРВЬЮ НОМЕРА

## INTERVIEW

**А.В. Мунтян.** МЫ ВСТУПИЛИ В ЭПОХУ ЦИФРОВОГО ОГОРАЖИВАНИЯ И НАЦИОНАЛИЗАЦИИ (ПЕРСОНАЛЬНЫХ) ДАННЫХ 8

**A.V. Muntyan.** WE HAVE ENTERED THE ERA OF DIGITAL ENCLOSURE AND NATIONALIZATION OF PERSONAL DATA

## ТЕМА НОМЕРА: ПЕРСОНАЛЬНЫЕ ДАННЫЕ

## TOPIC OF THE ISSUE: PERSONAL DATA

**Н.А. Дмитрик.** ЛЮДИ В СВОЕМ ПРАВЕ: ОТ ПРАВОСПОСОБНОСТИ К ИДЕНТИЧНОСТИ И ОБРАТНО 16

**N.A. Dmitrik.** HUMANS IN THEIR RIGHT: FROM LEGAL CAPACITY TO PERSONAL IDENTITY AND BACK

**С.Д. Афанасьев, И.А. Терещенко, Д.А. Яцкевич.** БИОМЕТРИЧЕСКАЯ ИДЕНТИФИКАЦИЯ И ПРАВА ЧЕЛОВЕКА: ДЕМАРКАЦИОННАЯ ЛИНИЯ 33

**S.D. Afanasev, I.A. Tereshchenko, D.A. Yatskevich.** BIOMETRIC IDENTIFICATION AND HUMAN RIGHTS: THE LINE OF DEMARCATION

№ 3 Март 2022
March 2022
ЗАКОН

**А.Н. Изотова.** РОЛЬ ИДЕНТИФИКАЦИИ В ИНСТИТУТЕ ТАЙНЫ СВЯЗИ 47

**A.N. Izotova.** THE ROLE OF IDENTIFICATION FOR THE COMMUNICATION SECRECY

**В.В. Архипов.** ПЕРСОНАЖИ (АВАТАРЫ) В МНОГОПОЛЬЗОВАТЕЛЬСКИХ КОМПЬЮТЕРНЫХ ИГРАХ: ВОПРОСЫ ПРАВОВОЙ КВАЛИФИКАЦИИ В СВЕТЕ МЕЖДИСЦИПЛИНАРНЫХ ИССЛЕДОВАНИЙ 58

**V.V. Arkhipov.** CHARACTERS (AVATARS) IN MULTIPLAYER COMPUTER GAMES: ISSUES OF LEGAL QUALIFICATION IN THE CONTEXT OF INTERDISCIPLINARY STUDIES

**А.И. Савельев, М.А. Иманалиева.** НОВОЕ ЗАКОНОДАТЕЛЬСТВО КНР В ОБЛАСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ: ПРИВАТНОСТЬ «С КИТАЙСКОЙ СПЕЦИФИКОЙ» 75

**A.I. Savelyev, M.A. Imanalieva.** CHINA'S NEW LEGISLATION ON PERSONAL DATA: PRIVACY "WITH A CHINESE TWIST"

**А.О. Абышко.** КОНЕЦ ОБЩЕДОСТУПНЫХ ПЕРСОНАЛЬНЫХ ДАННЫХ В РОССИИ? К ВОПРОСУ О ФЕДЕРАЛЬНОМ ЗАКОНЕ ОТ 30 ДЕКАБРЯ 2020 ГОДА № 519-ФЗ 97

**A.O. Abyshko.** END OF PUBLICLY AVAILABLE PERSONAL DATA IN RUSSIA? TO THE ISSUE OF FEDERAL LAW No. 519-FZ

## ДИСКУССИОННЫЙ КЛУБ

## DISCUSSION BOARD

**Е.И. Дискин.** ФЕЙКОВЫЕ НОВОСТИ КАК ПОЛИТИКО-ПРАВОВОЙ ФЕНОМЕН 108

**E.I. Diskin.** FAKE-NEWS AS A POLITICAL AND LEGAL PHENOMENON

# содержание / contents

## ЮРИДИЧЕСКАЯ ХРОНИКА

## LEGAL CHRONICLE


I. Санкции и контрсанкции: с чем мы столкнулись в этот раз?
*М.Б. Жужжалов, Р.М. Янковский* 121

II. В канун тяжелых испытаний.
*В.Б. Румак* 126

III. Приглашение на казнь.
*А.П. Евсеев* 130

IV. Уголовное законодательство [спецоперационного] времени.
*Г.А. Есаков* 135

V. Конституционный суд, недобросовестная конкуренция и экономика права.
*П.Д. Блохин* 139

I. Sanctions and counter-sanctions: what are we facing this time?
*M.B. Zhuzhzhalov, R.M. Yankovskiy*

II. On the eve of severe trials.
*V.B. Rumak*

III. An invitation to execution.
*A.P. Evseev*

IV. Criminal legislation of the [special operation] time.
*G.A. Esakov*

V. Constitutional Court, unfair competition and economics of law.
*P.D. Blokhin*


## ПРЕСС-РЕЛИЗ

## PRESS RELEASE


ЧТО НАС ЖДЕТ ЗА ГОРИЗОНТОМ: КОНФЕРЕНЦИЯ ОКЮР
О ВЫЗОВАХ 2022 ГОДА 144

WHAT'S LOOKING BEYOND THE HORIZON: 2022 CHALLENGES
CONFERENCE OF ASSOCIATION OF CORPORATE LAWYERS

# ЗАКОН

## ТЕОРИЯ И ПРАКТИКА

## THEORY AND PRACTICE

**Г.В. Цепов, Н.В. Иванов.** К ЦИВИЛИСТИЧЕСКОЙ ТЕОРИИ СМАРТ-КОНТРАКТОВ 149

**G.V. Tsepov, N.V. Ivanov.** TOWARDS A CIVIL-LAW THEORY OF SMART CONTRACTS

**А.А. Иванов.** САМЫЙ ЛУКАВЫЙ НАЛОГ 173

**A.A. Ivanov.** THE MOST WILY TAX

## ЗАРУБЕЖНЫЙ ОПЫТ

## FOREIGN EXPERIENCE

**А.С. Филяшин.** УГОЛОВНО-ПРОЦЕССУАЛЬНАЯ ПОЛИТИКА *CRIME CONTROL* В США, ЕЕ КОНТЕКСТ И ИДЕОЛОГИЯ 180

**A.S. Filiashin.** “CRIME CONTROL TURN” AND AMERICAN LAW OF CRIMINAL PROCEDURE: CONTEXT AND IDEOLOGY

На вопросы редакции журнала «ЗАКОН» отвечает соучредитель и член правления *Russian Privacy Professionals Association*
**Алексей Витальевич МУНТЯН**

# МЫ ВСТУПИЛИ В ЭПОХУ ЦИФРОВОГО ОГОРАЖИВАНИЯ И НАЦИОНАЛИЗАЦИИ (ПЕРСОНАЛЬНЫХ) ДАННЫХ

Основатель и CEO в компании *Privacy Advocates*, соучредитель и член правления *Russian Privacy Professionals Association*. Внешний *Data Protection Officer* в двух транснациональных холдингах, член Совета Торгово-промышленной палаты РФ по развитию антикоррупционного комплаенса и деловой этики. Эксперт *Privacy & Legal Tech* кластера РАЭК, участник комитета по безопасности данных партнеров и пользователей при Консультативном совете по развитию экосистемы «Яндекса».

**— Как получилось, что Вы выбрали такую область специализации, как персональные данные?**

— К этой профессии я пришел не случайно, а осознанно. В 2003 году поступил в МИФИ на факультет правового обеспечения информационной безопасности. Сейчас этого факультета, к сожалению, уже нет в институте. В 2008 году устроился работать в Управление комиссара по правам человека ООН в Восточно-Африканском региональном офисе в Эфиопии. Здесь я проработал год специалистом по информационной безопасности. Моей главной задачей была защита персональных данных лиц, которые обращались в Управление с жалобами на нарушение прав человека. Так как были попытки несанкционированного доступа к этим данным, я в течение года занимался тем, что пересматривал и улучшал те подходы к обеспечению защиты персональных данных, которые применялись ранее. Увы, более подробно рассказать не смогу, так как связан бессрочными обязательствами по *NDA*.

Потом я окончил магистратуру в Колледже королевы Марии при Лондонском университете по специализации в области права *IT/IP*, телекоммуникационного права. Кроме того, был опыт работы в компании, которая занималась администрированием портала персональных данных Роскомнадзора; в компании — системном интеграторе, где оказывал консультационные услуги по защите персональных данных, коммерческой тайны. Еще работал менеджером по защите персональных данных в ряде крупных российских и международных компаний. Сейчас я также занимаюсь общественной деятельностью в области приватности данных и выступаю в качестве внешнего консультанта по вопросам в данной области.

**— А кто сейчас готовит специалистов в сфере защиты персональных данных в России?**

— Есть определенные программы в МГУ, НИУ ВШЭ, но это не специализированная подготовка, а, скорее, организационно-юридическая специализация в рамках *IT/IP*. Такого комплексного образования, как было в МИФИ, сейчас нет. В МИФИ мы изучали и технические вопросы, и экономику информационной безопасности, психологические аспекты информационного противоборства. Сегодня в нашей стране я не знаю ни одной аналогичной по содержанию полноценной программы высшего образования в этой сфере. Но проводятся курсы повышения квалификации и тренинги по *Data privacy*. Мы, *RPPA.ru*, совместно с МГУ запустили свой учебный курс повышения квалификации. Я думаю, что в ближайшее время появятся и полноценные программы обучения в сфере защиты персональных данных.

**— Что сейчас понимается под персональными данными? Изменяется ли содержание этого понятия со временем?**

— Последние годы мы наблюдаем рецепцию именно европейского подхода к трактовке понятия «персональные данные». Хочу обратить внимание, что само регулирование в сфере информационной приватности, защиты персональных данных в нашей стране появилось благодаря европейской правовой традиции, после присоединения России в 2005 году к Конвенции № 108[1]. И как раз в рамках взятых нами на себя обязательств был принят Закон № 152[2] в 2006 году.

Согласно европейскому подходу, персональные данные — это любая информация, которая прямо или косвенно относится к определенному или определяемому физическому лицу. В нашей стране в первоначальной редакции Закона была попытка перечислить некоторые категории персональных данных (ФИО, паспортные данные и т.п.). Но в 2011 г. были внесены изменения и примеры исключили из определения, так как это порождало много толкований, сужая сферу применения Закона. Сейчас в нем содержится гармонизированное определение персональных данных, соответствующее Конвенции № 108 и *GDPR*[3]. Поэтому в целом на сегодня мы находимся в едином понятийном поле с европейским регулированием. Но на практике до сих пор встречается непоследовательный подход и толкование содержания понятия «персональные данные». Например, в нашей стране в отношении номера телефона или государственного номера автомобиля еще идут споры, потому что Роскомнадзор официально не считает их персональными данными. Но в отдельных случаях есть возможность в конечном счете установить персональные данные лица, которое допущено к управлению автомобилем, и идентифицировать его, — и тогда с точки зрения европейского понимания это в чистейшем виде персональные данные. При отнесении тех или иных данных к персональным большое значение имеет контекст, и у нас только-только появляется понимание некоторых вопросов.

Другой пример: когда вы включаете новый ноутбук, заходите в Сеть и вводите поисковый запрос в любой поисковой системе, при этом еще нигде не зарегистрировавшись, данные о ваших запросах и предполагаемых интересах фиксируются поставщиками интернет-рекламы. То есть не обязательно знать, кто вы такой, вы можете быть определенным или определяемым лицом. Но вас можно выделить по техническим данным среди другой массы людей и с вами можно будет взаимодействовать прямо или косвенно (например, таргетировать в Интернете и показывать нацеленную на ваши интересы рекламу). Это говорит о том, что технических данных

[1] Конвенция о защите физических лиц при автоматизированной обработке персональных данных (заключена в г. Страсбурге 28.01.1981). URL: http://www.consultant.ru/document/cons_doc_LAW_121499/ (дата обращения: 15.03.2022).

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

[3] Общий регламент защиты персональных данных, принятый постановлением Европейского союза 2016/679.

вашего компьютера, браузера и т.п. достаточно, чтобы вступить с вами во взаимоотношения в части демонстрации рекламы.

**— Тогда где пределы определения содержания понятия «персональные данные» с точки зрения права?**

— С точки зрения права это любая информация, которая прямо или косвенно относится к определяемому или определенному лицу. Понимание персональных данных давно сложилось в судебной практике и идет по пути расширительного толкования как раз в сторону европейского подхода. В 2016 году был целый ряд громких кейсов: дело МГТС, дело «Сумма телеком» — где суд прямо указал, что хеш-сумма пользовательских данных, *IP*-адрес являются персональными данными. И странной выглядит ситуация, когда кто-то из надзорных органов или регуляторов занимает позицию, что номер телефона — это не персональные данные, а, например, всего лишь номер персонального устройства. В Европе такая позиция была бы невозможна, так как этот номер абонентского устройства принадлежит какому-то конкретному пользователю. При этом надо различать персональные и личные данные как часть персональных данных. Личные данные — это данные, принадлежащие определенной личности как социальному отражению индивида. Личность — это то, что формируется в процессе взаимодействия с обществом. Персональные данные кроме данных о личности включают еще и наши нативные характеристики, биологические, генетические и т.п.

**— Чтобы нащупать границы этого понятия, давайте уточним: рекламный звонок по моему телефону без моего согласия — это нарушение персональных данных, а если мне бросают рекламу в почтовый ящик — это разве не то же самое?**

— Разносчик рекламы по почтовым ящикам не знает, что этот ящик принадлежит именно вам, не знает, что именно вы живете в определенной квартире. С одной стороны, звонок сам по себе — это вторжение в личное пространство человека, что, конечно, является в некоторой степени вопросом субъективной оценки. С другой стороны, часто подобного рода звонки носят мошеннический характер и номер телефона может быть использован, чтобы записать образец вашего голоса, который в условиях технологий голосовой идентификации является ценнейшей информацией. Например, вам звонит автоинформатор, который просит отвечать на вопросы в форме «да» или «нет». Ваши ответы записываются, а потом запись используется для обхода систем биометрической идентификации в банках. Поэтому, отвечая на входящий звонок с неизвестного номера, лучше первым не заговаривать.

Выбор способа коммуникации с субъектом персональных данных имеет значение. В *GDPR* предусмотрен такой механизм, как *DPIA* (*Data Privacy Impact Assessment*), т.е., когда мы хотим использовать персональные данные для той или иной цели, мы должны заблаговременно продумать, какие риски это может нести для субъекта персональных данных, насколько будет соответствовать его разумным ожиданиям. Например, в рамках маркетинговых коммуникаций большинство людей преимущественно выбирают вариант связи посредством электронной почты и мало кто выберет связь по телефону. И многие раздражаются, когда компании звонят или используют номер телефона для коммуникаций в мессенджерах. У людей есть разумные ожидания в отношении коммуникации, и по статистике надзорных органов, наших и европейских, больше половины жалоб — это жалобы на маркетинговую коммуникацию.

**— Мы сами оставляем огромное количество данных о себе, выкладывая ролики в социальных сетях, которые, получается, можно использовать в нарушение наших интересов?**

— Действительно, чем больше материала, аудио-, видеороликов вы оставляете о себе в Сети, тем больше возможностей для создания соответствующих моделей, которые будут на очень хорошем уровне вас имитировать. Есть технология *Puppet Master* («Кукловод»), с помощью которой можно полностью создать иллюзию вашего лица и дать возможность другому человеку, используя видеосигнал, полностью подделать вас в видео. И тут опасно даже не то, что кто-то может разместить какой-то порочащий вас ролик с вашим лицом, а в большинстве случаев злоумышленники будут использовать такие технологии, чтобы обойти системы биометрической аутентификации (удостоверения личности).

**— Если с помощью технологий можно так качественно подделать видеоизображение человека, то, может быть, понятие компромата скоро станет неактуальным?**

— Данный вопрос обсуждается давно. Как только появилась фотография, появился фотомонтаж, фотошоп.

Вспомним, к примеру, истории с видеороликами с человеком, похожим на генерального прокурора, и т.п., в 90-х годах. Уже тогда говорили о том, что современная технология позволяет лицо одного человека «посадить» на лицо другого человека. Сейчас технологии очень быстро развиваются, порог получения доступа к продвинутым технологиям все ниже, и если сейчас создание качественных дипфейков еще достаточно дорого, то скоро этот процесс, думаю, станет проще и дешевле. Например, в Китае проблема создания и использования дипфейков уже регулируется. Это вопрос права на личность.

**— Наши данные уже широко распространены в Сети: записи лекций, фотографии, видеоролики. Мы знаем о рисках, а регулирования соответствующего нет, притом что само государство интенсивно внедряет технологии идентификации, например с помощью биометрических данных. Почему, на Ваш взгляд, не развивается соответствующее регулирование?**

— Обычно в начале развиваются технологии, в данном случае технологии создания дипфейков. Потом в отношении этой технологии складываются определенные общественные отношения, которые могут иметь явные признаки общественной опасности. После чего появляется адекватное правовое регулирование, когда государство начинает, например, требовать обозначения материалов, созданных с помощью такой технологии, указанием, что это дипфейк. При этом использование изображения другого человека также должно регулироваться. И создание дипфейков без таких меток станет административным правонарушением как минимум.

**— Получается, что само государство интенсивно внедряет эти технологии вне регулирования?**

— Редко бывает обратный порядок, когда в начале появляется регулирование, а потом технология. Пока само явление и его масштаб не вызывают общественного резонанса. Десять лет назад мало кто знал закон о персональных данных, мало кто специализировался в этой сфере, а сейчас с персональными данными сталкиваются все, в связи с чем к этой сфере очень повысилось внимание. Сами персональные данные появились, конечно, не в 2006 году, они всегда существовали, но регулирование появилось только тогда, когда существующие возможности, которые были на рубеже 60–70-х годах прошлого века, уже позволяли получать огромную власть и возможности через автоматизированную, а потом и автоматическую обработку данных. И самое потенциально опасное для обладателя персональных данных состоит не в самом объеме данных, которые о нем могут собрать и систематизировать, а в возможности выявления тех знаний о нас и моделей нашего поведения тем, кто сможет соответствующим образом наши данные обработать. Есть данные достоверные и актуальные, а есть данные предполагаемого характера, о нашем предполагаемом поведении в той или иной ситуации, например данные о прогнозе развития болезни, информация о его привычках, образе жизни, частоте полетов на самолете и т.п. Такая предиктивная аналитика позволит управлять нашим с вами поведением, поскольку, используя подобные технологии и понимая, как устроено поведение человека, можно непосредственно влиять на него.

**— Как защитить персональные данные от самого государства?**

— Сам по себе правовой институт защиты персональных данных появился как ответ на социальные волнения, произошедшие в Европе в 60-х годах XX века, и реакцию правительств, в том числе и в Европе, которые очень серьезно усилили роль спецслужб. Европейский союз в 60–70-е годы только как поколение назад прошел через опыт оккупации в ходе Второй мировой войны, когда данные архивов использовались, чтобы выявлять людей еврейской и других национальностей[4]. Местное население испугалось, что усиление роли спецслужб угрожает демократическому обществу и что накопление данных о гражданах может быть использовано против них самих.

**— Эти опасения сегодня только усилились.**

— Тогда технологии обработки информации были в начале развития, достаточно быстро в 80-е годы в аккумулировании и создании массивов персональных данных стала расти роль бизнеса и особенно транснациональных корпораций, возможности которых стали превосходить возможности государств.

**— Но у этих корпораций все же нет политической власти.**

— Да, но у них есть мягкая власть, *soft power*, и есть много исследований, которые подтверждают, что эти корпо-

[4] См., напр.: Нюрнбергские расовые законы от 1935 года.

рации воздействуют на людей и их мнение, в частности в рамках избирательных кампаний.

Понятно, что государства не откажутся от технологии, например биометрической идентификации/аутентификации. Однако в Европейском союзе идет работа по ограничению использования технологий распознавания лиц и о запрете использования технологий искусственного интеллекта для этой цели.

**— Может, это разумно?**

— Каждое общество выбирает свой путь. С одной стороны, разумно, когда мы говорим, что каждый имеет право на приватность и безопасное выражение своей общественной позиции. С другой стороны, здесь проходит тонкая грань, ведь на общественных мероприятиях и политических акциях могут быть провокаторы, например как во время манифестаций «желтых жилетов» во Франции. Поэтому в реальности большинство государств, хотя бы нелегально, не откажутся от использования этих технологий.

**— При таком обширном характере распространения наших персональных данных насколько мы реально можем обеспечить их безопасность?**

— Под защитой персональных данных надо понимать не столько техническую защиту, сколько применение мер по соблюдению принципов обработки данных. Например, в рамках соблюдения права на частную жизнь вы имеете право запрещать доступ чужим лицам к частной информации и защищать это право посредством обращения в суд и правоохранительные органы при его нарушении, т.е. в данном случае используется метод запрета. А есть институт защиты персональных данных *(data protection)*, в соответствии с которым применяется следующий подход: ваше право на личную и семейную жизнь и информационную приватность признается, но без обработки ваших персональных данных функционирование современного общества и экономики невозможно. Поэтому вы даете согласие обрабатывать ваши данные, но с соблюдением определенных принципов: законности, справедливости, пропорциональности, соблюдения цели обработки и т.д. Дьявол, конечно, кроется в деталях. У нас в стране инструментарий пока недостаточно развит для соблюдения этого подхода. В Европе государство не диктует, как тебе технически защищать персональные данные, а предоставляет право выбора способов соблюдения установленных принципов. Но если что-то пойдет не так, то применяется оборотный штраф. У нас традиционно все более бюрократизировано. Если в Европе больше смотрят на содержание мер защиты персональных данных, то в России больше смотрят на форму. В конце прошлого года у нас была утечка данных в одной очень крупной компании, ей выписали штраф в размере 30 000 рублей. Естественно, в такой ситуации никакого экономического стимула защищать персональные данные не возникает. Например, в Китае был принят закон, который позволяет государству противодействовать утечкам данных, их противоправному раскрытию, также посредством установления оборотного штрафа до 5%. И должностные лица, которые персонально ответственны за утечку, фактически получают волчий билет от государства — они могут попрощаться со своей карьерой. Я думаю, что надо изменить меры ответственности и акцентировать внимание на компании, которая допустила утечку, нужно стигматизировать именно ее, обязывая указывать информацию о том, что компания допустила утечку персональных данных. Или вносить такие компании в специальный реестр нарушителей, т.е. воздействовать на них не только финансово, но и через репутационные риски.

**— Хватит ли у нас мощностей в масштабах страны, учитывая количество компаний, ресурсов, чтобы контролировать и расследовать факты таких утечек?**

— Утечка утечкам рознь. Например, с этого года должна быть запущена система выявления утечек баз с персональными данными, работа в эту сторону идет. Безусловно, учитывая, что у нас несколько миллионов субъектов малого и среднего бизнеса, это непростая проблема, но в данной ситуации нам требуется дифференцированное регулирование. Если большая компания может нанять и консультанта, и технические условия обеспечить, то малому бизнесу это не по карману. В Европе, например, есть поблажки для малого бизнеса. В Германии в компаниях с менее чем 20 сотрудниками можно не назначать отдельное лицо, ответственное за защиту персональных данных *(Data Protection Officer)*. Считается, что даже если утечка или иное нарушение безопасности обработки персональных данных произойдет в таких компаниях, то это не создаст такого общественного резонанса, как в огромных корпорациях.

**— Как быть с депривацией персональных данных, когда они обрабатываются без нашего согласия**

**и создаются новые данные о нас, а мы об этом не знаем? Нужно ли запретить такую обработку или регулировать ее особым образом?**

— Данная проблема возникает в результате того, что мы взаимодействуем с огромным количеством сервисов и компаний, которым нужны наши персональные данные. С одной стороны, закон дает возможность запрашивать у любой компании подтверждение факта обработки ваших персональных данных с выяснением, какие данные, с какими целями обрабатываются, кому передавались. С другой стороны, какого-то тотального и полного контроля возможности управлять этими данными у субъекта нет. Следует сразу определиться, что полная и абсолютная приватность — это миф. Например, вы оплатили в интернет-магазине товар, а после этого просите магазин уничтожить ваши персональные данные. В этом случае вы получите ответ, что все данные уничтожить невозможно, потому что есть обязательства в соответствии с правилами бухгалтерского и налогового учета хранить определенную информацию о покупателях. Поэтому абсолютизировать право на информационную приватность не стоит — могут быть нарушены права и интересы других лиц, например интересы компании на ведение деятельности законным способом. Другой вопрос, что сейчас много разговоров о создании неких систем, через которые субъект может давать разрешения на обработку своих персональных данных всем заинтересованным лицам. Например, предлагается использование государственной ЕСИА[5] для целей получения гражданами РФ сервисов и услуг в Интернете. Покупая что-то в интернет-магазине, вы в нем регистрируетесь через учетную запись ЕСИА и предоставляете возможность магазину получить ваши данные. Учитывая, что наши с вами действия и действия в отношении нас с вами порождают новые данные, создание некоего единого хранилища персональных данных проблему защиты данных не решит, потому что фактически данные появляются не в этой системе, а являются результатом кропотливой работы по их сбору и аналитике.

Есть другие аспекты использования персональных данных. Например, возникает вопрос, можно ли платить своими персональными данными за те или иные услуги и товары. С одной стороны, есть европейский подход, согласно которому персональные данные не могут быть товаром. Человек не может отказаться от своего естественного права на защиту собственных персональных данных, и любая сделка об обратном будет ничтожна. С другой стороны, у любого субъекта есть право на управление своими персональными данными и распоряжение ими. В рамках европейских норм и судебной практики транслируется устоявшаяся позиция, что в принципе субъект может заплатить своим согласием на обработку персональных данных той или иной компании, если он получает в качестве встречного предоставления какие-то блага, например бесплатное участие в лотерее, возможность скачать бесплатно приложение, которым можно пользоваться при условии предоставления организации — собственнику приложения возможности отслеживать геолокацию такого субъекта. Согласие можно в любой момент отозвать, но при этом будет утрачена возможность пользоваться этим сервисом. Вопрос гражданского оборота персональных данных очень дискуссионный, и в ближайшее время дискуссия будет продолжаться.

**— Если обеспечить контроль за своими персональными данными и их защиту так сложно, может, надо искать иные инструменты идентификации человека для совершения юридически значимых действий? Может быть, ввести какие-то персонифицированные чипы?**

— Я считаю, что это решение не найдет поддержки в обществе. Всегда будут люди, которые против использования каких-то технологических новшеств. К тому же, на мой взгляд, использование таких инструментов не соответствует демократическим принципам общественного устройства.

> Скорее, зная о проблеме обработки персональных данных, люди станут внимательнее относиться к ним и соблюдать так называемую информационную гигиену.

Например, среди молодых людей все чаще становится популярным не иметь собственные аккаунты в социальных сетях и минимизировать информацию о себе в Сети. Они создают небольшие виртуальные площадки, на которых общаются. Возможно, в ближайшее время вернется интерес к интернет-форумам или чему-то похожему, но на новом технологическом уровне, а социальные сети все больше и больше будут ограничиваться регулированием.

[5] Единая система идентификации и аутентификации.

**— Создает ли использование *QR*-кодов в рамках борьбы с распространением коронавирусной инфекции угрозу безопасности персональным данным?**

— Один из чиновников Роскомнадзора по Санкт-Петербургскому управлению заявил, что это вообще не персональные данные. К сожалению, в целях достижения текущих целей государство может либерально подходить к толкованию содержания персональных данных, считая, что номер телефона и *QR*-код не являются персональными данными, хотя *QR*-код может содержать в кодированном виде и инициалы, и паспортные данные человека. В ЕС даже сомнений бы не возникло, что это, конечно, персональные данные. Сама по себе технология создания и использование *QR*-кодов, посредством которых можно получить информацию о том, что его предъявитель вакцинирован или переболел, хорошая, но то, как часто ее используют и как трактуют, вызывает определенную озабоченность. Непоследовательность в этом вопросе создает много проблем в правоприменении. Даже безотносительно того, насколько подходы соответствуют мировой практике, хочется просто стабильного правоприменения.

**— Не идем ли мы в данном случае по китайскому пути?**

— Да, в Китае есть система социального рейтинга, причем она имеет двойную природу. Одна система касается физических лиц, другая — юридических. И последняя вызывает даже большую обеспокоенность международных компаний, которые работают на китайском рынке. Но модель Китая в целом специфичная, связанная с культурным кодом, своими представлениями о демократии, правах человека, построении общества и государства. В то же время мы в целом находимся в эпохе цифрового огораживания, национализации данных, когда все крупные страны пытаются оградить персональные данные граждан от конкурентов. В России приняты Закон о локализации персональных данных[6], «пакет Яровой»[7] и другие меры, которые приводят к повышению издержек бизнеса в связи с обработкой и хранением персональных данных. Но такие акты есть не только у нас. Гораздо раньше подобное регулирование появилось, например, в Германии. В 2020 г. Европейским судом было принято решение по делу Максимилиана Шремса *(Max Schrems)*[8], которое как раз очень существенно ограничило право передачи персональных данных из Европы в США в связи с негативной оценкой американского законодательства в части возможности слежки за гражданами и получения данных о них. После этого решения европейский бизнес, который в основном использовал американские системы, приложения для обработки персональных данных и аналитики, получил неофициальные рекомендации пользоваться отечественными платформами, провайдерами и т.п. Прямой запрет не установили, но были созданы все условия, чтобы максимально ограничить использование европейским бизнесом зарубежных сервисов, в первую очередь сервисов США, так как этот рынок составляет около 1 трлн евро в год.

**— Мы же не можем полностью избежать того, чтобы не передавать свои персональные данные за рубеж, и не можем полностью контролировать процесс их обработки. В чем тогда цель защиты персональных данных?**

— Никто и не призывает это делать. Вопрос состоит в возможности контроля за объемом передачи данных и их использования. Вопрос защиты персональных данных, информационной приватности — это именно тот элемент, который склоняет чашу весов в сторону защиты более слабого субъекта: работник — работодатель, потребитель — производитель. И, на мой взгляд, такой подход будет усиливаться. Сейчас в публичном поле РФ обсуждается законопроект о регулировании рекомендательных сервисов. Это аналитические алгоритмы, которые анализируют ваше поведение и предлагают вам приобрести тот или иной товар или услугу. И есть существенный риск или угроза, что через данные сервисы можно регулировать ваше поведение. Например, эти алгоритмы используются в социальных

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

[7] Федеральный закон от 06.07.2016 № 374-ФЗ «О внесении изменений в Федеральный закон „О противодействии терроризму“ и отдельные законодательные акты Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности»; Федеральный закон от 06.07.2016 № 375-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и Уголовно-процессуальный кодекс Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности».

[8] URL: https://curia.europa.eu/juris/document/document.jsf?docid=228677&doclang=EN (дата обращения: 15.03.2022).

сетях, когда в зависимости от сети друзей, высказываний и предпочтений людей пользователю предлагается информация и построение сети контактов исходя из его взглядов. Таким образом при помощи алгоритмов люди разводятся по своим идейным нишам, варятся в своем бульоне, они не учатся взаимодействовать друг с другом и с людьми отличающихся взглядов. Другой пример применения подобных технологий — дело «Кембридж Аналитики»[9], которую обвиняли уже в более жестком манипулировании, когда аудитории подаются только определенные новости, фейк-ньюз. Когда мы говорим о потребительском поведении, то существует много разных способов подсунуть вам любой товар, привлечь ваше внимание. Собственно, то, как эти рекомендательные сервисы выстраивают свои алгоритмы, почему они решают вам показать то или иное сообщение сейчас или в другой момент времени — это большая коммерческая тайна. Но нужно, чтобы такие данные раскрывались, чтобы не допускалось манипулирование поведением потребителей. Например, у любого крупного банка достаточно информации о человеке, чтобы стимулировать его совершить определенную крупную покупку, приводить в правильное расположение духа. Потенциал у этих технологий огромный.

**— Насколько безопасно расширение применения технологий с использованием биометрических данных человека?**

— Сейчас обработка биометрических данных начала регулироваться в рамках Закона № 479[10]. Этот Закон фактически открыл новую главу в регулировании обработки биометрических данных, которая сейчас у нас серьезно ограничена. Только очень крупные организации, *IT*-компании смогут позволить себе обрабатывать биометрические данные с соблюдением всех новых требований. Государство четко разделило биометрию для целей идентификации (установление, определение личности) и аутентификации (удостоверение личности). Теперь регулируется процесс сбора и создания библиотек биометрических данных, но в Законе большое количество пробелов, например в Единой биометрической системе (ЕБС) предусмотрено хранение информации только о лице и голосе. Притом что есть и другие биометрические персональные данные, статические (например, генотип, отпечатки пальцев) и динамические (походка, голос). Еще одна из самых больших проблем в том, что у нас не регулируются некоторые вопросы, например точность применяемой технологии. Что делать, если происходит положительное срабатывание в несоответствующем случае (ложноположительное срабатывание, когда система принимает одно лицо за другое) или, наоборот, система не может распознать человека? А это создает затруднения и для внедрения технологий, и для доверия к результатам использования этих технологий с юридической точки зрения.

**— Вы организовали *Russian Privacy Professionals Association* — Сообщество профессионалов в области приватности. Расскажите о нем, пожалуйста. В чем цель его создания?**

— Наше сообщество существует больше двух лет, объединяет около 750 участников — физических лиц. Бóльшая часть из них — это корпоративные юристы, также много коллег, которые являются консультантами в области защиты персональных данных, сотрудниками Роскомнадзора, коллеги из академической сферы. Мы защищаем в первую очередь интересы профессионалов, понимаем трудности бизнеса, консультантов, проблемы защиты персональных данных. В последние полтора года мы активно проводим мероприятия информационного, просветительского характера, семинары, конференции. В прошлом году у нас была большая международная конференция «Евразийский конгресс по защите данных», в которой участвовали представители из разных стран, например руководитель Европейского инспектора по защите данных. Также мы являемся сообществом, которое уже два года подряд выбирает и награждает компании и физических лиц, которые смогли проявить себя на поле защиты персональных данных, в рамках премии *Russian Privacy Awards*. Основная цель сообщества — построение взаимодействия между профессионалами, так как мы работаем в непрозрачной и непредсказуемой регуляторной среде. В рамках сообщества мы общаемся, обмениваемся опытом, информацией, принимаем участие в законотворческой деятельности. Мы считаем, что развитие данной отрасли и регулирование персональных данных должны идти по пути человекоцентричности, постановки во главу угла прав и законных интересов человека.

---

[9] *Громов А.* Как Cambridge Analytica «взламывала выборы» по всему миру https://tass.ru/mezhdunarodnaya-panorama/5048632 // ТАСС. 2018. 5 апр. (дата обращения: 15.03.2022 ).

[10] Федеральный закон от 29.12.2020 № 479-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации».

**НИКОЛАЙ АНДРЕЕВИЧ ДМИТРИК**

заведующий лабораторией правовой информатики и кибернетики юридического факультета МГУ имени М.В. Ломоносова, доцент факультета права Национального исследовательского университета «Высшая школа экономики», кандидат юридических наук

# ЛЮДИ В СВОЕМ ПРАВЕ: ОТ ПРАВОСПОСОБНОСТИ К ИДЕНТИЧНОСТИ И ОБРАТНО

Статья завершает тему источников правового регулирования в киберпространстве, начатую в работах «Государства в своем праве» и «Корпорации в своем праве». В статье проводится необходимая после появления киберпространства актуализация представлений о таких базовых для права понятиях, как правоспособность и правосознание, правосубъектность и правопорядок. Основная проблема, рассматриваемая в исследовании, — проблема идентичности субъекта (тождества его самому себе в рамках правоотношения и правопорядка). Идентичность при этом рассматривается и как условие, и как результат правового регулирования. По результатам исследования обосновывается право на идентичность как один из элементов цифрового гражданства.

***Ключевые слова**: идентичность субъекта права, первоначальные и производные субъекты права, искусственные субъекты права, правоспособность, правосознание, цифровое гражданство*

DOI: 10.37239/0869-4400-2022-18-3-16-32

## 1. Проблема идентичности в киберпространстве

В киберпространстве намного чаще, чем в офлайновых отношениях, одно и то же лицо становится участником отношений, урегулированных разными правопорядками (законами разных государств, правилами разных транснациональных компаний). Если в офлайне это, скорее, исключение, то в киберпространстве

это, скорее, правило. В киберпространстве, как и в офлайне, статус субъекта не перетекает автоматически из одних отношений в другие: в каких-то случаях можно говорить об идентичности субъекта в разных отношениях (например, когда важно, что лицо, от которого пришла оплата за билет, и лицо, на которое выписан билет, — это одно и то же лицо), в каких-то случаях — нет (когда рекламный модуль на сайте, где заказывают билеты, не имеет доступа к фамилии и имени пассажира). Эта ситуация нормальна для гражданского оборота, но нежелательна с точки зрения технологий обработки данных (технологий профайлирования, агрегирования, Больших данных), которые требуют сквозной идентификации субъекта для повышения ценности накопленных о нем данных.

В киберпространстве его участники имеют дело не с материальными сущностями — субъектами или объектами, а с записями о них в документах или информационных системах, т.е. с так называемыми цифровыми двойниками или цифровыми тенями. «Цифровая тень, которую физический объект „отбрасывает в виртуальное пространство“, — это набор данных, получаемых с датчиков, и модель, которая позволяет прогнозировать свойства объекта в определенных пределах»[1]. В ситуации, когда право начинает иметь дело не с реальными субъектами и объектами, а с записями о них, позволяющими моделировать поведение объекта, требует переосмысления вся структура правоотношения. Как минимум нам нужно понимать, как и по каким принципам можно объединять такие записи.

Базовые процессы киберпространства как раз таки связаны с объединением записей (или невозможностью такого объединения), что, в свою очередь, предопределяется решением вопроса об идентичности (тождестве самому себе) объекта или субъекта, к которому относится запись:

— *объединение* данных о лице из самых разных сфер отношений — профайлирование — является основой технологии Больших данных и в целом основой современного цифрового уклада;

— *запрет* такого объединения, напротив, является краеугольным камнем законодательства о персональных данных, запрещающего обработку данных в несовместимых целях;

— *фактическая* возможность объединения данных о лице из разных сфер отношений представляет собой концентрацию доступа к информации, которая выступает главным риском киберпространства, поскольку способствует его монополизации и превращению в «сингулярность» в рамках той или иной экосистемы, метавселенной и т.п.

> Поскольку настоящее исследование посвящено правовым вопросам, т.е. возможности регулирования определенных отношений определенным образом, его главный тезис можно сформулировать так: идентичность субъекта (другими словами, возможность или невозможность сделать вывод о том, что субъект в разных правоотношениях — это одно и то же лицо) влияет на саму возможность правового регулирования отношений в киберпространстве.

Нужно сразу предупредить, что настоящая работа носит теоретико-правовой или даже философско-правовой характер. Это вызвано тем, что появление киберпространства как новой сферы общественного взаимодействия и обсуждение вызванной этим проблемы идентичности субъекта требует возврата к вопросам, которые очень много лет были неактуальны, а именно о субъектности (правосубъектности) и источнике правовых норм (суверене). Иначе говоря, перед кем и в отношении чего можно ставить вопрос об идентичности субъекта в рамках разных правоотношений[2].

## 2. От правоспособности к правосознанию

Философ И.А. Ильин уже более ста лет напоминает нам, что «право создается человеком и распространяется только на людей»[3]. Для понимания частно-

[1] *Прохоров А.*, *Коник Л.* Цифровая трансформация. Анализ, тренды, мировой опыт. М., 2019. С. 21–25.

[2] Здесь нужно еще раз оговорить, что эти вопросы не имеют практического смысла в реальных отношениях, когда люди взаимодействуют друг с другом напрямую, без использования технических средств, или, во всяком случае, когда речь не идет о взаимодействии с «цифровыми двойниками».

[3] *Ильин И.А.* Общее учение о праве и государстве // Собрание сочинений: в 10 т. Т. 4. М., 1994. С. 45.

правового регулирования важны обе части этого утверждения. Вроде бы они самоочевидны.

*«Право создается человеком»*. Этот тезис закреплен на конституционном уровне. В ст. 3 Конституции Российской Федерации говорится о том, что носителем суверенитета и единственным источником власти в Российской Федерации является ее многонациональный народ. Аналогичные нормы содержатся, например, в ст. 20 Основного закона Федеративной Республики Германия[4] и ст. 2 Конституции Китайской Народной Республики[5]. Но в новых работах по автоматизации права можно найти предложения о создании права машинами: «Существенная часть норм права может быть автоматизирована… Автоматизация права предполагает возможность создания, интерпретации и исполнения норм в автоматическом режиме с помощью информационных технологий»[6]. В Средневековье считалось, что право имеет своим источником волю божества и является выражением вечного закона *(lex aeterna)*, имманентного божественной Сущности как таковой[7]. Развитие науки социобиологии, пройдя через этап социального дарвинизма, на котором биологические законы используются для объяснения социальных процессов (что прослеживается в концепциях Г. Тарда, Л. Уорда, Ф. Гиддингса, Э. Дюркгейма), сейчас переходит к этапу переноса представлений о человеческом обществе на социальных животных, допуская создание такими животными неких правил поведения[8]. Получается право, пусть и теоретически, могут создавать машины (искусственный интеллект), божество (или инопланетяне), животные?

«*Право распространяется только на людей*». Ильин сам считал этот тезис нуждающимся в некотором обосновании и писал в том же абзаце: «По общему правилу, правоспособным, т.е. субъектом права, может быть только человек. Ни вещи, ни животные не могут иметь ни полномочий, ни запретностей, ни обязанностей. Признавать дерево собственником, судить животных за преступления (как бывало в средние века), наказывать за ослушание стихии природы (Ксеркс бичевал море), — является, с точки зрения современного просвещенного правосознания, нелепым»[9]. С точки зрения просвещенного правосознания век спустя животных все же следует в некоторых случаях признавать имеющими права, например: не удерживаться и не использоваться в противоправных целях; не претерпевать вред; получать заботу; иметь жизненное пространство; быть в надлежащем владении; владеть имуществом; быть стороной договоров; заявлять деликтные требования[10]. Тема «субъектности» искусственного интеллекта еще более актуальная, поскольку она так или иначе затрагивается в сотнях, если не тысячах работ на правовую тематику ежегодно[11]. Исследующие тематику «искусственный интеллект как субъект права» авторы часто придерживаются консервативной позиции, делая вывод о том, что искусственный интеллект — это объект права. Но иногда вывод бывает и осторожно противоположным: искусственному интеллекту предлагается придать статус, аналогичный животному, юридическому лицу, человеку либо создать для него совершенно новый субъектный статус[12].

---

[4] Основной закон Федеративной Республики Германия от 23.05.1949. Текст приводится по сборнику Конституции зарубежных государств: учеб. пособие / сост. проф. В.В. Маклаков. 4-е изд., перераб. и доп. М., 2003.

[5] Конституция КНР (в редакции 2018 г.) URL: https://chinalaw.center/constitutional_law/china_constitution_revised_2018_russian/ (дата обращения: 22.03.2022).

[6] *Вашкевич А.М.* Автоматизация права: право как электричество. М., 2019. С. 16.

[7] См.: *Гессен В.М.* Основы конституционного права. 2-е изд. Пг., 1918. С. 28.

[8] Обзор таких теорий см.: *Парфёнов А.И.* Социальные отношения животных в свете социобиологии // Известия Саратовского университета. 2009. Т. 9. Серия философия, психология, педагогика. Вып. 3. С. 41–47.

[9] *Ильин И.А.* Указ. соч. С. 45.

[10] См.: *Афанасьева Е.Г.*, *Афанасьева Е.А.* Животные — объекты или субъекты права? (Обзор) // Социальные и гуманитарные науки. Отечественная и зарубежная литература. Серия 4: Государство и право. 2019. № 2. С. 107–116. URL: https://cyberleninka.ru/article/n/2019-02-027-e-g-afanasieva-e-a-afanasieva-zhivotnye-obekty-ili-subekty-prava-obzor (дата обращения: 22.03.2022). В данной работе приводится подробный обзор европейской доктрины и положений законодательства, признающих некоторых животных «не просто имуществом».

[11] Поиск по названию статьи «Искусственный интеллект как субъект права» в научной электронной библиотеке *elibrary.ru* по состоянию на конец 2021 года возвращает более 26 тыс. работ. В отношении такого массива данных возможен лишь статистический, а не сущностной анализ.

[12] Обзор теорий см.: *Архипов В.В.*, *Бакуменко В.В.*, *Волынец А.Д. и др.* Регулирование робототехники: введение в «робоправо». Правовые аспекты развития робототехники и технологий искусственного интеллекта / под ред. А.В. Незнамова. М., 2018.

Для И.А. Ильина была очевидна связь двух частей его высказывания: право нужно только человеку, поэтому только человек его создает. Приводя пример со статусом рабов в Древнем Риме, он писал: «…признать человека *совсем неправоспособным*, значит окончательно снять с него все правовые позволения, воспрещения и повеления и оставить его жизнь и его действия *вне подчинения правовым нормам* <…> в обществе людей, живущих в подчинении праву, *всякий живой человек является правоспособным*, хотя не всякий способен иметь все полномочия, запретности и обязанности»[13]. Практически дословно этот тезис закреплен в ст. 6 Всеобщей декларации прав человека: *Everyone has the right to recognition everywhere as a person before the law*[14] («Каждый, где бы он ни был, имеет право на признание его *персоной*[15] правом»).

> В понимании И.А. Ильина правоспособность — это присущая только человеку способность и создавать право, и подчиняться ему. Этот тезис был забыт впоследствии, но только он объясняет «магию» права. Это люди создают правила. Это люди, и в конечном счете только люди разумно руководствуются правилами как обязательными.

Впрочем, никакой магии, обычная обратная связь: люди создают правила, чтобы следовать им; нет практического смысла в правилах, которым не получится следовать. Впоследствии это единое понимание правоспособности распалось на два: правосознание как человеческая способность знать и оценивать правила, следовать им и создавать их[16] — и правоспособность как правосубъектность (т.е. как наша способность иметь права и нести обязанности[17]). Такое разделение подспудно ставит вопрос в том, что правила создают одни люди («суверен» — в терминологии некоторых ранних позитивистов, например Джона Остина[18]), а следовать им должны совсем другие. Ответом на это потенциальное возражение является интуитивное суждение: никто не может быть заведомо уверен, что ему не придется подчиниться тем правилам, которые он создает «для других»[19]. Любые правила предполагают, что создающие их люди собираются прежде всего сами руководствоваться ими. Это касается любых источников частного права, в том числе обычаев и норм международного права, а также договорных правил, в том числе правил, устанавливаемых многосторонними договорами.

## 3. От правосознания к правопорядку

Если расценивать правоспособность как признаваемую правом возможность иметь права и нести обязанности, то она ничем не отличается от других признаваемых правом возможностей (субъективных прав), хотя, наверное, и является первой среди равных. Но еще «первее» в этой ситуации оказывается правосубъектность, т.е. сам факт признания правом (сувереном) человека субъектом права, за чем следует наделение этого субъекта правоспособностью. Логическое утверждение следует тогда строить следующим образом: права и обязанности у человека возникают потому, что он признан субъектом права. Сначала возникает некое «первоправо», т.е. правоспособность, а затем уже и все остальные права.

---

[13] *Ильин И.А.* Указ. соч. С. 45–47.

[14] Universal declaration of human rights. United Nations official website. URL: https://www.un.org/en/about-us/universal-declaration-of-human-rights (дата обращения: 22.03.2022).

[15] Здесь необходимо уточнить термин *persona*. В официальном русском переводе статья изложена так: «Каждый человек, где бы он ни находился, имеет право на признание его правосубъектности». В то же время физическое лицо — это не человек, а правовая маска человека, лицо, личина. См. об этом: *Гаджиев Г.А.*, *Войниканис Е.А.* Может ли робот быть субъектом права (поиск правовых норм для регулирования цифровой экономики)? // Право. Журнал Высшей школы экономики. 2018. № 4. С. 24–48, 30–31.

[16] *Радько Т.Н.*, *Лазарев В.В.*, *Морозова Л.А.* Теория государства и права: учебник для бакалавров. М., 2014. С. 222–223.

[17] Статья 17 ГК РФ.

[18] *Austin J.* The Province of Jurisprudence Determined. 1832. URL: https://www.cambridge.org/core/books/austin-the-province-of-jurisprudence-determined (дата обращения: 23.03.2022).

[19] Назовем это «казусом Васильева» по фамилии выдающегося российского деятеля в области телекоммуникаций Е.С. Васильева. Будучи государственным служащим, он создавал отечественное законодательство о связи, а потом, став генеральным директором крупной телекоммуникационной компании, оказался вынужден соблюдать написанные им же правила. И не согласившись с некоторыми из них, даже оспорил в ВАС РФ. См.: Решение ВАС РФ от 23.04.2013 № ВАС-899/13. О судьбе Е.С. Васильева см.: https://www.iksmedia.ru/articles/4972586-Evgenij-VASILEV-Chelovek-dejstviya.html (дата обращения: 23.03.2022).

Такая логика рассуждений хороша в текущем моменте, но право не всегда было таким, как сейчас, и наверняка через какое-то время опять станет другим.

> Поэтому парадокс «что было раньше — право или субъект права» схож с парадоксом курицы и яйца. Субъекты права появились потому, что люди создали право. Люди всё время создают право, именно поэтому субъекты права могут быть самыми разными: животными, идолами, кораблями, деревьями, искусственным интеллектом. Неизменен только один субъект права — человек.

Проведем простой мысленный эксперимент. Можно назвать много примеров субъектов права, не обладающих качеством правоспособности: идолы[20], корабли[21], колокола[22], роботы[23]. Наделение этих сущностей статусом субъекта, по всей видимости, никак не нарушает гражданский оборот и может продолжаться достаточно долгое время, до второго пришествия. Но после второго пришествия люди утратят правоспособность, поскольку она перейдет к Сыну Божьему[24]. Будут ли по-прежнему после второго пришествия субъектами права идолы, корабли, колокол и роботы? Вероятно, нет, поскольку они не смогут быть субъектами права в отсутствие людей, которые признают их в таком качестве.

Мы не можем исключать, что в мире есть еще какие-то существа, которые создают для себя «правила» и следуют им. Это могут быть животные, грибы, инопланетяне — если они существуют. Вопрос в том, что ни мы, люди, не сможем следовать их правилам, ни они не смогут следовать нашим. Право — это достояние человечества, и только его. Научным объяснением этому обстоятельству является то, что структуры рациональности всех тех, кто, возможно, тоже обладает сознанием, отличаются от структуры рациональности человека. Обсуждение и обоснование данного тезиса в философии сознания происходит по примерно следующей схеме.

Во-первых, право имеет смысл только для тех, у кого есть сознание. Для роботов, крабов или зомби нет права в объективном смысле (хотя могут быть команды): просто потому, что у всех этих сущностей нет той совокупности признаков, которые понимаются как сознание.

Во-вторых, наличие права предполагает не просто сознание, а рациональность, т.е. способность следовать аргументам. Джон Сёрль коротко излагает эти постулаты следующим образом: «…рациональное принятие решений заключается в выборе средств, которые позволят нам достигнуть нашей цели. Цели — это не что иное, как наши желания. Мы подходим к принятию решения с заранее намеченной целью, а рациональность выступает как инструмент, позволяющий нам находить средства для достижения этой цели»[25]. Такая модель рациональности практически без изменений воспроизводится в советских работах по гражданскому праву, например у В.П. Грибанова: «…потребность составляет содержание интереса. Форма же, в которой эта потребность проявляется в деятельности, в поведении людей, может быть различной, но она всегда выражает определенную целенаправленность их действий»[26].

В-третьих, право предполагает свободу воли. Конечно, при рассмотрении проблемы свободы воли «нам придется столкнуться с самым запутанным, с самым сложным вопросом из всех тех, которые когда-либо

---

[20] По индуистскому праву они могут быть наследниками имущества и осуществлять свои права на него, в том числе в суде. См.: Bombay High Court: Pramatha Nath Mullick vs Pradyumna Kumar Mullick on 28 April, 1925. L.R. 52, Ind. App. 252.

[21] В американской судебной практике корабли могли наделяться статусом, аналогичным статусу юридического лица. См.: U.S. Supreme Court. Tucker v. Alexandroff, 183 U.S. 424 (1902). Tucker v. Alexandroff. No. 303. January 6, 1902. 183 U.S. 424.

[22] «Колоколъ этотъ былъ наказанъ „за доносъ“ кнутомъ и съ вырваннымъ ухомъ отправленъ въ Сибирь, раздѣливъ такимъ образомъ, участь двухсотъ угличанъ, пострадавшихъ по тому жѳ дѣлу отъ Бориса Годунова» (Ссыльный колокол // Исторический вестник. 1888. Т. 34. № 10. С. 255–256).

[23] В Резолюции Европарламента от 16.02.2017 предлагалось исследовать вопрос наделения в перспективе роботов особым правовым статусом. См.: Civil Law Rules on Robotics, European Parliament resolution of 16 February 2017 with recommendations to the Commission on Civil Law Rules on Robotics (2015/2103(INL).

[24] «…Καὶ ἐξουσίαν ἔδωκεν αὐτῷ κρίσιν ποιεῖν ὅτι υἱὸς ἀνθρώπου ἐστίν» — «…И дал Ему власть производить и суд, потому что Он есть Сын Человеческий» (от Иоанна 5:27).

[25] Цит. по: *Сёрль Дж.* Рациональность в действии / пер. с англ. А. Колодия, Е. Румянцевой. М., 2004. С. 16.

[26] *Грибанов В.П.* Интерес в гражданском праве // Советское государство и право. М., 1967. № 1. С. 49–56, 52.

интересовали человеческую мысль»[27]. Но тем не менее, как пишет А.Э. Ковров, «можно сколько угодно говорить, что свободы воли не существует, но это не избавит меня от необходимости принимать решения»[28].

> Несмотря на серьезную дискуссию между компатибилистами (утверждающими, что свобода воли совместима с детерминизмом)[29] и инкомпатибилистами (утверждающими, что в силу детерминизма люди не обладают свободой воли, необходимой для моральной ответственности)[30], право как феномен существует только при допущении свободы воли и связанной с нею ответственности[31]. Право заведомо не регулирует рефлекторную деятельность, где нет и не может быть свободы воли, а значит, и ответственности за эти рефлекторные действия.

Мы не можем не дышать, не расти, не питаться, не выделять. Не размножаться, если говорить о человечестве в целом. «Право, для того, чтобы создаваться и осуществляться, должно сознаваться людьми. Качество и свойства этого сознания могут быть различны — это может быть извращенное сознание, заполненное иллюзорными представлениями, это может быть и правильное, адекватное сознание. Следовательно, там, где есть право, там есть и сознание права»[32]. Право предполагает сознательное, рациональное, свободное подчинение созданным людьми правилам — это есть качество, присущее, как мы выяснили в результате мысленного эксперимента, только человеку.

Для целей дальнейшего исследования в настоящей работе те правила, которые созданы в некоторой общности людей и которым эта общность следует, мы будем рассматривать как правопорядок. Правопорядок может быть государственным (и в качестве производного от государственного — международным) или корпоративным (в том числе договорным) — в зависимости от общности, к которой он относится. Также мы будем исходить из того, что правопорядок должен содержать определенные элементы:

— правотворческий процесс (описывающий, кто и при каких условиях может создавать новые правила, признаваемые обязательными в рамках данного правопорядка; а также каким требованиям должны отвечать создаваемые правила);

— процесс рассмотрения споров (описывающий юрисдикцию, правила рассмотрения споров и правила выбора норм);

— правоприменительный процесс (описывающий условия и цели применения мер принуждения, правила выбора и обязанности лиц, которые могут применять меры принуждения, содержание мер ответственности)[33].

В государственных правопорядках эти элементы будут отражать три традиционные ветви власти, в остальных видах правопорядков эти элементы могут проявляться различным образом и в некоторых случаях использовать элементы государственного правопорядка (в частности, когда договорный правопорядок предполагает рассмотрение споров между сторонами по договору в суде того или иного государства).

Правопорядок может появиться из ниоткуда — в том смысле, что невозможно предугадать, откуда он появится: из применимого законодательства того или иного государства, из договора, из правил сообщества или даже из программного кода. Идея о том, что код есть право (*code is law*), была высказана в середине 1990-х годов Уильямом Митчел-

[27] *Виндельбанд В.* О свободе воли. М., 2000. С. 510.
[28] *Ковров А.Э.* Постановка вопроса о свободе воли // Вестник Московского университета. Серия 7. Философия. 2010. № 5. С. 35.
[29] См., напр.: *Taylor R.* Metaphysics. Englewood Cliffs: Prentice-Hall, 1974. 2nd ed.; *Ginet C.* On Action. Cambridge: Cambridge University Press, 1990; *Kane R.* The Significance of Free Will. N.Y.: Oxford University Press, 1996; *Mele A.* Free Will and Luck. N.Y.: Oxford University Press, 2006.
[30] Наиболее известный современный инкомпатибилист — Дерк Перебум. См.: *Pereboom D.* Determinism al Dente // Noûs. 1995. Vol. 29. No. 1. P. 21–45; *Idem.* Living without Free Will. Cambridge: Cambridge University Press, 2001.
[31] *Виндельбанд В.* Указ. соч. С. 513.
[32] *Вейнгольд Ю.Ю.* Право как социологическая категория. Фрунзе, 1962. С. 198–199.
[33] См. об элементах правопорядка: *Дворкин Р.* О правах всерьез. М., 2004. С. 6.

лом[34] и обрела всемирную популярность благодаря Лоуренсу Лессигу и его книге «Код и другие законы киберпространства» в 1999 году. В этой работе и ее второй редакции «Код 2.0» Лессиг обратил внимание на то, что код является средством государства и корпораций контролировать поведение пользователей киберпространства[35]. Сочетание права и кода также называют *lex informatica*[36]: «Если в правовом режиме содержание норм определяется законом и судебными решениями, в *lex informatica* правила поведения определяются техническими возможностями и практикой применения технологий»[37]. Автор термина *lex informatica* Джоэл Рейденберг рассматривал его как систему, параллельную «традиционному» праву[38] (его аргументация отражена в таблице).

**Отличия правового регулирования от *lex informatica* (по Рейденбергу)**

| Категории для сравнения | Правовое регулирование | *Lex informatica* |
|---|---|---|
| Что задает структуру регулирования | Законодательство | Архитектура информационных систем |
| Территориальные пределы | Территория | Сеть |
| Содержание | Положения нормативных актов и решения судов | Технические возможности, доступные пользователям |
| Источник | Государство | Технические специалисты |
| Правила, создаваемые пользователями системы | Договоры | Пользовательские настройки |
| Принудительное правоприменение | Судом | Автоматически, в том числе самостоятельно пользователем |

Но можно ли говорить о *lex informatica* как об элементе правопорядка? С одной стороны, да, поскольку компьютерный код — это такой же результат человеческой деятельности, как и правила, выраженные в законах или договорах. С другой стороны, как было показано выше, правило предполагает сознательное, рациональное и волевое следование ему, в то время как компьютерный код позволяет контролировать поведение, но не регулировать его. С этой точки зрения нет никаких оснований отказываться от традиционного понимания правоотношения как отношения волевого[39] — пусть и со всеми необходимыми уточнениями, касающимися отношений с участием недееспособных или деликтных обязательств[40]. Об этих уточнениях — важнейших для целей настоящего исследования — будет идти речь далее применительно к вопросу о связи идентичности и правоспособности.

Способность создавать формальные правила и разумно следовать им уникально связывает человека (разумеется, с оговоркой о человеческих коллективах, совместно создающих правила) и порождаемое им право. Только человек создает право, только человек следует праву. Это предопределяет познаваемость права как предел правового регулирования[41] и является воплощением принципа правовой определенности: люди должны понимать те требования, которым они должны подчиняться[42]. Правила могут дополняться самыми разными техническими средствами, повышающими их эффективность, пример этому — регулирование дорожного движения. Но технические средства сами по себе не могут создать правила: линия разметки на дороге, разделяющая встречные потоки, для инопланетян будет выглядеть как удобная осевая разметка, которая должна идти по центру их транспортного средства. Как они могут

[34] *Mitchell W.J.* City of bits: Space, Place and Infobahn. MIT Press. 1995.
[35] *Lessig L.* Code and other laws of cyberspace. N.Y., 1999. P. 6.
[36] *Reidenberg J.R.* Lex Informatica: The Formulation of Information Policy Rules through Technology // Tex. L. Rev. Vol. 76. No. 3. P. 553 (1997–1998). URL: https://ir.lawnet.fordham.edu/faculty_scholarship/42 (дата: обращения: 23.03.2022).
[37] *Войниканис Е.А.* Право интеллектуальной собственности в цифровую эпоху: парадигма баланса и гибкости. М., 2013. С. 54.
[38] *Reinderberg J.R.* Op. cit. P. 569.
[39] *Маркс К.* Капитал. Т. I. М., 1931. С. 41.
[40] См. дискуссию о волевом характере правоотношений по советскому гражданскому праву между С.Н. Братусем и О.С. Иоффе (*Братусь С.Н.* Юридические лица в советском гражданском праве (понятие, виды, государственные юридические лица) / Ученые труды ВИЮН Министерства юстиции СССР. М., 1947. Вып. XII. С. 10–33; *Иоффе О.С.* Правоотношение по советскому гражданскому праву. Ленинград, 1949).
[41] Данный вопрос обсуждался ранее в работе: *Дмитрик Н.А.* Пределы правового регулирования в цифровую эпоху // Информационное общество. 2018. № 3. С. 47–58.
[42] См.: *Покровский И.А.* Основные проблемы гражданского права. М., 2003. С. 91.

думать иначе, если они не читали наши правила дорожного движения?

Джоэл Рейденберг замысливал *lex informatica* как новый *Lex Mercatoria*, общие основные правила. «В эпоху сетевых и коммуникационных технологий участники, путешествующие по информационным инфраструктурам, сталкиваются с нестабильной и неопределенной средой, состоящей из множества законов, меняющихся национальных правил и противоречивых нормативных актов. Для информационной инфраструктуры основные правила по умолчанию так же важны для участников информационного общества, как *Lex Mercatoria* был для торговцев сотни лет назад»[43]. Нельзя не согласиться с постановкой задачи, однако предложенное решение — код как средство контроля — обречено на провал. Проблема здесь не только и не столько в том, что Рейденберг путает, говоря языком Кельзена, «правила бытия и правила долженствования»[44], а в том, что такой подход противоречит принципу правовой определенности.

## 4. От правопорядка к идентичности

Нельзя не заметить, что одного лишь правосознания недостаточно, чтобы породить правопорядок. Не породят правопорядок автоматически и разного рода технические методы: как ни проектируй архитектуру сетей, дорог, чего угодно, это все не будет работать, пока люди не захотят этим пользоваться[45].

> Чтобы правопорядки возникли и тем более сложились в систему в условиях их множественности, нужно, чтобы лица осознали (идентифицировали) себя и других участников отношений в качестве правосубъектных.

Лицо предполагается субъектом тогда, когда предполагается правоотношение, а для правоотношения нужно как минимум двое участников. Робинзон Крузо двадцать пять лет обустраивал свой остров в соответствии со своими представлениями о порядке, но правопорядок на острове возник только тогда, когда появился Пятница. Человечеству понадобилось много тысяч лет, чтобы во Всеобщей декларации прав человека появилась ст. 6 о праве каждого на признание его персоной правом. До этого в истории человечества можно было увидеть множество примеров, когда люди, обладающие правосознанием, не признавались правосубъектными: рабы[46], женщины[47], прошедшие через гражданскую казнь[48], «низшие расы»[49]. Можно найти и множество примеров обратного, когда неправоспособные сущности (например, колокол) признавались субъектами права. Поэтому говорить о том, что правосубъектность всегда следует из правосознания, все же нельзя. Справедливо это или нет, но любой правопорядок может так или иначе превращаться в *No Homers Club* (клуб не-Гомеров) из мультсериала, поскольку может по тому или иному основанию дискриминировать отдельных субъектов или, наоборот, предоставлять субъектность неправоспособным сущностям. Общество анонимных алкоголиков может распространять свои правила только на тех, кто хочет бросить пить, и это можно понять.

Поэтому связь между правосознанием и правосубъектностью менее однозначна и складывается из нескольких моментов. Во-первых, поскольку правила не могут существовать без тех, кто их создает, правосубъектность первоначально основывается на чьем-то правосознании: того, кто идентифицировал себя и других в качестве субъектов созданных им правил. Можно теоретически допустить, что кошка будет участником юридического лица, но несколько кошек никогда не смогут создать юридическое лицо, если среди них не будет ни одного человека[50].

---

[43] *Reinderberg J.R.* Op. cit. P. 554.

[44] См. дискуссию Г. Кельзена и О. Эрлиха: *Эрлих О.* Основоположение социологии права. СПб., 2011. С. 639.

[45] Хелен Ниссенбаум предлагает для этого термин «социотехничный» *(sociotechnical)*, т.е. технологический, но обеспеченный системой отношений по использованию этой технологии. См.: *Nissenbaum H.* Privacy in context: technology, policy and the integrity of social life. Stanford University Press, 2010. P. 4–6.

[46] См.: *Новицкий И.Б.* Основы римского гражданского права. М., 2007.

[47] См.: *Kelleher M.* „San-ts'ung ssu-te". In Taylor, Rodney L.; Choy, Howard Y.F. (eds.). The Illustrated Encyclopedia of Confucianism. 2 N-Z. N.Y.: The Rosen Publishing Group. P. 496.

[48] См.: Гражданская казнь в истории // Дилетант. 2016. 31 мая. URL: https://diletant.media/articles/29129441/ (дата обращения: 22.03.2022).

[49] См. статью «Нацистская расовая политика» в Википедии. URL: https://ru.wikipedia.org/wiki/Нацистская_расовая_политика (дата обращения: 23.02.2022).

[50] Слово «кошка» можно без потери смысла заменить на слова «робот», «искусственный интеллект», «киберфизическая система» и т.п.

Во-вторых, теперь есть прямое указание ст. 6 Всеобщей декларации прав человека и ст. 16 Международного пакта о гражданских и политических правах в отношении государств и создаваемых ими правопорядков, что человек должен признаваться персоной в рамках создаваемого государствами права. Так было не всегда, отныне всегда должно быть именно так, и в этом принципиальное значение данного положения: оно выступает своего рода минимальным требованием к связи между правосознанием и правосубъектностью человека, установленным в отношении государств как субъектов международного права.

В-третьих, можно осторожно говорить о своего рода презумпции правосубъектности в отношении всего, что взаимодействует с человеком и ведет себя при этом аналогично тому или иному субъекту частного права. *On the Internet nobody knows you're a dog* («В Интернете никто не знает, что ты собака») — этот тезис был выдвинут Питером Штайнером еще в 1993 году[51] и до сих пор остается актуальным[52]. В Интернете много искусственных (виртуальных) личностей, которые другие пользователи идентифицируют в качестве субъектов права и ведут себя с ними соответствующе[53]. Поскольку невозможно возложить на пользователей Интернета обязанности проверять правосубъектность всех контрагентов, единственный вариант — исходить из презумпции правосубъектности для таких сущностей, впрочем, опровержимой в установленном законом порядке[54].

Наконец, можно говорить о взаимосвязи коллективного правосознания и коллективной правосубъектности. Как уже неоднократно отмечалось выше, способность создавать формальные правила и разумно следовать им предполагает наличие некоторой общности, создающей правила и следующей им. Поэтому любые формы коллективов, создающие правила, будут правосубъектными как минимум в рамках создаваемого ими правопорядка[55]. Наиболее очевидный пример такого коллективного субъекта — государство. Это общность людей, создающая для себя формальные правила и следующие им. Государство само признает себя субъектом гражданского права, что для России зафиксировано в ст. 124 ГК РФ.

Таким образом, связь между правосознанием и правосубъектностью может быть непосредственной (когда правосознание субъекта влечет его правосубъектность) и опосредованной (когда правосубъектность у некоторой сущности возникает из правосознания других). По критерию связи между правосознанием и правосубъектностью все субъекты права могут быть разделены на первоначальные и производные. Первоначальными субъектами являются люди и создаваемые ими коллективные субъекты, обладающие индивидуальным или коллективным правосознанием и в силу этого правосубъектностью (государства, общины, цеха, университеты и т.п.). Из истории государства и права и из их текущего состояния, по-видимому, невозможно вывести каких-либо положений, делающих невозможным создание любых производных субъектов частного права. Однако применительно к производным субъектам важно понимать, что их существование и участие в частных правоотношениях невозможно без первоначальных субъектов частного права. «В отличие от физического лица, необходимой предпосылкой или условием возникновения юридического лица является сознательная волевая деятельность людей — органов государственной власти, определенной группы или одного дееспособного физического лица»[56].

[51] The New Yorker. July 5, 1993.

[52] *Morteza Vesali Naseh*. Person and personality in cyber space: a legal analysis of virtual identity // Masaryk University Journal of Law and Technology. 2016. Vol. 10. Iss. 1.

[53] Для таких субъектов психологами предложен термин «виртуальные коллективные субъекты». См.: *Козлова Н.С.* Коллективный субъект как среда проявления жизнедеятельности личности // Вестник Костромского государственного университета. Серия: Педагогика. Психология. Социокинетика. 2015. № 2. URL: https://cyberleninka.ru/article/n/kollektivnyy-subekt-kak-sreda-proyavleniya-zhiznedeyatelnosti-lichnosti (дата обращения: 23.03.2022).

[54] Похожий вывод применительно к юридическим лицам на анализе советской судебной практики делает Н.В. Козлова в работе «Понятие и сущность юридического лица» (М., 2003). Существует и небольшая современная судебная практика, в рамках которой перед судами стоял вопрос о правосубъектности в гражданско-правовом смысле того или иного виртуального субъекта. Во всех случаях суд, устанавливая отсутствие правосубъектности по смыслу ст. 17 и 48 ГК РФ, отказывал в иске. См.: апелляционные определения СК по гражданским делам Свердловского областного суда от 02.11.2016 по делу № 33-17985/2016; Московского городского суда от 14.12.2015 № 33-43803/15.

[55] См.: *Козлова Н.В.* Понятие и сущность юридического лица. М., 2003. С. 190–191.

[56] *Братусь С.Н.* Юридические лица в советском гражданском праве. М., 1947. С. 51.

Интересным внешним признаком, позволяющим разграничить первоначальных и производных субъектов права (как минимум в современном праве), является публично-правовая ответственность за насильственное прекращение их существования. Например, в российском Уголовном кодексе есть статьи, которые предусматривают ответственность за умышленное причинение смерти другому человеку (ст. 105) и насильственное изменение основ конституционного строя или нарушение территориальной целостности Российской Федерации (ст. 279 и 280). Нет и не может быть ответственности за умышленное прекращение существования юридического лица, как и любых других производных субъектов.

Прекращение существования субъектов неизбежное, но все же нежелательное событие для любого правопорядка. Это обусловлено все тем же принципом правовой определенности: субъекты, вступая в правоотношения с другими субъектами, рассчитывают на стабильность этих отношений и их завершение в результате достижения цели отношения, а не в результате проблем с их сторонами. Это, в свою очередь, вплотную подводит нас к вопросу об идентичности субъектов права и правоотношений.

> Если правосознание — это качество, с которым право ничего не может сделать (мы не можем запретить человеку и социальным общностям создавать правила или следовать им), то правосубъектность — статус субъекта в рамках правопорядка, который можно видоизменять в том числе в интересах повышения правовой определенности.

Мы уже установили, что минимальным требованием к правосубъектности является ее признание государством за каждым человеком. С одной стороны, это логично, так как вытекает из связи правосубъектности с правосознанием и тем обстоятельством, что человек — это первоначальный субъект в любом правопорядке. С другой стороны, качество правосознания проявляется не всеми людьми и не всегда. Почему же всем и всегда государство должно предоставить правосубъектность?

И.А. Ильин писал: «В обществе людей, живущих в подчинении праву, всякий живой человек является правоспособным, хотя не всякий способен иметь все полномочия, запретности и обязанности. Особое положение здесь занимают те люди, которых нельзя признать вполне разумными, сознательными существами; так, малолетние и душевнобольные не могут сознавать значения своих поступков, и поэтому право делает для них целый ряд исключений»[57]. Кроме того, человек не способен разумно следовать правилам, когда спит или когда находится под общим наркозом во время хирургической операции. Обладавший правосознанием человек может потерять возможность следовать правилам в результате травмы головного мозга или заболевания. Тем не менее ни в одном правопорядке такое отсутствие правосознания как качества конкретного человека не является основанием для утраты им правосубъектности. В российском гражданском праве для создания особого правового статуса таких лиц используется понятие дееспособности. В соответствии со ст. 21 ГК РФ это способность гражданина своими действиями приобретать и осуществлять гражданские права, создавать для себя гражданские обязанности и исполнять их. Она не может быть одинаковой у всех людей, поэтому в некоторых случаях «законодатель принимает во внимание физиологические особенности физического лица — его малолетний возраст и болезненное состояние психики. В этих случаях ограниченная или полная недееспособность физического лица восполняется дееспособностью родителей, усыновителей, опекунов и попечителей, что является юридическими гарантиями правосубъектности таких лиц»[58].

> Недееспособность — это способ сохранить правосубъектность фактически неправоспособного человека, настроив его правовой статус, создав для него исключение. Недееспособность не может быть правилом: если в результате какого-нибудь вируса все человечество вдруг превратится в зомби и потеряет способность разумно следовать правилам, право исчезнет.

---

[57] *Ильин И.А.* Указ. соч. С. 46.
[58] *Ермолаева Т.А.*, *Ананьева А.А.* Гражданская правосубъектность физических лиц: эволюция содержания // Lex Russica. 2019. № 12. С. 9–18.

По этой причине институт недееспособности не имеет смысла в отношении юридических лиц. Юридические лица, являясь по российскому гражданскому праву производными субъектами, всегда правосубъектны, поскольку правосубъектность — это главная цель их создания. Хотя Н.В. Козлова и С.Ю. Филиппова указывают на возможность неполной и ограниченной дееспособности юридических лиц[59], речь идет об особом правовом статусе (постоянном или временном) тех или иных юридических лиц, т.е. об особенностях их правосубъектности. Ограниченная или неполная дееспособность юридического лица по российскому законодательству возникает не из-за того, что юридическое лицо полностью или частично утрачивает фактическую возможность разумно следовать правилам, а в силу указания закона или предписания суда.

Признание субъектом должно быть постоянным. Любой правопорядок, как показывает нам пример с дееспособностью, создает механизмы, позволяющие сохранить статус субъекта права в течение всего срока всех правоотношений с его участием, — напомним, это вытекает из принципа правовой определенности. При этом характеристики той сущности, которая признается субъектом, могут меняться со временем. Человек из ребенка превращается во взрослого, затем стареет. У юридического лица меняются учредители и руководство. И граждане, и юридические лица могут поменять свое имя (наименование), адрес, сферу деятельности. Человек может изменить свою внешность и даже пол. Но это не помешает остаться тем же самым субъектом права. Это — идентичность субъекта права, особое требование, без которого функционирование частного права невозможно. Требование идентичности относится именно к субъектам права, объекты права могут утрачивать идентичность в результате, например, переработки или вообще определяться родовыми признаками.

Говоря об идентичности, можно иметь в виду две стороны этого явления. С одной стороны, это тождественность самому себе на протяжении времени. Вопрос о тождестве человеческой личности *(personal identity)* занимает ученых многие тысячи лет. Считается, что сюжет одной из древнегреческих комедий был основан на этом парадоксе: должник отказывался вернуть долг, мотивируя это тем, что время прошло, и он — уже совсем не тот, кто брал деньги. Развязка была соответствующей: заимодавец избил должника, а на суде сказал, что не он бил, время-то прошло, и он теперь совсем другой[60]. Современная теория идентичности основывается на трудах Джона Локка, который полагал, что тождество личности определяется наличием у человека сознания, благодаря которому он сознает себя как одно и то же мыслящее существо, поскольку оно (вместе с мышлением и памятью) связывает воедино прошлое и настоящее этой личности[61]. Подход Локка не был идеальным: например, согласно ему получалось, что человек, потерявший память, становится другой личностью. Эта и другие проблемы были разработаны в труде Дэвида Юма, который сравнивал наше собственное тождество и тождество, приписываемое нами растениям и животным. Насекомое, которое проходит стадии личинки, куколки, наконец, бабочки, для нашего сознания — это одно и то же насекомое, но фактически в куколке гусеница умирает, разлагается до отдельных белков, из которых уже рождается бабочка. Поэтому для Юма вопрос о тождестве был вопросом о том, что связывает наш сознательный опыт, наши восприятия в одно целое[62]. Мен де Биран в своих работах обратил внимание, что существование нашего «я» для нас самих бесспорно, и в этом и стоит искать причину тождества

[59] «Так, автономное учреждение не вправе распоряжаться недвижимым имуществом, закрепленным за ним собственником, без согласия последнего (абз. 1 п. 2 ст. 298 ГК РФ). Неполной деликтоспособностью обладают, в частности, казенные предприятия (ст. 115 ГК РФ), частные и казенные учреждения (абз. 4 п. 2 ст. 120 ГК РФ). Они отвечают по своим обязательствам только находящимися в их распоряжении денежными средствами. Субсидиарную ответственность по их обязательствам несет собственник их имущества. С момента введения арбитражным судом наблюдения в порядке, установленном законом, юридическое лицо может совершать определенные действия только с письменного согласия временного управляющего. Как отмечает Конституционный Суд РФ, введение наблюдения влечет существенные ограничения дееспособности должника». См.: *Козлова Н.В., Филиппова С.Ю.* Гражданская правосубъектность юридического лица: комментарий новелл Гражданского кодекса РФ // Законодательство. 2014. № 9.

[60] Фрагменты ранних греческих философов. Ч. I. М., 1989. С. 250–260.

[61] *Локк Дж.* Сочинения в 3 т. Т. I. М., 1985.

[62] *Юм Д.* Трактат о человеческой природе. Кн. 1. М., 1995..

нашей личности — а по образу этого бесспорного тождества мы судим о тождестве других личностей и самых разных одушевленных и неодушевленных предметов[63]. Дискуссия о тождестве личности в философии продолжается до настоящего времени.

С другой стороны, идентичность — это набор характеристик человека и его поведенческих, социальных и личных особенностей, которые отличают его от других людей *(personality)*[64], а также соотносят его с различными социальными группами или общностями *(identity)*[65]. Я — юрист, я — россиянин, я — лысый: все это определяет мою идентичность.

Для целей настоящего исследования важно перейти от философского вопроса об идентичности личности к юридическому вопросу об идентичности субъекта права в рамках правопорядка или правоотношения. Здесь важны обе составляющие этого понятия. Для правоотношения принципиально важно тождество субъектов правоотношения самим себе на всем протяжении этого отношения. Но для правоотношения равно важно, чтобы характеристики субъектов оставались неизменными (или, точнее, предсказуемо изменялись) на протяжении отношения.

> Отсюда следует, что вопрос об идентичности субъекта правоотношения состоит из двух взаимосвязанных элементов. Это, во-первых, вопрос об идентификации субъекта права, т.е. о его тождестве в рамках правоотношения и правопорядка в целом[66]. Во-вторых, это вопрос об обеспечении актуальности и непротиворечивости информации о субъекте, которую используют стороны правоотношения и другие участники данного правопорядка. Этими проблемами занимаются, соответственно, правовые институты идентификации и персональных данных.

При этом надо отметить, что вопрос об идентичности субъекта права может проявляться в самых разных институтах частного права и гражданского процесса. Например, в рамках дел особого производства (подраздел IV Гражданского процессуального кодекса РФ) рассматриваются дела об установлении факта принадлежности правоустанавливающих документов лицу, имя, отчество или фамилия которого, указанные в документе, не совпадают с именем, отчеством или фамилией этого лица, указанными в паспорте или свидетельстве о рождении; факта владения и пользования недвижимым имуществом; факта несчастного случая; факта смерти в определенное время и при определенных обстоятельствах в случае отказа органов записи актов гражданского состояния в регистрации смерти; факта принятия наследства и места открытия наследства. Во всех этих делах предметом рассмотрения является идентичность субъекта частного права в рамках того или иного правоотношения.

В рамках материального права вопросам идентичности посвящена, в частности, ст. 46 «Последствия явки гражданина, объявленного умершим» ГК РФ. Судебная практика по ней ожидаемо невелика, но каждое рассмотренное судами дело демонстрирует принципиальную значимость вопроса об идентичности, поскольку в таких делах идентичность напрямую связана с правосубъектностью. Дела о явке гражданина, объявленного умершим, зачастую оказываются связаны с незаконным лишением свободы или даже с рабством. Таких людей суды признают умершими, и, как в Древнем Риме, они утрачивают правосубъектность. Восстановление их в правах и, что не менее важно, в правоотношениях — главная задача судов, рассматривающих дела в соответствии со ст. 46 ГК. Убедившись в идентичности человека, суд принимает решение об идентичности субъекта правоотношения, восстанавливая его жилищные, трудовые и иные гражданские правоотношения[67].

---

[63] *Кротов А.А.* Философия Мен де Бирана. М., 2000.

[64] *Morteza Vesali Naseh*. Person and personality in cyber space: a legal analysis of virtual identity // Masaryk University Journal of Law and Technology. 2016. Vol. 10. Iss. 1.

[65] *Абушенко В.Л.* Идентичность // Социология: энциклопедия. Минск, 2003. С. 344–349.

[66] Об идентификации как процессе признания тождества см.: *Наумов В.Б.* Институт идентификации в информационном праве: автореф. дис. … д-ра юрид. наук. М., 2020. С. 23.

[67] См., напр.: определения СК по гражданским делам Свердловского областного суда от 22.12.2011 по делу № 33-17948/2011, СК по гражданским делам Четвертого кассационного суда общей юрисдикции от 12.11.2020 по делу № 8Г-22750/2020[88-22443/2020; апелляционное определение Тамбовского областного суда от 09.09.2015 по делу № 33-2649/2015.

## 5. От идентичности к правопорядку, правосубъектности и правосознанию

Все приведенные выше соображения об идентичности человека как субъекта частного права практически неприменимы к коллективным и тем более к производным субъектам частного права. Даже в самых запутанных делах об идентичности человека: об останках царской семьи Романовых, о царевне Анастасии, Лжедмитрии, даже о Шекспире — всегда есть какие-то, в терминах Джона Локка, «субстанции», т.е. явления материального мира, существующие объективно и доступные для исследования. Спор об идентичности юридического лица может рассматриваться только на основании свидетельств людей как первоначальных субъектов частного права. Такие свидетельства могут быть устными либо письменными, т.е. содержаться в документах, реестрах, информационных ресурсах и системах.

На искусственный характер такого производного субъекта, как юридическое лицо, обращает внимание Н.В. Козлова: «Юридическое лицо есть искусственное общественное образование в том смысле, что так или иначе оно создается людьми по правилам, установленным законом»[68]. В законодательстве Российской Федерации есть одно, вполне конкретное правило, относящееся к идентичности юридических лиц: «Правоспособность юридического лица возникает с момента внесения в единый государственный реестр юридических лиц сведений о его создании и прекращается в момент внесения в указанный реестр сведений о его прекращении» (п. 3 ст. 49 ГК РФ). Из этого можно сделать вывод о том, что единственный критерий правоспособности юридического лица по российскому гражданскому законодательству — его идентичность, которая обеспечивается единым государственным реестром юридических лиц. Это, разумеется, не отменяет признаков юридического лица, закрепленных в п. 1 ст. 48 ГК РФ. Но тем не менее: нет идентичности — нет правосубъектности. Таковы правила. Аналогичные положения содержатся и в законодательстве иных стран. Как указывает О.А. Рузакова, «государственная регистрация юридических лиц, имея определенные национальные особенности, в то же время обладает рядом характерных черт. Например, приобретение юридическим лицом правоспособности всегда определяется моментом государственной регистрации»[69].

Коллективный субъект права может являться или не являться юридическим лицом, поэтому вопрос о его правосубъектности не может быть решен однозначно. В традиции стран общего права существует подход к корпорациям как к естественным лицам, образующимся естественным путем[70]. «Всякий раз, когда общество при отправлении правосудия считает целесообразным игнорировать отдельных членов организации для определенной цели и с этой целью рассматривать организацию как единое целое, организация в этой степени или с этой целью становится юридическим лицом. Это справедливо даже в тех случаях, когда группа организована как партнерство или другое неинкорпорированное объединение»[71]. Коллективный субъект права может быть государством, тогда вопрос о его правосубъектности становится еще более сложным, поскольку оказывается связан с вопросом о суверенитете и о признании этого суверенитета со стороны населения и других государств (легитимности). Тем не менее в отсутствие в праве положения, аналогичного ст. 6 Всеобщей декларации прав человека, для юридических лиц и государств мы можем говорить только об одном критерии правосубъектности для коллективных субъектов — их признании другими субъектами частного права.

Такое признание также ставит вопрос об идентичности, и решаться он может только теми же способами, что и вопрос об идентичности юридических лиц в российском праве: нет идентичности — нет правосубъектности. Чтобы правосубъектность могла быть признана за государством, неинкорпорированной организацией или аналогичными общностями, должна быть обеспечена их идентичность. Данное условие можно распространить и на любые производные субъекты права: не может быть субъектом права народ (но может быть государство) или божество (но может быть идол). Это также является следствием

[68] *Козлова Н.В.* Понятие и сущность юридического лица. М., 2003. С. 193.

[69] *Рузакова О.А.* Проблемы государственной регистрации в гражданском праве // Законодательство. 2002. № 2.

[70] *Козлова Н.В.* Указ. соч. М., 2003. С. 195.

[71] *Smith B.* Legal personality // Yale Law Journal. 1928. No. 3. P. 289.

принципа правовой определенности и связанных с ним пределов правового регулирования: право не может регулировать то, что не определенно и непонятно людям. «Г-н Дьюи говорит, что мы не делаем молекулы и деревья юридическими лицами, потому что „молекулы и деревья продолжали бы вести себя точно так же, независимо от того, были ли им приписаны права и обязанности или нет“. Но хотя функция правосубъектности, как следует из цитаты, заключается в регулировании поведения, она не только регулирует поведение субъекта, которому правосубъектность предоставлена; она также регулирует поведение людей по отношению к такому субъекту или друг к другу. В интересах общества сделать судно юридическим лицом, конечно, не потому, что это будет влиять на поведение судна, а потому, что его субъектность является эффективным инструментом для контроля в определенных деталях поведения его владельца или других людей. Широкая цель правосубъектности, будь то корабль, идол, молекула или человек, и кому бы или чему бы она ни предоставлялась, состоит в том, чтобы способствовать регулированию организованным обществом человеческого поведения и общения»[72].

И это опять-таки возвращает нас к идее правопорядка. Изначально рассматриваемые правом как основной его источник, государственные правопорядки всё больше вступают в конкуренцию с корпоративными (договорными) правопорядками, создаваемыми транснациональными компаниями. Эти компании становятся «цифровыми государствами», обладающими фактическими и юридическими возможностями по созданию правил, а также относительной автономией, и не могут быть сведены к суверенитету какого-либо одного государства. При этом мы, люди, оказываемся в сложном положении: мы являемся гражданами наших государств и в силу положений конституций можем в той или иной степени влиять на законы наших стран; но у нас нет статуса «цифровых граждан», как нет и непосредственной возможности влиять на правопорядок, создаваемый «цифровыми государствами»[73], хотя, скорее всего, мы идентифицируем себя (и нас идентифицируют) в качестве членов и той, и другой общности. Правосознание и правоспособность людей «работают» в любой общности, и это неизбежно должно привести к участию нас, «цифровых граждан», в создании правил и для цифровых государств тоже.

Интересы людей как субъектов права слабо защищены против «цифровых государств», с которыми субъекты вынуждены вступать в разного рода правоотношения. Это вызвано как тенденциями развития относительно автономных корпоративных (договорных) правопорядков, универсализацией систем идентификации и связанным с этим риском дискриминации, формализацией процедур защиты персональных данных, так и присущим человеку качеством создания разных персон для разных контекстов[74]. С одной стороны, киберпространство создает все возможности для множества контекстов и множества персон в каждом из них, которые может создать субъект. С другой стороны, универсализация систем идентификации и технологии Больших данных создают идеальные условия для объединения данных и персон субъекта из разных контекстов, что приводит к причинению вреда субъекту. В качестве решения этой проблемы можно предложить концепцию «права на идентичность» как права на создание идентичности (персоны), соответствующей контексту. Такое решение позволит не допустить смешения информации из разных контекстов .

Постулирование этого права и в целом идентичности как особого нематериального блага будет являться предметом отдельной статьи. Тем не менее уже сейчас можно коротко описать его следующим образом:

— право контролировать идентичность является разумным балансом между правом на имя, контроль над которым уже ничего не дает в эпоху Больших данных, и правом на защиту персональных данных, контроль над которыми требует значительных ресурсов;

— идентичность в киберпространстве (и не только в нем) складывается из сравнительно небольшого

[72] *Smith B.* Legal personality // Yale Law Journal. 1928. No. 3. P. 296. В приведенной цитате автор ссылается на работу: Dewey J. The Historic Background of Corporate Legal Personality // Yale Law Journal. 1926. Vol. 35. No. 6. P. 661.

[73] Этот вопрос обсуждался ранее в работах: *Дмитрик Н.А.* Корпорации в своем праве // Закон. 2021. № 12. С. 103–114; *Он же.* Государства в своем праве // Закон. 2021. № 11. С. 65–77.

[74] Этот вопрос обсуждался ранее в работе: *Дмитрик Н.А.* История, смысл и перспективы института персональных данных // Вестник гражданского права. 2020. № 3. С. 43–82.

числа идентификаторов, которые могут работать как сквозные, т.е. давать возможность смешивать информацию из разных контекстов (например, если мы пользуемся одним и тем же смартфоном дома и на работе), — их, а не все связанные с человеком данные и нужно контролировать;

— обозначение внутри «большого» режима персональных данных специальной категории идентификаторов, обеспечение транспарентности их использования и, по умолчанию, запрета на их передачу позволит и регулированию, и нашему вниманию сфокусироваться на ключевом факторе управления данными о нас.

«Право на идентичность» отсутствует в каком-либо правопорядке, как государственном, так и корпоративном (договорном), но нет смысла приводить его как предложения по изменению законодательства. Даже применительно к российскому законодательству о персональных данных можно отметить, что оно уже содержит необходимые элементы для защиты частной жизни и информации о человеке. Необходимо, однако, полное переосмысление данного законодательства как правоприменительными органами, так и операторами, чтобы перейти от формальной защиты данных к защите интересов личности.

Что может стать фактором, способствующим такому осознанию? Что может заставить государственные органы и транснациональные компании создавать подходы к приватности в интересах субъектов? Конечно, определенная роль здесь будет принадлежать международному праву, в рамках которого проблема так или иначе уже заявлена[75]. Но наибольшие перспективы для массового воздействия имеет метод *частного* права, основанный в условиях киберпространства на конкуренции правопорядков и — в этом отличие современной эпохи — на инструментах «цифрового гражданства», дающих возможность ухода от нежелательных правопорядков.

> Множественность правопорядков и возможность выбора между ними и есть решение проблемы идентичности субъекта права: такие качества человека, как правосознание и правоспособность; такое качество человека, как способность создавать персоны для разных контекстов; такая особенность киберпространства, как возможность выбора правопорядка в конкретном контексте, обеспечивают такие правила для каждого из контекстов, которые в конечном итоге будут справедливыми для участников этого контекста.

Это и есть доказательство тезиса, выдвинутого в начале настоящей работы: если человек, индивид, контролирует свою идентичность, набор своих сквозных идентификаторов (имя, адрес электронной почты, номер телефона, сетевые адреса или физические адреса устройств) в рамках «права на идентичность», он может сам решать, участвовать в нужном ему правопорядке или правоотношении (т.е. поддерживать идентичность) или уходить от вредного правопорядка или правоотношения (разрушая идентичность — например, удалив все связанные с данным индивидом идентификаторы). Право на идентичность (уже без кавычек) — это правовое средство достижения равенства в киберпространстве.

Равенство как первоначало частноправового регулирования, закрепленное в п. 1 ст. 1 ГК РФ, не может рассматриваться как фантазия или недостижимый идеал. Оно — в силу правонаделительного, инициативного характера частноправового регулирования, возможности субъектов частности создавать для себя гражданские права и обязанности — является краеугольным камнем существования самого частного права в цифровую эпоху. Множественность (правопорядков, персон, идентичностей) является залогом равенства и противовесом концентрации (монополизации рынков, универсализации систем идентификации, объединению профайлов из разных контекстов). Множественность не исключает взаимодействие: обеспечение совместимости разных правопорядков, переносимости данных, интероперабельности информационных и телекоммуникационных систем. Множественность не только

[75] Интересна в связи с этим позиция Европейского парламента, который в своей Резолюции от 06.10.2021 подчеркнул, что «люди не только имеют право на правильную идентификацию, но и право не быть идентифицированными вообще, за исключением случаев, когда этого требует закон в силу непреодолимых и законных общественных интересов» (см.: п. 8 Резолюции, URL: https://www.europarl.europa.eu/doceo/document/TA-9-2021-0405_EN.html; дата обращения: 23.03.2022).

не исключает, а, наоборот, предполагает единство киберпространства и предотвращение балканизации[76] Интернета.

> Частное право в целях решения проблемы идентичности может и должно дополнить свой метод методами фактической возможности, *lex informatica*. Одним из важнейших методов *lex informatica* будет обезличивание, позволяющее оторвать идентичность от субъектности.

Обезличенные данные будут связаны с контекстом, что позволяет их обрабатывать в рамках технологий Больших данных, но больше не будут связаны с субъектом, а соответственно, не смогут причинить ему вред. Кроме того, *lex informatica* — это способ уйти от формальной правовой охраны интересов личности к охране по существу. Как известно, «процедура — это логика, вынесенная вовне, она создает для проявления разума социальный институт как своего рода “искусственный интеллект”»[77]. Технологии позволяют получать результат без обременительных процедур, что облегчает субъектам защиту их интересов. Но, как было указано выше, технологии не могут стать правом. Право создается только людьми и распространяется только на людей.

## Humans in Their Right: from Legal Capacity to Personal Identity and Back

This article constitutes the final part of research devoted to the sources of legal regulation in cyberspace, started by the articles “States in their right” and “Corporations in their right”. The article provides an updated, due to rise of cyberspace, views on such basic legal concepts as legal capacity and legal awareness, legal personality and law and order. The main problem considered in the study is the problem of the personal identity. At the same time, personal identity is considered both as a prerequisite and an upshot of legal regulation. As the result of the study, the right to identity is justified as one of the elements of digital citizenship.

***Keywords:*** *personal identity, initial and derivative legal persons, artificial personality, legal capacity, legal awareness, digital citizenship*

### INFORMATION ABOUT THE AUTHORS

**Nikolay A. Dmitrik**
Head of Laboratory for Legal Informatics and Cybernetics at Lomonosov Moscow State University, Associate Professor of Faculty of Law at National Research University Higher School of Economics, Candidate of Juridical Sciences (e-mail: dmitric@mail.ru).

### REFERENCES

Austin, J. The Province of Jurisprudence Determined. 1832. URL: https://www.cambridge.org/core/books/austin-the-province-of-jurisprudence-determined.

Bratus, S.N. Legal entities in Soviet civil law [*Yuridicheskie lica v sovetskom grazhdanskom prave*]. Moscow, 1947. 227 p.

Dworkin, R. Taking Rights Seriously [*O pravah vseryoz*]. Moscow, 2004. 392 p.

Dmitrik, N.A. States in Their Right [*Gosudarstva v svoem prave*]. Statute [*Zakon*]. 2021. No. 11. P. 65–77.

Dmitrik, N.A. Corporations in Their Right [*Korporatsii v svoem prave*]. Statute [*Zakon*]. 2021. No. 12. P. 103-114.

Dmitrik, N.A. History, Essence and Prospects of the Institute of Personal Data [*Istoriya, smysl i perspektivy instituta personal’nyh dannyh*]. Civil Law Review [*Vestnik grazhdanskogo prava*]. 2020. No. 3. P. 43–82.

Ermolaeva, T.A., Ananyeva, A.A. Civil Legal Personality of Individuals: Jevolution of Content [*Grazhdanskaya pravosub”ektnost’ fizicheskih lic: evolyuciya soderzhaniya*]. Lex Russica. 2019. No. 12. P. 9–18.

Gribanov, V.P. Interest in Civil Law [*Interes v grazhdanskom prave*]. The Soviet State and Law [*Sovetskoe gosudarstvo i pravo*]. Moscow, 1967. No. 1. P. 49–56.

Ilyin, I.A. The General Doctrine of Law and the State [*Obschee ucheniye o prave i gosudarstve*]. Collected works: In 10 vols. Moscow, 1994. Vol. 4. P. 45.

Kozlova, N.V. The Concept and Essence of a Legal Entity [*Ponyatie i sushchnost’ yuridicheskogo lica*]. Moscow, 2003. 318 p.

Kozlova, N.S. The Collective Subject as an Environment for the Manifestation of a person’s Vital Activity [*Kollektivnyj sub’ekt kak sreda proyavleniya zhiznedeyatel’nosti lichnosti*]. Bulletin

[76] Балканизация — термин начала XX века, означавший коллапс большого государства, его фрагментацию и образование множества недружелюбно настроенных друг к другу сообществ на его месте (см.: *Тодорова М.Н.* Imagining the Balkans. Oxford University Press, 1997. С. 33). В цифровую эпоху балканизация означает разделение общемирового киберпространства, функционирующего по одинаковым для всех правилам, на множество региональных сетей, каждая из которых основывается на собственных стандартах и нормах.

[77] *Мусхелишвили Н.Л.*, *Сергеев В.М.*, *Шрейдер Ю.А.* Ценностная рефлексия и конфликты в разделенном обществе // Вопросы философии. 1996. № 11. С. 6–7.

of Kostroma State University. Series: Pedagogy. Psychology. Sociokinetics [*Vestnik Kostromskogo universiteta. Seriya: Pedagogika. Psihologiya. Sociokinetika*]. 2015. No. 2. URL: https://cyberleninka.ru/article/n/kollektivnyy-subekt-kak-sreda-proyavleniya-zhiznedeyatelnosti-lichnosti.

Kovrov, A.E. Posing the Question of Freedom of Will [*Postanovka voprosa o svobode voli*]. Bulletin of Moscow University. Series 7. Philosophy [*Vestnik Moskovskogo universiteta. Seriya 11. Filosofiya*]. 2010. No. 5. P. 30–53.

Krotov, A.A. Philosophy of Men de Biran [*Filosofiya Men de Birana*]. Moscow, 2000. 104 p.

Lessig, L. Code and Other Laws of Cyberspace. 1999. P. 6.

Mitchell, W.J. City of Bits: Space, Place and Infobahn. MIT Press. 1995. 223 p.

Morteza, V.N. Person and Personality in Cyber Space: a Legal Analysis of Virtual Identity. Masaryk University Journal of Law and Technology. 2016. Vol. 10. Iss. 1.

Muskhelishvili, N.L., Sergeev, V.M., Schrader, Yu.A. Value Reflection and Conflicts in a Divided Society [*Cennostnaya refleksiya i konflikty v razdelennom obshchestve*]. Questions of Philosophy [*Voprosy Filosofii*]. 1996. No. 11. P. 6–21.

Naumov, V.B. Institute of Identification in Information Law [*Institut identifikacii v informatsionnom prave*]: A Summary of a Doctor Thesis in Law [*avtoreferat diss. na soiskanie uchenoi stepeni doctora yurid. nauk*]. Moscow, 2020. 48 p.

Pereboom, D. Determinism al Dente. Noûs. 1995. Vol. 29. No. 1. P. 21–45.

Pokrovskiy, I.A. Main Problems of Civil Law [*Osnovnyye problemy grazhdanskogo prava*]. Moscow, 2003. 351 p.

Prokhorov, A; Konik, L. Digital Transformation. Analysis, Trends, Worldwide Experience [*Cifrovaya transformaciya. Analiz, trendy, mirovoj opyt*]. Moscow, 2019. 213 p.

Radko, T.N., Lazarev, V.V., Morozova, L.A. Theory of State and law: a Textbook for Bachelors [*Teoriya gosudarstva i prava, uchebnik dlya bakalavrov*]. Moscow, 2014. 568 p.

Reidenberg, J.R. Lex Informatica: The Formulation of Information Policy Rules through Technology. Tex. L. Rev. Vol. 76. No. 3. P. 553 (1997–1998).

Searle, J. Rationality in Action. Translated from the English by A. Kolodia, E. Rumyantseva. M., 2004. 336 p.

Smith, B. Legal Personality. Yale Law Journal. 1928. No. 3. P. 289.

Vashkevich, A.M. Automation of Law: Law as Electricity [*Avtomatizatsiya prava: pravo kak elektrichestvo*]. Moscow, 2019. 256 p.

Voynikanis, E.A. Intellectual Property Law in the Digital Age: the Paradigm of Balance and Flexibility [*Pravo intellektual'noj sobstvennosti v cifrovuyu epohu: paradigma balansa i gibkosti*]. Moscow, 2013. 723 p.

Weingold, Yu.Yu. Law as a Sociological Category [*Pravo kak sociologicheskaya kategoriya*]. Frunze, 1962. 317 p.

Windelband, W. On Freedom of Will [*O svobode voli*]. Moscow, 2000. 510 p.

**СЕРГЕЙ ДМИТРИЕВИЧ АФАНАСЬЕВ**

ведущий специалист Национального центра цифровой экономики МГУ имени М.В. Ломоносова, доцент кафедры конституционного и муниципального права юридического факультета Московского государственного областного университета, кандидат юридических наук

**ИГОРЬ АЛЕКСАНДРОВИЧ ТЕРЕЩЕНКО**

руководитель направления правовых исследований и юридического сопровождения Центра компетенций НТИ по направлению «Технологии хранения и анализа больших данных» на базе МГУ имени М.В. Ломоносова

**ДАРЬЯ АЛЕКСЕЕВНА ЯЦКЕВИЧ**

заместитель руководителя направления правовых исследований и юридического сопровождения Центра компетенций НТИ по направлению «Технологии хранения и анализа больших данных» на базе МГУ имени М.В. Ломоносова

# БИОМЕТРИЧЕСКАЯ ИДЕНТИФИКАЦИЯ И ПРАВА ЧЕЛОВЕКА: ДЕМАРКАЦИОННАЯ ЛИНИЯ

Основной вопрос использования технологий биометрической идентификации и обработки биометрических данных — обеспечение и защита основных прав и свобод человека. В настоящей статье на основе анализа подходов различных государств исследованы понятие, наполнение и подходы к выделению категории «биометрические персональные данные». Рассмотрев соотношение необходимости обеспечить основные права человека, связанные с информационными технологиями (информационное самоопределение; право на перенос данных *[data portability]*; право на приватность) и технологий биометрической идентификации, авторы сформулировали выводы об ограничениях обработки и требованиях к обработке биометрических данных (таких, как минимизация и ограничение хранения данных, проектируемая защита и возможность быстрого уничтожения данных, альтернативность форм доступа к услугам без обязательной биометрической идентификации и др.), которые призваны обеспечить соблюдение основных прав и свобод человека.

***Ключевые слова:*** *биометрические персональные данные, биометрический идентификатор, право на информационное самоопределение, право на перенос данных, data portability, право на приватность, видеораспознавание*

DOI: 10.37239/0869-4400-2022-18-3-33-46

## 1. Постановка проблемы

Развитие технологий биометрической идентификации объясняется рядом преимуществ (как на уровне самой технологии, так и на уровне бизнес-процессов, связанных с ее использованием). Но новая технология создает и новые риски, влекущие необходимость проведения «демаркационной линии» с правами человека. Основные преимущества (на уровне технологий и в бизнес-процессах) и риски использования технологий биометрической идентификации представлены

в табл. 1. По границе данных преимуществ и рисков проходит демаркационная линия биометрической идентификации и прав человека, которая должна стать определяющей в правовом регулировании использования биометрической идентификации.

Таблица 1

**Преимущества и риски биометрических технологий**

| | |
|---|---|
| **Преимущества на уровне технологий** | — Сложность подделки данных;<br>— уникальность физических черт человека;<br>— возможность дистанционной идентификации;<br>— не нужны дополнительные действия по идентификации (например, не нужно создавать и запоминать пароль) |
| **Преимущества в бизнес-процессах** | — Оптимизация финансовых операций;<br>— облегченные механизмы проверки безопасности;<br>— повышенная точность процедуры идентификации;<br>— снижение рисков обмана;<br>— превенция противоправных действий;<br>— совершенствование механизмов привлечения к ответственности |
| **Риски использования технологии*** | — Простота несанкционированной идентификации человека в силу уникальности биометрических характеристик (нет необходимости подбирать пароль, достаточно «подсмотреть» характеристики);<br>— возможность сбора характеристик и идентификации скрытно, на расстоянии и без осознанного участия субъекта данных (например, технологии распознавания лица);<br>— возможность дискриминации человека, идентифицированного по биометрическим особенностям человека (например, по признаку генетической предрасположенности к определенным заболеваниям);<br>— неизменность уникальных биологических характеристик человека (в отличие от номеров и паролей);<br>— невозможность восстановления ситуации после компрометации биологических характеристик (в результате чего человек подвергается повышенному риску кражи личных данных и, вероятно, откажется от использования биометрических данных в дальнейшем) |

Устранение указанного противоречия — между возможностями и рисками биометрической идентификации — и есть основная задача для правового регулирования. Законодатель (или иной регулятор) может правовыми средствами защитить интересы гражданина как уязвимой стороны в отношениях, которые требуют биометрической идентификации, но в то же время и дать ему возможность пользоваться благами информационного общества, что легче, удобнее и иногда даже безопаснее с использованием биометрических характеристик.

В настоящем исследовании рассмотрим проблему использования биометрической идентификации в контексте так называемых новых, или «цифровых», прав человека, т.е. прав, которые в последнее время закрепляет законодательство, посвященное регулированию цифровой экономики. К этим правам, в частности, относятся: право на защиту частной жизни в цифровую эпоху (включая право на забвение), право на переносимость данных, право на информационное самоопределение и некоторые другие[1].

## 2. Правовые режимы биометрических персональных данных

Представим знакомую почти каждому человеку ситуацию: при оформлении на работу работодатель просит либо сдать личную фотографию для пропуска на территорию организации, либо сфотографироваться с использованием техники работодателя. Факт, что в данном случае происходит обработка персональных данных, для чего нужно получить согласие субъекта, является неоспоримым. Но происходит ли в данном случае обработка именно биометрических данных? Ответ не столь очевиден.

Чтобы ответить на этот вопрос, необходимо определить, что относится к биометрическим данным человека.

> Российское законодательство закрепляет определение биометрических персональных данных как сведений, характеризующих физиологические и биологические особенности человека, на основании которых можно установить его личность и которые используются оператором для установления личности субъекта персональных данных (ч. 1 ст. 11 Федерального закона «О персональных данных»[2]). Данное определение содержит, по сути, два ключевых признака биометрических данных: 1) особое содержание; 2) особая цель обработки — установление личности.

* Подробнее о рисках см.: *Детерманн Л.* Путеводитель в правовом регулировании персональных данных. М., 2018. С. 258.

[1] См., напр.: The Privacy, Data Protection and Cybersecurity Law Review (Seventh Edition) / ed. Alan Charles Raul. London: Law Business Research Ltd. 2020. P. 20–25.

[2] Федеральный закон от 27.07.2006 № 152-ФЗ (в ред. от 02.07.2021) «О персональных данных» // СЗ РФ. 2006. № 31 (ч. 1). Ст. 3451 (далее по тексту — Закон о персональных данных).

Примерный перечень того, что в Законе о персональных данных понимается под биометрическими персональными данными, содержался в разъяснениях Роскомнадзора[3], утративших силу 19 ноября 2021 года. В соответствии с ними к биометрическим персональным данным относятся: дактилоскопические данные, радужная оболочка глаз, анализы ДНК, рост, вес, изображение человека (фотография и видеозапись). Аналогичный перечень биометрических персональных данных указан в Методических рекомендациях Минцифры России[4]. Хотя эти акты не носят обязательный нормативный характер, они могут служить ориентиром для правоприменителей.

Обращаясь к зарубежному опыту, следует отметить, что в состав биометрических персональных данных традиционно включаются: отпечатки пальцев, сканирование радужной оболочки глаза, запись голоса, изображение человека. Различные правопорядки добавляют к этому перечню дополнительные сведения, такие как сканирование геометрической формы руки (штаты Иллинойс[5] и Техас[6] в США, Китай[7]), рисунок вен (штат Калифорния[8] в США, Южная Корея[9]), сканирование ушных раковин (Китай), поведенческие характеристики (Калифорния, США) и др.

Дискуссионным является вопрос об отнесении генетической информации к числу биометрических персональных данных[10]. С одной стороны, отмечается, что генетический код и соответствующая информация, однозначно связанная с биологическими особенностями, уникальны для человека и могут использоваться для его идентификации.

> С другой стороны, в генетическом коде может содержаться определенная информация не только о самом человеке, но и о его родственниках, что делает ее особой разновидностью конфиденциальной информации.

В рамках текущего регулирования в Европейском союзе (далее — ЕС) генетические данные не включаются в категорию биометрических, однако выделяются в особую категорию персональных данных наряду с биометрическими (ст. 9 Общего регламента Европейского союза по защите персональных данных[11] [далее — *GDPR*]). Противоположный подход реализован в законодательстве штата Калифорния США, в соответствии с Актом о конфиденциальности потребителей которого данные о ДНК человека включаются в состав биометрической информации. Российское законодательство на этот счет не дает однозначного ответа, хотя Методические рекомендации Минцифры относят анализы ДНК к биометрическим персональным данным. В настоящее время во втором чтении в Государственной Думе РФ рассматривается законопроект о включении в состав биометрических персональных данных генетической информации[12].

---

[3] Разъяснения Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций 2013 г. // Экономика и жизнь (Бухгалтерское приложение). 2013. № 36. 13 сент. Утратили силу в связи с изданием письма Роскомнадзора от 19.11.2021 № 09-78548 «О неактуальности разъяснений Роскомнадзора» // СПС «КонсультантПлюс».

[4] См., напр.: письмо Минцифры России от 28.08.2020 № ЛБ-С-074-24059 «О методических рекомендациях» // СПС «КонсультантПлюс».

[5] Biometric Information Privacy Act of 2008 (Акт штата Иллинойс о конфиденциальности биометрической информации). URL: https://www.akingump.com/a/web/101105/Biometric-Information-Privacy-Act-740-ILCS-14-1-et-seq...pdf (дата обращения: 25.03.2022).

[6] Capture or Use of Biometric Identifiers Act of 2009 (Акт штата Техас о сборе или использовании биометрических идентификаторов). URL: https://statutes.capitol.texas.gov/Docs/BC/pdf/BC.503.pdf (дата обращения: 25.03.2022).

[7] Закон Китайской Народной Республики от 07.11.2016 № 53 «О кибербезопасности». URL: http://www.pkulaw.cn/fulltext_form.aspx?Db=chl&Gid=283838 (дата обращения: 25.03.2022).

[8] California Consumer Privacy Act of 2018 (Акт штата Калифорния о конфиденциальности потребителей). URL: https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5 (дата обращения: 25.03.2022).

[9] Закон Корейской Республики «Об иммиграционном контроле». URL: https://www.law.go.kr/%EB%B2%95%EB%A0%B9/%EC%B6%9C%EC%9E%85%EA%B5%AD%EA%B4%80%EB%A6%AC%EB%B2%95 (дата обращения: 25.03.2022).

[10] Подробно об этом см.: *Рассолов И.М.*, *Чубукова С.Г.*, *Микурова И.В.* Биометрия в контексте персональных данных и генетической информации: правовые проблемы // Lex Russica. 2019. № 1 (146). С. 108–118.

[11] Регламент (ЕС) 2016/679 Европейского парламента и Совета от 27.04.2016 «О защите физических лиц в отношении обработки персональных данных и о свободном перемещении таких данных и отмене Директивы 95/46 ЕС от 27.04.2016» (Общий регламент защиты персональных данных). URL: https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32016R0679&from=EN (дата обращения: 25.03.2022).

[12] Законопроект № 744029-7 «О внесении изменений в статью 11 Федерального закона „О персональных данных“ в части обработки биометрических персональных данных».

Примерный открытый перечень сведений, составляющих биометрические данные, в зарубежных государствах дополняется определением содержательных характеристик таких данных: уникальность физических, физиологических или поведенческих черт человека, которые позволяют идентифицировать его. При этом в некоторых случаях содержится уточнение о том, что сведения должны быть получены в результате специальной технической или автоматизированной обработки (Вашингтон[13] США, *GDPR*).

Таким образом, современное технологическое развитие не позволяет с точностью очертить перечень тех данных, которые являются биометрическими. С этой точки зрения российское законодательное определение, не ограничивающее биометрические персональные данные конкретными характеристиками человека (отпечатки пальцев, сканирование радужной оболочки и др.), выглядит удачным и позволяющим отнести к соответствующей категории различные виды данных. Однако в этом кроется и опасность, выявленная в правоприменительной практике.

> Отсутствие примерного перечня того, что относится к биометрическим данным, порождает правовую неопределенность и влечет за собой необходимость в каждом отдельном случае рассматривать вопрос о том, содержат ли конкретные данные биологические или физиологические характеристики человека.

В контексте этого вернемся к приведенному в начале раздела примеру с фотографией человека на пропуске. Арбитражные суды, рассматривая соответствующее дело, пришли к выводу, что оформление и использование такого пропуска является способом обработки биометрических персональных данных, поскольку имеет своей целью идентифицировать конкретного человека[14].

Сведения о биологических или физиологических характеристиках человека не всегда используются именно для идентификации личности. Так, например, биометрическая информация, полученная от пациента в медицинском учреждении, используется в целях лечения. Данные о состоянии здоровья лица также характеризуют его биологические признаки, но сами по себе не являются биометрическими[15] до момента использования в целях идентификации личности. В связи с этим субъективный подход к определению биометрических персональных данных, предполагающий наличие у оператора специальной цели установления личности при определении биометрических данных, представляется оправданным.

Однако, даже если нет специальной цели установить личность, это не значит, что биометрические данные перестают иметь особую ценность для личности. В любом случае они относятся к персональным данным.

> Поэтому всякая обработка биометрических данных, даже не связанная целью идентификации, должна подчиняться требованиям законодательства о персональных данных. В то же время в рамках общего правового режима персональных данных биометрические могут быть разделены на две категории: биометрические персональные данные (вне зависимости от цели их обработки) и биометрические идентификаторы (используемые в целях идентификации личности).

В мировой практике реализуются два подхода к решению вопроса о соотношении персональных данных, биометрических персональных данных и биометрических идентификаторов.

*Первый* подход предполагает отсутствие специального правового режима биометрических данных (этот подход реализуется, например, в Китае, Южной Ко-

URL: https://sozd.duma.gov.ru/bill/744029-7 (дата обращения: 25.03.2022).

[13] Washington Biometric Privacy Act of 2017 (Акт штата Вашингтон о биометрической конфиденциальности) (WBPA) // Revised Code of Washington (Обновленный кодекс Вашингтона), глава 19.375 «Биометрические идентификаторы». URL: https://law.justia.com/codes/washington/2020/title-19/chapter-19-375/ (дата обращения: 25.03.2022).

[14] Постановление Тринадцатого ААС от 27.07.2017 № 13АП-12966/2017 по делу № А42-342/2017 // СПС «КонсультантПлюс». С выводами данного решения согласился ВС РФ в Определении от 05.03.2018 № 307-КГ18-101 по делу № А42-342/2017 // СПС «КонсультантПлюс».

[15] См.: *Савельев А.И.* Научно-практический постатейный комментарий к Федеральному закону «О персональных данных». М., 2021 // СПС «КонсультантПлюс».

рее, Японии). В его рамках сведения о биологических и физиологических особенностях человека входят в категорию персональных данных и защищаются по «общим» для них правилам (рис. 1).

**Рис. 1.** Подход, не связанный с выделением биометрических данных в особую категорию персональных данных

*Второй* подход предполагает выделение биометрических персональных данных в особую категорию персональных данных, обладающую повышенными правовыми гарантиями защиты (подход реализуется прежде всего в европейских государствах на основе *GDPR*, а также в некоторых штатах США). При этом можно выделить две вариации данного подхода (рис. 2 и 3):

1) мягкий вариант предполагает обработку биометрических данных по стандартным для обработки персональных данных правилам и лишь при наличии специальной цели идентификации характеризуется механизмами особой правовой защиты (подход ст. 9 *GDPR*[16]);

**Рис. 2.** Мягкий подход регулирования обработки особой категории биометрических данных

[16] *Bisztray T.*, *Gruschka N.*, *Bourlai T.*, *Fritsch L.* Emerging Biometric Modalities and their Use: Loopholes in the Terminology of the GDPR and Resulting Privacy Risks // 2021 International Conference of the Biometrics Special Interest Group (BIOSIG). 2021. P. 1–5.

2) жесткий вариант предполагает защиту биометрических данных, по особым правилам выделенных в отдельную категорию, вне зависимости от целей обработки (подход штатов Иллинойс и Техас США).

**Рис. 3.** Жесткий подход регулирования обработки особой категории биометрических данных

В российском Законе о персональных данных под биометрическими персональными данными подразумеваются биометрические идентификаторы без их конкретного перечисления, что позволяет формально отнести его к мягкому подходу регулирования. Наличие отдельной категории, на первый взгляд, свидетельствует о стремлении ввести особое регулирование соответствующей категории данных. Однако, исходя из действующего законодательства, единственной особенностью обработки биометрических персональных данных является требование наличия письменного согласия (ч. 1 ст. 11 Закона о персональных данных), а в отдельных случаях допускается обработка без согласия субъекта (ч. 2 той же статьи). Соответствующее правило вряд ли можно отнести к особым механизмам правовой защиты, отличающим категорию биометрических персональных данных от иных категорий персональных данных. Фактически действующее российское регулирование занимает промежуточную позицию между первым и вторым подходом.

> При этом в российской судебной практике вырабатывается подход обособления категории биометрических данных путем повышения размера ответственности в случае их обработки при нарушении установленных правил.

По общему правилу, получившему распространение в судебной практике, соответствующее административное правонарушение в отношении значительного круга лиц наказывается однократным штрафом.

Так произошло, например, в деле школы «Мастерград» в Перми, администрация которой использовала биометрическую систему распознавания лиц для организации пропускного режима[17]. Требование Роскомнадзора по Пермскому краю о прекращении обработки биометрических персональных данных школа не выполнила. В связи с этим суд признал соответствующие действия нарушающими законодательство в области персональных данных и привлек к административной ответственности в соответствии с ч. 5 ст. 13.11 КоАП РФ[18] с назначением административного штрафа в размере 25 000 руб. Несмотря на наличие очевидно большого количества несовершеннолетних пострадавших субъектов персональных данных, наказание было назначено однократно.

Интересно отметить: в деле о нарушении правил обработки биометрических персональных данных университетом «Синергия» суд привлек оператора к административной ответственности пять раз в рамках одного инцидента. Представители университета 28 октября 2019 года провели в гимназии № 2 г. Красногорска тестирование учащихся, чтобы выявить их способности и склонности к тем или иным профессиям. При этом они использовали специальное оборудование для сканирования пальцев рук. Результаты тестирования, которые содержали индивидуальные результаты биометрического теста, организаторы затем выслали обучающимся на электронную почту. Данные действия были проведены без получения согласия на обработку биометрических данных. Ключевое отличие от дела пермской школы «Мастерград» состоит в том, что в деле университета «Синергия» суд по жалобам родителей обучающихся привлек к ответственности в каждом случае отдельно[19]. Всего было вынесено пять постановлений по делам об административных правонарушениях на общую сумму 150 000 руб. Основанием для привлечения к ответственности стала ч. 1 ст. 13.11 КоАП РФ.

## 3. Влияние прав человека на использование биометрической идентификации

Основные права человека, традиционный «каталог» которых формировался в конце XVIII – первой половине XX века, только в настоящее время стали включать в свой состав так называемые информационные или цифровые права. В дискуссиях о четвертом поколении прав человека распространена точка зрения, что именно данное поколение составляют права, связанные с современными информационными технологиями[20]. Однако в текстах как основополагающих международных актов в сфере прав человека, так и национальных конституций информационные права все еще не получили широкого распространения.

В связи с этим ключевые права человека, связанные с информационными технологиями, данными и идентификацией, выводятся из традиционных прав и свобод, которые наполняются новым содержанием.

> К числу таких прав человека, оказывающих непосредственное влияние на использование технологий биометрической идентификации, относятся право на информационное самоопределение, право на перенос данных *(data portability)* и право на защиту неприкосновенности частной жизни (право на приватность).

Из содержания этих прав вытекает необходимость гарантировать субъекту персональных данных определенные правомочия, связанные с обработкой его биометрических данных. Примеры таких правомочий, гарантируемых в соответствии с законодательством зарубежных государств, представлены в табл. 2. В ней приведено сравнение предоставляемых правомочий субъекту персональных данных в контексте рассматриваемых прав человека.

---

[17] См.: постановление Седьмого кассационного суда общей юрисдикции от 24.07.2020 № 16-2185/2020 // СПС «КонсультантПлюс». В дальнейшем дело было возвращено на новое рассмотрение в связи с наличием согласия родителей (законных представителей) на обработку персональных данных учащихся.

[18] КоАП РФ от 30.12.2001 № 195-ФЗ (в ред. от 30.12.2021) // СЗ РФ. 2002. № 1 (ч. 1). Ст. 1.

[19] См.: постановления мирового судьи судебного участка № 383 Мещанского района города Москвы от 29.01.2020 по делам № 5-0119/383/2020, 5-0120/383/2020, 5-0121/383/2020, 5-0122383//2020, 5-0123/383/2020. URL: https://mos-sud.ru/383/cases/admin (дата обращения: 27.03.2022).

[20] Подробнее об этом см.: *Лебединская А.С.*, *Тишаков М.П.* Четвертое поколение прав человека: общетеоретический аспект // Актуальные проблемы сравнительного правоведения. Материалы IV Всероссийской научно-практической конференции с международным участием профессорско-преподавательского состава, аспирантов и магистров. Симферополь, 2019. С. 433–438.

*Таблица 2*

**Права субъекта биометрических персональных данных**

| Государство | Информационное самоопределение | Право на перенос данных *(data portability)* | Право на приватность |
|---|---|---|---|
| **США** | — Право обжалования решений государственных органов, касающихся биометрических данных, содержащихся в информационных системах;<br>— защита от дискриминации на основании генетической информации, содержащейся в биометрических данных | Право требовать удаление записей в информационных системах, содержащих персональные данные (биометрические данные) | — Право знать и получать информацию о сборе и использовании персональных данных (биометрических данных);<br>— право на доступ к записям в информационных системах, содержащих биометрические данные;<br>— право на получение информации о сбоях или несанкционированном доступе к информационным системам, содержащим биометрические данные;<br>— право на гражданский иск в случае нарушения законодательных требований обработки биометрических данных |
| **Великобритания*** | — Право на возражение против обработки персональных данных в любое время;<br>— права в отношении автоматизированного принятия решений и профилирования | — Право на переносимость данных другому контроллеру;<br>— право на исправление неточных персональных данных;<br>— право на удаление личных данных («право на забвение») | Право на получение информации о том, каким образом и для каких целей происходит обработка данных |
| **Европейский союз (*GDPR*)** | — Право на ограничение обработки персональных данных;<br>— право на возражение против обработки персональных данных | — Право на исправление неточных данных;<br>— право на переносимость данных субъекта от одного контроллера к другому;<br>— право на удаление персональных данных, относящихся к субъекту данных («право на забвение») | Право на доступ к сведениям относительно обработки персональных данных |
| **Китай** | — Право принимать решения об обработке своих персональных данных;<br>— право ограничивать или отказывать в обработке своих персональных данных другим лицам | — Право попросить оператора личной информации исправить или дополнить ее;<br>— право запросить удаление персональных данных | — Право знать об обработке своих персональных данных;<br>– право запрашивать у операторов персональных данных разъяснения правил обработки личной информации |
| **Южная Корея** | Право определять, давать ли согласие и объем согласия в отношении обработки личной информации | Право приостановить обработку и запросить исправление, удаление или уничтожение личной информации | — Право на получение информации об обработке личной информации;<br>— право подтверждать, обрабатывается ли личная информация, и запрашивать доступ к ней;<br>— право на надлежащее возмещение любого ущерба |
| **Япония** | Право возражать против раскрытия своей личной информации третьей стороне | — Право на направление запроса об изменении или уточнении хранящихся данных;<br>— право на удаление персональных данных, относящихся к субъекту данных («право на забвение») | Право требования от оператора раскрыть сохраненные персональные данные, по которым они могут быть идентифицированы |

* Data Protection Act 2018 (Акт о защите данных Великобритании). URL: https://www.legislation.gov.uk/ukpga/2018/12/contents (дата обращения: 27.03.2022).

Анализ соотношения технологий биометрической идентификации и рассматриваемых прав человека в информационной среде позволяет сформулировать ряд ключевых ограничений и требований, которым должно подчиняться регулирование обработки биометрических персональных данных.

## 4. Биометрическая идентификация и право на информационное самоопределение

Еще в середине XX века Алан Уэстин писал о праве каждого решать самостоятельно, как, когда и в какой степени информация о нем самом будет распространяться[21]. Позже Конституционный суд Германии[22] обозначил такое право как «право на информационное самоопределение», т.е. способность каждого человека самостоятельно определять, как раскрывать и использовать личные данные. Подобное нашло воплощение и в России.

В российской правовой системе право на информационное самоопределение вытекает из взаимосвязанных ч. 1 ст. 23 и ст. 24 Конституции РФ, закрепляющих право на неприкосновенность частной жизни и запрет сбора, хранения, использования и распространения информации о частной жизни лица без его согласия. Право на информационное самоопределение было развито как ответ на угрозу для свободы нового вида: создание и развитие мощных компьютеризированных систем для сбора, управления и использования информации о любом человеке[23]. Информационный аспект частной жизни наиболее уязвимым для правонарушений, связанных с использованием биометрических данных.

Действующий российский Закон о персональных данных особенностью обработки биометрических данных называет необходимость получения письменного согласия на обработку таких данных. Но, конечно же, важнейшим аспектом является не формальный документ — согласие, а конкретные намерения человека. Подразумевается, что в момент подписания согласия субъект персональных данных свободно и осознанно соглашается на то, чтобы его данные обрабатывались и использовались. Именно в этом проявляется право на информационное самоопределение личности. Согласие не может быть вынужденным или обусловленным необходимостью получения тех или иных благ, даже в случае когда обработка иных (не биометрических) данных может осуществляться без согласия субъекта, т.е. на ином законном основании[24].

> Согласие как средство защиты интересов субъекта плохо работает в случае неизвестности логических и алгоритмических процессов обработки данных[25]. Поэтому в контексте права на информационное самоопределение обработка биометрических данных должна быть возможна лишь в том случае, когда человек действительно осознанно соглашается на это, понимает все возможные риски своего решения и имеет реальную альтернативу, т.е. возможность воспользоваться сервисом или иным благом, не предоставляя своих биометрических идентификаторов.

В этом контексте ценным для защиты приватности может стать принцип, который можно описать как обеспечение альтернативных форм доступа к сервисам и иным благам**.** Для всех услуг, которые сегодня оказываются с применением биометрической идентификации, следует предусматривать и равноценную возможность их оказания без обработки биометрических персональных данных. Так, регулятор оштрафовал польскую школу на 20 000 *PLN* (примерно 380 000 руб.) за обработку отпечатков пальцев 680 учеников без правового основания в целях идентификации в школьной столовой для проверки оплаты за питание. При этом предусмотренные в школе альтернативные меры идентификации не предоставляли субъектам равнозначного права доступа и условий[26].

---

[21] *Westin A.* Privacy and Freedom. N.Y., 1967.

[22] Решение Федерального конституционного суда Германии от 18 и 19 октября 1983 года по конституционной жалобе г-на Гюнтера Фрр. URL: https://www.servat.unibe.ch/dfr/bv065001.html (дата обращения: 27.03.2022).

[23] См.: *Цадыкова Э.А.* Гарантии охраны и защиты персональных данных человека и гражданина // Конституционное и муниципальное право. 2007. № 14. С. 15–18.

[24] В судебной практике существует позиция, согласно которой условия договора должны быть изложены таким образом, чтобы гражданин имел возможность свободно выразить согласие или отказаться от обработки персональных данных, в частности по вопросу передачи персональных данных третьим лицам. См., напр.: решения Арбитражного суда г. Москвы от 11.06.2014 по делу № А40-721/14, от 09.06.2021 по делу № А40-20962/2021-147-153 // СПС «КонсультантПлюс».

[25] См.: *Vivarelli A.* The Crisis of the Right to Informational Self-Determination // The Italian Law Journal. 2020. No. 1. P. 301–319.

[26] См.: Fine for processing students' fingerprints imposed on a school. URL: https://edpb.europa.eu/news/national-news/2020/fine-processing-students-fingerprints-imposed-school_en (дата обращения: 27.03.2022).

Обеспечение рассматриваемого права предполагает не просто необходимость подписания документа-согласия, но принципиальную возможность согласиться или не согласиться на обработку биометрических данных, возражать против такой обработки (в том числе если она осуществляется без согласия субъекта), требовать ограничения такой обработки.

## 5. Биометрическая идентификация и право на перенос данных *(data portability)*

*Data portability* (право на перенос данных), известное из права ЕС, представляет собой проявление информационного самоопределения каждого из нас. *Data portability* является новеллой действующего *GDPR*.

Перенос данных, предусмотренный ст. 20 *GDPR*, предоставляет физическим лицам право получать персональные данные, предоставленные контроллеру данных в структурированном, широко используемом и машиночитаемом формате, и передавать эти данные другому контроллеру. В этом смысле можно утверждать, что право на переносимость данных соответствует основополагающему характеру защиты данных путем усиления информационного самоопределения[27].

Рассматриваемое право состоит из ряда элементов: самого права и его объекта, формата данных, перечисленных «балансировочных» механизмов, а также его соотношения с иными правами субъектов персональных и биометрических персональных данных.

В настоящее время могут быть перенесены только данные, касающиеся конкретного субъекта персональных данных, и только в том случае, если он сам их предоставил. В свою очередь, объект переноса возможно рассматривать в узком и широком смыслах, от чего может зависеть сценарий переноса данных.

Согласно узкому (ограничительному) толкованию к предоставленным данным следует относить только те персональные данные, которые явно указаны в письменном согласии или же договоре, т.е. данные могут быть получены контроллером только от самого субъекта персональных данных. С другой стороны, в широком смысле объектом переноса будут считаться все персональные данные, которые контроллеры данных собрали с согласия или в соответствии с договором, например с помощью *GPS* (данные о местоположении), файлов *cookie*, информации о предпочтениях и т.д., — т.е. такие данные, которые субъект не предоставил явным образом. В первом случае особенно заметна активная роль субъекта данных, в отличие от второго, где субъект принимает тот факт, что его данные кем-то собираются. Представляется, что подобный подход применим к переносу биометрических персональных данных, но со значительными ограничениями, вызванными характером данных и связанными с ними рисками.

Для реализации права на перенос данных важен баланс с другими правами: согласно *GDPR*, осуществление права на переносимость данных должно «не наносить ущерб» праву на забвение и «не должно отрицательно сказываться на правах и свободах других лиц». Эта формулировка подчеркивает более осторожный подход европейского законодателя к возможным рискам и конфликтам с другими правами и интересами.

Наличие риска невозможности удаления персональных данных предопределило необходимость закрепления в п. 3 ст. 20 *GDPR* правила о преобладании права на забвение («право быть забытым») над правом на переносимость данных. В п. 3 также разъясняется, что переносимость данных не применяется в случае обработки данных в общественных интересах, правоохранительных целях (например, для раскрытия преступлений). Наконец, в п. 4 ст. 20 устанавливается — право на перенос данных не должно отрицательно сказываться на правах и свободах других лиц. Не имеет значения, влияет ли перенос данных на права или свободы других лиц, в данном случае важно, чтобы это влияние не было неблагоприятным (например, оно не должно приводить к разглашению коммерческой тайны или нарушать права интеллектуальной собственности).

Возвращаясь к вопросу понимания объектов переноса данных, следует сказать о двух возможных сце-

[27] См.: *Lynskey O.* Aligning data protection rights with competition law remedies? The GDPR right to data portability // European Law Review. 2017. Vol. 42. No. 6. P. 793–814.

нариях осуществления *data portability* — удаление и слияние.

> Реализация того или иного сценария тесно связана с реализаций права на забвение — именно на него ссылается законодатель в ст. 20 *GDPR*: осуществление права на перенос данных должно осуществляться без ущерба для права на забвение. Право на забвение не включается в процесс реализации *data portability* — это самостоятельное право. Получается, что субъект не может одновременно перенести и по умолчанию удалить свои данные, он должен проявить уважение к первому — применить право на забвение отдельно.

Таким образом, в случае реализации права на забвение можно говорить о сценарии удаления, когда при переходе к другому контроллеру данные у первого незамедлительно удаляются. Как альтернативу следует рассматривать сценарий слияния, когда субъекты данных, создавая, к примеру, учетную запись, экспортируют данные из нее в другие цифровые сервисы. Соотношение обозначенных сценариев с ранее рассмотренными подходами к пониманию объекта переноса данных и права на забвение может быть представлено следующим образом (табл. 3).

*Таблица 3*

**Соотношение узкого и широкого подхода к пониманию объекта *data portability***

| Категория для сравнения | Узкое (ограничительное) понимание | Широкое понимание |
|---|---|---|
| Объект *data portability* | Только данные, явно указанные в письменном согласии или договоре | Все данные, доступные контроллерам данных |
| Связь с правом на забвение | Прямая (перенос данных неразрывно связан с удалением данных у первого контроллера данных) | Косвенная (перенос данных по умолчанию не подразумевает удаление данных у первого контроллера данных) |
| Сценарий | Сценарий удаления | Сценарий слияния |

Право на перенос данных — ключевой фактор обеспечения субъектами персональных данных самостоятельного контроля за использованием предоставляемых данных, как «дополнительная гарантия»[28]. Говоря про *data portability* в контексте биометрической идентификации, можно отметить высокую роль защитного механизма, которым обладают субъекты данных. Во-первых, такое право предполагает распространение единых требований к формату собираемых биометрических персональных данных. Во-вторых, возможность безопасно перенести свои данные позволяет каждому реализовать право на информационное самоопределение, а также предпринять экстренные меры в случае утечек данных, реализовав право на забвение.

## 6. Биометрическая идентификация и право на приватность в цифровую эпоху

Право на неприкосновенность частной жизни — одно из основных прав человека *(fundamental rights)*. Оно находит отражение в ст. 8 Европейской конвенции по правам человека[29], а также в большинстве основных законов современных государств. Данное право, являясь живым инструментом и механизмом реализации свободы личности, глобально представляет комплекс таких прав, как право на тайну переписки и корреспонденции, личную неприкосновенность, защиту чести и достоинства, сведений о личной и семейной жизни и иные права. В американской доктрине[30] и европейской судебной практике данное право раскрывается в том числе через право человека быть оставленным наедине с собой *(right to be let alone)* и право на анонимность в общественном месте *(right to anonymity in publicly accessible place)*. Наиболее активно право на непри-

[28] Guidelines on the right to data portability as last revised and adopted on 5 April 2017 // Article 29 Data Protection WP, 16/EN, WP 2042, rev. 01. P. 6. URL: https://ec.europa.eu/newsroom/document.cfm?doc_id=44099 (дата обращения: 27.03.2022). См. также: European Commission, Building a New Data Economy Communication (January 2017). URL: https://ec.europa.eu/digital-single-market/en/policies/building-european-data-economy (дата обращения: 27.03.2022).

[29] Конвенция о защите прав человека и основных свобод (заключена в г. Риме 4 ноября 1950 года) // СЗ РФ. 2001. № 2. Ст. 163. Конвенция ратифицирована Федеральным законом от 30.03.1998 № 54-ФЗ «О ратификации Конвенции о защите прав человека и основных свобод и Протоколов к ней» // СЗ РФ. 1998. № 14. Ст. 1514.

[30] *Warren S.*, *Brandeis L.* The Right to Privacy // Harvard Law Review. 1890. Vol. 4. No. 5. P. 193–220.

косновенность частной жизни сейчас развивается в части защиты персональных данных.

> Так, среди основных принципов обработки персональной информации, нашедших отражение в *GDPR*, отдельного внимания с точки зрения ограничения операторов и сохранения гарантий на защиту права на неприкосновенность частной жизни заслуживают принципы минимизации используемых/собираемых данных и ограничения хранения. Эти принципы устанавливают необходимость для операторов собирать и обрабатывать только то количество данных, которое необходимо для решения конкретной задачи, а не максимально возможное количество.

Так, например, видеонаблюдение можно использовать, если другими средствами, оказывающими меньшее влияние на права и свободы субъекта, цель обработки персональных данных не может быть достигнута. При этом необходимо ограничивать срок хранения записей и область наблюдения до предельно необходимых[31]. Сбор чувствительных данных там, где в этом нет крайней необходимости, может повлечь далеко идущие последствия в стиле известной антиутопии Джорджа Оруэлла.

Интересен тот факт, что сегодня при оказании некоторых государственных и муниципальных услуг на портале государственных услуг Москвы *(mos.ru)* пользователю требуется предоставить свою фотографию, сделанную при четком соблюдении правил съемки[32]. Помимо использования для оказания самой услуги, оператор портала также планирует передавать фотографии в качестве эталонных правоохранительным органам[33]. Выявление преступников, безусловно, представляет собой существенный публичный интерес, однако какое количество людей, в отношении которых собирают подобные данные, может преступить закон? С учетом широкого современного инструментария силовых ведомств по поиску правонарушителей тем не менее мы наблюдаем тенденцию накопления правоохранительными органами внушительного объема данных, собранных из сторонних ресурсов, в частности при получении гражданами государственных услуг. Насколько подобный сбор данных и возможная общественная опасность от потенциально нераскрытых преступлений соотносятся с вторжением в право на неприкосновенность частной жизни миллионов граждан? Примечательна позиция Европейского парламента, который в своей Резолюции от 6 октября 2021 года подчеркнул, что «люди не только имеют право на правильную идентификацию, но и право не быть идентифицированными вообще, за исключением случаев, когда этого требует закон в силу непреодолимых и законных общественных интересов»[34].

Масштаб рисков, с которыми связано нарушение базовых принципов обработки персональных данных при использовании технологий распознавания лиц, демонстрирует решение Савеловского районного суда Москвы по делу № 02а-577/19[35]. Суть дела заключалась в обработке биометрических персональных данных административного истца без его письменного согласия оператором камер уличного видеонаблюдения в лице столичного Департамента информационных технологий (далее — ДИТ). В связи с отсутствием в действиях цели установления личности административного истца на видеозаписях, а следовательно, факта обработки биометрических персональных данных, в удовлетворении иска было отказано. При этом изображения с камер хранятся и обрабатываются в государственной информационной системе «Единый центр хранения и обработки данных» (далее — ЕЦХД), в которую как раз и планируется передача фотографий с портала *mos.ru*. Когда следственным органам требуется использо-

[31] Guidelines 3/2019 on processing of personal data through video device. URL: https://edpb.europa.eu/sites/default/files/consultation/edpb_guidelines_201903_videosurveillance.pdf (дата обращения: 27.03.2022).

[32] Требования к фотографиям портала *mos.ru*. URL: https://www.mos.ru/pgu/common/photo.pdf (дата обращения: 27.03.2022).

[33] См.: Власти Москвы решили передать фото с *mos.ru* в систему распознавания лиц. URL: https://www.rbc.ru/technology_and_media/13/10/2021/61665e719a79476733b5c3a3 (дата обращения: 27.03.2022).

[34] См.: European Parliament resolution of 6 October 2021 on artificial intelligence in criminal law and its use by the police and judicial authorities in criminal matters. P. 8. URL: https://www.europarl.europa.eu/doceo/document/TA-9-2021-0405_EN.html (дата обращения: 27.03.2022).

[35] Решение Савеловского районного суда города Москвы от 11.11.2019 по делу № 02а-0577/2019. URL: https://mosgorsud.ru/rs/savyolovskij/services/cases/kas/details/988f386e-be51-47b0-b48f-e871043ef1fc?caseNumber=02%D0%B0-577/19 (дата обращения: 27.03.2022).

вать ЕЦХД для поиска преступника, то они передают в ДИТ фото, с которым необходимо провести сравнение. В такой ситуации ДИТ выполняет функцию сравнения двух изображений человека (полученную с камер видеонаблюдения и предоставленную правоохранительным органом), но не производит идентификацию гражданина, поскольку не располагает их ФИО и иными персональными данными. По факту эту идентификацию производит ГУ МВД по г. Москве, которое следовало бы рассмотреть в качестве оператора персональных данных и оценить реализацию принципов минимизации и ограничения хранения используемых данных при их обработке. Пусть наличие публичного интереса порой и позволяет производить обработку персональных данных без согласия субъекта, но принципы подобной обработки все равно должны соблюдаться.

Выдержал бы в принципе в приведенной ситуации законный общественный интерес «балансировку ценностей» *(sensu sctricto)* и в целом пятиступенчатый «тест пропорциональности»[36], когда на чаше весов основные права из ст. 23 Конституции РФ и ст. 8 Европейской конвенции по правам человека? Близкой кажется позиция европейских исследователей о том, что доступ правоохранительных органов к данным, собранным в частном порядке, без уточнения необходимости и обоснованных причин для такого доступа по отношению к конкретным распознанным лицам, должен быть прямо исключен, равно как и систематический доступ к подобным данным. Эта потребность также связана с растущей интероперабельностью и использованием биометрических баз данных[37].

*EDRi* (общественная организация «Европейские цифровые права») высказалась в отношении Закона ЕС об искусственном интеллекте[38] и поддержала идею о том, что различие между распознаванием «в реальном времени» и «постфактум» не имеет значения, когда речь идет о влиянии этих технологий на основные права. «Постфактум»-идентификация на самом деле несет в себе более высокий потенциал вреда, поскольку для проведения идентификации можно собрать больше данных из разных источников. Таким образом, использование подобных технологий может рассматриваться как практика, экспансивная и навязчивая до такой степени, что она представляет собой несоразмерное вмешательство в права на неприкосновенность частной жизни и защиту персональных данных. Причем это касается не только сбора и обработки лиц, но и походки, голоса и других биометрических или поведенческих сигналов[39].

> При обработке биометрических персональных данных следует выделить и принцип проектируемой защиты данных *(Privacy by design)*. Он подразумевает обязанность предусматривать защиту конфиденциальности в информационных системах уже на этапе их проектирования, ориентируясь на интересы пользователя и четкое ограничение целей и объема собираемых данных.

При обработке чувствительной информации данный принцип полезно дополнить возможностью быстрого уничтожения этих данных**.** Критерием успешной реализации принципа должна стать скорость, с которой чувствительная информация о конкретном человеке может быть удалена из всех источников и в принципе — гарантированно удалена.

Подобная гарантия должна являться важным принципом при построении систем, обрабатывающих биометрические персональные данные. Такой вывод можно сделать из заключения расследования *ICO* и *OAIC* по деятельности *Clearview AI, Inc.*[40] В частности, в данном заключении в качестве основания наложения санкций на компанию указано, что в подходе компании не реализован процесс, препятствующий хранению данных неопределенно долго. Несмотря

[36] См.: решение Федерального конституционного суда Германии от 15.01.1958 № BVerfGE 7, 198 («Дело Люта»). URL: https://germanlawarchive.iuscomp.org/?p=51 (дата обращения: 27.03.2022).

[37] См.: Privacy and Data Protection Issues of Biometric Applications: A Comparative Legal Analysis Law, Governance and Technology Series. Vol. 12. Springer Science & Business Media, 2013.

[38] European Commission adoption consultation: Artificial Intelligence Act. URL: https://edri.org/wp-content/uploads/2021/08/European-Digital-Rights-EDRi-submission-to-European-Commission-adoption-consultation-on-the-Artificial-Intelligence-Act-August-2021.pdf (дата обращения: 27.03.2022).

[39] См. там же.

[40] См.: OAIC and UK's ICO open joint investigation into Clearview AI Inc. URL: https://www.oaic.gov.au/updates/news-and-media/oaic-and-uks-ico-open-joint-investigation-into-clearview-ai-inc (дата обращения: 27.03.2022).

на различные методы сбора данных, в чем-то схожие опасения вызывает и российская Единая биометрическая система (далее — ЕБС), возведенная в декабре минувшего года в статус государственной информационной системы[41]. При явной тенденции централизации хранения биометрических персональных данных именно в рамках ЕБС тем не менее при исследовании различных ведомственных актов, а также локальных актов ПАО «Ростелеком» пользователь не может убедиться, как скоро после отзыва согласия на обработку персональных данных они будут удалены и будут ли удалены окончательно[42].

С точки зрения соблюдения баланса между публичными интересами при обработке биометрических персональных данных и правом на неприкосновенность частной жизни правильным видится мягкий регуляторный подход, но с обязательным соблюдением «сплошной двойной линии» в виде принципов минимизации и ограничения хранения данных, проектируемости защиты данных, возможности быстрого уничтожения данных, а также ограничения количества лиц, имеющих право на обработку биометрических идентификаторов без согласия субъектов, даже при наличии публичных интересов.

## 7. Выводы

Анализ влияния основных прав человека, связанных с информационным пространством и биометрической идентификацией, позволяет сделать следующие выводы. В контексте защиты рассмотренных прав личности использование биометрических идентификаторов должно подчиняться специальным правилам. В силу особой «чувствительности» биометрических данных их обработка требует обеспечения повышенных стандартов правовой защиты. Это влечет необходимость соблюдения «общих» правил обработки биометрических данных вне зависимости от целей такой обработки, не ограничиваясь целью идентификации личности. В случаях использования биометрических данных в соответствии с указанной целью необходимо выделить их в отдельную правовую категорию биометрических идентификаторов, для обработки которых должны быть предусмотрены особые правила.

Эти правила должны учитывать ограничения и требования, которые вытекают из существа основных прав человека в информационной среде: права на информационное самоопределение, права на перенос данных *(data portability)* и права на приватность. Ограничения и требования накладываются реализацией таких принципов, как: возможность (не) согласиться на обработку биометрических данных и альтернативность форм доступа к услугам без обязательной биометрической идентификации; возможность возражать против обработки биометрических данных; единство требований к формату собираемых биометрических данных; возможность безопасно перенести свои данные к другому контроллеру; возможность требовать удаления своих биометрических данных; минимизация и ограничение хранения данных; проектируемость защиты данных, возможность быстрого уничтожения данных; ограничение количества лиц, имеющих право на обработку биометрических идентификаторов без согласия субъектов; применение «теста пропорциональности» при такой обработке. Перечисленные права и принципы не ставят крест на обработке биометрических персональных данных, но представляют собой существенные границы (ту самую «демаркационную линию» между биометрической идентификацией и правами человека), которые должны быть соблюдены при использовании биометрии.

## Biometric Identification and Human Rights: the Line of Demarcation

The main issue of modern regulation of the use of technologies for biometric identification and processing of biometric data is the ensuring and protecton of fundamental human rights and freedoms. In this article, on the basis of an analysis of the approaches of various states, the concept and content of the category “biometric personal data”, as well as approaches

[41] Федеральный закон от 29.12.2020 № 479-ФЗ (в ред. от 30.12.2021) «О внесении изменений в отдельные законодательные акты Российской Федерации» // СЗ РФ. 2021. № 1 (ч. I). Ст. 18.

[42] См.: абз. 2 п. 10 Приложения № 1 к приказу Минкомсвязи России от 25.06.2018 № 321 «Об утверждении порядка обработки, включая сбор и хранение, параметров биометрических персональных данных в целях идентификации…». URL: http://pravo.gov.ru/proxy/ips/?docbody=&nd=102476395 (дата обращения: 27.03.2021).

to the selection of this category of personal data, are investigated. As a result of considering the relationship between biometric identification and fundamental human rights related to information technology (information self-determination; the right to data portability; the right to privacy), conclusions were formulated on the restrictions and requirements for the processing of biometric data, which are designed to ensure the observance of fundamental rights and human freedoms. Restrictions and requirements are imposed by the implementation of such principles as minimization and limitation of data storage, privacy by design, the possibility of fast erasure of data, alternative forms of access to services without mandatory biometric identification, limitation of the number of persons entitled to process biometric identifiers without the consent of the subjects and the use of "proportionality test" with such processing.

***Keywords:*** *Biometric personal data; biometric identifier; the right to informational self-determination; the right to data portability; the right to privacy; video surveillance*

## INFORMATION ABOUT THE AUTHORS

**Sergei D. Afanasev**
Leading specialist for National Center for Digital Economy at Lomonosov Moscow State University, Associate professor for Department of Constitutional and Municipal Law at Faculty of Law at Moscow Region State University, PhD in Law (e-mail: sergei.afanasev@digital.msu.ru).

**Igor A. Tereshchenko**
Head of Legal Research and Legal Support for Big Data Storage and Analysis Center at Lomonosov Moscow State University (e-mail: igor.tereshchenko@digital.msu.ru).

**Daria A. Yatskevich**
Deputy Head of Legal Research and Legal Support for Big Data Storage and Analysis Center at Lomonosov Moscow State University (e-mail: darya.yatskevich@digital.msu.ru).

## REFERENCES

Bisztray, T., Gruschka, N., Bourlai, T., Fritsch, L. Emerging Biometric Modalities and their Use: Loopholes in the Terminology of the GDPR and Resulting Privacy Risks, in: 2021 International Conference of the Biometrics Special Interest Group (BIOSIG). 2021. P. 1–5.

Determann, L. Guide to the Legal Regulation of Personal Data [*Putevoditel' v pravovom regulirovanii personal'nykh dannykh*]. Moscow, 2018. 258 p.

Lebedinskaya, A.S., Tishakov, M.P. The four Generation of Human Rights — General Theoretical Aspect [*Chetvertoe pokolenie prav cheloveka: obshcheteoreticheskiy aspekt*], in: Actual Problems of Comparative Jurisprudence. Materials of the IV All-Russian Scientific and Practical Conference with International Participation of the Teaching Staff, Graduate Students and Masters [*Aktual'nye problemy sravnitel'nogo pravovedeniya. Materialy IV Vserossiyskoy nauchno-prakticheskoy konferentsii c mezhdunarodnym uchastiem professorsko-prepodavatel'skogo sostava, aspirantov i magistrov*]. Simferopol, 2019. P. 433–438.

Lynskey, O. Aligning Data Protection Rights with Competition Law Remedies? The GDPR Right to Data Portability. European Law Review. 2017. P. 793–814.

Privacy and Data Protection Issues of Biometric Applications: A Comparative Legal Analysis. Law, Governance and Technology Series. Vol 12. Springer Science & Business Media. 2013. 975 p.

Rassolov, I.M., Chubukova, S.G., Mikurova, I.V. Biometrics in the Context of Personal Data and Genetic Information: Legal Challenges [*Biometriya v kontekste personal'nykh dannykh i geneticheskoy informatsii: pravovye problemy*]. Lex Russica. 2019. No. 1 (146). P. 108–118.

Savelyev, A.I. Scientific and Practical Article-by-Article Commentary on the Federal Law "About Personal Data" [*Nauchno-prakticheskiy postateynyy kommentariy k Federal'nomu zakonu "O personal'nykh dannykh"*]. Moscow, 2021. 468 p.

The Privacy, Data Protection and Ctbersecurity Law Review (Seventh Edition) / ed. Alan Charles Raul. London, Law Business Research Ltd. 2020. 506 p.

Tsadykova, E.A. Guarantees of Protection and Protection of Personal Data of a Person and Citizen [*Garantii okhrany i zashchity personal'nykh dannykh cheloveka i grazhdanina*]. Constitutional and Municipal Law [*Konstitutsionnoe i munitsipal'noe pravo*]. 2007. No. 14. P. 15–18.

Vivarelli, A. The Crisis of the Right to Informational Self-Determination. The Italian Law Journal. 2020. No. 1. P. 301–319.

Warren, S., Brandeis, L. The Right to Privacy. Harvard Law Review. 1890. Vol. 4. No. 5. P. 193–220.

Westin, A. Privacy and Freedom. New York, 1967. 487 p.

**АНЖЕЛИКА НИКОЛАЕВНА ИЗОТОВА**

руководитель проектов юридического департамента ПАО «Мобильные ТелеСистемы», младший научный сотрудник Института права цифровой среды Национального исследовательского университета «Высшая школа экономики»

# РОЛЬ ИДЕНТИФИКАЦИИ В ИНСТИТУТЕ ТАЙНЫ СВЯЗИ

Статья содержит анализ нормативно-правового регулирования, а также доктринальных подходов к идентификации пользователей в сфере коммуникаций с точки зрения значения идентификации для института тайны связи. Автором уделено внимание таким аспектам идентификации, как: а) ценности для коммуникационных интернет-сервисов, а также государства при реализации публичных функций; б) угрозы причинения вреда и нарушения тайны связи. Связь с личностью (возможность идентификации) пользователя определяется автором как квалифицирующий признак тайны связи. В статье предложены возможные условия обработки сведений, составляющих тайну связи с точки зрения риск-ориентированного подхода и контекстуальной целостности конфиденциальной информации, в том числе посредством обезличивания информации о коммуникациях.

***Ключевые слова:*** *тайна связи, конфиденциальность, идентификация, персональные данные, коммуникации*

DOI: 10.37239/0869-4400-2022-18-3-47-57

Информация, передаваемая в процессе коммуникаций, может быть самой разнообразной с точки зрения ее правового режима. Это может быть как общедоступная информация, защита которой не требуется, так и персональные данные, личная тайна пользователя, любой вид профессиональной тайны, коммерческая тайна организаций и т.д. Так как в организации коммуникаций участвует информационный посредник (оператор связи, организатор распространения информации в сети «Интернет»), то участник коммуникации (пользователь) фактически утрачивает контроль над этой информацией, возможность ограни-

чить доступ к передаваемой информации. Поэтому требуется применение правовых механизмов защиты данной информации. Тайна связи является таким механизмом. Иными словами, назначение тайны связи заключается в обеспечиваемой информационным посредником защите информации, передаваемой в процессе коммуникаций.

> Основная цель установления правового режима тайны связи — ограничение информационным посредником доступа к сведениям, составляющим тайну связи, со стороны третьих лиц. При этом у самого участника коммуникаций (отправителя, получателя, уполномоченных ими лиц) остается право доступа к информации о своих коммуникациях[1].

> Идентификация в таких условиях выступает инструментом обеспечения правового режима тайны связи. Суть процедуры идентификации заключается в отождествлении субъекта правоотношений, установлении его идентичности, что позволяет выделить субъекта из множества других лиц.

Клэр Салливан назвала это идентичностью транзакции *(transaction identity)*, отметив, что речь идет не только об установлении личности, но и подтверждении права этой личности совершить определенную транзакцию[2].

В правоотношениях, возникающих по поводу коммуникаций, в процессе идентификации можно выделить как минимум два этапа: установление (регистрацию) субъекта — пользователя услугами связи, коммуникационными сервисами[3] при заключении договора и последующую аутентификацию, авторизацию пользователя в процессе пользования услугами связи, коммуникационными сервисами для управления ими, получения доступа к своим сведениям, в том числе составляющим тайну связи, и т.п. Так как идентификация пользователя проводится при совершении каждой транзакции, тем самым обеспечивается контроль доступа к сведениям, составляющим тайну связи.

Наряду с тем, что идентификация выступает одной из гарантий обеспечения прав участников коммуникаций на тайну связи, результаты идентификации представляют ценность для третьих лиц, в том числе для государства. Однако роль идентификации в коммуникациях не столь однозначна, поскольку она может создавать угрозу для участников коммуникаций.

## 1. Идентификация в коммуникациях как ценность

Законодательство подробно регулирует *процедуру идентификации пользователей, проводимую операторами связи*, которая направлена не просто на узнавание пользователя среди других лиц, но и на установление его личности посредством документов, удостоверяющих личность, а также обеспечение актуальности сведений о пользователе на протяжении всего периода его обслуживания. Порядок идентификации, проводимый операторами связи при заключении договора об оказании услуг связи, с течением времени ужесточался. Этому способствовало несколько причин.

*Во-первых, это борьба с преступностью, в особенности с терроризмом*.

Широкое распространение «серых» сим-карт без заключения договора об оказании услуг связи, заключение фиктивных договоров об оказании услуг связи с использованием паспортных данных третьих лиц способствовали совершению противоправных действий с использованием таких сим-карт, а также затрудняли работу правоохранительных органов[4]. В 2014 году это привело к появлению обязанности операторов связи

[1] См., напр.: ч. 3 ст. 63 Федерального закона от 07.07.2003 № 126-ФЗ «О связи» // СПС «КонсультантПлюс»; § 2702 Communication Act of 1934 of USA. URL: https://www.law.cornell.edu/uscode/text/18/2702 (дата обращения: 20.03.2022).

[2] *Sullivan C.* Digital identity: An Emergent Legal Concept. 2011. URL: https://www.jstor.org/stable/10.20851/j.ctt1sq5wqb.8 (дата обращения: 20.03.2022).

[3] Далее для удобства используется обобщающий термин «пользователь».

[4] Пояснительная записка к Проекту Федерального закона «О внесении изменений в Федеральный закон „О связи“». URL: https://sozd.duma.gov.ru/bill/1058353-7 (дата обращения: 20.03.2022).

проводить проверку достоверности сведений об абонентах, которые они предоставляли при заключении договора. В 2018 году законодатель предусмотрел перечень способов проверки достоверности полученных сведений[5].

В результате принятых изменений оператор связи должен обеспечивать очень высокий уровень идентификации абонента. Применительно к дистанционному заключению договора *идентификация обеспечивается сразу двумя группами мер*. С одной стороны, это *способ заключения договора*, который предполагает идентификацию абонента посредством усиленной квалифицированной электронной подписи (УКЭП) либо сочетания иных видов электронной подписи с государственными информационными системами (включая Единую систему идентификации и аутентификации [ЕСИА] и Единую биометрическую систему). С другой стороны, это *процедура проверки достоверности* предоставленных абонентом — физическим лицом сведений посредством использования УКЭП, ЕСИА либо иных государственных информационных систем с помощью системы межведомственного взаимодействия[6]. Данная процедура распространяется и на пользователей абонентов — юридических лиц (за рядом исключений) и индивидуальных предпринимателей.

Однако недостаточная эффективность борьбы с «серыми» сим-картами привела к введению с 2021 года дополнительных обязанностей операторов связи по проверке достоверности данных о пользователях абонентов — юридических лиц, индивидуальных предпринимателей. Для таких пользователей предусмотрено обязательное подтверждение установленных сведений с использованием ЕСИА.

С 2021 года предусмотрен государственный мониторинг соблюдения операторами связи обязанности по проверке достоверности сведений об абонентах, пользователях[7].

*Вторая причина* ужесточения процедуры идентификации связана с первой. Это *развитие законодательства о противодействии легализации доходов, полученных преступным путем, и финансированию терроризма* (ПОД/ФТ)[8].

Признание операторов подвижной связи и операторов по передаче данных, занимающих существенное положение на рынке услуг связи, организациями, которые осуществляют операции с денежными средствами, повлекло распространение на них ряда требований к идентификации лиц, принимаемых на обслуживание, как и для классических организаций финансового сектора[9]. Порядок проведения идентификации, установленный законодательством о ПОД/ФТ, во многом совпадает с порядком проведения идентификации согласно законодательству о связи. Идентификация абонента, пользователя (известная как *know your client*) имеет важное значение не только для целостности рынка финансовых услуг, в том числе электронной, мобильной коммерции, но и для ограничения доступа преступников к финансовым услугам[10].

Угроза терроризма стала причиной ужесточения подхода к идентификации своих клиентов операторами связи и за рубежом. Если ранее в Европе можно было свободно приобрести предоплаченную сим-карту без предъявления документов и начать ею пользоваться, то после терактов 2015–2016 годов идентификация клиентов операторов связи стала включать проверку документов, удостоверяющих личность. Первыми европейскими странами, внедрившими такой уровень идентификации, стали Франция, Бельгия,

[5] Федеральный закон от 29.07.2017 № 245-ФЗ «О внесении изменений в Федеральный закон „О связи“» // СПС «КонсультантПлюс».

[6] Статья 44 Федерального закона от 07.07.2003 № 126-ФЗ «О связи» // СПС «КонсультантПлюс».

[7] Федеральный закон от 30.12.2020 № 533-ФЗ «О внесении изменений в Федеральный закон „О связи“» // СПС «КонсультантПлюс».

[8] Федеральный закон от 07.08.2001 № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма» // СПС «КонсультантПлюс».

[9] Положение Банка России от 12.12.2014 № 444-П «Об идентификации некредитными финансовыми организациями клиентов, представителей клиента, выгодоприобретателей, бенефициарных владельцев в целях противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма» // СПС «КонсультантПлюс».

[10] См.: *Arner D.W.*, *Zetzsche D.A.*, *Buckley R.P.*, *Barberis J.N.* The Identity Challenge in Finance: From Analogue Identity to Digitized Identification to Digital KYC Utilities (September 25, 2018) // European Business Organization Law Review, Forthcoming, UNSW Law Research Paper No 18–45. URL: http://dx.doi.org/10.2139/ssrn.3224115 (дата обращения: 20.03.2022).

Германия[11]. Не все были согласны с таким подходом, и не только в ЕС. Некоторые страны Восточной Европы, Балтии, Скандинавии, Португалия, а также США, Канада, Великобритания и ряд других стран[12] не пришли к законодательно закрепленной обязательной идентификации в телекоммуникациях по документам ввиду отсутствия доказательств эффективности таких мер борьбы с преступностью, а также рисков нарушения неприкосновенности частной жизни. В этих странах идентификация осуществляется без обязательного установления личности пользователя. Так, американский оператор *T-mobile* для активации сим-карты предусматривает электронную регистрацию пользователя[13]. Оператор *MINTmobile* также использует регистрацию пользователей услугами связи и указывает на необходимость подтверждения личности пользователя для реализации его права на запрос либо удаление личной информации[14].

Таким образом, регулирование идентификации пользователей услугами связи демонстрирует направленность на достоверное установление личности пользователя, в том числе на установление сведений, позволяющих это лицо найти. Это условие обуславливает ценность идентификации для государственных органов (в первую очередь правоохранительных) для эффективной реализации их полномочий.

Российское законодательство в области регулирования отношений *в коммуникационных сервисах* также предъявляет ряд требований к идентификации их пользователей[15].

> Идентификация пользователей вменена в качестве обязанности лишь российским организаторам сервиса обмена мгновенными сообщениями (далее — организаторы СОМС) и сведена к установлению абонентского номера подвижной связи пользователя сервиса и проверке на основании договора об идентификации наличия сведений о пользователе такого номера у оператора связи[16]. Сами сведения о пользователе не передаются оператором связи организатору СОМС. Такой подход позволяет уйти от избыточной обработки данных пользователей организаторами СОМС, сохраняя при этом возможность установления личности пользователя для уполномоченных государственных органов с помощью оператора связи.

Аналогичная законодательная инициатива имела место в отношении идентификации пользователей сервисов электронной почты[17], но не была реализована. При рассмотрении законопроекта в первом чтении остались неразрешенными вопросы, связанные с идентификацией пользователей иностранными организаторами сервисов электронной почты, а также возможным отсутствием у пользователя сервиса мобильного телефон (хотя сейчас сложно такое представить), что сделает невозможным использование сервиса электронной почты.

Как мы видим, проведение идентификации организаторами коммуникационных сервисов значительно менее урегулировано в сравнении с идентификацией при предоставлении услуг связи. Объясняется это тем, что при предоставлении коммуникационных сервисов используются услуги связи независимо от того, как пользователь получает доступ к этим сервисам — с помощью мобильного телефона или через компьютер. В связи с этим государственные органы имеют воз-

[11] См., напр.: ст. 172 Telekommunikationsgezetz. URL: https://www.gesetze-im-internet.de/tkg_2021/index.html (дата обращения: 20.03.2022).

[12] GSMA Access to Mobile Services and Proof-of-Identity: Global policy trends, dependencies and risks/ URL: https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2018/02/Access-to-Mobile-Services-and-Proof-of-Identity.pdf (дата обращения: 20.03.2022).

[13] T-mobile Privacy Notice. URL: https://www.t-mobile.com/privacy-center/our-practices/privacy-policy (дата обращения: 20.03.2022).

[14] MINTmobile Privacy policy. URL: https://www.mintmobile.com/privacy-policy/ (дата обращения: 20.03.2022).

[15] См.: *Куфлева В.Н., Кубрак В.С.* Проблемы реализации права на тайну переписки в мессенджерах: теоретический и компаративистский аспекты // Гуманитарные, социально-экономические и общественные науки. 2018. № 10. С. 15.

[16] Постановление Правительства РФ от 20.10.2021 № 1801 «Об утверждении Правил идентификации пользователей информационно-телекоммуникационной сети „Интернет“ организатором сервиса обмена мгновенными сообщениями» // СПС «КонсультантПлюс».

[17] Паспорт проекта Федерального закона № 808655-7 от 16.10.2019 «О внесении изменений в ст. 10.1 Федерального закона „Об информации, информационных технологиях и о защите информации“» (в части установления обязанностей организатора сервиса электронной почты). URL: https://sozd.duma.gov.ru/bill/808655-7 (дата обращения: 20.03.2022).

можность использовать абонентскую базу операторов связи для выполнения своих задач.

Важно сделать акцент на том, что *информация, устанавливаемая, передаваемая в процессе коммуникаций, представляет ценность главным образом тогда, когда есть возможность соотнести эту информацию с конкретным лицом.*

> И доктрина, и судебная практика признают, что тайна связи защищает любые сведения, передаваемые, сохраняемые и устанавливаемые с помощью телефонной аппаратуры, включая данные о входящих и исходящих сигналах соединений телефонных аппаратов *конкретных пользователей*[18]. Связь с конкретным пользователем — один из определяющих признаков информации, которая подпадает под режим тайны связи.

Информацию, составляющую тайну связи, можно условно разделить на содержание соединения и сведения о соединении. Если содержание соединения можно довольно просто определить, то сведения о соединении представляют собой широкую и неопределенную категорию. Вместе с тем интерес представляют сведения о соединении, идентифицирующие либо позволяющие идентифицировать пользователя. В отношении абонентов — физических лиц такие сведения квалифицируются как персональные данные.

В настоящее время в российском законодательстве, как и в ЕС[19], заложен экспансионистский подход к понятию персональных данных, когда под персональными данными понимается любая информация, прямо или косвенно относящаяся к определенному или определяемому лицу.

В США аналогичный подход рассматривается в контексте концепции *PII 2.0*[20] *(personally identifiable information)*, согласно которой любые сведения об идентифицированном лице и сведения, позволяющие идентифицировать лицо в будущем, признаются эквивалентными. Эта концепция пришла на смену редукционистской концепции *PII*, когда под личной информацией понималась только такая, которая относилась к идентифицированному лицу. Исходя из редукционистского подхода, при отсутствии информации, позволяющей идентифицировать человека, риски для конфиденциальности отсутствуют. Однако концепция *PII* была подвергнута жесткой критике как «фатально ошибочная»[21], поскольку существует множество источников информации, позволяющих косвенно определить лицо в информационной сфере.

Фактически редукционистский подход применялся и в России до расширения в 2011 году определения персональных данных[22], после чего судебная и правоприменительная практика, связанная с персональными данными, перешли на рельсы европейского экспансионистского подхода. Указанный подход по аналогии может быть применен к сведениям об абоненте — юридическом лице, его пользователях, особенно учитывая описанный ранее порядок их идентификации. То же самое актуально для корпоративных пользователей сервисов распространения информации в сети «Интернет».

Опираясь на приведенные аргументы, можно сделать вывод, что связь с конкретным пользователем строится на сведениях о соединениях, включая сведения об абоненте и его устройстве, которые прямо или косвенно позволяют определить абонента. К ним можно отнести сведения непосредственно об абоненте (имя, адрес места жительства, паспортные данные); уникальный идентификатор, выделяемый абоненту при заключении договора об оказании услуг связи

---

[18] Определение КС РФ от 02.10.2003 № 345-О; п. 11 Постановления Пленума ВС РФ от 01.06.2017 № 19; п. 4 Постановления Пленума ВС РФ от 25.12.2018 № 46 // СПС «КонсультантПлюс».

[19] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679 (дата обращения: 20.03.2022).

[20] *Schwartz P.M., Solove D.J.* The PII Problem: Privacy and a New Concept of Personally Identifiable Information // New York University Law Review. 2011. Vol. 86. P. 1814. URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1909366 (дата обращения: 20.03.2022).

[21] *Ohm P.* Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization. 57 UCLA L. REV. 1701 (2010). URL: https://www.uclalawreview.org/pdf/57-6-3.pdf (дата обращения: 20.03.2022).

[22] Федеральный закон от 25.07.2011 № 304-ФЗ «О внесении изменений в Федеральный закон „О персональных данных“» // СПС «КонсультантПлюс».

(номер телефона или иной идентификатор); сведения об абонентском оборудовании, посредством которого установлено соединение (*IMEI, IP*-адрес и т.п.).

> Учитывая квалифицирующую роль сведений о соединении, позволяющих определить пользователя (назовем их идентифицирующими сведениями), представляется, что тайна связи имеет место в любых случаях, когда имеется или возникает совокупность идентифицирующих сведений и иных сведений о соединении и/или содержания соединения. Это можно сравнить с картинкой, собранной из двух пазлов как минимум. Если к пазлу с идентифицирующими сведениями добавить пазл с иными сведениями о соединении (например, геолокацией или номером вызываемого абонента) или пазл с содержанием соединения, то картинка становится целой и должна охраняться режимом тайны связи. То же самое будет происходить, если есть пазл со сведениями о соединении или содержанием соединения, которому добавляется пазл с идентифицирующими сведениями.

Анализ судебной практики позволяет проиллюстрировать сказанное на примере взаимодействия операторов связи, организаторов распространения информации в сети «Интернет» с государственными органами.

## 2. Идентификационные запросы государственных органов

Здесь мы рассмотрим ситуацию, когда у государственного органа есть пазл со сведениями о соединении и органом запрашивается недостающий пазл с идентифицирующими сведениями.

Как было отмечено ранее, одной из целей идентификации пользователей коммуникационных сервисов выступил публичный интерес — обеспечение общественной безопасности, борьба с преступностью, терроризмом. В действительности эта цель может толковаться довольно широко.

Сведения об абонентах, пользователях — физических лицах, установленные операторами связи при проведении идентификации, — это персональные данные. Такой правовой режим позволяет государственным органам обрабатывать для выполнения возложенных на них законодательством полномочий такие данные без согласия субъектов персональных данных. Это также означает, что при наличии необходимых полномочий у соответствующего государственного органа оператор связи обязан предоставить сведения об абоненте, пользователе такому государственному органу[23]. Данным инструментом активно пользуются в своей деятельности налоговые органы, служба судебных приставов, антимонопольная служба и т.п.

Однако в ряде случаев возникают сложности с выполнением операторами связи такой обязанности ввиду пересечения режимов персональных данных и тайны связи.

Так, Управление Федеральной антимонопольной службы (ФАС) привлекло оператора связи к административной ответственности за отказ предоставить сведения об абоненте, который, по данным ФАС, посещал определенный сайт в конкретное время с определенного *IP*-адреса. Оператор связи мотивировал свой отказ необходимостью вмешательства в тайну связи[24] абонента для предоставления запрашиваемой информации, что противоречит ст. 23 Конституции России, а также ст. 63 Федерального закона «О связи». Хотя ранее российские суды относили такую информацию к тайне связи[25], рассматривая весь комплекс данных в совокупности, в этом споре ВС РФ встал на сторону ФАС и обязал оператора связи предоставить запрошенную информацию[26].

В основу позиции суда легли доводы о том, что сведения о пользователе услугами связи относятся к персональным данным и не относятся к тайне связи, поскольку эти данные не установлены в процессе оказания услуг связи. Обработка оператором связи

[23] См.: подп. 2 п. 1 ст. 6, ст. 7 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» // СПС «КонсультантПлюс».

[24] Согласно Определению КС РФ от 02.10.2003 № 345-О к тайне связи относятся любые сведения, передаваемые, сохраняемые и устанавливаемые с помощью телефонной аппаратуры, включая данные о входящих и исходящих сигналах соединений телефонных аппаратов конкретных пользователей.

[25] Определение Московского городского суда от 06.03.2012 № 33-7194 // СПС «КонсультантПлюс».

[26] Постановление ВС РФ от 30.03.2016 № 82-АД16-1 // СПС «КонсультантПлюс».

информации, хоть и составляющей тайну связи (время интернет-соединения, адрес сайта, *IP*-адрес и пр.), для установления сведений о пользователе в таком случае не будет являться нарушением тайны связи. Другие суды в последующих спорах следовали приведенной позиции ВС РФ[27].

> Приведенный вывод суда расходится с европейским подходом, направленным на более серьезную защиту сведений, составляющих тайну связи.

Европейский суд по правам человека в деле *Benedik v. Slovenia*[28] дал оценку действий интернет-провайдера в схожем споре. Поводом для жалобы послужило то, что интернет-провайдер в ответ на запрос полиции предоставил сведения о пользователе, посещавшем определенный сайт с использованием определенного динамического *IP*-адреса. ЕСПЧ обратил внимание на то, что для ответа на запрос полиции интернет-провайдер должен был оценить установленные и сохраненные данные, касающиеся телекоммуникационных событий. Использование этих данных само по себе вызывает нарушение неприкосновенности частной жизни и конфиденциальности коммуникаций. Поэтому ЕСПЧ признал действия интернет-провайдера нарушающими ст. 8 Конвенции ЕС о защите прав человека и основных свобод[29], которая признает право каждого на уважение его частной и семейной жизни, жилища и корреспонденции. Подобная практика не единична[30].

## 3. Запросы государственными органами обезличенных сведений о соединениях

В этой части показаны ситуации, когда у государственного органа есть пазл с идентифицирующими сведениями и запрашивается недостающий пазл со сведениями о соединении.

Ранее мы указали: для организаторов сервиса электронной почты не установлено обязанности по идентификации пользователей в смысле установления личности пользователя. На практике это породило споры, связанные с отнесением обезличенных сведений о переписке к тайне связи.

В деле ООО «Рамблер Интернет Холдинг» суд указал на то, что сведения о сообщениях, передаваемых по электронной почте, которые не позволяют определить пользователя сервиса, не являются сведениями, составляющими тайну связи[31]. По мнению суда, хотя переписка по электронной почте и охраняется тайной связи, но сведения о сообщениях не подпадают под такое регулирование именно ввиду отсутствия связи переписки с конкретной личностью. Вывод суда был сделан на основании того, что в пользовательском соглашении почтового сервиса нет обязанности пользователя указывать свои персональные данные. Законодательное регулирование идентификации пользователя сервиса электронной почты также отсутствует.

В 2021 году судами использовался аналогичный аргумент в ряде решений по делам об оспаривании действий налогового органа о привлечении операторов связи к ответственности за отказ предоставить детализацию телефонных соединений, совершенных с использованием определенного номера телефона. По мнению судов, под тайной телефонных переговоров понимается любая информация, имеющаяся у оператора связи и касающаяся конкретного абонента, которая позволяет его идентифицировать, а также установить содержание переговоров. А отсутствие у налогового органа сведений об имени пользователя номера, в отношении которого запрошены сведения о соединениях, позволяет утверждать, что такие сведения являются обезличенными и поэтому не могут быть отнесены к тайне связи[32].

---

[27] См.: постановления Восьмого арбитражного апелляционного суда от 01.11.2016 № А70-4914/2016; Девятого арбитражного апелляционного суда от 26.11.2019 № 09АП-57241/2019 // СПС «КонсультантПлюс».

[28] Постановление ЕСПЧ от 24.04.2018 по делу *Benedik v. Slovenia* (№ 62357/14). URL: https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-154288%22]} (дата обращения: 20.03.2022).

[29] Европейская конвенция по правам человека. URL: https://www.echr.coe.int/documents/convention_rus.pdf. (дата обращения: 20.03.2022).

[30] См., напр.: C-207/16 Ministerio Fiscal, ECLI:EU:C:2018:788, October 2. 2018. URL: https://curia.europa.eu/juris/liste.jsf?num=C-207/16 (дата обращения: 20.03.2022).

[31] См.: постановления Девятого арбитражного апелляционного суда от 19.09.2013 № 09АП-29641/2013, Федерального арбитражного суда Московского округа от 15.01.2014 № Ф05-16359/2013 по делу № А40-56844/13-149-539; Определение об отказе в передаче дела в Президиум ВАС РФ от 16.06.2014 № ВАС-5501/14 // СПС «КонсультантПлюс».

[32] См.: постановления Девятого арбитражного апелляционного суда от 08.06.2020 № 09АП-17966/202, Арбитражного

Выводы судов по указанным спорам, безусловно, вызывают ряд вопросов. Запросы государственных органов были направлены на получение сведений о соединениях с конкретного идентификатора (*IP*-адреса, номера телефона, адреса электронной почты). При этом, как справедливо отмечается в научной литературе[33] и что было основным предметом критики в описанной ранее редукционистской концепции *PII*, лицо может быть определено посредством различных идентификаторов.

> Исследования последних лет о приватности показывают, что обезличивание посредством удаления имени пользователя не исключает нарушения тайны связи. Существует большое количество источников, информация из которых после объединения с анонимными данными позволяет идентифицировать человека[34]. Поскольку государственному органу в обоих случаях известен идентификатор пользователя, то говорить о невозможности идентификации пользователя услугами связи не приходится.

Если вспомнить позицию российских судов по отношению к идентификационным запросам, то государственному органу не составляет труда обратиться к оператору связи с запросом о предоставлении сведений об абоненте, совершившем конкретное соединение, и получить недостающий пазл с идентифицирующими сведениями, составив тем самым полную картину о соединениях конкретного лица.

Учитывая квалифицирующую роль идентификации и экспансионистский подход, правовой режим тайны связи должен применяться в любых случаях, когда имеется или возникает совокупность идентифицирующих сведений и иных сведений о соединении и/или содержания соединения.

Итак, идентификация посредством установления личности и сведений о ней на основании документов, удостоверяющих личность, представляет ценность для государства, его органов. Ценность объясняется именно тем, что идентификация позволяет соотнести сведения, составляющие тайну связи, с конкретным (идентифицированным либо идентифицируемым) лицом. Вместе с тем нельзя забывать о соблюдении законодательно закрепленных требований, которые должны соблюдаться при ограничении права на тайну связи этого конкретного лица.

## 4. Идентификация как угроза причинения вреда при обработке тайны связи

Идентификация и возможность идентификации пользователя в коммуникациях могут быть как условием обеспечения конфиденциальности коммуникаций, так и фактором риска ограничения тайны связи.

Помимо этого, в современных условиях невозможно игнорировать тенденции к обработке различных видов информации, в том числе информации ограниченного доступа. Для признания допустимой обработки информационными посредниками сведений, составляющих тайну связи, для исключения либо минимизации вероятности наступления вреда от обработки сведений, составляющих тайны связи, эффективным может быть риск-ориентированный подход Э. Граттон[35].

В основе ее подхода лежат две гипотезы:

1) определенные Д. Солове типы действий с информацией, которые могут причинить вред приватности, — сбор, использование, распространение и личные вторжения[36] (Э. Граттон опиралась на первые три типа действий, которые относятся к обработке конфиденциальной информации);

2) выделенные Р. Кало виды вреда, возникающего при нарушении конфиденциальности — субъективный

суда Московского округа от 21.09.2020 по делу № А40-272978/2019; Определение ВС РФ от 19.01.2021 № 305-ЭС20-21500. URL: https://kad.arbitr.ru/Card/7109553c-f3c2-4a7e-a9dd-408bd98be43f (дата обращения: 20.03.2022).

[33] См., напр.: *Савельев А.И.* Научно-практический постатейный комментарий к Федеральному закону «О персональных данных». М., 2017.

[34] См.: *Ohm P.* Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization // UCLA Law Review. 2010. Vol. 57. P. 1701. URL: https://www.uclalawreview.org/pdf/57-6-3.pdf (дата обращения: 20.03.2022).

[35] *Gratton E.* Understunding personal information: managing privacy risks. Markham, 2013.

[36] *Solove D.* A Taxonomy of Privacy // University of Pennsylvania Law Review. 2006. Vol. 154. No. 3. P. 477–564. URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=667622 (дата обращения: 20.03.2022).

вред (психологический, эмоциональный ущерб в виде страдания, унижения, стыда, смущения, гнева, ощущения постоянного наблюдения и пр.) и объективный вред (физический, финансовый вред, неравенство в результате дискриминации, профилирования, поведенческого маркетинга и т.д.)[37].

В исследовании Э. Граттон продемонстрировано, что вид возможного вреда напрямую связан с типом обработки информации: сбор информации приводит к субъективному ущербу, использование — объективному и субъективному, раскрытие — субъективному вреду, а также к объективному вреду в результате использования информации третьими лицами, получившими доступ к ней в результате раскрытия. Отмечено, что для субъективного вреда характерны критерии: *возможность идентификации лица*, которому принадлежит информация; чувствительность информации для лица; степень доступности информации для третьих лиц. Для объективного вреда обычно существует один критерий — причинит ли использование информации вред или нет. Но в отдельных случаях объективный вред может быть причинен при *идентифицируемости субъекта* (адаптивное ценообразование, дискриминация, профилирование). Этому способствовало появление цифровых технологий, которые позволяют анализировать данные и принимать решения, влияющие на человека, стоящего за профилем, без необходимости знать его имя. Достаточно понимания, что влияние оказывается на конкретного (пусть и анонимного) человека.

> Поскольку возможность идентификации — важный критерий при оценке возможности причинения вреда, то обработка конфиденциальной информации допустима только при условии необратимой утраты связи с конкретным лицом, что, в свою очередь, нуждается в нормативной правовой поддержке[38].

Применяя риск-ориентированный подход к обработке информационным посредником сведений, составляющих тайну связи, условия допустимости обработки сведений, составляющих тайну связи, могут быть следующими.

*Сбор* данных уже сейчас осуществляется операторами связи и организаторами коммуникационных сервисов в силу оказания услуг связи и предоставления сервиса. Поэтому субъективный вред лицу не причиняется, за исключением ситуаций, которые мы затронем ниже.

*Использование* данных сопряжено с субъективным и объективным ущербом, поэтому необходима разработка комплекса мер по предотвращению такого ущерба. В части предотвращения субъективного ущерба потребуется *исключение возможности идентификации*, использование наименее чувствительных данных (например, данных о соединениях без вмешательства в их содержание), обработка данных без участия человека, но с возможностью контроля с его участием. Для исключения вероятности причинения объективного вреда выход видится в получении согласия лица, чьи данные планируются к обработке. Помимо указанных мер, следует обеспечить соблюдение общих условий обработки конфиденциальной информации, которые подробно описаны в законодательстве о защите персональных данных.

При таком способе обработки, как использование, важно учитывать концепцию контекстуальной целостности Х. Ниссенбаум[39]. Концепция вытекает из применяемой на Западе доктрины разумного ожидания[40]. Идея концепции применительно к обработке информации заключается в том, что все события (сбор, использование, распространение информации) происходят в конкретном контексте, этот контекст определяет применимый набор норм, роли, ожидания и вытекающие из этого действия. Однако это не значит, что обработка возможна только для обеспечения коммуникаций. Рассматривая вопрос о перемещении информации между контекстами, Н.А. Дмитрик обратил внимание на согласие субъекта, чья информация обрабатывается, как на инструмент, который обеспечивает связь

[37] *Calo R.* The Boundaries of Privacy Harm // Indiana Law Journal. 2011. Vol. 86. URL: http://ilj.law.indiana.edu/articles/86/86_3_Calo.pdf (дата обращения: 20.03.2022).

[38] См.: *Двинских Д.Ю., Талапина Э.В.* Риски развития оборота данных в государственном управлении // Вопросы государственного и муниципального управления. 2019. № 3. С. 17.

[39] *Nissenbaum H.* Privacy as Contextual Integrity // Washington Law Review. 2004. Vol. 79. Iss. 1. P. 119–158. URL: https://crypto.stanford.edu/portia/papers/RevnissenbaumDTP31.pdf (дата обращения: 20.03.2022).

[40] Katz v. United States, 389 US 347 (1967). URL: https://supreme.justia.com/cases/federal/us/389/347/ (дата обращения: 20.03.2022).

между субъектом и контекстом[41]. То есть при согласии субъекта с изменением контекста обработка информации может иметь место. В литературе отмечается, что согласие в таких случаях — единственная защита от нарушения обязанностей в отношении вторжения или публичного раскрытия информации[42]. При выражении согласия с обработкой своих данных, данных о своей переписке лицо имеет возможность найти баланс между своим правом на тайну переписки и иными правами, ценностями, потребностями.

Распространение сведений, которые составляют тайну связи, мы не рассматриваем, так как разглашение таких сведений недопустимо в силу прямого запрета в международных документах, конституционных нормах, закрепляющих тайну связи, а также в связи с тем, что распространение сведений с высокой вероятностью может повлечь как субъективный, так и объективный ущерб.

Наряду с указанным выше, может быть рассмотрен вопрос о допустимости обработки обезличенных данных, составляющих тайну связи, причем таких, которые представляются наименее чувствительными для пользователя (хотя вопрос о чувствительности данных также является дискуссионным).

Например, Европейская директива о конфиденциальности электронных коммуникаций[43] допускает обработку данных о местонахождении пользователей при условии их анонимности. Американский закон о телекоммуникациях[44] позволяет операторам связи использовать агрегированную пользовательскую информацию (совокупные данные, относящиеся к группе или категории услуг или клиентов, из которых были удалены индивидуальные идентификационные данные и характеристики) в целях, отличных от целей оказания услуг связи. Примером может служить взаимодействие немецкого оператора связи *Deutsche Telecom* с институтом *Robert Koch*, который занимается инфекционными заболеваниями и является одним из главных учреждений, куда стекается информация о *COVID*-19, по предоставлению данных о передвижениях населения страны в виде «тепловых карт»[45]. Аналогичное взаимодействие было налажено между французским оператором связи *Orange* и национальным институтом здравоохранения Франции *Inserm*[46] *по передаче данных о местонахождении мобильных устройств в обезличенном и агрегированном виде.*

Учитывая описанное выше, обработку сведений, составляющих тайну связи, можно считать допустимой при соблюдении условий, которые исключают возможный ущерб. Это, в свою очередь, при надлежащей правовой проработке позволит решить часть проблем, связанных с нахождением баланса между интересами человека, государства и информационных посредников.

## The Role of Identification for the Communication Secrecy

The article contains an analysis of legal regulation, as well as doctrinal approaches to the identification of users in communications in terms of the significance of identification for the communication secrecy. The author pays attention to such aspects of identification as: a) its value for communication Internet services and the state in the course of implementation of public functions, b) risks of harm. Relations to personality (possibility of identification) of the user is

[41] *Дмитрик Н.А.* История, смысл и перспективы института персональных данных // Вестник гражданского права. 2020. № 3. Т. 20. С. 56. URL: https://doi.org/10.24031/1992-2043-2020-20-3-43-82 (дата обращения: 20.03.2022).

[42] *Hubbard P.* The Need for Privacy Torts in an Era of Ubiquitous Disclosure and Surveillance // Cudd A., Navin M. (eds) Core Concepts and Contemporary Issues in Privacy. Amintaphil: The Philosophical Foundations of Law and Justice. Vol. 8. Springer, Cham, 2018. P. 148. URL: https://link.springer.com/chapter/10.1007%2F978-3-319-74639-5_10 (дата обращения: 20.03.2022).

[43] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector. URL: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32002L0058 (дата обращения: 20.03.2022).

[44] 47 U.S. Code § 222. Privacy of customer information // Legal Information Institute. URL: https://www.law.cornell.edu/uscode/text/47/222 (дата обращения: 20.03.2022).

[45] Deutsche Telekom überlässt Robert Koch-Institut Bewegungsprofile von Nutzern. URL: https://deutsch.rt.com/inland/99427-deutsche-telekom-ueberlasst-robert-koch/ (дата обращения: 20.03.2022).

[46] Les statistiques issues du réseau de téléphonies mobiles au service de la lutte contre la pandémie de Covid-19. URL: https://presse.inserm.fr/les-donnees-des-telephones-mobiles-au-service-de-la-lutte-contre-la-pandemie-de-covid-19/38831/ (дата обращения: 20.03.2020).

defined by the author as a qualifying sign of the communication secrecy. The author also considers possible conditions for the processing of communication secrecy data from the point of view of a risk-based approach and the contextual integrity of confidential information, including through depersonalization of information about communications.

***Keywords***: *communication secrecy, confidentiality, identification, personal data, communications*

## INFORMATION ABOUT THE AUTHOR

**Anzhelika N. Izotova**
Head of projects of the legal department Mobile TeleSystems PJSC, junior researcher for the Institute for Law in the Digital Environment National Research University Higher School of Economics (e-mail: anzheliki@rambler.ru).

## REFERENCES

Calo, R. The Boundaries of Privacy Harm. Indiana Law Journal. 2011. Vol. 86. P. 1131–1162.

Dvinskih, D.Ju., Talapina, Je.V. Risks of Development of Data Circulation in Public Administration [*Riski razvitija oborota dannyh v gosudarstvennom upravlenii*]. Issues of State and Municipal Management [*Voprosy gosudarstvennogo i municipal'nogo upravlenija*]. 2019. No. 3. P. 7–30.

Dmitrik, N.A. History, Essence and Prospects of Personal Data Protection [*Istorija, smysl i perspektivy instituta personal'nyh dannyh*]. Civil Law Review [*Vestnik grazhdanskogo prava*]. 2020. No. 3 (20). P. 43–82.

Gratton, E. Understunding Personal Information: Managing Privacy Risks. Markham: LexisNexis, 2013. 515 p.

Hubbard, P. The Need for Privacy Torts in an Era of Ubiquitous Disclosure and Surveillance. In: Cudd A., Navin M. (eds) Core Concepts and Contemporary Issues in Privacy. Amintaphil: The Philosophical Foundations of Law and Justice. Vol. 8. Springer, Cham. 2018. P. 137–157.

Kufleva, V.N., Kubrak, V.S. Problems of Realization of the Right to Privacy of Correspondence in Messengers: Theoretical and Comparative Aspects [*Problemy realizacii prava na tajnu perepiski, v messendzherah: teoreticheskij i komparativistskij aspekty*]. Humanities, Socio-economic and Social Sciences [*Gumanitarnye, social'no-jekonomicheskie i obshhestvennye nauki*]. 2018. No. 10. P. 153–157.

Nissenbaum, H. Privacy as Contextual Integrity. Washington Law Review. 2004. Vol. 79. Iss. 1. P. 119–158.

Ohm, P. Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization. 2010. 57 UCLA L. REV. P. 1701–1777.

Savelyev, A.I. Scientific and practical article-by-article commentary to the Federal Law "On Personal Data" [Nauchno-prakticheskij postatejnyj kommentarij k Federal'nomu zakonu "O personal'nyh dannyh"]. Moscow: Statut, 2017. 320 p.

Schwartz, P.M., Solove D.J. The PII Problem: Privacy and a New Concept of Personally Identifiable Information. New York University Law Review. 2011. Vol. 86. P. 1814–1894.

Solove, D. A Taxonomy of Privacy. University of Pennsylvania Law Review. 2006. Vol. 154. No. 3. P. 477–564.

Sullivan, C. Digital Identity: An Emergent Legal Concept. University of Adelaide Press. 2011. 162 p.

**ВЛАДИСЛАВ ВЛАДИМИРОВИЧ АРХИПОВ**

доцент, заведующий кафедрой теории и истории государства и права юридического факультета СПбГУ, доктор юридических наук

# ПЕРСОНАЖИ (АВАТАРЫ) В МНОГОПОЛЬЗОВАТЕЛЬСКИХ КОМПЬЮТЕРНЫХ ИГРАХ: ВОПРОСЫ ПРАВОВОЙ КВАЛИФИКАЦИИ В СВЕТЕ МЕЖДИСЦИПЛИНАРНЫХ ИССЛЕДОВАНИЙ*

Правовой режим персонажей (аватаров) многопользовательских компьютерных игр и виртуальных миров — вопрос малоисследованный (не считая проблематику виртуальной собственности). С внешней точки зрения аватары соотносятся с виртуальными мирами как часть и целое, вследствие чего могут рассматриваться как предмет правоотношений в области интеллектуальной собственности, ограничений на распространение информации, регулирования коммуникационных сервисов, пределов правового регулирования внутриигровых отношений. Однако с внутренней точки зрения аватары — способ самопрезентации пользователей, выражения их идентичности или даже части «цифрового тела» в медиафилософском смысле. Это, в свою очередь, позволяет соотносить аватаров с категориями персональных данных и нематериальных благ. Наконец, отдельно может возникать вопрос о различении игровых персонажей (аватаров) и ботов. Реализовать принцип идентификации искусственного интеллекта можно лишь в значимых случаях, которые определяются согласно той или иной концепции «магического круга». В статье намечен методологический потенциал представленных идей для теоретико-правового анализа проблем субъектности и идентичности в праве.

***Ключевые слова:*** *компьютерные игры, виртуальные миры, персонажи, аватары, интеллектуальная собственность, Интернет, информационное право, «магический круг», семантические пределы права, смысловые пределы права, идентичность, субъектность*

DOI: 10.37239/0869-4400-2022-18-3-58-74

* Статья подготовлена при финансовой поддержке РФФИ — научный проект 18-29-16015 «Комплексное исследование правовых и этических аспектов, связанных с разработкой и применением систем искусственного интеллекта и робототехники». Автор выражает благодарность К.А. Очеретяному за рекомендации междисциплинарных исследований по вопросам отношения игроков к аватарам в многопользовательских играх и Н.А. Дмитрику за конструктивные комментарии к статье.

## 1. Введение

Исследователи правовых проблем многопользовательских компьютерных игр и виртуальных миров знают несколько практических примеров, упоминание которых считалось своего рода признаком дурного тона еще десять лет назад. Отчасти потому, что к тому моменту подобные примеры были на слуху уже практически у всех; отчасти потому, что за ними не последовали какие-либо заметные изменения в соответствующих социальных практиках, и их ценность в итоге оказалась сомнительной. К числу таких примеров можно отнести следующий: в 2007 году предприниматель Алисса ЛаРош *(Alyssa LaRoche)* инициировала в США процесс регистрации своего аватара «Эйми Вебер» *(Aimee Weber)* в виртуальном мире *Second Life* в качестве товарного знака по 42-му классу — «Разработка программного обеспечения, в частности создание контента для виртуальных миров и трехмерных платформ» *(Computer programming services, namely, content creation for virtual worlds and three dimensional platforms)*[1]. Сведения о данном товарном знаке доступны на сайте Бюро по патентам и товарным знакам США *(United States Patent and Trademark Office)*, номер записи 3531683[2]. Дата прекращения регистрации товарного знака — 12 июня 2015 года.

Пример сам по себе интересный, поднимающий немало теоретических вопросов в области права интеллектуальной собственности и в области правового значения связи между пользователем и аватаром, но на тот момент его значение казалось исчерпанным: аватар зарегистрирован как товарный знак — хорошо, и что дальше?[3] Возможно, сейчас ситуация поменялась, и вспомнить об этом примере вновь, но под другим углом зрения, вполне своевременно. Более того, его можно отнести к актуальной теме метавселенных, которая не является принципиально новой, хотя из различных маркетинговых материалов может показаться, что вопросы метавселенных именно таковы[4]. Правда, если изначально вопрос об аватарах в основном рассматривался в контексте проблем виртуальной собственности[5] и интеллектуальных прав[6], то сейчас актуализировались другие проблемы,

[1] См., напр.: *Дюранске Б.Т.*, *Кейн Ш.Ф.* Виртуальные миры, реальные проблемы // Известия высших учебных заведений. Правоведение. 2013. № 2. С. 115–134.

[2] См.: Trademark Electronic Search System (TESS) // United States Patent and Trademark Office. URL: https://tmsearch.uspto.gov/ (дата обращения: 27.03.2022). Описание товарного знака (он графический, запись сопровождается его изображением): «Цвет(а) черный, белый, зеленый, персиковый и голубой заявлен(ы) как характеристика знака. Голубой цвет присутствует в крыльях и аксессуарах для волос. Зеленый цвет присутствует в рубашке и юбке. Черный цвет присутствует в волосах, глазах, бровях, губах, очках, ожерелье, бюстгальтере, поясе, в полосатом узоре на руках и чулках, а также в области носка и голенища сапог. Все элементы рисунка также очерчены черным цветом. Белый цвет присутствует в глазах, в полосатом узоре на руках и ногах, в качестве акцентов на черных кончиках сапог, передней части сапог и на шнурках. Персиковый цвет присутствует на коже».

[3] На конференции "*Mastering the Game. Business and Legal Issues for Video Game Developers. Baltic Sea Region Perspective*" в 2015 году автор статьи был свидетелем негативной реакции аудитории, которая состояла преимущественно из юристов, практикующих в области игровой индустрии, на один из докладов представителя польского университета, где он привел этот пример (уже тогда пример рассматривался как устаревший).

[4] Отечественный медиафилософ В.В. Савчук отмечал: «нет более скоропортящегося интеллектуального продукта, чем слово „новое“». См.: *Савчук В.В.* Медиафилософия. Приступ реальности. СПб., 2014. С. 50. В схожей ситуации сейчас исследователи правовой проблематики искусственного интеллекта, которые встречают высказывания о мнимой новизне соответствующих правовых проблем. Правовая проблематика «метаверса» (за исключением некоторых специальных и характерных не для всего, что называется на практике этим словом, явлений вроде распределенного блокчейна или *NFT*) по существу не изменилась со времен первых многопользовательских игр. Их появление обычно относят к концу 1970-х – началу 1980-х годов, причем аналитические статьи по междисциплинарной проблематике взаимодействия между пользователями относятся к этому же периоду. См. напр.: *Morningstar C.*, *Randall F.F.* The Lessons of Lucasfilm's Habitat // Stanford University. URL: http://web.stanford.edu/class/history34q/readings/Virtual_Worlds/LucasfilmHabitat.html (дата обращения: 27.03.2022). Особое внимание необходимо обратить на тот факт, что даже сама концепция трехмерной виртуальной реальности и, более того, определенный опыт ее технической реализации, пусть и без блокчейна, известна уже десятилетия — речь идет о решениях на основе *VRML (Virtual Reality Modeling Language)*. См. напр.: *Raggett D*. Extending WWW to support Platform Independent Virtual Reality // W3C. 1994. URL: https://www.w3.org/People/Raggett/vrml/vrml.html (дата обращения: 27.03.2022). Любопытно, что *VRML* упоминается еще у Л. Мановича в книге: *Manovich L*. The Language of New Media. London: MIT Press: Cambridge, Massachusets. 2001. P. 30.

[5] См. напр.: *Рожкова М.А.* Виртуальное имущество и многопользовательская онлайн-игра — как различать возникающие по их поводу отношения? // Закон.ру. 2020. 6 декабря. URL: https://zakon.ru/blog/2020/12/06/virtualnoe_imuschestvo_i_mnogopolzovatelskaya_onlajn-igra__kak_razlichat_voznikayuschie_po_ih_povodu (дата обращения: 27.03.2022).

[6] Пример для данного тезиса — рассуждения Р. Бартла в статье «Подводные камни виртуальной собственности» *(Pitfalls of Virtual Property)*, в которой он рассматривает ряд контраргументов против признания виртуальной собствен-

которые по разным причинам не рассматривались в предшествующих исследованиях как приоритетные. В их число входят персональные данные[7], а также связанная с ними проблема идентификации в цифровой среде (в том смысле, что юридическое значение имеет различение между реальными субъектами и ботами, которые могут скрываться за цифровыми аватарами).

Действительно, *правовая* проблематика, связанная с персонажами (аватарами) в многопользовательских компьютерных играх, ранее почти не становилась предметом самостоятельных научных исследований. Однако сейчас, когда мы становимся свидетелями *очередной* попытки создать массовую трехмерную виртуальную реальность (метавселенную)[8], представляется возможным по-новому осмыслить известные правовые институты применительно к отношениям в современной цифровой среде. В целом это соответствует предложенному много ранее подходу, согласно которому «в виртуальных мирах представлен полный спектр проблем интернет-права» и «виртуальные миры могут использоваться как модели реального мира и как пространство для социального эксперимента»[9]. Если исходить из такого положения дел, то принципиальная разница в правовой проблематике аватаров в многопользовательских онлайн-играх и иных вариациях виртуальной реальности, которые мы видим сейчас или можем увидеть в будущем, должна отсутствовать. Попробуем разобраться, так ли это на самом деле.

## 2. Внешняя точка зрения: аватар как часть цифровой среды с правовой позиции (безотносительно связи с пользователем)

В качестве основного объекта изучения в этой статье взяты аватары — в том смысле, в котором это понятие используется в контексте именно многопользовательских онлайн-игр (которые, в свою очередь, в системе используемых терминов[10] являются разновидностью виртуальных миров в широком смысле слова и при этом могут или не могут обладать признаком виртуальной социальной реальности[11]). Выбор именно игровых виртуальных сред в качестве основной области

ности в имущественном смысле, завершая подробным анализом составляющей, связанной с интеллектуальными правами. См.: *Bartle R.* Pitfalls of Virtual Property. The Themis Group. 2004. URL: https://mud.co.uk/richard/povp.pdf (дата обращения: 27.03.2022).

[7] Здесь уместно обратить внимание на то обстоятельство, что в западной среде (где, прежде всего, актуализировались вопросы «виртуального права») новый виток дискуссии по поводу персональных данных связан с принятием 27 апреля 2016 года и вступлением в силу 25 мая 2018 года Регламента № 2016/679 Европейского парламента и Совета Европейского союза «О защите физических лиц при обработке персональных данных и о свободном обращении таких данных, а также об отмене Директивы 95/46/ЕС (Общий регламент по защите персональных данных)» *(GDPR)*.

[8] В этом контексте следует приветствовать новый виток интереса авторов к проблематике виртуальной реальности в том смысле, в котором этот термин используется в настоящей статье. Начали появляться публикации, вновь направляющие исследовательский интерес в область виртуальных миров, но уже в ином контексте. См. напр.: *Рожкова М.А.* Виртуальная реальность и Метавселенная: предмет правового исследования // Закон.ру. 2021. 12 января. URL: https://zakon.ru/blog/2022/01/12/virtualnaya_realnost_i_metavselennaya_predmet_pravovogo_issledovaniya__virtual_reality_and_metaverse (дата обращения: 27.03.2022).

[9] *Архипов В.В.* Виртуальное право: основные проблемы нового направления юридических исследований // Известия высших учебных заведений. Правоведение. 2013. № 2. С. 103–106.

[10] За точку отсчета принимается терминология, предложенная в упомянутой статье: *Архипов В.В.* Виртуальное право: основные проблемы нового направления юридических исследований. «Применительно к информационным технологиям он [виртуальный мир], в самом общем смысле, означает моделируемую компьютерными средствами относительно постоянную среду, предназначенную для взаимодействия между пользователями посредством цифровых образов, за которыми закрепилось название „аватар“» (С. 95); «…чтобы считать многопользовательскую игру виртуальным миром в широком смысле слова, она необязательно должна быть ролевой, а просто отвечать трем упомянутым признакам: содержать моделируемый мир (среду), допускать участие нескольких пользователей, которые могут быть идентифицированы, и обеспечивать возможность взаимодействия между пользователями» (С. 97). Предметом нашего исследовательского интереса являются в большей степени несессионные игры.

[11] Хотя данное качество принципиально не повлияет на основные выводы настоящей статьи, квалификация игр именно как виртуальной социальной реальности существенным образом усилит аргумент, поддерживающий тезис, связанный со значимостью аватаров для игроков. Концепция виртуальной социальной реальности подразумевает наличие социальных институтов в смысле социального конструкционизма (П. Бергер и Т. Лукман), которые развиваются в ходе взаимодействия пользователей (игроков), опосредованного виртуальной реальностью в техническом смысле слова. См.: *Архипов В.В.* Виртуальное право: основные проблемы нового направления юридических исследований. С. 98–100. Также см.: *Arkhipov V.V.* Virtual Worlds in Legal Studies. An Inquiry into the Subject of Research / 25th IVR World Congress of Philosophy of Law and Social Philosophy Paper. URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2117762 (дата обращения: 27.03.2022).

для изучения, помимо субъективных симпатий автора, также обусловлен методологически.

> Игровой характер виртуального взаимодействия сам по себе, в дополнение ко всем возможным правовым проблемам, связанным с взаимодействием субъектов права в виртуальной среде, дополняет проблематику вопросом о соотношении виртуального и реального, т.е. о пределах применения норм реального права к виртуальным отношениям.

Данная проблема также известна как проблема «магического круга», уже достаточно полно исследованная в зарубежной и отечественной литературе[12]. Преломление данной проблемы в контексте аватаров предполагает анализ того, в каком конкретно ракурсе аватары и «отношения» между ними являются частью игрового мира, который как бы выведен из-под действия реального права, а в каком — напротив, сама природа аватара определяет «разрыв» того самого «магического круга» (именно с последним ракурсом и связан один из ключевых тезисов настоящей статьи, который раскрывается в следующих частях).

Лев Манович, автор книги «Язык новых медиа» — одной из ключевых для современных междисциплинарных исследований в данной области, отмечал, что исследуемые объекты модулярны или фрактальны: «Элементы медиа, будь это изображения, звуки, формы или паттерны поведения, представлены в виде коллекции дискретных образцов (пиксели, полигоны, воксели, знаки, скрипты). Данные элементы собираются в объекты большего масштаба, но продолжают сохранять свои отдельные идентичности… Если кратко, новые объекты медиа состоят из независимых частей, каждая из которых состоит из независимых частей поменьше, и так далее, вплоть до уровня самых маленьких “атомов” — пикселей, *3D*-точек (в оригинале — *3D points* — *В.А.*) или текстовых символов»[13]. Данное наблюдение — наглядная иллюстрация тезиса, согласно которому каждая из частей объекта новых медиа должна (или, по крайней мере, может) сохранять качества всего объекта в целом. Многопользовательские онлайн-игры — объект новых медиа. Аватар (персонаж) — часть многопользовательской онлайн-игры. Попробуем оценить сходство качеств целого и его части.

С точки зрения внешнего наблюдателя, по большей части игнорирующего внутреннее субъективное отношение пользователей («внешняя точка зрения»), многопользовательская компьютерная игра или ее отдельные аспекты — объекты правоотношений, которые по-разному квалифицируются в зависимости от соответствующей отрасли права. Причем таких квалификаций может оказаться много[14]. В то же время игры по своей природе представляют собой информацию в широком смысле слова. Они интерактивны (игрок как бы «соучаствует» в создании последовательности виртуальных событий) и часто «медиальны» (игры, как правило, выражают различные социально-значимые смыслы, хотя это не обязательный признак). В силу данных обстоятельств можно выделить как минимум четыре ключевые правовые квалификации компьютерных игр как объекта правоотношения, с которыми должны тогда соотноситься и правовые квалификации аватаров (возможно, не всегда прямолинейно):

1) **интеллектуальная собственность**. Компьютерная игра, как правило, охраняемый результат интеллектуальной деятельности, который квалифицируется либо как программа для ЭВМ, либо как сложный объект[15]. Возможны и альтернативные мнения, которые при этом не отменяют основного тезиса о правовой природе игр и, в общем, не влияют на квалификацию всей или части игры как *произведения* с точки зрения авторского права (даже если речь идет о сложном объекте или о применении правового режима произведения к

[12] См. краткое обобщение истории вопроса, которая насчитывает уже много лет: *Архипов В.В.* Действие правовых норм в цифровом медиапространстве и семантические пределы права // Правоведение. 2019. Т. 63. № 1. С. 8–27.

[13] *Manovich L.* The Language of New Media. London: MIT Press: Cambridge, Massachusets. 2001. P. 30-31.

[14] Например, реализация «виртуальной собственности» как объект налогообложения с точки зрения налогового права, игра сама по себе как орудие преступления с точки зрения уголовного права и т.п. Также и в рамках отдельных рассматриваемых далее направлений возможны различные специфические случаи и нюансы: например, имя персонажа может потенциально рассматриваться как способ использования товарного знака. См. напр.: *Davis I.* Everquest 2 Fan Site Harassed By Trademark Claim // The Escapist. July 27. 2013. URL: https://www.escapistmagazine.com/everquest-2-fan-site-harassed-by-trademark-claim/ (дата обращения: 27.03.2022).

[15] По крайней мере в теории допустимо представить компьютерную игру, которая состоит из неохраняемых результатов интеллектуальной деятельности.

программе для ЭВМ). Это дает нам возможность рассмотреть вопрос об аватарах не просто как о частях произведения в функциональном смысле технического объекта, но как о частях произведения, которые могут пользоваться самостоятельной правовой охраной в смысле п. 7 ст. 1259 ГК РФ. Согласно ей «авторские права распространяются на часть произведения, на его название, на *персонаж* (курсив мой — *В.А.*) произведения, если по своему характеру они могут быть признаны самостоятельным результатом творческого труда автора и отвечают требованиям, установленным пунктом 3 настоящей статьи» (выражены в объективной форме). Такого рода формулировки в контексте исследуемой темы порождают смешение терминов, но в то же время и объясняют, почему мы нуждаемся в отдельном слове «аватар», чтобы обозначить цифровые репрезентации пользователей виртуальных миров.

> Слово «персонаж» в обыденной речи нередко используется для описания аватаров. Но в авторском праве персонаж — это часть произведения, которая выражена в объективной форме и по своему характеру может быть признана самостоятельным результатом творческого труда автора. В большинстве случаев речь идет о разных понятиях.

Обратимся к судебной практике.

Как следует из п. 82 Постановления Пленума ВС РФ от 23 апреля 2019 года № 10 «О применении части четвертой Гражданского кодекса Российской Федерации», «под персонажем следует понимать совокупность описаний и (или) изображений того или иного *действующего лица в произведении* (курсив мой — *В.А.*) в форме (формах), присущей (присущих) произведению: в письменной, устной форме, в форме изображения, в форме звуко- или видеозаписи, в объемно-пространственной форме и др.». В п. 82 указанного Постановления Пленума ВС РФ, в абз. 2, указано: «Не любое действующее лицо произведения является персонажем в смысле пункта 7 статьи 1259 ГК РФ… учитывается, обладает ли конкретное действующее лицо произведения достаточными индивидуализирующими его характеристиками: в частности, определены ли внешний вид действующего лица произведения, *характер* (курсив мой — *В.А.*), отличительные черты (например, движения, голос, мимика, речевые особенности) или другие особенности, в силу которых действующее лицо произведения является узнаваемым даже при его использовании отдельно от всего произведения в целом».

> В целом для нас важно то, что во многих случаях, связанных с многопользовательскими онлайн-играми, весьма сомнительно, что аватары могут рассматриваться по общему правилу как охраноспособные персонажи с точки зрения авторского права. Чтобы аватар считался персонажем, он должен быть «вписан» в сюжет, чтобы быть именно «действующим лицом»[16]. Однако примечательно и другое: в некоторых случаях мы все же вполне определенно можем считать, что такое возможно, и этот вывод как раз представляется новым и интересным.

Дело в том, что некоторые, хотя и очень редкие на сегодня многопользовательские игры предусматривают правило об обязательном отыгрыше роли персонажа *(roleplay enforced)*. Одна из наиболее известных таких игр — текстовая ролевая онлайн-игра *Achaea* от компании *Iron Realms*[17]. Суть правила сводится к тому, что каждый игрок (в идеале) продумывает авторское внешнее описание персонажа[18], его «мягкие» характеристики (установки, ценности и пр.) и во внутриигровом общении выступает от лица персонажа. Разговоры на любые темы не от лица персонажа в большинстве внутриигровых чатов запрещены. В итоге игра может быть уподоблена коллективному созданию пьесы посредством импровизации, а каждый аватар в то же время теоретически может рассматриваться в

[16] Здесь мы исходим из гипотезы о том, что этого как раз не происходит в *MMORPG* с «сюжетом», имеющим по факту ту же творческую природу, что и сюжет однопользовательских игр, когда каждый игрок условно представляется в качестве единственного «избранного». Но таких «избранных» на игровом сервере одновременно находится великое множество — этим «грешат» и уже ставшие классическими игры вроде *World of Warcraft* или *Star Wars: the Old Republic*, и новинки в жанре вроде недавнего *New World*.

[17] См.: https://www.achaea.com/ (дата обращения: 28.03.2022).

[18] Аутентичный пример описания одного из персонажей автора в упомянутом игровом мире, который с учетом всех остальных обстоятельств и контекста вполне может претендовать на режим части литературного произведения как элемента сложного объекта: «He is a stout dwarf of particularly strong physique. Five feet tall, he is of those dwarves who could never ever conceal protruding muscles. His square cut face is adorned with a scar going down from left ear through burly nose to cheek. A few wrinkles appear on his expansive forehead. He has a voluminous burning red hair beard and fizzled moustache».

качестве персонажа, но уже как часть произведения. С практической точки зрения данная ситуация не вызывает существенных затруднений в тех случаях, когда лицензионное соглашение с конечным пользователем предусматривает переход интеллектуальных прав на создаваемый игроками контент правообладателю игры, но с теоретической точки зрения этот пример представляется крайне интересным и релевантным;

2) **информация**. Данная правовая квалификация может зависеть от того, рассматривается ли информация как общий объект правоотношений в конкретной правовой системе. В Российской Федерации игры будут рассматриваться как информация независимо от обстоятельств в силу общего определения. Согласно п. 1 ст. 2 Федерального закона от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (далее — Закон об информации), информация — это сведения (сообщения, данные) независимо от формы их представления. Данный подход косвенно подтверждается и тем широким пониманием информации, которое встречается в нормативных правовых актах (например, в п. 2 ч. 2 ст. 15.2 Закона об информации используется словосочетание «информация, содержащая объекты авторских и [или] смежных прав») и в правоприменительной практике. Из этого следует: и к играм, и к аватарам должно применяться информационное законодательство в части норм, непосредственно установленных Законом об информации (например, об ограничении доступа к определенным видам информации), и в части специальных норм, предусмотренных иными нормативными правовыми актами, нацеленными на регулирование отношений по поводу особых видов информации, например о защите детей от информации, причиняющей вред их здоровью и развитию;

3) **средство коммуникации**. Многопользовательские компьютерные игры обычно воспринимаются как «несерьезные» среды, в которых лишь изредка может разрываться «магический круг» (что не вполне соответствует действительности). Однако некоторые нормы действующего на момент написания статьи российского законодательства не содержат исключений в отношении контекста применения — игрового или неигрового. К числу таких норм относятся, в частности, положения ст. 10.1 Закона об информации и соответствующих подзаконных актов. Так, согласно ч. 1 ст. 10.1 Закона об информации, «лицо, осуществляющее деятельность по обеспечению функционирования информационных систем и (или) программ для электронных вычислительных машин, которые предназначены и (или) используются для приема, передачи, доставки и (или) обработки электронных сообщений пользователей сети „Интернет“» является «организатором распространения информации в сети „Интернет“». Аналогичное по содержанию определение с поправкой на применимость к объекту, а не к субъекту, дано и «коммуникационным интернет-сервисам» на уровне подзаконных актов[19].

> Приведенные широкие определения практически не дают возможности игровым компаниям избежать потенциальной правовой квалификации их самих как организаторов распространения информации в Интернете, а их многопользовательских игр — как коммуникационных интернет-сервисов.

В то же время теоретически сохраняется возможность говорить о том, что в случае, если игра ролевая и содержит упомянутое выше правило об обязательном отыгрыше роли персонажа, общение происходит как бы между аватарами (так как в этом реализуется художественный замысел игроков), а не между пользователями сети «Интернет». Фигурально выражаясь, между взаимодействием аватаров и действиями игроков появляется своего рода «четвертая стена». Содержание высказываний игроков в таком случае является частью творческого создания результатов интеллектуальной деятельности, а не передает сообщение в узком смысле этого слова, которое относилось бы к «реальному» миру;

4) **«игры как… игры»**. Данная условная квалификация раскрывает одно из наиболее интересных качеств многопользовательских компьютерных игр, которое,

[19] Согласно п. 2 Постановления Правительства РФ от 23.09.2020 № 1526 «О Правилах хранения организаторами распространения информации в информационно-телекоммуникационной сети „Интернет“…», «коммуникационный интернет-сервис» — это «информационная система и (или) программа для электронных вычислительных машин, которая предназначена и (или) используется для приема, передачи и (или) обработки электронных сообщений пользователей сети „Интернет“ в целях обмена электронными сообщениями между пользователями сети „Интернет“, в том числе для передачи электронных сообщений неопределенному кругу лиц».

среди прочего, красной нитью пронизывает всю дискуссию относительно «виртуальной собственности». Это качество выражается в том, что, с точки зрения обыденного здравого смысла, игры в целом рассматриваются как нечто «несерьезное». Предполагается, что взаимодействие в играх не должно порождать последствий для реального мира. В то же время появление в отношениях между пользователями, опосредуемыми игровыми средами, предметов таких отношений, которые реальны с точки зрения права (например, каких-либо объектов или действий, которые представляют ценность, выражаемую в фиатных деньгах, или же каких-либо действий, которые посягают на реальные охраняемые законом ценности — честь, достоинство или деловую репутацию), как бы разрушает «магический круг» и приводит к применению реального права.

Помимо узкой проблемы реконструкции «магического круга» для целей права, такое положение дел, связанное с играми, позволяет высказать и развить более значимую идею. Данная проблема, на самом деле, гораздо шире. Она связана не только с компьютерными играми, но и с другими явлениями, которые относятся к «несерьезному» (в том числе к иным видам художественных произведений, шуткам, анекдотам и пр.). Все это обусловливает развитие концепции особого рода пределов права, которые можно назвать «смысловыми» или «семантическими». С практической точки зрения данное качество игр главным образом преломляется через правоприменительную практику, связанную со ст. 1062 ГК РФ. Согласно ей требования граждан и юридических лиц, связанные с организацией игр и пари или с участием в них, не подлежат судебной защите (при этом вопрос о том, подразумеваются ли в тексте данной статьи лишь азартные игры все еще остается открытым). Применительно к аватарам настоящий ракурс и логика рассуждения требуют постановки вопроса о том, являются ли аватары «обычным» элементом игрового интерфейса (игрового дизайна), который в целом должен находиться за пределами «серьезного» отношения к играм со стороны правовой системы, или же ситуация складывается иным образом. Возможно, диаметрально противоположным. Именно этот аспект, по сути, объединяет все предыдущие и служит методологическим основанием для следующего шага исследования — анализа внутренней точки зрения, или отношения пользователя к своему аватару в цифровой (в нашем случае и игровой) среде.

## 3. Внутренняя точка зрения: что аватар значит для пользователя?

В обыденном восприятии аватар в многопользовательской онлайн-игре представляет собой просто одну из жанровых особенностей или определенный способ организации интерфейса, который предполагает «персонифицированное» структурирование игрового опыта пользователя.

> В то же время в современных междисциплинарных исследованиях отмечается гораздо более серьезное значение аватаров — данные объекты выступают в качестве *способа саморепрезентации пользователей*.

Как отмечают К. Новак и Дж. Фокс, «согласно Гофману (1959), люди тщательно выбирают то, как представить себя для того, чтобы оптимизировать свою способность достигать социальных целей. В цифровых средах аватары используются для саморепрезентации и влияют на то, как люди оценивают их цифровые тела, по мере определения того, как и когда они могут выбрать их в качестве аватаров… Выбор аватара в виртуальном мире в определенном смысле аналогичен процессу выбора одежды в физическом мире, хотя пределы такого выбора зависят от технологических ограничений, а не от того, какая одежда находится в шкафу данного человека»[20]. Пользователи выбирают аватары исходя из практических соображений — данные элементы цифровой среды позволяют им выбрать, какие части собственной идентичности представить другим пользователям, а какие скрыть, что может помочь достичь определенных социальных целей[21].

Аватары при этом используются пользователями (и игроками, если речь идет о многопользовательских онлайн-играх), чтобы «реализовать желание идентифицировать и выразить себя другим»[22]. Пользователи

[20] *Nowak K.L.*, *Fox J.* Avatars and Computer-Mediated Communication: A Review of the Definitions, Uses, and Effects of Digital Representations // Review of Communication Research. 2018. Vol. 6. P. 40. URL: https://rcommunicationr.org/index.php/rcr/article/view/39/49 (дата обращения: 28.03.2022). В статье авторы исходят из достаточно широкой интерпретации термина «аватар».

[21] *Ibid.*

[22] *Ibid.*

могут не только прямо выражать себя посредством аватаров, но использовать их как инструмент для изучения своей идентичности, других идентичностей на своем виртуальном опыте или для сокрытия части своей идентичности[23].

> Одно остается неизменным — аватар непосредственно связан с пользователем и не выступает просто как некий объект (вещь), который может легко сменить своего владельца без последствий для него.

Отметим, что в практике взаимодействия, характерной для многопользовательских компьютерных игр, есть немало примеров передачи между игроками отдельных аватаров (где это позволяют технические условия) или аккаунтов с целью передачи аватаров, либо же временного предоставления учетных записей друзьям и партнерам, чтобы они совершили какие-то действия посредством аватаров исходного игрока. Все это, однако, не отменяет главного тезиса, согласно которому аватар, во-первых, так или иначе все же связан с определенным субъектом (как, например, в случае временной передачи аккаунта), а во-вторых, может влиять на своего владельца, даже если он меняется (как, например, в случае отчуждения аватара или аккаунта с аватаром). Собственно, в медиаисследованиях подчеркивается так называемый эффект Протея, подразумевающий обратное влияние аватара на поведение пользователя как онлайн, так и офлайн[24].

История изучения серьезной роли аватаров не исчерпывается цитируемой статьей К. Новак и Дж. Фокс. Например, еще много ранее, в 2014 году, А.Д. Мередит представил в Университете Ноттингем Трент диссертацию по теме «Презентация себя в массовых многопользовательских онлайн-играх» — объемное исследование, основанное, в том числе, на применении качественных и количественных методов для оценки гипотез. Автор поставил четыре основных вопроса: 1) как игроки используют многопользовательские игры, чтобы представлять концепции себя; 2) если игроки создают версию себя, почему они это делают; 3) если некоторые игроки этого не делают, то почему; 4) если игроки представляют версию себя в многопользовательских играх, какое значение это имеет для их повседневных офлайновых жизней?[25] Отвечая на данные вопросы, автор заметил, что в первом случае для игроков характерно представлять различные *версии* себя, используя при этом существующие Я-схемы *(self-schema)*, автобиографическую и собственную память. Мотив такого поведения лежит в возможностях, которые предоставляет виртуальное пространство, — игроки могут выходить за пределы офлайновых версий себя, поскольку контролируемый игроком аватар находится внутри игрового мира и может делать «невозможные» вещи, в том числе в условиях безопасности, вне «конфликтующих социальных сфер»[26]. Любопытно, что на третий вопрос при этом автор дает весьма необычный ответ: те, кто не создают альтернативную версию себя в виртуальном мире, как бы просто остаются собой, поскольку не усматривают принципиальной разницы между виртуальным и реальным миром (мы понимаем это в том смысле, что в контексте исследования вывод по данному вопросу подразумевает отношение к виртуальному миру именно как к своего рода средству коммуникации)[27]. Наконец, отвечая на последний вопрос, автор отмечает, что действие посредством аватара подразумевает «ряд „невидимых“, но продолжающихся точек воздействия, следующих из представления версий себя в многопользовательской игре — в которых игрок изменяется как продукт взаимодействия»[28]. Акт игры в многопользовательскую игру воздействует на игрока как в форме фиксируемого опыта внутри игрового мира, так и в части создания автобиографических воспоминаний, которые влияют на существующие Я-схемы и новые цели рабочей памяти[29].

Следует особо подчеркнуть: прямо или косвенно тематика аватаров в виртуальных мирах в целом и в многопользовательских играх в частности исследовалась в ряде других, в том числе более ранних работах. В целом они восходят к классическим трудам по психологии личности, подобно тому как игровые исследова-

[23] *Ibid*. P. 40-41.
[24] *Ibid*. P. 41.

[25] *Meredith A.D.* The Presentation of Self in Massively Multiplayer Online Games. A thesis submitted in partial fulfilment of the requirements of Nottingham Trent University for the degree of Doctor of Philosophy. October 2014. URL: https://core.ac.uk/download/pdf/30624339.pdf?fbclid=IwAR3axl7smS0gxOMlGyArw4echEWigB1hrZ7F6o05PSkWBA6Ehy5-ESZxCNE (дата обращения: 28.03.2022).
[26] *Ibid*. PP. 208–210.
[27] *Ibid*. P. 210.
[28] *Ibid*. P. 211.
[29] *Ibid*. P. 210.

ния восходят к классическим трудам по культурологии и иным социально-гуманитарным наукам). Поэтому цитируемые публикации К. Новак и Дж. Фокс, а также А. Мередита могут послужить не только как содержательные работы по теме, но и как качественные средства библиографической навигации для тех, кого эта проблема и этот ракурс заинтересуют в достаточной степени.

> В рамках же данной статьи нам следует обратить внимание на то обстоятельство, что, независимо от всех возможных нюансов, аватары связаны с определенными физическими лицами, и такая связь не просто инструментальна, а соотносится с определенными личными психологическими ценностями.

В юридической плоскости данные факты приведут нас к вполне закономерным выводам практического характера.

## 4. Аватары как персональные данные и объекты нематериальных благ

Итак, аватары связаны с определенными физическими лицами, при этом такая связь должна рассматриваться в контексте определенных психологических ценностей. Ранее мы уже отметили, что аватары как часть целого являются «носителями» юридических качеств многопользовательских компьютерных игр как таковых[30] (интеллектуальная собственность, информация, средство коммуникации, «игры как… игры»), причем информационно-правовая квалификация, как видно, теперь подразумевает возможность применения законодательства о персональных данных не только в силу логической необходимости, но и в силу природы аватаров, как она понимается междисциплинарно. По общему правилу, как мы увидели, аватары *могут* быть не просто связаны с определенным физическим лицом, но представлять часть его основной или альтернативной идентичности (с учетом свободных практик, существующих в среде многих игроков и пользователей, подчеркнем — именно «могут», но не «должны во всех случаях»).

> Такая связь означает только одно: информацию, составляющую аватары, по общему правилу следует рассматривать как разновидность персональных данных.

Согласно п. 1 ст. 3 Закона о персональных данных персональные данные — любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

Более того, в некотором специфическом смысле аватары, в зависимости от объема технологических возможностей, которые предоставляет тот или иной виртуальный мир (например, технически допуская возможность аватара «надеть» одежду с какой-либо надписью, наносимой по замыслу пользователя), могут быть даже «информационно-нейтральны» и допускать отражение информации различного правового режима. Помимо прежних наблюдений, согласно которым информация, составляющая игру (в том числе многопользовательскую) в целом, может потенциально составлять любой квалифицированный вид информации — от запрещенной до различных видов тайн — получается, что аватар как информация, составляющая персональные данные, может потенциально содержать и их отдельные особые виды. Например, специальные категории персональных данных, которые касаются расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни (ч. 1 ст. 10 Закона о персональных данных).

Отдельного внимания заслуживает вопрос, который может, на первый взгляд, показаться странным с точки зрения российской правовой среды, но постановка которого окажется легитимна в контексте Регламента № 2016/679 Европейского парламента и Совета Европейского союза «О защите физических лиц при обработке персональных данных и о свободном обращении таких данных, а также об отмене Директивы 95/46/ЕС (Общий регламент о защите персональных данных)» (далее — *GDPR*). Так, согласно ст. 11 Закона о персональных данных к биометрическим персональным данным относятся сведения, характе-

[30] И, разумеется, с некоторой поправкой, неигровых виртуальных миров, включая в перспективе современную концепцию метавселенных (здесь хочется иронично отметить, что все новое — это хорошо забытое старое, к которому добавили блокчейн или, еще лучше, *NFT*).

ризующие только физиологические и биологические особенности человека, на основании которых можно установить его личность. В то же время согласно ст. 4 (14) *GDPR* биометрические персональные данные, помимо указанных категорий, включают также и *поведенческие характеристики (behavioural characteristics)* физического лица, которые предусматривают или подтверждают уникальную идентификацию указанного физического лица. Применение концепции «поведенческих характеристик» к паттернам поведения, проявляющимся через аватары, представляется возможным, тем более что п. 24 Декларативной части *(Recitals) GDPR* использует схожий термин «поведенческая активность» в привязке к профилированию физических лиц в Интернете и применительно к критерию территориальной применимости *GDPR*, установленному ст. 3(2)(a) и связанному с мониторингом такой активности.

Надо полагать, однако, что в свете европейского подхода это не должно вызывать гипотез об абсурдности такого толкования или приводить к существенным затруднениям на практике. Дело в том, что из ст. 4(14) *GDPR* прямо следует, что поведенческие характеристики, как и иные разновидности биометрических персональных данных, должны предусматривать или подтверждать уникальную идентификацию физического лица и при этом возникать в результате особой технической обработки. В случае с первым признаком можно предположить, что некоторые характерные паттерны поведения игрока посредством аватара могут подтверждать такую идентификацию. А в случае со вторым, вероятно, и расставляются все точки над *"i"* — если какая-либо информационная система действительно используется для анализа поведенческих паттернов игроков, чтобы определить уникальную идентификацию физического лица по поведению аватара, и при этом используется особая техническая обработка соответствующих данных для этих целей, вряд ли будет чрезмерным считать полученные данные биометрическими. Такого рода обработка явно выходит за пределы «обычной хозяйственной деятельности» игровых компаний, и она была бы более характерна для деятельности, например, правоохранительных органов.

Таким образом, мы можем исходить из следующего: есть опровержимая правовая презумпция того, что информация, составляющая аватары в многопользовательских играх и виртуальных мирах, должна рассматриваться как персональные данные.

> Но, как отмечено ранее, связь между игроком (пользователем) и персонажем (аватаром) по общему правилу значительно более глубока, чем кажется на первый взгляд. Это не просто сведения, которые характеризуют присутствие человека в цифровой среде и его деятельность в ней, но способ проявления идентичности, — буквально часть этого самого человека, проявляемая в цифровой среде.

Безотносительно возможной дискуссии о том, могут ли персональные данные (в том числе, составляющие аватар) рассматриваться как нематериальные блага[31], из представленных в настоящей статье рассуждений закономерно следует вывод о том, что сам по себе аватар связан с определенными нематериальными благами. Представляется, что эта мысль одновременно пересекается как с практическими и доктринальными представлениями о нематериальных благах как таковых (по выражению М.М. Агаркова, это блага, *неотделимые от личности*[32], — а именно на этом обстоятельстве и акцентируют внимание междисциплинарные исследования аватаров), так и с протодоктринальными представлениями в области персональных данных времен С. Уоррена и Л. Брандейса, которые проводили аналогию между защитой интеллектуальных прав и защитой приватности по общему признаку охраны ценностей, связанных с выражением мыслей, чувств и эмоций[33]. Подчеркнем: данный тезис не означает с необходимостью то, что конкретно внешнее техническое выражение аватара и является соответствующим нематериальным благом. Он означает лишь то, что с таким аватаром определенное охраняемое нематериальное благо связано, тогда как аватар может выступать как «токен» такого блага или, иными словами, внешний референт ценности определенного обобщенного символического

[31] См.: *Архипов В.В.* Проблема квалификации персональных данных как нематериальных благ в условиях цифровой экономики, или Нет ничего более практичного, чем хорошая теория // Закон. 2018. № 2. С. 52–68.

[32] См.: *Нохрина М.Л.* Понятие и признаки нематериальных благ: законодательство и цивилистическая наука // Известия высших учебных заведений. Правоведение. 2013. № 5 (310). С. 146.

[33] *Warren S.D.*, *Brandeis L.D.* The Right to Privacy // Harvard Law Review. 1890. Vol. 4. No. 5. 198-199.

посредника, если применять концепцию смысловых или семантических пределов права[34].

Таким образом, получается, что в многопользовательских играх и виртуальных мирах, помимо хорошо всем известной проблематики виртуальной собственности, которая часто может стать основанием для разрыва того самого магического круга и применения реального права, есть еще одно самостоятельное измерение. Оно определяет некоторые из сквозных случаев реальности и серьезности[35] отношений в многопользовательских играх — это тонкая связь, которая существует между игроком (пользователем) и персонажем (аватаром), имеющая психологическое измерение и связанная с определенным нематериальным благом. Для целей и задач настоящей статьи этого вывода уже достаточно, хотя в качестве исследовательской гипотезы на будущее определенно необходимо акцентировать внимание на том, что, во-первых, нарушение прав (в реальном юридическом смысле) на персонажа не обязательно должно анализироваться с точки зрения имущественных отношений — можно исходить из концепции нарушения прав на нематериальные блага и, как следствие, причинения морального вреда. А во-вторых, можно представить далеко идущие последствия, связанные с экстраполированием данной логики и на виртуальную собственность. Гипотетически (для последующих исследований) данный вид ценности тоже не обязательно может анализироваться через чисто имущественные концепции: раз виртуальная собственность в игровом мире принадлежит аватару, она может рассматриваться как своего рода продолжение этого аватара в виртуальном мире, что несколько пересекается с логикой того наблюдения, которое будет отмечено ниже.

Как отмечал Л. Лессиг, изучая киберпространство, мы одновременно можем извлечь полезные уроки и в отношении права реального мира[36]. Кажется, здесь как раз такой случай. Аватар может быть интерпретирован через юридические концепции персональных данных и нематериальных благ, но и это еще не все. Так, в медиафилософии развивается расширенная концепция *тела* (субъекта, физического лица). Как отмечает в своем диссертационном исследовании «Тело как медиа: опыт реконструкции» медиафилософ К.А. Очеретяный, «тело человека не является всецело природным, естественным объектом и получает свой завершенный образ в общественно-коммуникационных практиках, которые во второй половине XX века объективируются в цифровых медиа»[37]. Понимание тела зависит от моделей медиа, образ тела — предмет социального конструирования, а в опыте человека преимущественное значение получают «технически смоделированные образы [тела]». Соответственно, «в информационную эпоху техники тела, модели чувственности и стратегии желания определяются информационно-коммуникационными технологиями»[38]. В контексте данных представлений в медиафилософии формируется идея «тела геймера» (см. п. 3.3 исследования К.А. Очеретяного «Формирование тела геймера»). По словам автора, «единство переживания и управления», характерное для игрового опыта, «все более смещается в сторону длительности», причем «эта длительность превращается из стихийного переживания в практику себя, подчиненную имманентному руководящему правилу». Как заключает автор, «мы можем с уверенностью констатировать: одновременно с усложнением аппаратной начинки игрового автомата и совершенствованием интерфейса увеличивается длительность интеракции, а вместе с ней степень соотнесенности играющего с машиной. Результатом предельной длительности этой интеракции становится геймер — мутация в эволюционной спирали *homo ludens*»[39].

В продолжение автор пишет: «тело человека начинает рассматриваться не столько биологически, сколько символически, поскольку становится неотделимо от технических гаджетов, т.к. именно посредством них человек по большей части ориентируется в современности. Посредством медиа он изымает из фактов этого мира опыт, мыслит о нем, проживает его. В медиа человек находит свой образ, т.е. определяет себя»[40]…

[34] См. напр.: *Архипов В.В.* Действие правовых норм в цифровом медиапространстве и семантические пределы права // Правоведение. 2019. Т. 63. № 1. С. 8–27.

[35] Данные термины используются в специальном смысле концепции «смысловых» («семантических») пределов права.

[36] См.: *Lessig L.* The Law of the Horse: What Cyberlaw Might Teach. URL: http://cyber.law.harvard.edu/works/lessig/finalhls.pdf (дата обращения: 28.03.2022).

[37] *Очеретяный К.А.* Тело как медиа: опыт реконструкции: дис. … канд. философ. наук. СПб., 2015. С. 15.

[38] Там же.

[39] Там же. С. 164-165.

[40] Там же. С. 167.

Сопутствующий настоящему исследованию юридический вывод, который с некоторой долей неожиданности следует из этой грани изучения аватаров в многопользовательских играх, представляется достаточно значимым, чтобы отметить его уже здесь в качестве гипотезы, пусть и более уместно будет развить его в иных работах:

> право на цифровые репрезентации сейчас уже необязательно должно интерпретироваться как право, связанное с неприкосновенностью частной жизни (в информационном смысле) и персональными данными. Может ставиться вопрос об интерпретации данного права в контексте права на свободу и личную неприкосновенность.

Иными словами, кажется легитимной постановка вопроса о том, что ст. 5 Конвенции о защите прав человека и основных свобод имеет в данном контексте не меньшее значение, чем ст. 8. Можно выразить эту мысль и иными словами. Ранее Н.А. Дмитрик в своей статье «Пределы правового регулирования в цифровую эпоху» отмечал несколько этапов понимания *privacy* по Стефано Родота (право быть забытым; право контролировать то, как другие используют информацию о нас; право контролировать собственную информацию и определять способ выстраивания собственной частной сферы)[41]. Возможно, этот список следует дополнить концепцией «охраны неприкосновенности цифровых репрезентаций в цифровой же среде». Правда, данный анализ будет уже существенным образом выходить за пределы задач настоящей публикации.

## 5. Идентификация в цифровой среде: как отличить человека от бота. И надо ли…

Последний вопрос, который стоит рассмотреть в настоящей статье, непосредственно связан со сквозной темой этого номера — идентификацией. Как известно, в многопользовательских онлайн-средах, включая виртуальные миры и онлайн-игры, нередко встречаются боты (т.е. в широком смысле данного слова «искусственный интеллект») под видом реальных пользователей[42]. В некоторых случаях боты используются лицами, желающими получить несправедливые преимущества в игре и нарушающими условия пользовательского соглашения. В некоторых случаях такого рода практики инициируются самими разработчиками, чтобы достичь различные маркетинговые и репутационные цели. Например, в 2017 году в контексте 1 апреля компания *Riot Games* якобы ввела новый игровой режим кооперативной игры против «продвинутых» ботов в киберспортивной игре *League of Legends*. Не все игроки сразу сумели разобраться, что к чему, и кто-то действительно полагал, что играет против самообучаемого искусственного интеллекта. Однако игровая компания просто заменяла игровые псевдонимы (никнеймы) игроков противоположной команды на формализованные типовые названия ботов. Хотя данная информация не стала публичной, можно предположить, что *Riot Games* получила определенное количество ценной информации о стереотипах поведения игроков в зависимости от того, сражаются ли они с другими «живыми» игроками, либо их противниками являются боты (к вопросу о виртуальных средах как пространствах для социального эксперимента)[43].

Приведенный пример кажется особенно уместным в свете обсуждений различных принципов и практических мер, направленных на соблюдение прав человека при использовании систем искусственного интеллекта[44]. В контексте нашего рассуждения речь, в первую

[41] *Дмитрик Н.А.* Пределы правового регулирования в цифровую эпоху // Информационное общество. 2018. № 3. С. 54.

[42] Доведенная до крайности интерпретация данного обстоятельства даже породила особую «теорию заговора» о том, что Интернет на самом деле как бы в действительности мертв: реальных пользователей там немного, а контент, реакции и пр. в основном генерируются искусственным интеллектом. См. напр.: *Tiffany K.* Maybe You Missed It, but the Internet “Died” Five Years Ago // The Atlantic. August 31, 2021. URL: https://www.theatlantic.com/technology/archive/2021/08/dead-internet-theory-wrong-but-feels-true/619937/ (дата обращения: 28.03.2022).

[43] Упоминание этого события можно найти в разных источниках в Интернете. См. напр.: League April Fool’s Day from 2009 to 2017 // Boosteria. URL: https://boosteria.org/guides/league-april-fools-days (дата обращения: 28.03.2022).

[44] Обратим внимание, что для целей настоящей стать словосочетание «искусственный интеллект» используется в инструментальном и широком смысле — в том же смысле, как он используется в игровой индустрии. Такое словоупотребление, при условии, что оно осуществляется осознанно, представляется вполне легитимным. Так, например, один из ведущих авторов в области правовых проблем искусственного интеллекта Р. Сасскинд допускает применение данного термина и к технологиям «первой волны», к которым относятся экспертные системы, основанные на

очередь, идет о требовании к лицам, которые используют системы искусственного интеллекта, уведомлять людей о факте взаимодействия с искусственным интеллектом, а не с человеком, если неочевидно, что функции выполняет искусственный интеллект. Например, как это представлено, в исследовании *(feasibility study)* Комитета Совета Европы *ad hoc* по искусственному интеллекту *(CAHAI)*[45]. Пункт 7.1(1) данного исследования связывает указанное требование с новой интерпретацией права на человеческое достоинство и права на физическую и психическую неприкосновенность, вытекающими из положений Конвенции о защите прав человека и основных свобод. Собственно, и в Концепции развития регулирования отношений в сфере технологий искусственного интеллекта и робототехники до 2024 года (утв. Распоряжением Правительства РФ от 19 августа 2020 года № 2129-р) в п. 4 раздела I также упоминаются концептуальные проблемные направления регулирования технологий искусственного интеллекта и робототехники. К их числу и относится идентификация системы искусственного интеллекта при взаимодействии с человеком, включая его информирование о взаимодействии с такой системой. Однако далее в указанной Концепции говорится уже о том, что проработка вопроса об условиях идентификации системы искусственного интеллекта при прямом взаимодействии с человеком может быть актуальной при наличии *реального* риска нарушения прав и свобод человека, а не во всяком возможном случае (п. 2 раздела II).

Такой подход вполне согласуется с последовательностью настоящего рассуждения. С одной стороны, с точки зрения междисциплинарного подхода аватары в многопользовательских виртуальных средах представляют собой форму саморепрезентации пользователей и тесно связаны с ними как с личностями в психологическом и социологическом смысле (как минимум, при условии, что речь идет об аватарах физических лиц — хотя нельзя принципиально исключать экстраполирование логики настоящей статьи и на аватаров юридических лиц, которые могут быть связаны с нематериальными активами вроде деловой репутации[46]).

> В этом, скорее, общетеоретическом ракурсе различение аватаров, управляемых людьми, и ботов, управляемых искусственным интеллектом различной степени сложности, имеет принципиальное значение, поскольку скрытое и (или) недобросовестное использование ботов будет нарушать естественный порядок коммуникации, опосредованный виртуальной средой.

Собственно говоря, фундаментальное различие персонажа настоящего игрока и бота в многопользовательских средах и будет проводиться по качествам, приведенным во второй и третьей части настоящей статьи, что можно считать ответом на вопрос: в чем заключается существенное различие между игроками и ботами в многопользовательской среде.

С другой стороны, возлагать на каждого разработчика каждой виртуальной среды обязанности обеспечивать пользователям инструменты идентификации искусственного интеллекта в таких средах представляется чрезмерным и непропорциональным с учетом значительного числа возможных вариантов построения виртуальных сред с технической и социологической точек зрения. Можно смоделировать немало ситуаций, в которых отсутствие такой идентификации не только не будет нарушать права пользователей, но и, наоборот, будет способствовать их реализации (как это происходит в игровых и художественных проектах). В связи с этим можно заключить: проблема, безусловно, теоретически значимая, но с практической точки зрения она вряд ли нуждается в каком-либо радикальном изменении текущей ситуации. Известно неявное положение «мягкого права» индустрии, согласно которому игровые и соответствующие интернет-компании должны на уровне пользовательских соглашений и практики их применения обеспечивать соответствие своей виртуальной среды разумным ожиданиям поль-

«эксплицитных» алгоритмах. См., напр.: *Susskind R.E.* Online courts and the future of justice. Oxford, 2019. P. 264-265. Так или иначе, независимо от особенностей конкретной итерации искусственного интеллекта, не меняется одна из ключевых характеристик технологии, определяющая возможность автоматизированного действия.

[45] Ad Hoc Committee on Artificial Intelligence (CAHAI). 2020. URL: https://rm.coe.int/cahai-2020-23-final-eng-feasibility-study-/1680a0c6da (дата обращения: 28.03.2022).

[46] Вопрос о том, может ли быть категория нематериальных благ применима к объектам гражданских прав юридических лиц, в литературе не новый. См. напр.: *Трофимова Т.В.* Нематериальные блага юридических лиц и их гражданско-правовая защита // Вестник ОмГУ. 2009. № 3. С. 244–248.

зователей. В числе таких разумных ожиданий может быть и запрет на использование ботов, и разрешение на использование таковых в каких-то конкретных случаях. Игровые компании должны рассматривать возможные правовые конфликты по принципу «от случая к случаю», по сути применяя ту или иную интерпретацию концепции «магического круга» и (или) смысловых пределов права.

## 6. Заключение

Итак, если придерживаться методологической установки, что изучение проблем многопользовательских компьютерных игр будет полезным для цифрового права, поскольку данные виртуальные среды содержат своего рода срез проблем интернет-права и могут рассматриваться как модели реальных отношений (а равно и пространство для социального эксперимента), то анализ юридически значимых качеств персонажей (аватаров) многопользовательских игр может оказаться весьма полезен, в том числе и в свете современных попыток индустрии построить метавселенную(-ые).

Формально аватары и компьютерные игры соотносятся как частное и целое, поэтому аватары также можно рассматривать с точки зрения права интеллектуальной собственности, информационного права и иных юридически значимых признаков компьютерных игр — от аватаров как аналогов учетных записей в коммуникационных интернет-сервисах до рассмотрения контекста использования аватаров с точки зрения различных концепций «магического круга».

Междисциплинарный взгляд при этом акцентирует внимание на то, что между пользователем и аватаром существует тесная связь, значение которой часто выходит за пределы технической функциональности виртуального мира.

> С точки зрения медиафилософии, аватары, как правило, выступают в качестве способа саморепрезентации пользователя, части его идентичности или даже «цифрового тела». На этом основании можно сделать переход к правовому контексту и закономерный вывод о том, что аватары, должны также рассматриваться как персональные данные и соотноситься с определенными нематериальными благами.

Наконец, общий контекст различных практик виртуальных миров располагает к рассмотрению вопроса о том, каковы различия между аватарами и ботами, которые нередко могут встречаться в различных виртуальных средах. Собственно, указанные психологические и социологические качества аватаров и определяют наиболее фундаментальное различие. Хотя из этого еще не следует необходимость принципиальным образом изменять подходы к правовому регулированию в данной области, это не отменяет значимость внимательного учета данных особенностей в тех случаях, когда это применимо с учетом концепций магического круга.

Каковы дальнейшие теоретические и практические перспективы исследовательского ракурса, предложенного в настоящей статье? Представляется, что некоторые выводы уже в том виде, как они были представлены, могут вызвать интерес и обладают определенной новизной (возможность рассматривать аватары в некоторых частных виртуальных мирах как персонажей с точки зрения авторского права, общие основания для применения режимов персональных данных и нематериальных благ), однако этим методологический потенциал идей не исчерпывается. По выражению Н.А. Дмитрика, высказавшего ряд конструктивных замечаний к настоящей статье, правовые режимы аватара, на первый взгляд, могут показаться непересекающимися и не конфликтующими между собой. В то же время такая видимость может оказаться обманчивой, и соотношение правовых режимов в контексте общей идеи о «теле игрока» из медиафилософии может спровоцировать ряд мысленных экспериментов, способствующих появлению нового правового знания. Некоторые мысленные эксперименты и способы развития представленных идей заслуживают упоминания уже сейчас.

Так, например, как быть с ситуацией, в которой аватар «продается»?[47] Или же аватар не имеет антропоморфных качеств (или, в принципе, каких-либо иных качеств, соотносимых с каким-то одушевленным существом иной природы, — например, аватар-танк т.п.)? Оба этих примера можно объединить в один контекст

[47] Слово используется в кавычках, поскольку в правовом, а не экономическом смысле могут использоваться различные правовые конструкции: возмездное оказание услуг, изменение стороны в лицензионном договоре и т.д.

рассуждения, поскольку представляется, что ответы на подразумеваемые вопросы также отличаться не будут.

Во-первых, конечно, не каждый аватар будет отвечать «тесту» на прямую и безусловную соотносимость с «телом игрока» («телом пользователя»). Предыдущий анализ подразумевал необязательность, но возможность такого положения дел, даже если соответствующая ситуация будет распространенной. В юридической плоскости это означает, что вопрос о глубокой личной психологической связи с человеком, стоящим за тем или иным аватаром, *de facto* стоит включать в предмет доказывания в ряде спорных ситуаций. Возможно, в перспективе речь может идти и об определенной правовой презумпции. При этом не исключено и «гранулярное» рассмотрение соответствующих вопросов: например, даже если аватар не представляет идентичность пользователя в том смысле, как это рассматривалось в статье, он может все равно отражать часть интереса пользователя, охраняемого концепцией нематериальных благ. То есть, например, аватар можно рассматривать по аналогии с «любимым» и индивидуализированным элементом спортивного инвентаря. Это сравнение напрашивается в том числе и потому, что используемые в киберспорте компьютерные игры официально в России рассматриваются как «спортивный инвентарь»[48], — допустим, порча которого может причинить моральный вред.

Во-вторых, как это работает в случае с анализом многих других правовых явлений, напрашивается гипотеза о корреляции между вовлеченностью аватара в систему артефактов, используемых субъектом (в обычном смысле слова) для коммуникации, и юридической значимостью данного явления, в том числе, в смысле настоящей статьи[49]. Причем эта мысль также соотносится с классической психологической концепцией личности как социального явления. Так, в ситуации с типичной экосистемой отношений вокруг многопользовательской онлайн-игры, можно представить себе две разные ситуации:

1) аватар (персонаж) принадлежит игроку уже долгое время, и с ним связано членство в каком-либо сообществе (гильдии), виртуальная (или даже невиртуальная) дружба со многими другими игроками через аватары последних, записи контактов и пр.;

2) аватар, в зависимости от того, как выстроена архитектура игры, создается или в какой-либо момент времени развивается специально для последующей «продажи» (например, он привязывается к специально созданному для этого аккаунту и развивается исключительно в коммерческих целях).

В первом случае ситуация с аватаром вполне соответствует магистральным идеям, отраженным в данной статье, а во втором речь идет лишь о разновидности виртуальной собственности. Также совершенно ясно, почему в обычных, нацеленных на погружение пользователей в вымышленную вселенную, многопользовательских играх пользовательские соглашения, как правило, запрещают разного рода обмен и торговлю аватарами[50].

---

[48] Согласно п. 1.1 Правил вида спорта «компьютерный спорт» (утв. Приказом Министерства спорта Российской Федерации от 22.01.2020 № 22, с изм., внесенными приказом Минспорта России от 30.04.2020 № 335), «Видеоигра — **инвентарь компьютерного спорта** (выделено мною — *В.А.*), состоящий из программного обеспечения, позволяющего осуществить организацию соревновательного процесса (геймплея) соревнующимся сторонам (спортсменам), формирующего соревновательное пространство (арену), создающее объекты управления, воспринимаемые органами чувств человека, где участник соревнований через устройства ввода/вывода воздействует на объекты управления. Видеоигра автоматически либо с помощью контролируемых настроек/запретов обеспечивает равные условия соревнующимся сторонам». Такая квалификация может немного удивить не очень знакомого с тематикой читателя, однако она очень логична: в киберспорте идет соревнование между людьми с использованием компьютерной игры как способа такого соревнования. Иммерсия (погружение) в виртуальный мир для киберспорта абсолютно вторична.

[49] Данная мысль сама по себе коррелирует с методологическими установками коммуникативной концепции права, близкой автору статьи.

[50] В этом контексте нельзя не упомянуть так называемые *NFT*-игры и значение использования технологии блокчейна в целом в игровых вселенных и разновидностях виртуальной реальности. Обзор правового значения данных технологических решений выходит уже за пределы целей и задач данной публикации. Ограничимся лишь той общей гипотезой, что использование *NFT* чаще всего сопряжено с приданием качеств «реальности» и «серьезности» цифровым объектам с точки зрения упомянутой концепции смысловых (семантических) пределов права, поскольку *NFT* — это, прежде всего, инструмент коммодификации цифровых объектов. См. напр.: What Are NFT Games and How Do They Work? // Binance Academy. 2021. September 2. URL: https://academy.binance.com/en/articles/what-are-nft-games-and-how-do-they-work?utm_campaign=googleadsxacademy&utm_source=-googleads&utm_medium=cpc&gclid=Cj0KCQiAxoiQBhCRARIs-

Наконец, нельзя обойти вниманием и еще один важный аспект. Ранее Н.А. Дмитрик уже обосновывал категорию «фактической возможности» в контексте методов правового или, точнее, социального регулирования[51]. В этом смысле, коррелирующем с идеей «архитектурной модальности регулирования» (Л. Лессиг), с точки зрения исследователя, правовое значение киберпространства заключается в том, что оно может перераспределять фактические возможности участников правоотношений по сравнению с тем, как это заложено в моделях законодательства. Поэтому важно заметить, что сами по себе аватары некоторым образом структурируют игровой (пользовательский) опыт, предопределяя границы возможностей и способы саморепрезентации пользователей. Владельцы сервисов, таким образом, потенциально могут подталкивать пользователей в каком-либо направлении самовыражения или определения идентичности (в том числе, «мягко» закладывая определенную концептуальную модель). Если принять во внимание представления о «теле игрока», о которых говорилось ранее и которые актуальны в некоторых случаях, то в юридическом смысле получается, что владельцы сервисов достаточно часто сохраняют исключительные права (не только в строгом смысле терминологии права интеллектуальной собственности) на часть идентичности пользователей. И мало того что такое положение дел явно открывает новые направления для изучения правовых аспектов киберпространства, оно же может открыть пространство и для нового витка еще более фундаментальной теоретико-правовой дискуссии о субъектности и идентичности в праве. Не будет ли здесь уместна параллель между виртуальным и реальным миром? Если взглянуть на социальный мир с точки зрения социального конструкционизма, может показаться, что, подобно игровым компаниям, предоставляющим готовый и контролируемый инструментарий для выражения идентичности в виртуальном мире средствами, которые игрокам не принадлежат, такой же готовый и контролируемый инструментарий (и, возможно, также не принадлежащий нам) предоставляет каждому и человеческое общество. Вероятно, есть смысл в будущем продолжить это рассуждение, исходя из той методологической идеи, что модели и метафоры киберпространства могут нам помочь лучше понять и обычную социальную реальность.

APsvo-yZiGbiNqUnc4yaCMyEoMqjY0wSjJl6jSnnECfPA_M5eUZ-P7UCFGjMaAoEGEALw_wcB (дата обращения: 28.03.2022).

[51] См. напр.: *Дмитрик Н.А.* Цифровая трансформация: правовое измерение // Правоведение. 2019. Т. 63. № 1. С. 28–46.

## Characters (Avatars) in Multiplayer Computer Games: Issues of Legal Qualification in the Context of Interdisciplinary Studies

The legal regime of characters (avatars) in multiplayer computer games and virtual worlds is a little-studied issue (apart from the problematic of virtual property). From the external point of view avatars relate to virtual worlds as part and whole and, as a consequence, can be considered in terms of intellectual property law, limitations of information law, regulation of communication services, the limits of legal regulation of in-game relations. However, from an internal point of view, avatars are a way of self-presentation of users, an expression of their identity or even a part of the “digital body” in the media-philosophical sense. This, in turn, allows us to relate avatars to the categories of personal data and intangible goods. Finally, the distinction between game characters (avatars) and bots may arise separately. The implementation of the identification principle proposed for artificial intelligence is proposed only in significant cases, defined according to one or another concept of the magic circle. The methodological potential of the presented ideas for the theoretical and legal analysis of the problems of agency and identity in law is outlined.

***Keywords:*** *computer games, virtual worlds, characters, avatars, intellectual property, Internet, information law, magic circle, semantic limits of law, identity, agency*

### INFORMATION ABOUT THE AUTHOR

**Vladislav V. Arkhipov**
Associate professor, head of the department of theory and history of law and state of Saint Petersburg State University, doctor of legal sciences (e-mail: v.arhipov@spbu.ru).

### REFERENCES

Arkhipov, V.V. “The Effect of Legal Norms in the Digital Media Space and the Semantic Limits of Law” [*Deystvie pravovyh norm v cifrovom mediaprostranstve i semanticheskie predely prava*]. The Legal Studies [*Pravovedenie*]. 2019. No. 1. P. 8–27.

Arkhipov, V.V. “Personal Data as Nonmaterial Values (or There is Nothing More Practical than a Good Theory)” [*Problema kvalifikacii personal’nyh dannyh kak nematerial’nyh blag v usloviyah cifrovoy*

*ekonomiki, ili net nichego bolee praktichnogo, chem horoshaya teoriya*]. Statute [*Zakon*]. 2018. No. 2. P. 52–68.

Arkhipov, V.V. "Virtual Law: Main Problems of the New Direction of Legal Studies" [*Virtual'noe parvo: osnovnye problem novogo napravleniya yuridicheskikh issledovaniy*]. Proceedings of Higher Education Institutions. The Legal Studies [*Izvestiya vysshikh uchebnykh zavedeniy. Pravovedenie*]. 2013. No. 2. P. 93–114.

Arkhipov, V.V. Virtual Worlds in Legal Studies. An Inquiry into the Subject of Research / 25th IVR World Congress of Philosophy of Law and Social Philosophy Paper. URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2117762

Bartle, R. Pitfalls of Virtual Property. The Themis Group, 2004. URL: https://mud.co.uk/richard/povp.pdf

Dmitrik, N.A. "Digital Transformation: the Legal Dimension" [*Cifrovaya transformaciya: pravovoe izmerenie*]. The Legal Studies [*Pravovedenie*]. 2019. No. 1. P. 28–46.

Dmitrik, N.A. "The Limits of Legal Regulation in Digital Age" [Predely pravovogo regulirovanya v cifrovuyi epohu]. Information Society [*Infromacionnoe obschestvo*]. 2018. No. 3. P. 47–58.

Duranske, B.T., Kane, S.F. "Virtual Worlds, Real Problems" [*Virtualnye miry, realnye problemy*]. Proceedings of Higher Education Institutions. The Legal Studies [*Izvestiya vysshikh uchebnykh zavedeniy. Pravovedenie*]. 2013. No. 2. P. 115–134.

Lessig, L. The Law of the Horse: What Cyberlaw Might Teach. Harvard Law Review. 1999. V. 113. P. 501–546.

Manovich, L. The Language of New Media. London: MIT Press: Cambridge, Massachusets. 2001.

Meredith, A.D. The Presentation of Self in Massively Multiplayer Online Games. A thesis submitted in partial fulfilment of the requirements of Nottingham Trent University for the degree of Doctor of Philosophy. October 2014. URL: https://core.ac.uk/download/pdf/30624339.pdf?fbclid=IwAR3axl7smS0gxOMIGyArw4echEWigB1hrZ7F6o05PSkWBA6Ehy5-ESZxCNE

Morningstar, C., Randall Farmer, F. The Lessons of Lucasfilm's Habitat. Cyberspace: First Steps. Stanford University. MIT Press. 1990. URL: http://web.stanford.edu/class/history34q/readings/Virtual_Worlds/LucasfilmHabitat.html

Nokhrina, M.L. "Concept and Characteristics of Intangible Benefits: Legislation and Civil Law Science" [*Ponyatie i priznaki nematerial'nykh blag: zakonodatel'stvo i tsivilisticheskaya nauka*]. Proceedings of Higher Education Institutions. The Legal Studies [*Izvestiya vysshikh uchebnykh zavedeniy. Pravovedenie*]. 2013. No. 5. P. 143–160.

Nowak, K.L., Fox, J. Avatars and Computer-Mediated Communication: A Review of the Definitions, Uses, and Effects of Digital Representations. Review of Communication Research. 2018. Vol. 6. P. 40.

Raggett, D. Extending WWW to support Platform Independent Virtual Reality. W3C. 1994. URL: https://www.w3.org/People/Raggett/vrml/vrml.html

Rozhkova, M.A. "Virtual Property and Multiplayer Online Game – How to Discern the Relations Emerging in Respect of Them?" [*Virtual'noe imushhestvo i mnogopol'zovatel'skaya onlajn-igra — kak razlichat' voznikajushhie po ih povodu otnoshenija?*]. Zakon.ru. 2020. 6 December. URL: https://zakon.ru/blog/2020/12/06/virtualnoe_imuschestvo_i_mnogopolzovatelskaya_onlajn-igra__kak_razlichat_voznikayuschie_po_ih_povodu.

Rozhkova, M.A. "Virtual Reality and Metaverse: Subject of Legal Studies" [*Virtual'naja real'nost' i Metavselennaja: predmet pravovogo issledovanija*]. Zakon.ru. 2021. 12 January. URL: https://zakon.ru/blog/2022/01/12/virtualnaya_realnost_i_metavselennaya_predmet_pravovogo_issledovaniya__virtual_reality_and_metaverse.

Savchuk, V.V. "Media philosophy. Attack of Reality" [*Mediafilosofiya. Pristup real'nosti*]. Saint Petersburg, 2014. 162 p.

Susskind, R.E. Online Courts and the Future of Justice. Oxford, 2019. 347 p.

Trofimova, T.V. "Classification of Intangible Benefits and Its Legal Meaning" [*Klassifikatsiya nematerial'nykh blag i ee pravovoe znachenie*]. Civil Law [*Grazhdanskoe parvo*]. 2005. No. 3. P. 22–26.

Warren, S.D., Brandeis, L.D. The Right to Privacy. Harvard Law Review. 1890. Vol. 4. No. 5. P. 193–220.

# НОВОЕ ЗАКОНОДАТЕЛЬСТВО КНР В ОБЛАСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ: ПРИВАТНОСТЬ «С КИТАЙСКОЙ СПЕЦИФИКОЙ»*

**АЛЕКСАНДР ИВАНОВИЧ САВЕЛЬЕВ**

доцент факультета права Национального исследовательского университета «Высшая школа экономики», старший юрист компании *IBM* Восточная Европа/Азия, заместитель председателя Комиссии по правовому обеспечению цифровой экономики Ассоциации юристов России (московское отделение), член консультативного совета при Роскомнадзоре, кандидат юридических наук, магистр частного права (РШЧП)

**МАРИЯ АЛМАЗОВНА ИМАНАЛИЕВА**

студентка магистратуры «Цифровое право» Национального исследовательского университета «Высшая школа экономики»; *Peking University Law School, Chinese law LL.M student*

В центре внимания статьи — новый закон КНР о защите личных данных. Рассматриваются причины его принятия, соотношение с иными актами, регламентирующими порядок обработки персональных данных. Раскрывается содержание ряда основных положений, которые представляют особый интерес для российского дискурса по вопросам поиска оптимальных подходов к регулированию оборота данных: понятие персональных данных и правовой режим различных их видов (чувствительные данные, биометрические, обезличенные, общедоступные), содержание требований локализации и новых ограничений на трансграничную передачу персональных данных, а также установленная ответственность за нарушение норм нового закона. Данный анализ сделан с учетом комментариев, содержащихся в китайской доктрине, а также ряда подзаконных актов, которые конкретизируют общие нормы данного закона, но при этом существуют преимущественно на китайском языке. В ряде случаев проводится сравнение китайского подхода с европейским и российским.

***Ключевые слова:*** *персональные данные, трансграничная передача данных, приватность*

DOI: 10.37239/0869-4400-2022-18-3-75-96

## 1. Введение

Законодательство о персональных данных является в последнее время одним из наиболее активно развивающихся в большинстве стран. Данный факт —

* Высказанные в настоящей статье суждения являются личным мнением авторов и могут не совпадать с официальной позицией компании *IBM*, НИУ ВШЭ или какой-либо иной организации.

логическое следствие цифровизации различных сфер общественных отношений, в результате которых граждане всё в большей степени превращаются в совокупность данных, которые циркулируют в различных информационных системах. При этом от содержания и качества этих данных зависит не только фактическая, но и юридическая возможность реализации ими своих прав и обязанностей.

Долгое время внимание бизнес-сообщества, экспертов и профильных государственных органов было сосредоточено преимущественно на европейском регламенте по защите персональных данных 2016 года (*General Data Protection Regulation, GDPR*) с некоторыми отступлениями в пользу калифорнийского Закона о защите частной жизни потребителей 2018 года (*California Consumer Privacy Act, CCPA*). Однако с принятием в КНР всеобъемлющего Закона о защите личной информации, вступившего в силу с 1 ноября 2021 года, китайский подход к регулированию персональных данных стал вызывать все больший интерес. И на то есть ряд причин. Во-первых, Китай — одна из крупнейших экономик мира с большими амбициями в области развития передовых информационных технологий, включая искусственный интеллект, что предопределяет повышенное внимание к тому, какие решения он принимает по вопросам регулирования оборота данных. Во-вторых, Китай уже достаточно давно проводит политику, направленную на обеспечение информационного суверенитета страны, что в настоящее время стало одним из ключевых вопросов на повестке дня у многих стран, в том числе и России, обеспечивая тем самым идеологическую близость китайского подхода. В-третьих, Китай заслужил репутацию цивилизации, склонной к заимствованию лучших зарубежных практик в определенной области с последующей адаптацией их под свои нужды. Это открывает богатые возможности для нахождения оригинальных решений проблем, которые никак не получалось решить, оставаясь замкнутым в парадигме регулирования, реализованного в рамках определенного правопорядка. Для России же Китай — один из стратегических партнеров, в том числе в экономической сфере, что также способствует повышению запроса со стороны российского бизнеса о китайском регулировании в области обработки персональных данных, особенно принимая во внимание его экстерриториальный характер.

Однако, несмотря на все вышеизложенные факторы интереса к китайскому законодательству в этой области, его изучение является делом куда более сложным, чем изучение того же европейского и американского регулирования, что в значительной мере обусловлено наличием существенного языкового барьера. В основном информацию о китайском праве черпают из переводных источников на английском языке. В то время как они могут быть и весьма высокого качества, использование исключительно подобных источников чревато фрагментарностью формируемой картины, а также создает условия для различного рода манипуляций. В частности, когда, ссылаясь на китайский опыт, чиновники или представители бизнеса пытаются оправдать определенные законодательные инициативы, понимая, что проверить это будет крайне сложно.

Например, нередко приходится слышать мнение, что в Китае нет как таковой частной жизни, все контролируется государством и все находятся под его слежкой, а крупные компании имеют почти безграничные возможности по обработке данных граждан в корпоративных и публичных целях. И именно такие широкие возможности по обработке данных без оглядки на строгие требования законодательства обеспечивают рост инновационного потенциала китайской экономики.

Например, как отметил один из руководителей *Credit Suisse*, «именно тот факт, что в Китае отсутствует серьезное законодательство в сфере защиты неприкосновенности частной жизни и обеспечит успех Китая в технологиях искусственного интеллекта и больших данных»[1]. Примечательно, что сам Китай так не думает. Напротив, в Стратегии развития технологии искусственного интеллекта нового поколения, опубликованной Государственным Советом КНР в июле 2017 года совершенствование законодательства, обеспечивающего защиту неприкосновенности частной жизни, было обозначено в качестве первой из шести основных мер достижения данной цели[2]. Судя

[1] *Yen Nee Lee*, China will win the A.I. race, according to Credit Suisse // CNBC, 22 March 2018. URL: https://www.cnbc.com/2018/03/22/credit-suisse-china-will-win-the-ai-race-due-to-lack-of-serious-laws-on-data-protection.html (дата обращения: 22.03.2020).

[2] К пяти другим относятся: совершенствование политик, стимулирующих разработку систем ИИ; установление

по ряду публикаций в американской прессе, Китай вполне справляется с реализацией данной стратегии, так как по ряду аспектов догнал и перегнал США в области исследований искусственного интеллекта[3] (далее — ИИ), и это несмотря на то, что законодательство о защите персональных данных за последний период времени претерпело значительный скачок в развитии и существенно ужесточило порядок обработки данных. Однако, как будет показано далее, это не только не стало препятствием, а наоборот — рассматривается китайским правительством как важное средство достижения амбициозных целей по цифровизации экономики и глобальному лидерству в области информационных технологий.

> Таким образом, вопреки расхожему мнению о том, что законодательство о персональных данных — барьер для инноваций, китайский опыт может дать иллюстрацию того, что инновации и все более усиливающаяся защита персональных данных граждан вполне могут идти рука об руку, а не сдерживать друг друга.

## 2. История формирования законодательства о персональных данных и его политико-правовое значение в КНР

Китай начал формировать законодательную базу по вопросам регулирования обработки персональных данных существенно позднее, чем Европейский союз и США, что создало условия для внимательного изучения их опыта и постепенной трансплантации в национальное законодательство наиболее удачных и подходящих положений с точки зрения специфики правовой системы, менталитета и политики. Как следствие, если перефразировать наименование официальной идеологии Китая — «социализм с китайской спецификой», — можно говорить о приватности «с китайской спецификой».

Действующая конституция КНР 1982 года не содержит положений, непосредственно посвященных защите неприкосновенности частной жизни или защите персональных данных. Защита неприкосновенности частной жизни как один из важнейших элементов социального устройства западного мира являлась чуждой политическому и социальному устройству коммунистического Китая. При этом в Гонконге в 1995 году был принят первый в Азии всеобъемлющий Закон о защите персональных данных[4], а законодательство Тайваня в этой области является одним из самых строгих в Азии[5]. Таким образом, причины умолчания в Конституции КНР о неприкосновенности частной жизни кроются именно в особенностях политического устройства материкового Китая, и вряд ли их следует искать в особенностях азиатского менталитета как такового. В явном виде в Конституции КНР говорится лишь о неприкосновенности жилища и тайне корреспонденции (ст. 39 и 40 соответственно). В китайской доктрине отмечается, что данные права могут быть косвенно выведены из совокупности положений ст. 33 и 38. В ст. 33 Конституции КНР содержится общее правило о том, что государство уважает и гарантирует права человека. А в ст. 38 закреплено: «Честь и достоинство граждан Китайской Народной Республики неприкосновенны. Запрещается каким бы то ни было способом подвергать граждан оскорблениям, клевете, ложным обвинениям и травле». По мнению китайских конституционалистов, право на защиту персональных данных является частным по отношению к общему праву граждан на защиту достоинства граждан[6]. В свою очередь, положения ст. 51 Конституции КНР закрепляют правило об ограничении прав и свобод лица правами и свободами других лиц, что также трактуется как одно из оснований для конституционной защиты персональных данных[7].

стандартов и благоприятного правового режима в рамках законодательства об интеллектуальной собственности для технологий ИИ; установление систем оценки и контроля безопасности ИИ; развитие обучения кадров для работы с ИИ; осуществление широкого спектра научных активностей по тематике ИИ.

[3] *Daitian Li, Tony W. Tong and Yangao Xiao*. Is China Emerging as the Global Leader in AI? // Harvard Business Review, 18 February 2021. URL: https://hbr.org/2021/02/is-china-emerging-as-the-global-leader-in-ai (дата обращения: 22.03.2022).

[4] *Greenleaf G*. Asian Data Privacy Laws: Trade and Human Rights Perspectives. Oxford University Press, 2014. P. 80.

[5] Op. cit. P. 167.

[6] *Ван Сисинь, Пэн Чан*. Конституционные основы правовой системы защиты личной информации, 2021 CLI.A. 7118734 (на кит.). URL: https://www.pkulaw.com/specialtopic/8bb547fc13eb3f3391b0158c754eb7e5bdfb.html (дата обращения: 22.03.2022).

[7] *Джоу С.*. Конституционный анализ о праве персональных данных. 2021(1):133–140. DOI:10. 11835/ jissn. Журнал Чун-

> Тем не менее отсутствие конкретных положений о защите персональных данных или частной жизни граждан не послужило препятствием для принятия ряда актов в данной области. Во многом это связано с тем, что Конституция в Китае носит преимущественно организационный характер, будучи адресованной высшим органам власти в качестве ориентирующего начала для вырабатываемых решений, и не является актом, предполагающим возможность гражданина ссылаться на его положения в ходе судебного процесса.

Ни один суд в КНР, включая Верховный суд, не имеет права констатировать, что принятый закон противоречит Конституции, — это исключительная прерогатива высшего органа законодательной власти. Все это обусловливает тот факт, что на Конституцию в КНР не ссылаются в судебных решениях[8], а лишь упоминают в начальных статьях принимаемых законов в качестве «источника вдохновения» для них.

Впервые право на неприкосновенность частной жизни появилось в Законе о деликтной ответственности от 2009 года[9], наряду с правами на защиту репутации, правом на изображение, правом на имя и рядом иных прав, которые бы в российской доктрине подпадали под категорию «нематериальные блага». Однако на основе данных положений не сформировалось какой-либо значимой практики, хотя отдельные примеры применения этих положений для разрешения межличностных конфликтов, связанных с персональными данными, все же встречаются[10].

На ранних этапах становления законодательства о защите персональных данных китайское правительство было более озабочено защитой национальной безопасности и публичных интересов, что нашло свое отражение в постановлении Постоянного комитета Всекитайского собрания народных представителей (парламента КНР) «Об усилении защиты информации, передаваемой по сетям связи» от 28 декабря 2012 года[11]. Данное постановление, состоящее из 12 статей, сформулированных в весьма общем виде, явилось прообразом будущего Закона о кибербезопасности. В постановлении, в частности, прямо обозначалась обязанность провайдеров сетевых услуг и иных предприятий, собирающих и обрабатывающих электронную информацию о гражданах в процессе своей коммерческой деятельности, соблюдать принципы законности, необходимости, прозрачности, а также получать согласие от таких граждан на обработку данных. В явной форме установлен запрет на незаконное приобретение и продажу персональных данных. Причем одной из целей данного требования обозначалась защита национальной безопасности и социального порядка.

Впоследствии законодательство КНР о персональных данных развивалось по американской секторальной модели, предполагающей принятие точечных законодательных норм о защите персональных данных в определенных сферах и типах отношений. Общие положения о защите персональных данных были включены в 2013 году в Закон о защите прав потребителей[12] в виде права потребителя на защиту

цинского университета (издание по общественным наукам) / ZHOU Sijia. Constitutional analysis about the personal data right[J]. Journal of Chongqing University (Social Science Edition), 2021(1):133–140.

[8] *Чен Я*. Конституционное толкование и практическая объективность // Юридические методы. 2022 / 杨陈, 宪法解释与实践客观性, 《法律方法》, 2022. URL: https://www.pkulaw.com/qikan/d0c920c868f1c7479a61c9f27ce1d9b4bdfb.html (дата обращения: 22.03.2022).

[9] Закон Китайской Народной Республики «О деликтной ответственности», принят на 12-м заседании Постоянного комитета 11-го Всекитайского собрания народных представителей Китайской Народной Республики 26 декабря 2009 года / 中华人民共和国侵权责任法》已由中华人民共和国第十一届全国人民代表大会常务委员会第十二次会议于2009年12月26日通过.

[10] Например, данный закон использовался в качестве основания для обязания соседа демонтировать камеру видеонаблюдения, которая захватывала частную территорию истца. Но каких-либо споров с коммерческими компаниями на основе положений данного закона рассмотрено не было. См.: *Greenleaf G*. Asian Data Privacy Laws: Trade and Human Rights Perspectives. Oxford University Press. 2014. P. 203.

[11] Постановление Постоянного комитета Всекитайского собрания народных представителей «Об усилении защиты информации в сети Интернет», принято на 30-м заседании Постоянного комитета Всекитайского собрания народных представителей одиннадцатого созыва 28 декабря 2012 года / 全国人民代表大会常务委员会关于加强网络信息保护的决定, 2012年12月28日第十一届全国人民代表大会常务委员会第三十次会议通过.

[12] Закон Китайской Народной Республики «О защите прав и интересов потребителей» (с поправками от 2013 года), принятый на пятой сессии Постоянного комитета Всекитайского собрания народных представителей 12-го созыва от 25 октября 2013 года / 中华人民共和国消费者权益保护

своих персональных данных при приобретении товаров или услуг (ст. 14). Кроме того, в 2013 году Министерство промышленности и информатизации КНР, которое, помимо прочего, ответственно за регулирование Интернета, индустрии программного обеспечения и развитие информационного общества, издало Правила защиты персональных данных в телекоммуникационном секторе[13], которые включали принцип минимизации собираемых данных, обязанность уведомления регулятора об утечках данных. Были приняты положения о защите персональных данных и в иных сферах, в частности в отношении медицинских данных и сведений, содержащихся в кредитных историях[14].

Важной вехой в развитии законодательства о персональных данных стало принятие в 2016 году Закона о кибербезопасности, в который помимо технических вопросов регулирования онлайн-контента, обеспечения сетевой безопасности и защиты критической информационной инфраструктуры были включены некоторые положения, касающиеся защиты персональных данных: дефиниция персональных данных, общие принципы обработки персональных данных и даже отдельные запреты, адресованные операторам. Однако они носили весьма общий характер и предполагали возможность слишком широкой интерпретации. Текстам китайских законодательных актов в целом свойственна нечеткость и расплывчатость формулировок. Тем самым для правоприменителя создаются весьма комфортные условия по применению нечетких формулировок при решении задач государственно-политического характера, а также по трактовке правовой нормы в свою пользу[15].

В определенной степени расплывчатые и общие формулировки Закона о кибербезопасности были конкретизированы в Национальном стандарте «О безопасности личной информации»[16], принятом Национальным техническим комитетом по стандартизации в области информационной безопасности *TC260*. Данный стандарт вступил в силу, как и *GDPR*, в мае 2018 года и в значительной степени заимствовал многие его положения и концепции. Впоследствии он был модернизирован в 2020 году. Данный акт, хотя, как и прочие подобные стандарты, формально не является юридически обязательным актом, но обладает значительным авторитетом в индустрии и тем самым по факту носит характер квазиобязательного документа[17]. В нем уже можно наблюдать заимствование ряда элементов, характерных для европейской модели регулирования персональных данных, в частности его распространение на всех операторов, безотносительно их отраслевой принадлежности; выделение категории «чувствительные данные», установление права на переносимость данных, регулирование профайлинга и алгоритмического принятия решений и в целом — более жесткие формулировки принципов обработки (особенно принципа минимизации данных).

В 2020 году положения о защите персональных данных граждан были включены в новый Гражданский кодекс КНР (далее — ГК КНР)[18], вступивший в силу

法(2013修正), 根据2013年10月25日第十二届全国人民代表大会常务委员会第五次会议修正.

[13] Правила защиты персональных данных в телекоммуникационном секторе, принятые на 2-м исполнительном заседании Министерства промышленности и информационных технологий Китайской Народной Республики 28 июня 2013 года / 电信和互联网用户个人信息保护规定, 2013年6月28日中华人民共和国工业和信息化部第2次部务会议审议通过.

[14] *Pernot-Leplay E.* China's Approach on Data Privacy Law: A Third Way Between the U.S. and the E.U.? // The Penn State Journal of Law & International Affairs. 2020. No. 8. P. 72.

[15] См.: Правовые основы бизнеса в Китае / отв. ред. А.Е. Молотников, В. Шань. М., 2018. С. 91.

[16] Утвержден Государственным управлением по регулированию рынка и Национальным управлением по стандартизации Китая 22 октября 2019 года / 信息安全技术 个人信息安全规范, 市场监督管理总局、中国国家标准化管理委员会发布 2019年10月22日. URL: https://resources.pkulaw.cn/staticfiles/fagui/20200309/17/19/5/1ae09142b29677c0da685289d6c092d0.pdf (дата обращения: 22.03.2022).

[17] В какой-то степени национальные стандарты КНР в области персональных данных схожи с разъяснениями положений *GDPR*, издаваемых Европейским советом по защите персональных данных (*European Data Protection Board, EDPB*). Однако если разъяснения *EDPB* представлены в виде инструкций и иллюстраций, то национальные стандарты в КНР изложены в виде структурированных в пунктах положений, намекая на их квазиобязательный характер.

[18] 中华人民共和国民法典（2020年5月28日第十三届全国人民代表大会第三次会议通过）/ Гражданский кодекс Китайской Народной Республики (принят на третьей сессии 3-го Всекитайского собрания народных представителей 28 мая 2020 года). URL: https://www.pkulaw.com/en_law/aa00daaeb5a4fe4ebdfb.html?flag=chinese (дата обращения: 22.03.2022). С неофициальным переводом кодекса на английский язык можно ознакомиться по ссылке: http://english.www.gov.cn/archive/lawsregulations/202012/31/content_WS5fedad98c6d0f72576943005.html (дата обращения: 22.03.2022).

с 1 января 2021 года. Глава 6 раздела 4 Кодекса целиком посвящена вопросам защиты неприкосновенности частной жизни и персональных данных, признаваемыми разновидностью личных прав, к которым также относятся право на жизнь и здоровье, на имя, на изображение, защиту репутации и др. Кодекс устанавливает понятия частной жизни и недопустимые формы вмешательства в нее, например посредством направления незапрошенных сообщений, подслушивания или фотографирования лица в его частной территории (ст. 1023–1033 ГК КНР). Кроме того, устанавливается общее понятие персональных данных, а также весьма общие правила их обработки: наличие согласия или иного основания, указанного в законе; доступность правил обработки для ознакомления; четкое указание цели, метода и объема обработки информации; осуществление обработки в рамках законодательно установленных правил и ограничений и ее непротиворечие соглашению сторон (ст. 1035 ГК КНР). Также предусматриваются право гражданина делать копии такой информации и требовать ее уточнения и обязанность обработчика информации по обеспечению ее конфиденциальности.

> Следует отметить: несмотря на то, что данные нормы в определенной степени дублируют положения, которые обычно содержатся в законодательстве о персональных данных, они потенциально имеют весьма ограниченное действие. Во-первых, нормы законодательства о персональных данных носят специальный характер и в силу этого имеют приоритет перед нормами ГК КНР (ст. 11). Во-вторых, ГК КНР регулирует частноправовые отношения и тем самым ориентированы на горизонтальные отношения между гражданином и обработчиком информации, в то время как законодательство о персональных данных носит преимущественно административный характер и тем самым ориентировано на контроль за его соблюдением со стороны специальных органов.

Таким образом, ГК КНР, по сути, стал еще одним «секторальным» законом, регулирующим обработку персональных данных в определенном контексте. Вместе с тем определенные коллизии между положениями ГК КНР и специальными законами о защите персональных данных в принципе не исключены, особенно когда возникнет спор непосредственно между гражданином и обработчиком информации, на что указывают и в китайской доктрине[19].

Вопрос о необходимости принятия полноценного закона о защите персональных данных встал достаточно быстро. Главная причина — разрозненность этих законов, а также необходимость более детального регулирования процессов обработки персональных данных в свете распространения новых технологий, в частности Интернета вещей и мобильных приложений, в которых процессы сбора и обработки данных пользователей в ряде случаев происходили со злоупотреблениями и нарушениями. В частности, в мае 2021 года китайский уполномоченный орган по надзору в сфере киберпространства — Администрация киберпространства — привлек к ответственности крупные китайские компании, в числе которых *Tencent* и *Baidu*, за чрезмерный сбор данных пользователей 33 мобильных приложений[20]. В июле 2021 года через несколько дней после выхода на *IPO* в США китайская компания *DiDi* — оператор платформы по заказу услуг такси и каршерингу — получила предписание от Администрации киберпространства КНР об удалении ее приложения из китайских магазинов приложений в связи с нарушением порядка сбора и обработки персональных данных китайских пользователей[21]. Данные события послужили хорошим фоном для принятия в августе 2021 года на сей раз уже всеобъемлющего закона, посвященного обработке персональных данных.

---

[19] *Mingli Shi*. China's Draft Privacy Law Both Builds On and Complicates Its Data Governance // Digichina, Stanford University, 20 December 2020. URL: https://digichina.stanford.edu/work/chinas-draft-privacy-law-both-builds-on-and-complicates-its-data-governance/ (дата обращения: 22.03.2022).

[20] *Eileen Yu*. China calls out 33 apps for collecting more user data than deemed necessary // ZDNet. 1 May 2021. URL: https://www.zdnet.com/article/china-calls-out-33-apps-for-collecting-more-user-data-than-necessary/ (дата обращения: 22.03.2022).

[21] *Eileen Yu*. Didi barred from China appstores amidst government cybersecurity review // ZDNet. 4 July 2021. URL: https://www.zdnet.com/article/didi-barred-from-china-appstores-amidst-government-cybersecurity-review/ (дата обращения: 22.03.2022).

## 3. Общая характеристика нового Закона о защите личной информации

Новый Закон о защите личной информации[22], принятый 20 августа 2021 года и вступивший в силу с 1 ноября 2021 года, состоит из 74 статей и имеет своей декларируемой целью не только защиту прав и интересов граждан в области обработки их данных, но и стандартизацию подходов к такой обработке, а также стимулирование рационального использования персональных данных (ст. 1). В пресс-релизе, сопровождавшем принятие Закона, отмечается, что он призван обуздать хаос, который творится с обработкой персональных данных крупными интернет-платформами[23]. Несмотря на отсутствие в тексте Закона разделения на автоматизированную и неавтоматизированную обработку и его формальную применимость к обоим ее видам, он направлен именно на автоматизированную обработку персональных данных в интернет-среде. Об этом свидетельствует и назначение в качестве регулятора по данному Закону Администрации киберпространства КНР, о котором будет сказано далее.

Принятие данного Закона можно рассматривать как торжество европейской модели регулирования персональных данных, основы которой были заложены в китайское законодательство еще в национальных стандартах 2018 и 2020 годов по защите персональных данных. Таким образом, секторальная модель США была отвергнута. Примечательно, что многие положения нового Закона весьма созвучны с соответствующими положениями *GDPR*, в частности:

— принципы обработки данных — законности, минимизации данных, спецификации цели, прозрачности в части раскрытия сведений о порядке и целях обработки данных, обеспечения точности обрабатываемых данных, их конфиденциальности, а также принцип подотчетности операторов за принимаемые меры защиты данных;

— установление в ст. 13 перечня из 6 законных оснований для обработки персональных данных: 1) явно выраженное согласие; 2) необходимость заключения или исполнения договора, в котором гражданин является стороной либо если обработка осуществляется в рамках трудового законодательства; 3) выполнение требований законодательства; 4) защита жизни и здоровья гражданина, в том числе необходимость реагирования на внезапные ситуации чрезвычайного характера; 5) обработка данных в разумных объемах для целей освещения в новостях и иных публичных целях; 6) обработка в разумных объемах данных, ранее раскрытых самим гражданином либо раскрытых на иных основаниях. Иные основания для обработки могут быть предусмотрены в правовых актах[24];

— закрепление за гражданином ряда прав, характерных для европейского регулирования, — права на переносимость данных, права требовать уточнения или удаления данных при определенных обстоятельствах;

[22] Официальный текст закона на китайском языке доступен по ссылке: http://www.cac.gov.cn/2019-08/23/c_1124913903.htm. С неофициальным переводом закона на английский язык можно ознакомиться на сайте Стэндфордского университета по ссылке: https://digichina.stanford.edu/work/translation-personal-information-protection-law-of-the-peoples-republic-of-china-effective-nov-1-2021/ (дата обращения: 22.03.2022).

[23] China Focus: China adopts new law to protect personal information // Xinhua. 20 August 2021. URL: http://www.xinhuanet.com/english/2021-08/20/c_1310139417.htm (дата обращения: 22.03.2022).

[24] Примечательно, что по ранее действовавшим законодательным нормам единственным законным основанием для обработки персональных данных было, по сути, лишь согласие лица, что обусловливало необходимость его чрезмерно широкого толкования и появления так называемых подразумеваемых согласий. (См.: *Дини С., Цзяньпин Ш.* Исследование требования о согласии на коммерческое использование личной информации с точки зрения типизации личной информации // Северный юридический журнал. 2017. № 5 / 项定宜, 申建平, «个人信息商业利用同意要件研究—以个人信息类型化为视角», 《北方法学》, 2017 [5]). Теперь же согласие должно быть явным, информированным и добровольным (ст. 14), а также сопровождаться возможностью его отзыва, который не имеет ретроактивного действия и не затрагивает процессы обработки, реализованные до такого отзыва (ст. 15). При этом отказ в даче согласия или последующий его отзыв не может влечь отказ в предоставлении товара или услуги оператором, если только такие данные не являются безусловно необходимыми для их предоставления. Все вышеприведенные положения весьма созвучны с положениями *GDPR*, хотя отсутствие в китайском законодательстве такого основания, как законный интерес оператора, все же является одной из черт, которые отличают его от европейского и российского законодательства о персональных данных.

— возложение на операторов обязанностей по назначению ответственных за обработку персональных данных, проведение оценки воздействия на защиту персональных данных;

— экстерриториальный характер действия с критериями, аналогичными *GDPR,* — осуществление направленной деятельности по предложению товаров или услуг китайским гражданам или осуществление анализа и оценки их деятельности. Даже номер статьи, регламентирующей экстерриториальность в китайском и европейском законах, идентичен (ст. 3). При этом китайский закон сохраняет возможность установления иных оснований экстерриториальности в правовых актах, создавая условия для расширения перечня критериев в будущем.

Все эти основания также дополняются общей бланкетной нормой, допускающей обработку персональных данных без согласия гражданина и в иных случаях, предусмотренных законодательством. Тем самым многие положения, которые были ранее обозначены в Национальном стандарте «О безопасности личной информации» и имели статус квазиобязательных, приобрели юридически обязывающий характер.

> Вместе с тем китайские аналоги положений *GDPR* сформулированы в гораздо более общем виде и не имеют той степени детализации, которой может похвастать европейское законодательство. Таким образом создается большой простор для усмотрения государственных органов, администрирующих применение Закона о защите персональных данных КНР, а также для появления множества подзаконных актов и стандартов в этой сфере.

Однако было бы наивно полагать, что Китай просто скопировал основные положения *GDPR*, не привнеся пресловутой китайской специфики в свое регулирование. Так, например, в китайском законодательстве не проводится типичных для европейского регулирования различий между операторами и обработчиками данных. Обязанности, возникающие из факта обработки персональных данных гражданина, возникают в равной степени у любого лица, которое обрабатывает персональные данные и не подпадает под какое-либо из изъятий, например при обработке для личных и семейных нужд или в рамках законодательства об архивном деле (ст. 72)[25].

За рядом *GDPR*-подобных положений скрываются достаточно мощные публично-правовые начала, направленные на отстаивание государственных интересов на международной арене. Так, новый закон: 1) установил существенные ограничения на трансграничную передачу данных за пределы КНР; 2) расширил требования локализации данных, которые ранее были предусмотрены Законом о кибербезопасности лишь в отношении операторов объектов критической инфраструктуры; 3) имеет экстерриториальное действие; 4) предусматривает возможность блокировки иностранных интернет-ресурсов, нарушающих права китайских граждан на защиту их персональных данных или создающих угрозу национальной безопасности КНР; 5) предусматривает возможность принятия ответных симме-

[25] В этой связи китайский подход ближе к российскому подходу в его интерпретации Роскомнадзором. В обоих случаях предусматривается возможность заключения соглашения, в рамках которого одно лицо будет обрабатывать данные в интересах другого, а также предусматриваются схожие условия для заключения такого соглашения (см.: ст. 21 Закона о защите личной информации ч. 3 ст. 6 ФЗ «О персональных данных»). Позиция Роскомнадзора также сводится к тому, что в российском законодательстве нет фигуры «обработчика», поэтому все лица, которые обрабатывают персональные данные, являются по сути операторами. Данная позиция находила свое отражение в ряде разъяснений Роскомнадзора, данных в ходе семинаров для операторов, в частности в рамках дня открытых дверей 28 января 2022 года (см.: https://www.youtube.com/watch?v=jJJLbTS_AqM). Вместе с тем достаточно сложно согласиться с данной позицией по причине наличия в российском законе прямого положения о том, что «в случае, если оператор поручает обработку персональных данных другому лицу, ответственность перед субъектом персональных данных за действия указанного лица несет оператор. Лицо, осуществляющее обработку персональных данных по поручению оператора, несет ответственность перед оператором». Это положение прямо разграничивает статус оператора и лица, осуществляющего обработку персональных данных по его поручению, в отношениях с участием субъекта. Аналогичных положений в Законе КНР о защите личной информации не содержит, поэтому применительно к Китаю действительно можно говорить об отсутствии сущностных различий в правовом режиме оператора и обработчика. Однако для удобства в данной статье будет использован уже понятный для русскоязычного читателя термин «оператор персональных данных».

тричных мер в отношении иностранных государств или регионов, которые проводят дискриминационную политику в отношении КНР по вопросам регулирования оборота персональных данных.

Во многом такое внимание к публично-правовым аспектам обработки данных обусловлено значением персональных данных китайских пользователей для достижения Китаем лидирующих позиций в мире. Как отмечается, «алгоритмы, созданные средним инженером, могут превзойти алгоритмы, созданные ведущими мировыми экспертами, если средний инженер имеет доступ к гораздо большему количеству данных». Согласно официальной статистике, по состоянию на июнь 2021 года в Китае насчитывался уже 1 млрд пользователей Интернета[26]. Тем самым в Китае больше пользователей Интернета, чем в США и Европе, вместе взятых, и китайские компании получают самые качественные данные. В отличие от крупнейших *IT*-компаний США, которые накапливают данные об активности пользователей на онлайн-платформах (историю поисков, загруженные фотографии, просмотренные видео, лайки и пр.), китайские *IT*-гиганты вместо этого собирают данные из реальной жизни: что, когда и где вы покупали, какую еду заказывали, куда ездили, что фотографировали. Таким образом, технологическая экосистема Китая дает алгоритмам больше «глаз», позволяющих целиком увидеть картину нашей повседневной жизни[27]. Такой потенциал агрегированных интернет-платформами данных обусловливает их стратегический характер конкурентного преимущества для Китая и стремление ограничить доступ к ним со стороны других государств. В этой связи более не вызывают удивления действия Администрации киберпространства КНР в отношении компании *DiDi*, которая в результате *IPO* на рынке США могла тем самым создать угрозу для получения доступа к данным многих миллионов китайских пользователей со стороны США.

Но сводить всю политико-правовую составляющую нового Закона о защите персональных данных исключительно к внешней, геополитической составляющей было бы неверно. Как отмечалось, Закон имеет целью обуздать хаос, который творился в области сбора и обработки данных коммерческими операторами, главным образом из числа интернет-компаний и разработчиков мобильных приложений. Защита персональных данных — важный инструмент обеспечения доверия к цифровым сервисам[28].

> И наведение порядка в этой области, в том числе в части условий использования мобильных приложений, защитив пользователей от необоснованных аппетитов их операторов в отношении геолокационных данных, данных адресной книги с последующими несанкционированными звонками и сообщениями представляет собой важный месседж со стороны государства, что оно не оставит граждан один на один в борьбе с экономически и технически более сильной стороной.

И достаточно активная деятельность китайских регуляторов в этой области показывает серьезность намерений китайского правительства в области усиления позиций пользователей в их отношениях с интернет-компаниями[29], что должно способствовать дальнейшему генерированию качественных данных граждан, которые могут быть использованы в том числе и для нужд повышения эффективности государственного управления. Установление существенных штрафов, в том числе оборотных, также свидетельствует о том, что новый Закон не рассчитан на применение только к малому и среднему бизнесу, но и адресован в том числе трансграничным компаниям, ведущим деятельность в Китае, а также крупнейшим китайским компаниям.

---

[26] См.: http://www.news.cn/english/2021-08/27/c_1310151874.htm (дата обращения: 22.03.2022).

[27] См.: *Кай-Фу Л.* Сверхдержавы искусственного интеллекта. М., 2019. С. 136-137.

[28] *Цюань Л.* Безопасность данных: регулирование защиты личной информации // Law Review. 2022 (1) / 刘权, 数据安全认证：个人信息保护的第三方规制,《法学评论》, 2022 (1) URL: https://www.pkulaw.com/qikan/1ac48e59f7072063faad34f8ea075ebbdfb.html (дата обращения: 22.03.2022).

[29] Так, Министерство промышленности и информатизации КНР по результатам проверки указало в августе 2021 года на обнаруженные нарушения порядка обработки персональных данных в 43 мобильных приложениях. URL: https://www.miit.gov.cn/xwdt/gxdt/sjdt/art/2021/art_8c2a4fc09c234122a48174d4d850c214.html (дата обращения: 22.03.2022).

Основной регулятор и контрольно-надзорный орган, администрирующий правоприменительную практику по Закону о защите личной информации, — Администрация киберпространства КНР (国家互联网信息办公室, CAC), которая выполняет функции мегарегулятора в интернет-сфере, что роднит ее с отечественным Роскомнадзором. Примечательно, что Администрация киберпространства КНР является мажоритарным владельцем Инвестиционного фонда сети Интернет КНР, который, в свою очередь, является акционером многих китайских технологических компаний (*ByteDance, Weibo* и др.), тем самым сочетая административный контроль над технологическим сектором с корпоративным.

## 4. Понятие и категории персональных данных по новому Закону о защите персональных данных

В Законе о защите персональных данных КНР приводится следующая дефиниция персональных данных[30]: все виды информации, существующие в электронном или ином виде, относящиеся к определенному или определяемому физическому лицу, не включая информацию, прошедшую процедуру анонимизации. Кроме того, дефиниции персональных данных содержатся и в иных законах КНР. В частности, в ст. 76 (5) Закона о кибербезопасности, согласно которой к ним относятся «сведения различного рода, которые зафиксированы в электронной или иной форме и позволяют по отдельности или совместно с другими сведениями идентифицировать определенное физическое лицо, включая имя и фамилию, дату рождения, номер удостоверения личности, биометрические данные, адрес проживания, номер телефона, адрес электронной почты, сведения о здоровье, сведения о местах пребывания и другие сведения о физическом лице»[31]. Аналогичная дефиниция содержится и в ст. 1034 ГК КНР.

> Несмотря на текстуальные различия, из всех приведенных определений видно, что китайское законодательство исходит из широкого подхода к понятию персональных данных, на что указывается и в китайской доктрине[32].

Данный подход не должен вызывать удивления, если учесть те цели, которые преследовал китайский законодатель, принимая данный закон: интернет-платформы и мобильные приложения в основном злоупотребляют сбором и обработкой данных, которые представляют собой не столько прямые идентификаторы лица, сколько позволяющие выявить его определенные характеристики без определения его личности.

В Национальном стандарте (спецификации) по защите персональных данных 2020 года отмечается, что при отнесении той или иной информации к числу персональных данных необходимо руководствоваться двумя основными критериями: возможностью ее использования для идентификации конкретного физического лица либо возможностью ассоциирования этой информации с определенным физическим лицом, что будет иметь место применительно к геолокационной информации, сведениям о пользовательской активности в Интернете.

В таблице ниже приведены различные виды персональных данных и их примеры, перечисленные в данном Стандарте, которые весьма напоминают перечень данных, признаваемых персональными в соответствии с Законом Калифорнии о защите частной жизни потребителей 2018 года[33].

---

[30] Следует отметить, что китайский законодатель использует термин 个人信息, который в дословном переводе означает «личная информация». Однако, учитывая, что он выполняет те же функции, что и термин «персональные данные» в российском и европейском законодательстве, во избежание терминологической путаницы в данной статье используется термин «персональные данные» вместо «личная информация».

[31] Гражданский кодекс Китайской Народной Республики (принят на третьей сессии Третьего Всекитайского собрания народных представителей 28 мая 2020 г.) / 中华人民共和国民法典（2020年5月28日第十三届全国人民代表大会第三次会议通过). URL: https://www.pkulaw.com/en_law/aa00daaeb5a4fe4ebdfb.html?flag=chinese (дата обращения: 22.03.2022).

[32] *Чжан Лу*. Что такое личная информация? На основе обсуждения пересечения прав на неприкосновенность частной жизни и защиты личной информации в Гражданском кодексе // Журнал Университета политических наук и права Ганьсу. 2021. № 1 (на кит.) / 张璐, 何为私密信息？—基于《民法典》隐私权与个人信息保护交叉部分的探讨, 《甘肃政法大学学报》, 2021 (1). URL: https://www.pkulaw.com/qikan/65ed2d6ddb3105b6330702b2938b7967bdfb.html (дата обращения: 22.03.2022).

[33] California Consumer Privacy Act 2018, Section 1798. 140 (o).

**Персональные данные и их виды**

| | |
|---|---|
| Основные персональные данные | Имя, дата рождения, пол, этническая принадлежность, национальность, семейный статус, адрес проживания, личный номер телефона, адрес электронной почты и т.д. |
| Персональные идентификационные данные | Удостоверение личности, военный билет, паспорт, водительские права, разрешение на работу, карточка социального обеспечения, вид на жительство и т.д. |
| Биометрические данные | Личная информация о генах, отпечатки пальцев, голосовые данные, отпечатки ладоней, ушных раковин, радужной оболочки, функции распознавания лиц и т.д. |
| Идентификационная информация в Интернете | Номер аккаунта гражданина, *IP*-адрес, персональный цифровой сертификат и т.д. |
| Данные о здоровье | Личные записи, связанные с болезнью и лечением, такие как симптомы, записи о госпитализации, предписания врача, отчеты о результатах анализов, записи об операциях и анестезии, записи медсестер, записи о лекарствах, информация о лекарственной и пищевой аллергии, информация о фертильности, история болезни, диагностика и лечение, семейная история болезни, история текущего заболевания, история инфекционных заболеваний и т.д., а также информация, касающаяся личного состояния здоровья, — вес, рост, объем легких и т.д. |
| Данные о работе | Профессия, должность, образование, степень, опыт работы, сведения об обучении и т.д. |
| Данные о финансах | Банковский счет, идентификационная информация (пароль), информация о вкладах (включая сумму средств, записи о платежах и сборах и т.д.), информация о недвижимости, сведения о взятых кредитах, кредитная информация, записи о транзакциях и т.д., а также информация о наличии виртуальной валюты, виртуальных транзакциях — активационных кодах видеоигр и другая информация о виртуальной собственности |
| Данные об общении | Записи и содержимое сообщений, текстовые сообщения, *MMS*-сообщения, электронные письма, а также данные, характеризующие сами сообщения (часто называемые метаданными) и т.п. |
| Контактные данные | Контакты, список друзей, список групп, список адресов электронной почты и т.д. |
| Данные об активности в Интернете | Сведения о просмотренных веб-сайтах, кликах, используемом ПО, списках «избранных» страниц и т.д. |
| Информация об устройстве | Относится к информации, описывающей основное состояние часто используемых гражданином персональных устройств, включая серийный номер оборудования, *MAC*-адрес устройства, перечень используемого ПО, уникальный идентификационный код устройства (например, информацию *IMEI/Android ID/IDFA/OpenUDID/GUID/SIM*-карты *IMSI* и т.д.) |
| Данные о местонахождении личности | Точная информация о местоположении, размещении, долгота и широта и т.д. |
| Прочая информация | Сведения о заключенных браках, религиозных убеждениях, сексуальной ориентации, неопубликованной судимости и т.д. |

### 4.1. Чувствительные персональные данные

> Закон КНР о защите личной информации дополнительно выделяет категорию так называемых чувствительных персональных данных. Они определяются как «персональные данные, которые в случае утечки или незаконной передачи третьим лицам могут унизить достоинство физического лица или поставить под угрозу личную и имущественную безопасность» (ст. 28).

При этом в Законе приводится примерный перечень такой информации: биометрические данные, религиозные убеждения, данные банковского счета, информация о здоровье и месте нахождения, а также персональные данные несовершеннолетних до 14 лет. Как видно, в этой части есть определенные отличия китайского подхода от европейского и российского подхода к аналогичной по сути категории персональных данных — «специальным категориям персональных данных». В *GDPR* и ст. 10 ФЗ «О персональных данных» указан закрытый перечень данных, которые носят чувствительный характер и имеют особый правовой режим независимо от того, насколько эти данные являются чувствительными для конкретного субъекта с учетом всех сопутствующих обстоятельств. Формулировка же ст. 28 Закона о защите личной информации содержит не только виды данных, которые признаются чувствительными, но также и критерии, при которых к таковым могут

быть отнесены и другие виды информации, предполагая тем самым риск-ориентированный подход и определение чувствительного характера данных по результатам оценки совокупности обстоятельств.

Основным последствием отнесения персональных данных к категории чувствительных является то, что их обработка возможна только при наличии конкретной цели и безусловной необходимости. При этом оператор должен получить отдельное согласие гражданина на такую обработку, которое в случаях, предусмотренных законодательством, должно даваться в письменной форме (ст. 29). Дополнительно на оператора возлагается обязанность информировать гражданина о причинах, обусловливающих необходимость обработки чувствительных данных и потенциальных рисках, а в некоторых случаях, предусмотренных законом, еще и получить лицензию на обработку таких видов данных (ст. 30, 32).

### 4.2. Биометрические данные

Примечательно, что Закон о защите личной информации не содержит отдельного регулирования биометрических данных и даже не содержит дефиниции таких данных. Такой подход выглядит несколько удивительно, учитывая, что в Китае уже давно особое внимание уделяется системам распознавания лиц. Единственным положением Закона о защите личной информации, посвященном системам распознавания лиц, является ст. 24, согласно которой установка и использование таких систем в публичных местах допустима только в той мере, которая необходима для соблюдения общественного порядка и соблюдения регуляторных норм и при условии установки соответствующих предупреждений в явной форме.

> Собранные таким образом изображения граждан могут быть использованы исключительно в целях обеспечения общественной безопасности. Для использования в иных целях необходимо получение отдельного согласия гражданина.

Эти положения закрепляют сложившуюся судебную практику по данному вопросу.

Так, на уровне Верховного суда КНР еще в 2018 году были изданы разъяснения по вопросам использования технологии распознавания лиц для обработки личной информации[34]. По общему правилу для обработки таких данных требуется согласие гражданина. При этом Верховный суд КНР указал, что оно не будет иметь юридической силы, если оператор вынуждает пользователя дать такое согласие, потому что иначе сервис/сайт/приложение/платформа не смогут функционировать. Исключением являются случаи, когда без использования биометрии их функционирование реально невозможно. Кроме того, согласие на обработку биометрических данных должно даваться отдельно от других согласий, в противном случае оно может быть признано не имеющим юридической силы.

Достаточно показательным в этой связи является дело Сяо Ли. Он жил в апартаментах в элитном доме. В июне 2020 года управляющая компания решила ввести систему распознавания лиц под предлогом обеспечения безопасности жильцов. Сяо Ли был единственным жильцом, который отказался от подписания согласия на обработку биометрической информации, так как система распознавания лиц представляла, по его мнению, вторжение в частную жизнь. Несмотря на отказ Сяо Ли, компания установила систему и сообщила Сяо Ли: если он не предоставит необходимые данные в течение определенного срока, договор найма жилья будет с ним расторгнут. Сяо Ли обратился в суд. На стадии предварительного слушания стороны заключили мировое соглашение, по которому управляющая компания предоставила возможность Сяо Ли пользоваться картой-ключом для входа. Тем не менее судья опубликовал особое мнение по данному делу. В нем было указано, что, несмотря на удобство и стремительное развитие информационных технологий, любые технологические решения, использующие чувствительные персо-

[34] «Положения Верховного народного суда по некоторым вопросам применения законодательства при рассмотрении гражданских дел, связанных с применением технологии распознавания лиц для обработки персональных данных», принятые на 1841-м заседании Судебного комитета Верховного народного суда 1 августа 2018 года /《最高人民法院关于审理使用人脸识别技术处理个人信息相关民事案件适用法律若干问题的规定》已于由最高人民法院审判委员会第1841次会议通过，现予公布，自2021年8月1日起施行. URL: https://www.pkulaw.com/chl/452f945c46c4739fbdfb.html (дата обращения: 22.03.2022).

нальные данные, могут быть использованы только с согласия субъекта[35].

В другом деле компания *Kohler* (*China*) была привлечена к ответственности за установку в сети своих магазинов камер видеонаблюдения с функцией распознавания лиц без получения согласия от посетителей на сбор данных в виде их изображений[36].

В настоящее время разрабатывается Национальный стандарт «Требования к защите биометрической информации»[37], в котором ожидается подробное регулирование не только подходов к защите информационных систем обработки биометрических данных, но и конкретизация понятия и отличительных характеристик биометрических данных. Кроме того, на уровне отдельных регионов Китая может вводиться более жесткий режим обработки биометрических данных. Например, в городе Тяньцзинь установлен общий запрет на сбор коммерческими организациями биометрических данных в виде отпечатков пальцев, изображений и голоса[38].

### 4.3. Обезличенные и анонимизированные данные

Закон о защите личной информации предусмотрел в ст. 73 дефиниции процедур обезличивания и анонимизации, которые в большинстве своем отражают логику *GDPR* по соотношению данных категорий.

> Под обезличиванием понимается процесс обработки, по результатам которого нельзя осуществить идентификацию гражданина без привлечения дополнительной информации. Под анонимизацией понимается процесс обработки, по результатам которого невозможно отграничить одно физическое лицо от другого и данный результат при этом носит необратимый характер.

Анонимизированные данные прямо исключены из дефиниции персональных данных, указанной в ст. 4. При этом отсутствие такой оговорки в отношении данных, прошедших процедуру обезличивания, означает, что обезличенные данные продолжают считаться персональными. Обезличивание рассматривается как технический способ защиты информации (ст. 51 (3)), Закон о защите личной информации не предусматривает какого-то льготного порядка обработки таких данных в отличие от положений *GDPR* и ФЗ «О персональных данных», однако большое количество отсылок в нем к правилам, предусмотренным законодательством, сохраняют простор для установления подобного режима в иных актах.

Методологии обезличивания персональных данных закреплены на уровне Национального стандарта «Руководство по обезличиванию личной информации» [39]. Помимо самих методологий и рекомендаций по выбору оптимальной для определенных задач, данный стандарт предусматривает необходимость заключения соглашений об использовании обезличенных данных, предусматривающих обязанности получателя по недопущению реидентификации массива данных и его передаче третьим лицам, в том числе посредством размещения ссылок на него на внешних ресурсах.

---

[35] Высший народный суд провинции Цзянсу. «Десять типичных дел о продвижении превосходной традиционной китайской культуры», 24 сентября 2021 года / 江苏省高级人民法院发布十件弘扬中华优秀传统文化典型例 2021.09.24. URL: https://www.pkulaw.com/pfnl/c05aeed05a57db0a5f65f4923297f551b3e9eda94895e61fbdfb.html (дата обращения: 22.03.2022).

[36] Национальный стандарт «Руководство по обезличиванию личной информации», выпущен Государственным управлением по регулированию рынка и Национальным управлением по стандартизации Китая 15 августа 2017 года / 信息安全技术　个人信息去标识化指南市场监督管理总局、中国国家标准化管理委员会发布2017年8月15. URL: http://www.sac.gov.cn/bszn/202009/t20200924_346908.html (дата обращения: 22.03.2022).

[37] Уведомление о запросе комментариев к Национальному стандарту «Требования к защите биометрической информации» от 25 июня 2019 года / 关于国家标准《信息技术 安全技术　生物特征识别信息的保护要求》征求意见稿征求意见的通知, 2019年6月25日.

[38] «Тяньцзиньские правила социального кредита», приняты на 24-м заседании Постоянного комитета 17-го Тяньцзиньского муниципального собрания народных представителей 1 декабря 2020 года / 《天津市社会信用条例》已由天津市第十七届人民代表大会常务委员会第二十四次会议于2020年12月1日通过. URL: https://www.tc260.org.cn/front/bzzqyjDetail.html?id=20190625175932328888&norm_id=20180929110002&recode_id=34875 (дата обращения: 22.03.2022).

[39] Национальный стандарт «Руководство по обезличиванию личной информации», выпущен Государственным управлением по регулированию рынка и Национальным управлением по стандартизации Китая 15 августа 2017 года / 信息安全技术　个人信息去标识化指南市场监督管理总局、中国国家标准化管理委员会发布2017年8月15. URL: http://www.sac.gov.cn/bszn/202009/t20200924_346908.html (дата обращения: 22.03.2022).

### 4.4. Общедоступные персональные данные

Как таковой дефиниции общедоступных персональных данных в законодательстве КНР нет. Однако в соответствии со ст. 27 и 13 (6) Закона «О защите личной информации» и п. 2 ст. 1036 ГК КНР под ними можно понимать те данные, которые лицо самостоятельно публично раскрыло, или персональные данные, которые были публично раскрыты иными лицами на законных основаниях.

При этом под публичным раскрытием персональных данных понимается ситуация, в которой персональные данные становятся доступными для заранее неопределенного круга лиц[40]. В качестве иллюстрации возможного применения критерия доступности неопределенному кругу лиц можно привести дело Сун Чанбао против *Beiing Sohu Internet Information Service Co*., *Ltd* и *Baidu Netcom Company*[41]. В 2010 году истец загрузил свою фотографию и информацию об образовании в личный кабинет на сайте *China Alumni Record* — информационном ресурсе о выпускниках высших учебных заведений Китая, который был впоследствии закрыт в 2013 году. В 2018 году истец обнаружил, что при вводе его имени и фамилии в поисковой платформе *Baidu* в результатах поиска показывается его фотография, которая была им когда-то загружена на сайте *China Alumni Record*. Истец потребовал прекратить выдачу его фотографии в поисковой системе, а также возместить расходы на нотариальное заверение доказательств и убытки в размере 1 юаня. Ответчик, компания *Baidu*, указала, что отображение фотографии в результатах поиска не является нарушением, поскольку истец в свое время сам сделал ее общедоступной, а *Baidu* лишь выдавала в результатах поиска релевантную информацию из открытых источников. Другой ответчик, компания *Sohu Internet Information Service*, в своих доводах отметила, что не является надлежащим ответчиком по делу, так как закрыла веб-сайт еще в 2013 году, а администратором веб-сайта, с которого была взята фотография истца, является *Baidu*. Суд установил, что доступ к веб-сайту, на котором истец разместил фотографию, могли получить лишь зарегистрированные пользователи. Таким образом, в данном случае не было факта публичного раскрытия. В итоге суд постановил прекратить *Baidu* предоставлять в результатах выдачи фотографию истца, а также возместить расходы на нотариальное заверение доказательств и убытки.

> Еще одним важным условием допустимости обработки общедоступных персональных данных выступает разумный характер такой обработки. Тот факт, что данные были сделаны общедоступными гражданином, не означает, что их последующая обработка возможна в любых целях.

И ст. 13(6) Закона о защите личной информации, и п. 2 ст. 1036 ГК РФ говорят о том, что соответствующая обработка должна носить разумный характер. Конкретные критерии разумных пределов пока еще не выработаны практикой. В доктрине высказывается мнение, что стандарт разумных пределов предполагает соответствие разумным ожиданиям субъекта персональных данных[42]. Иными словами, обработка публично раскрытых персональных данных должна соответствовать субъективным ожиданиям лица и не нарушать его жизненно важные интересы, такие как возможное ущемление достоинства личности, угроза личным или имущественным правам. К примеру, в случае если личная страница пользователя и его действия на веб-сайте будут обрабатываться посредством

[40] *Ши Ченг*, «Правовые основы обработки личной информации в эпоху цифровой экономики» // Журнал Чунцинского технологического университета (социальные науки). 2021 (9) / 时诚, «数字经济时代个人信息处理的法律基础», 《重庆理工大学学报（社会科学）》2021 (9). URL: https://www.pkulaw.com/qikan/004a6de45afc6ea3f-3361f693b4d771fbdfb.html (дата обращения: 22.03.2022).

[41] Решение Пекинского интернет-суда по делу Сун Чанбао против Beijing Sohu Internet Information Service Co., Ltd и Baidu Netcom Company № 10989. 16 декабря 2020 года / 宋长宝诉北京搜狐互联网信息服务有限公司人格权纠纷民事一审判决 和百度网通公司北京互网法院 · 2020 年 12 月 16 日№ 10989. URL: https://www.qcc.com/wenshuDetail/911c4eac0b17dd04b6a8aaacfb710847.html (дата обращения: 22.03.2022).

[42] *Лю Шуанян.* «Разумное обращение» и преступный механизм преступления, заключающегося в посягательстве на личную информацию граждан» // Юридический факультет Юго-Восточного университета; Исследовательский институт прав человека Юго-Восточного университета, 2021 (на кит.) / 刘双阳 “合理处理”与侵犯公民个人信息罪的出罪机制» 东南大学法学院;东南大学人权研究院 2021.

алгоритмов для профайлинга и в последующем это приведет к дискриминации в процессе получения товаров и услуг, то такая обработка может быть признана незаконной[43]. Кроме того, в китайской доктрине отмечается, что последующая обработка персональных данных, публично раскрытых гражданином, должна соответствовать первоначальной цели раскрытия персональных данных и не выходить за ее пределы[44].

Как видно из приведенных положений, касающихся правового режима различных видов персональных данных, можно с уверенностью утверждать, что Китай не пошел по пути рестриктивного подхода к понятию персональных данных, распространяя его на самые разные виды информации, связанной с физическим лицом, и выводя из-под него обезличенные данные. Китайский законодатель поставил целью обеспечить защиту всего массива личной информации, в том числе наиболее ценные их виды, характеризующие поведенческие или личностные характеристики лица, т.е. косвенно определяющие такое лицо. В конечном счете это должно обеспечить доверие потребителей к цифровым сервисам крупных компаний, которые являются одними из основных адресатов нового регулирования, и тем самым к цифровизации в целом. И уже тем более данный широкий подход к персональным данным не воспринимается в Китае в качестве барьера на пути развития технологий искусственного интеллекта. Однако особенность китайской модели регулирования персональных данных проявляется, как отмечалось ранее, в совокупности публично-правовых положений, которые направлены на защиту национальных интересов Китая и обеспечение его конкурентного преимущества в гонке за технологиями.

## 5. Правила о локализации и трансграничной передаче персональных данных

### 5.1. Сфера применения требований о локализации персональных данных

Китайское законодательство содержит требования локализации определенных видов данных уже достаточно давно. Изначально данные требования начали появляться в отдельных секторальных законах, в частности, применительно к информации, составляющей финансовые данные кредитных учреждений, сведения о здоровье населения и даже данные, генерируемые агрегаторами такси[45]. Однако впервые требование локализации персональных данных приобрело достаточно масштабные очертания с принятием Закона о кибербезопасности 2016 года, в ст. 37 которого была предусмотрена обязанность операторов объектов критической информационной инфраструктуры (далее — КИИ), которые осуществляют сбор или создание персональных данных или иных «важных данных»[46] на территории континентального Китая, хранить их также на территории континентального Китая[47]. При этом передача данных за пределы континентального Китая допустима только по результатам согласования с уполномоченными государственными органами в области безопасности и оценки рисков подобной передачи.

> Таким образом, требование локализации в этом случае означает не просто хранение копии данных на соответствующей территории, но и локализацию всех процессов их обработки.

К КИИ относятся такие объекты, повреждение которых может повлечь серьезный урон национальным или публичным интересам. Согласно Национальной

[43] *Хуан Вэй*. Интерпретация Гражданского кодекса Китайской Народной Республики (часть 2) // Law Press. 2020 / 黄薇主编：《中华人民共和国民法典释义（下）》，法律出版社2020年版.

[44] *Цзоу Даньли, Лю Ян.* Исследование стандартов использования публичной личной информации (часть 2), Пекинская юридическая фирма Tongshang 2021-12-09 / 邹丹莉 刘洋 «已公开个人信息的使用规范研究（下)» 北京市通商律师事务所 2021-12-09. URL: https://www.pkulaw.com/lawfirmarticles/97405809cbdf2d4d4314c2aa3f9696a9bdfb.html (дата обращения: 22.03.2022).

[45] См.: http://www.nhc.gov.cn/zwgk/jdjd/201311/6149be829d1448c5b3f9966e5fcefd7c.shtml (дата обращения: 22.03.2022).

[46] Понятие важных данных не имеет четкой дефиниции в законодательстве КНР. В соответствии с позицией Администрации киберпространства КНР к ним могут относиться, в частности, данные о сети зарядных станций для электрокаров, сведения о загруженности дорог общего пользования и типах транспорта на них, данные автомобильных видеорегистраторов. См.: http://www.gov.cn/xinwen/2021-05/12/content_5606075.htm (дата обращения: 22.03.2022).

[47] Континентальный Китай — территория Китайской Народной Республики, за исключением Гонконга и Макао. Также в нее не включается Тайвань.

стратегии безопасности киберпространства КНР, к ним относятся: организации транспорта, телекоммуникационного и информационного секторов, энергоснабжения, водоснабжения, здравоохранения, финансовые организации, почта и др.[48]

Закон о защите личной информации КНР в ст. 40 распространил данную обязанность не только на операторов КИИ, но и на операторов персональных данных, которые обрабатывают персональные данные в объеме, превышающем установленные Администрацией киберпространства КНР пределы. По состоянию на момент подготовки данной статьи соответствующие акты еще не были приняты.

### 5.2. Порядок трансграничной передачи персональных данных

Обязанность по локализации персональных данных неразрывно связана с ограничениями, предъявляемыми к трансграничной передаче данных. Не будет сильным преувеличением сказать, что в этой области Китай строит еще одну Великую китайскую стену посредством введения существенных ограничений на трансграничную передачу данных за пределы страны.

Глава 3 Закона о защите личной информации, посвященная порядку трансграничной передачи персональных данных, не содержит определения «трансграничной передачи информации». Содержание данного понятия можно вывести из Руководства по трансграничной передаче, подготовленном Национальным комитетом КНР по стандартизации[49]. В соответствии с ним к трансграничной передаче персональных данных относятся следующие ситуации:

— предоставление иностранным компаниям удаленного доступа к серверам, на которых хранятся персональные данные и которые расположены на территории КНР;

— передача китайским подразделением международной группы компаний данных, генерируемых во время внутренних операций в адрес иных организаций группы, находящихся за пределами КНР;

— физическая передача данных за пределы КНР, в частности на съемном носителе.

> Подобно требованиям *GDPR* и ФЗ «О персональных данных» для правомерности трансграничной передачи персональных данных необходимо наличие одного из нескольких условий из числа предусмотренных в законе. Однако характер этих условий качественно отличается от европейского и российского подхода.

Так, согласно ст. 38 Закона о защите личной информации, если экспортером данных выступает субъект КИИ либо же иной субъект, но объем таких экспортируемых данных превышает лимиты, установленные Администрацией киберпространства КНР, то главным основанием для законной передачи таких данных выступает предварительное проведение оценки рисков, связанных с трансграничной передачей, которая осуществляется с привлечением Администрации киберпространства КНР, если только законодательство КНР в явной форме не будет содержать исключений в отношении подобных ситуаций.

Во всех иных случаях, т.е. когда речь идет не об операторах КИИ и иных крупных операторах персональных данных, допускается использование следующих оснований для трансграничной передачи персональных данных:

— проведение сертификации предпринимаемых мер защиты персональных данных посредством специализированных учреждений в соответствии с правилами Администрации киберпространства КНР;

— заключение соглашения на стандартных условиях, разработанных Администрацией киберпространства КНР с получателем данных, регламентирующем права

[48] Национальная стратегия безопасности киберпространства, опубликована 27 декабря 2016 года Управлением киберпространства Китая / 国家网络空间安全战略, 2016年12月27日 · 国家互联网信息办公室发布. URL: http://www.cac.gov.cn/2016-12/27/c_1120195926.htm (дата обращения: 22.03.2022).

[49] Национальный план стандартов «Рекомендации по оценке безопасности исходящих данных, связанных с технологиями информационной безопасности». 01.09.2018 / 国家标准计划《信息安全技术 数据出境安全评估指南》01.09.2018. URL: http://std.samr.gov.cn/gb/search/gbDetailed?id=625516672A96BD9BE05397BE0A0A265C (дата обращения: 22.03.2022).

и обязанности сторон — участников трансграничной передачи[50].

Кроме того, международные договоры, законодательство КНР, административные правила или акты Администрации киберпространства КНР могут предусматривать и иные основания, легитимирующие трансграничную передачу персональных данных за пределы Китая.

Как видно, китайское регулирование трансграничной передачи данных характеризуется высокой степенью административного вмешательства в процессы согласования допустимости и условий такой передачи. Простора для какой-либо самодеятельности со стороны китайских операторов практически не оставлено. В китайском законодательстве не предусмотрено таких оснований, типичных для европейского регулирования, как необходимость трансграничной передачи для целей защиты жизненно важных интересов субъекта либо для целей исполнения договора.

> Согласие субъекта на трансграничную передачу персональных данных не является самодостаточным основанием, легитимирующим такую передачу, его получение является лишь одной из сопутствующих обязанностей оператора, одним из юридических фактов в сложном юридическом составе.

В ст. 39 Закона о защите личной информации отмечается, что оператор обязан уведомить гражданина о планируемой трансграничной передаче его данных с указанием получателя данных, его контактной информации, целей передачи, видов передаваемых данных и способов обработки, а также возможных способов защиты гражданином своих прав в отношении иностранного получателя данных. При этом гражданин должен дать на передачу трансграничных данных свое согласие, отдельное от всех других предоставляемых им согласий.

В ряде случаев, помимо наличия специального основания для трансграничной передачи из числа указанных в ст. 38 Закона о защите личной информации и необходимости получения согласия, оператор должен выполнить еще и третье условие — провести оценку рисков, связанных с трансграничной передачей персональных данных, порядок осуществления которой содержится в проекте Руководства по оценке безопасности трансграничной передачи данных[51]. В определенной степени данные требования перекликаются и черпают вдохновение из европейского законодательства и практики, возникшей после вынесения Европейским судом справедливости решения по делу *Schrems II*[52]. Данное решение обязало европейских операторов, осуществляющих трансграничную передачу данных в страны, которые не обеспечивают адекватный уровень защиты, осуществлять оценку рисков, связанных с такой передачей (*Transfer Impact Assessment, TIA*). В развитие данных положений были приняты соответствующие разъяснения *EDPB*[53]. Как видно, они не прошли мимо китайского законодателя, и эта концепция была взята им на вооружение. При этом в проекте Руководства по оценке безопасности трансграничной передачи данных обязанность осуществлять оценку рисков возлагается не только на субъектов критической инфраструктуры, но и на крупных операторов персональных данных: 1) если такой оператор обрабатывает персональные данные более 1 млн граждан Китая; 2) если передаваемый за пределы КНР массив данных содержит данные более чем 100 000 граждан Китая либо более 10 000 граждан — в отношении чувствительных видов данных.

В соответствии с Руководством перед подачей заявления в Администрацию киберпространства КНР оператор должен провести самостоятельную оценку рисков, принимая во внимание следующие критерии:

1) законность и степень необходимости трансграничной передачи данных, предполагаемый способ такой передачи;

[50] Такая типовая форма договора на момент подготовки данной статьи еще не была разработана.

[51] Национальный план стандартов «Рекомендации по оценке безопасности исходящих данных, связанных с технологиями информационной безопасности». 01.09.2018 / 国家标准计划《信息安全技术 数据出境安全评估指南》01.09.2018. URL: http://www.cac.gov.cn/2021-10/29/c_1637102874600858.htm (дата обращения: 22.03.2022).

[52] Data Protection Commissioner v. Facebook Ireland Limited and Maximillian Schrems. CJEU — C-311/18 — Schrems II, 16 July 2020.

[53] Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data. EDPB. Version 2.0. Adopted on 18 June 2021.

2) количество, объем и степень чувствительности передаваемых данных, а также риски передачи данных, которые могут принести ущерб национальной безопасности, общественным интересам, а также законным правам и интересам отдельных лиц или организаций;

3) можно ли предотвратить риски утечки или повреждения данных посредством принятия управленческих и технических мер оператором на стадии их передачи;

4) объем ответственности и содержание обязанностей стороны — импортера данных, а также оценка возможности защиты переданных данных техническими средствами уже после их получения стороной-импортером;

5) оценка рисков утечки, повреждения, фальсификации, злоупотреблений и т.д. в отношении данных после их передачи, наличие возможности субъектов персональных данных обратиться за защитой своих прав и интересов после передачи данных;

6) предусматривает ли заключенное соглашение с получателем данных обязанности получателя по принятию технических мер защиты персональных данных.

Существующие ограничения на трансграничную передачу данных имеют явно выраженную публично-правовую направленность[54], на что достаточно прозрачно намекает включение в Закон о защите личной информации положений о реторсиях и возможности блокировки иностранных ресурсов. Так, согласно ст. 42, возможно введение ограничительных мер вплоть до запрета обработки для иностранных физических и юридических лиц, осуществляющих обработку персональных данных граждан КНР с нарушениями, либо если такая обработка наносит ущерб национальной безопасности. В свою очередь, ст. 43 гласит: если какая-либо страна или регион устанавливают дискриминационные условия, ограничения или другие подобные меры в отношении КНР в области защиты персональной информации, КНР может принять ответные меры. Здесь достаточно показательной является история запрета *TikTok* на территории США.

Так, 6 августа 2020 года президент США Дональд Трамп издал указ, которым запретил скачивание данного приложения лицам, находящимся под юрисдикцией США. В указе особенно отмечается риск шпионажа за государственными служащими[55]. 18 сентября 2020 года Федеральная торговая комиссия США объявила запрет на распространение *TikTok* на территории США. Причиной введения данного запрета явилась угроза использования приложения для причинения ущерба национальной безопасности, внешней политике и экономике США[56]. По мнению правительства США, пользователи, используя *TikTok*, выражают согласие на получение доступа данным приложениям к камере и микрофону, а также на сбор таких данных, как местоположение, информация о контактах и т.д. Таким образом, у *TikTok* есть возможность получать большое количество данных об американских гражданах, что представляет из себя угрозу национальным интересам. А в связи с тем, что компания *ByteDance* имеет головной офис в КНР, у правительства КНР потенциально есть возможность получить доступ к собираемым ею данным[57].

[54] К слову сказать, не следует демонизировать Китай за использование ограничений на трансграничную передачу данных в качестве инструмента для геополитической борьбы. Еще во времена холодной войны аналогичные ограничения применялись западными странами в отношении СССР. Так что нормы о трансграничной передаче данных в силу своего существа пропитаны государственными интересами и геополитическими целями. См.: *Kuner C.* Transborder Data Flows and Data Privacy Law. Oxford University Press, 2013. P. 28. В России тоже вполне следуют этому тренду. В частности, в числе мер понуждения к исполнению законодательства РФ иностранными лицами, осуществляющими деятельность в Интернете на территории РФ, фигурирует «запрет на сбор и трансграничную передачу персональных данных» (п. 6 ст. 9 Федерального закона от 01.07.2021 № 236-ФЗ «О деятельности иностранных лиц в информационно-телекоммуникационной сети „Интернет“ на территории Российской Федерации»).

[55] Указ от 06.08.2020 № 13942 «Устранение угрозы, исходящей от *TikTok*, и принятие дополнительных мер по устранению чрезвычайной ситуации в стране в отношении цепочки поставок информационно-коммуникационных технологий и услуг». URL: https://www.federalregister.gov/documents/2020/08/11/2020-17699/addressing-the-threat-posed-by-tiktok-and-taking-additional-steps-to-address-the-national-emergency (дата обращения: 22.03.2022).

[56] Интернет-ресурс: Министерство торговли запрещает транзакции *WeChat* и *TikTok* для защиты национальной безопасности США. URL: https://2017-2021.commerce.gov/news/press-releases/2020/09/commerce-department-prohibits-wechat-and-tiktok-transactions-protect.html (дата обращения: 22.03.2022).

[57] Интернет-ресурс: «Глобальная информационная сеть», «Почему Соединенные Штаты запрещают Douyin» / 环球信息网, «美国为什么封禁抖音». URL: https://www.gpbctv.com/jrrd/202008/19315.html (дата обращения: 22.03.2022).

Очевидно, что подобные действия не могли не вызвать раздражения со стороны китайского правительства и найти свое отражение в соответствующих законодательных актах, на что достаточно прозрачно намекает интервью с одним из ключевых разработчиков Закона о защите личной информации — проф. Джоу Хуаньхуа[58]. Новые положения о трансграничной передаче персональных данных способны существенно осложнить жизнь немногих западных компаний, которые пока еще сохраняют свое присутствие, в частности компании *Apple*. Ряд других американских компаний уже объявили о своем уходе с китайского рынка, например *Yahoo*[59] и *LinkedIn*[60].

## 6. Ответственность за нарушение требований Закона о защите личных данных

В самом общем виде о серьезности намерений государства в отношении обеспечения принудительного исполнения вновь принятого закона можно судить из норм, посвященных санкциям за его нарушение. В свое время *GDPR* наделал много шума как в самой Европе, так и за ее пределами благодаря весьма высоким санкциям за нарушение его положений: до 20 млн евро или оборотный штраф в размере до 4% всемирной годовой выручки. Несколько лет потребовалось, чтобы этой логикой прониклись и в России, что повлекло установление достаточно высокой по российским меркам ответственности за нарушения требований локализации. Китайский законодатель решил не изобретать велосипед и заимствовал подход *GDPR*, разбавив его некоторой китайской спецификой.

Согласно ст. 66, если персональные данные обрабатываются с нарушением требований закона, соответствующее территориальное подразделение Администрации киберпространства КНР вправе:

1) выдать предписание об устранении нарушений;

2) выдать предписание о конфискации дохода, полученного в результате такой незаконной деятельности;

3) выдать предписание о приостановлении или прекращении работы сервиса или программного приложения.

Если предписание об устранении нарушения не выполнено, то может быть наложен штраф в размере до 1 000 000 юаней (около 140 000 евро или 12 000 000 руб.), а непосредственно ответственные физические лица могут быть оштрафованы на сумму от 10 000 до 100 000 юаней (1400–14 000 евро или 120 000–1 200 000 руб.).

В случае совершения серьезных нарушений законодательства о персональных данных соответствующее территориальное подразделение Администрации киберпространства КНР обязано выдать предписание об устранении нарушения, конфисковать полученный в результате него доход и наложить штраф в размере не более 50 млн юаней (около 7 000 000 евро или 600 000 000 руб.) или до 5% годового дохода. Кроме того, может быть выдано предписание о приостановке деятельности организации-оператора до устранения нарушения, а также инициирован отзыв лицензии такой организации при осуществлении ею лицензируемой деятельности. Достаточно серьезные санкции ждут в таких случаях и физическое лицо, ответственное за нарушение: штраф в размере от 100 000 до 1 млн юаней (14 000–140 000 евро или 1 200 000–12 000 000 руб.), а также может быть принято решение о запрете занимать в течение определенного периода должности директора, руководителя, менеджера высокого уровня или сотрудника по защите персональной информации. Венчает эти санкции и неизбежное опубличивание такого нарушения и отражение информации о нем в кредитной истории такого физического лица, что повлечет разрушительные последствия для его социального рейтинга (ст. 67 Закона о защите личной информации).

Что могло послужить причиной принятия столь жестких санкций за нарушение законодательства о персональных данных? Одна из возможных причин — реакция китайского правительства на проблемы утечек данных. В 2020 году утечка и незаконная продажа личной

[58] *Huang Y., Shi M.* Top Scholar Zhou Hanhua Illuminates 15+ Years of History Behind China's Personal Information Protection Law // Digichina, Stanford University. 8 June. 2021. URL: https://digichina.stanford.edu/work/top-scholar-zhou-hanhua-illuminates-15-years-of-history-behind-chinas-personal-information-protection-law/ (дата обращения: 22.03.2022).

[59] См.: https://www.bbc.com/news/technology-59136937 (дата обращения: 22.03.2022).

[60] См.: https://www.wired.com/story/linkedin-exit-china-cuts-east-west-bridge/ (дата обращения: 22.03.2022).

информации граждан Китая по-прежнему являлись достаточно серьезной проблемой. Исследование показало: в прошлом году произошло почти 100 000 случаев утечки личной информации. За весь год было обнаружено в общей сложности 203 инцидента с незаконной продажей личной информации, из которых незаконная продажа личной информации клиентов банков, организаций, занимающихся ценным бумагами, и отраслей, связанных со страхованием, составила относительно высокую долю — около 40% от общего числа незаконных транзакций с данными. 20% утечек было из платформ электронной коммерции, а 12% — из образовательных учреждений[61].

Как видно, данные санкции являются достаточно ощутимыми для крупных компаний (оборотные штрафы) и их должностных лиц. Одно нарушение способно сломать их карьеру на всю оставшуюся жизнь.

> Таким образом, Закон о защите личной информации создал достаточные финансовые стимулы и личные стимулы для операторов и их должностных лиц для принятия необходимых мер по соблюдению законодательства о персональных данных. Ведь эффективность законодательства напрямую зависит от того, насколько последствия неисполнения закона превышают по своей «стоимости» издержки по его исполнению.

В России в настоящее время ситуация прямо противоположная. Максимальный размер штрафа за наиболее типичные виды нарушений законодательства о персональных данных, которые в основном сосредоточены в ч. 1 и 2 ст. 13.11 КоАП РФ (обработка данных без законного основания или с нарушением обозначенной цели либо в отсутствие согласия субъекта), в отношении юрлиц составляет 150 000 руб. (12 500 юаней, или 1700 евро), а в отношении физлиц — 40 000 руб. (около 3300 юаней, или 460 евро). Комментарии, как говорится, излишни.

Еще одна особенность Закона о защите личных данных — наделение гражданина возможностью предъявить иск к оператору с требованиями о выплате компенсации за допущенное нарушение. Размер такой компенсации может определяться либо размером понесенных гражданином убытков, либо размером полученной оператором выгоды от такого нарушения, либо определяться судом в каждом конкретном случае в зависимости от «практических соображений» (ст. 69). При этом вина оператора презюмируется, и бремя доказывания ее отсутствия лежит именно на нем. Соответствующий иск может быть подан в интересах множества граждан как прокуратурой, так и организациями по защите прав потребителей. Тем самым понуждение к соблюдению законодательства о персональных данных будет идти не только по административной линии от Администрации киберпространства КНР, хотя она и предполагается основной, но и по горизонтальной линии — со стороны самих граждан и их объединений. В свое время Комиссия по правовому обеспечению цифровой экономики Московского отделения Ассоциации юристов России подготовила заключение о целесообразности внедрения эффективных частноправовых механизмов защиты прав субъектов персональных данных[62]. Примечательно, что в Китае в определенной степени предлагаемый подход нашел свое отражение.

## 7. Выводы

Китайский опыт показывает: жесткое регулирование порядка обработки персональных данных с высокими штрафами за нарушения вполне совместимо с развитием высоких технологий и искусственного интеллекта. Китай не следует упрощенному и в некоторой степени пропагандистскому подходу, при котором законодательство о персональных данных рассматривается как барьер, а единственным возможным вектором его модернизации в условиях, когда необходимо развивать технологии и конкурировать с остальным миром, является его либерализация, а в идеале — замена на различного рода специальные правовые режимы. Не является препятствием на пути строгого законодательства о персональных данных и значительная роль государства в жизни общества, сопровождающаяся

[61] «Отчет о безопасности сети Интернет в Китае за 2020 год», опубликован Национальным центром реагирования на чрезвычайные ситуации в Интернете, 21 июля 2021 года / 国家互联网应急中心发布的《2020年中国互联网网络安全报告》, 2021年7月21日. URL: https://www.cert.org.cn/publish/main/upload/File/2020%20Annual%20Report.pdf (дата обращения: 22.03.2022).

[62] См.: https://alrf.msk.ru/no_value_selected_733225488 (дата обращения: 22.03.2022).

слежкой и профайлингом граждан. Китай разделяет приватность «по горизонтали» — между частными лицами, между ними и организациями, а также приватность «по вертикали» — между частными лицами и государством. В отличие от западного подхода к идее прав человека, который предполагает их естественно-правовой характер и тем самым возможность их реализации для защиты от государства, в Китае права человека предоставляются самим государством и, следовательно, не могут быть использованы против него. Но это не мешает наделению граждан достаточно большими возможностями по отстаиванию своих прав на частную жизнь и персональные данные по отношению друг к другу и крупным компаниям.

> Таким образом, приватность «с китайской спецификой» представляет собой гибрид европейской модели защиты неприкосновенности частной жизни гражданина с американской моделью, в основе которой — защита прав потребителей, с сохранением за государством высокой степени контроля над обработкой данных граждан в публично-правовых и геополитических целях.

В перспективе это может стать вектором развития и российского законодательства. Правда, вряд ли РФ может позволить себе установить подобие еще одного «великого китайского файрволла» в отношении данных, который сейчас формируется благодаря новым нормам о трансграничной передаче данных в законодательстве КНР. Дело в том, что, как уже отмечалось ранее, полезность данных для обучения систем ИИ о 124 млн пользователей Интернета в России[63] не может конкурировать с полезностью данных о более 1 млрд пользователей Интернета в Китае, тем более принимая во внимание качественно иной уровень цифровизации повседневной жизни китайского гражданина и вытекающая из нее подробность наборов данных о нем. Поэтому установление «железного занавеса» в РФ в отношении данных вряд ли пойдет ей на пользу, в отличие от Китая, который в части наличия у него данных для обучения систем ИИ является вполне самодостаточным.

Еще один вывод, который напрашивается по результатам изучения нового китайского законодательства о персональных данных, заключается в том, что Россия вполне в обозримом будущем может признать Китай страной, которая обеспечивает адекватный уровень защиты персональных данных. Или, другими словами, у России просто нет убедительных доводов, кроме сугубо политических, отказывать Китаю в этом статусе после принятия Закона о защите личной информации. В самом деле, будет довольно странно выглядеть ситуация, при которой такие страны, как Мали, Чад, Бангладеш, Того, Замбия, Нигер и др., признаны Роскомнадзором в качестве стран, которые обеспечивают адекватный уровень защиты прав субъектов персональных данных[64], а стратегический партнер РФ, к тому же принявший законодательство в этой области, которое является по жесткости сопоставимым с европейским, — нет. Вряд ли Роскомнадзор будет, как европейские регуляторы, смущаться того факта, что регулятором в Китае по вопросам персональных данных является Администрация киберпространства КНР, чья компетенция куда более широкая, чем проблематика персональных данных, и сводится к регулированию информационного пространства в Интернете в целом. При этом данный орган находится под контролем Центрального комитета коммунистической партии Китая. Во-первых, сам Роскомнадзор в определенной степени находится в схожей позиции. Во-вторых, Администрация киберпространства КНР показывает весьма впечатляющие результаты своей деятельности. Так, согласно Отчету о развитии цифрового Китая в 2020 году, подготовленному Администрацией киберпространства КНР к концу 2020 года, было принято более 17 000 жалоб от интернет-пользователей, протестированы и оценены более 40 000 приложений, более 556 приложений, которые незаконно собирали и использовали личную информацию, были уведомлены об устранении нарушений[65]. Есть все основания пола-

[63] Число пользователей интернета в России достигло 124 млн // ТАСС. 2021. 19 окт. URL: https://tass.ru/obschestvo/12698757 (дата обращения: 22.03.2022).

[64] Приказ Роскомнадзора от 15.03.2013 № 274 (ред. от 14.09.2021) «Об утверждении перечня иностранных государств, не являющихся сторонами Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных и обеспечивающих адекватную защиту прав субъектов персональных данных».

[65] Отчет о развитии цифрового Китая за 2020 г. Подготовлен Администрацией киберпространства КНР 2 июля 2021 г. / 中国互联网信息办公室《数字中国发展报告（2020）》。发表于2021年07月02日. URL: http://www.cac.gov.cn/2021-06/28/c_1626464503226700.htm (дата обращения: 22.03.2022).

гать, что масштабы контрольно-надзорной деятельности китайского «Роскомнадзора» только увеличатся в будущем и тем самым составят еще один источник вдохновения для отечественной правоприменительной практики, наряду с европейским опытом.

## China's New Legislation on Personal Data: Privacy "With a Chinese Twist"

The paper is focused on the new Chinese law on protection of personal information. It starts with the description of the background of its adoption and interrelation with other Chinese legal acts on personal information protection. Then it describes the core provisions of the new law, which are of particular interest for Russian discussion on the ways of optimal regulation of personal data protection: the definition of personal data and its types (sensitive, biometric, depersonalized, publicly available), personal data localization provisions and restrictions on transborder transfer of personal data, as well as established liability for violation of its provisions. Analysis of these provisions is made taking into account the commentaries provided in Chinese academic literature and subordinate legal acts, which exist mostly in Chinese. For certain situations comparisons with Russian and European approach to regulation is provided.

***Keywords:*** *personal data, transborder transfer of personal data, privacy*

### INFORMATION ABOUT THE AUTHOR

**Alexander I. Savelyev**
Associate Professor of the Faculty of Law at the National Research University "Higher School of Economics", Legal Attorney of IBM Russia/CIS, Deputy Chairman of the Commission for Regulation of Digital Economy of Association of Lawyers of Russia (Moscow Branch), Member of the Advisory Board of the Russian Data Protection Authority, PhD in Law, LLM (Russian School of Private Law). (Email: alexandersavelyev83@gmail.com.)

**Maria A. Imanalieva**
Master's student of the program "Digital Law" of the National Research University "Higher School of Economics"; Peking University Law School, Chinese law LLM student (email: imanalievamaria@gmail.com).

### REFERENCES

Greenleaf, G. Asian Data Privacy Laws: Trade and Human Rights Perspectives. Oxford University Press. 2014. P. 80–203.

Huang, W. Interpretation of the Civil Code of the People's Republic of China (Part 2). Law Press, 2020 edition.

Kuner, C., Transborder Data Flows and Data Privacy Law. Oxford University Press. 2013. P. 28.

Lee, K. Artificial Intelligence Superpowers. Moscow, 2019. P. 136-137.

Liu, Q. Data Security: Regulating the Protection of Personal Information. Law Review. 2022 (1). URL: https://www.pkulaw.com/qikan/1ac48e59f7072063faad34f8ea0075ebbdfb.html?

Liu, S. Reasonable Treatment and the Criminal Mechanism of the Crime of Infringing on the Personal Information of Citizens. Southeastern University Human Rights Research Institute. 2021.

Molotnikov, A.E., Shan, V. Legal Foundations of Business in China [*Pravovye osnovy biznesa v Kitae*]. Moscow, 2018.

Pernot-Leplay, E. China's Approach on Data Privacy Law: A Third Way Between the U.S. and the E.U.? // The Penn State Journal of Law & International Affairs. 2020. No. 8.

Shi, C., "Legal Basis for Personal Information Processing in the Digital Economy Era". Journal of Chongqing University of Technology (Social Sciences), 2021 (9). URL: https://www.pkulaw.com/qikan/004a6de45afc6ea3f3361f693b4d771fbdfb.html.

Wang, X., Peng, C. Constitutional Foundations of the Personal Information Protection Legal System, 2021 CLI.A. 7118734. URL: https://www.pkulaw.com/specialtopic/8bb547fc13eb3f3391b0158c754eb7e5bdfb.html.

Xiang, D., Shen, J. "Research on Consent Requirement for the Commercial Use of Personal Information from the Perspective of Personal Information Typing". Northern Law Journal. 2017 (5).

Yang, C. Constitutional Interpretation and Practical Objectivity. Legal Methods. 2022. URL: http://www.pkulaw.cn/fulltext_form.aspx?Gid=1510270483.

Zhang, L. What is personal information? Based on the Discussion of the Intersection of Privacy Rights and Protection of Personal Information in the Civil Code. Journal of Gansu University of Political Science and Law. 2021. No. 1. URL: https://www.pkulaw.com/qikan/65ed2d6ddb3105b6330702b2938b7967bdfb.html?

Zhou, S. Constitutional Analysis About the Personal Data Right. Journal of Chongqing University (Social Science Edition). 2021 (1). P. 133–140.

Zou, D., Liu, Y. Public Personal Information Use Standards Study (Part 2), Beijing Tongshang Law Firm. 2021. December 12. URL: https://szlx.pkulaw.com/lawfirmarticles/97405809cbdf2d4d4314c2aa3f9696a9bdfb.html.

**АЛЕКСАНДР ОЛЕГОВИЧ АБЫШКО**

аспирант Департамента теории права и межотраслевых юридических дисциплин факультета права Национального исследовательского университета «Высшая школа экономики», практикующий юрист

# КОНЕЦ ОБЩЕДОСТУПНЫХ ПЕРСОНАЛЬНЫХ ДАННЫХ В РОССИИ? К ВОПРОСУ О ФЕДЕРАЛЬНОМ ЗАКОНЕ ОТ 30 ДЕКАБРЯ 2020 ГОДА № 519-ФЗ

Статья посвящена вопросам регулирования общедоступных персональных данных в контексте принятия Федерального закона от 30 декабря 2020 года № 519-ФЗ «О внесении изменений в Федеральный закон „О персональных данных“». По результатам анализа принятого Закона автор приходит к выводу о концептуальной правильности предпринятой законодателем попытки наделения субъектов персональных данных эффективным средством контроля за информацией о себе. Вместе с тем вводимый законом новый механизм получения согласия на распространение персональных данных, несмотря на явные преимущества в виде повышения уровня осведомленности субъекта об обработке его данных и возможности самостоятельного определения условий такой обработки, *de facto* труднореализуем, что требует поиска новых решений анализируемого вопроса.

***Ключевые слова:*** *информационное право, персональные данные, общедоступные данные, согласие на обработку персональных данных, GDPR*

DOI: 10.37239/0869-4400-2022-18-3-97-107

---

Всё, что вы делаете сейчас, фиксируется навсегда. Лучший план — постараться заполнить *Google* хорошими вещами о себе и вести себя так, как будто вас снимает скрытая камера — потому что так и есть.

*С. Годин*

## 1. Введение

В 2020 году в Конституции РФ появилась норма, предусматривающая отнесение к предметам ведения РФ обеспечение безопасности личности, общества

и государства при обороте цифровых данных (п. «м» ст. 71 Конституции). Паспорт федерального проекта «Нормативное регулирование цифровой среды»[1] предусматривает обеспечение благоприятных правовых условий для сбора, хранения и обработки данных с использованием новых технологий. Помимо указанного, Стратегия развития информационного общества в Российской Федерации на 2017–2030 годы[2] предусматривает необходимость «обеспечить баланс между своевременным внедрением современных технологий обработки данных и защитой прав граждан, включая право на личную и семейную тайну».

Несмотря на провозглашение столь амбициозных целей, наблюдается снижение позиций России в международных рейтингах, связанных с развитием цифровизации и цифровой трансформации. Так, в 2020 году снизилось с 32-го до 36-го место России в рейтинге электронного правительства ООН (*EGDI*)[3], в Глобальном инновационном индексе (*Global Innovation Index*) по показателю качества регулирования позиция России снизилась с 96-го места в 2018 году[4] до 105-го — в 2020 году[5].

Особую актуальность в этом контексте обретает проблематика общедоступных персональных данных. Потенциал их использования колоссален: такие данные могут использоваться для аналитики профилей в социальных сетях и повышения эффективности работы государственных органов, для повторного использования в экономике и создания новых продуктов. При чем же здесь цитата, приведенная в эпиграфе к данной публикации? Как обоснованно отмечает Е. Войниканис, тотальность данных о человеке, которые хранятся в Интернете, по сути, эквивалентна тотальной слежке и имеет много общего с «паноптикумом» И. Бентама[6] и, на наш взгляд, с мониторами, позволяющими полиции мыслей следить за жителями Океании в известной антиутопии Дж. Оруэлла.

> Несмотря на всё возрастающий объем обрабатываемых данных, до недавнего времени субъект персональных данных практически не имел средств обеспечения эффективного контроля за находящимися в открытом доступе собственными данными, что во многом связано с присущей обработке персональных данных информационной и экономической асимметрией между оператором и субъектом[7], частично нивелировать которую, как представляется, и должно законодательство о персональных данных.

Особая роль законодательства о персональных данных связана и с широтой охвата общественных отношений, подпадающих под его регулирование, — так, Н. Пуртова[8] метко назвала его законодательством всего *(law-of-everything)* в связи широким определением персональных данных, влекущим квалификацию значительной части информационных массивов в качестве персональных данных.

Обсуждаемая проблематика отнюдь не является отвлеченной от жизненных реалий, наоборот, она касается всех и каждого — ведь субъектами персональных данных являются и читатели, и автор этой статьи. Возможно ли оперативно удалить неактуальную или ложную информацию о себе из открытого доступа? Российский аналог европейского «права на забвение», как известно, распространяется лишь на операторов поисковых систем[9], что же делать с иными источниками, например сайтами с отзывами о профессиональной деятельности? С этой проблемой

---

[1] Паспорт федерального проекта «Нормативное регулирование цифровой среды» (утв. президиумом Правительственной комиссии по цифровому развитию, использованию информационных технологий для улучшения качества жизни и условий ведения предпринимательской деятельности, протокол от 28.05.2019 № 9).

[2] Указ Президента РФ от 09.05.2017 № 203.

[3] UN E-Government Surveys. URL: https://publicadministration.un.org/en/Research/UN-e-Government-Surveys (дата обращения: 21.03.2021).

[4] Global Innovation Index 2018. URL: https://www.globalinnovationindex.org/userfiles/file/reportpdf/gii_2018-report-new.pdf (дата обращения: 21.03.2022).

[5] Global Innovation Index 2020. URL: https://www.globalinnovationindex.org/userfiles/file/reportpdf/gii-full-report-2020.pdf (дата обращения: 21.03.2022).

[6] *Войниканис Е.А.* Право быть забытым: правовое регулирование и его теоретическое осмысление // Правоведение. 2016. № 3 (326). С. 86.

[7] См.: *Nissenbaum H.* Protecting Privacy in an Information Age: The Problem of Privacy in Public // Law and Philosophy. 1998. Vol. 17. No. 5/6. P. 559–596.

[8] *Purtova N.* The law of everything. Broad concept of personal data and future of EU data protection law // Law, Innovation and Technology. 2018. Vol. 10. Iss. 1. P. 41.

[9] См.: ст. 10.3 Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

столкнулась истец по делу *Prodoctorov.ru*, которая сочла недостоверными отзывы о низком качестве оказываемых ею медицинских услуг, опубликованные на специализированном сайте. Подробнее об этом деле будет рассказано далее.

Отечественный законодатель попытался разрешить вышеуказанную проблему — Федеральный закон от 30 декабря 2020 года № 519-ФЗ «О внесении изменений в Федеральный закон „О персональных данных“» (далее — Закон № 519-ФЗ) ввел в отечественное законодательство принципиально новую конструкцию «персональных данных, разрешенных субъектом персональных данных для распространения».

## 2. Российское регулирование общедоступных персональных данных до 1 марта 2021 года

До 1 марта 2021 года в Законе о персональных данных[10] существовало понятие персональных данных, сделанных общедоступными, — ими признавались те персональные данные, доступ неограниченного круга лиц к которым предоставлен непосредственно субъектом персональных данных либо по его просьбе, обработка таких персональных данных допускалась без согласия субъекта (п. 10 ч. 1 ст. 6 Закона о персональных данных).

От персональных данных, сделанных общедоступных субъектом, необходимо было отличать данные, внесенные в общедоступные источники, создаваемые в целях информационного обеспечения (ст. 8 Закона о персональных данных), включение в которые допускалось исключительно с письменного согласия субъекта персональных данных[11].

Анализ практики российских судов показал, что в целом в ходе разрешения споров применялся один из трех подходов к допустимости обработки таких персональных данных. Первый подход сводился к игнорированию причин, по которым персональные данные стали общедоступными. Так, по одному из дел[12] суд, констатировав наличие контактов лица в его личном «Живом журнале», признал их общедоступными и подлежащими дальнейшей обработке[13].

Второй подход характеризовался, помимо констатации того, что персональные данные находятся в открытом доступе, вниманием к другому значимому фактору — правомерности попадания данных в открытый доступ, в точном соответствии с действовавшей тогда нормой, которая дозволяла обработку персональных данных, сделанных общедоступными *субъектом персональных данных либо по его просьбе*[14].

Третий подход был в целом аналогичен второму, за исключением дополнительного анализа соответствия целей первоначального распространения данных с целями последующей обработки[15]. Так, по одному из дел была признана нарушением публикация на сайте администрации электронного обращения гражданина, включавшего его персональные данные, а доводы ответчика о том, что те же самые персональные данные были размещены ранее на странице истца в социальной сети, были признаны судом несостоятельными[16].

Нельзя не отметить и дела, выбивающиеся из общего ряда. Во-первых, следует указать дело НБКИ[17], посвященное обработке персональных данных в социальных сетях и иных открытых источниках, когда суд, как

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

[11] Законодатель четко разграничивал эти понятия, о чем свидетельствовал использованный в п. 3 ч. 4 ст. 18 Закона о персональных данных союз «или», указывавший на эти понятия как на различные сущности: «персональные данные сделаны общедоступными субъектом персональных данных или получены из общедоступного источника».

[12] Апелляционное определение Московского городского суда от 30.03.2012 по делу № 11-2145.

[13] См. также: определение Московского городского суда от 26.09.2016 № 4г-11364/2016; решения Василеостровского районного суда города Санкт-Петербурга от 30.06.2016 по делу № 2-2006/2016~М-1091/2016, Прикубанского районного суда города Краснодара от 15.01.2018 по делу № 2-1560/2017, Привокзального районного суда города Тулы от 28.07.2020 по делу № 2-997/2020.

[14] Апелляционное определение Новосибирского областного суда от 11.12.2018 по делу № 33-9348/2018; решения Амурского городского суда от 24.11.2014 по делу № 12-98/2014, Советского районного суда города Красноярска от 11.01.2017 по делу № 2-5587/2017(2-21965/2016) и др.

[15] См., напр.: апелляционное определение Нижегородского областного суда от 11.10.2016 по делу № 33-12355/2016; решение Арбитражного суда города Москвы от 19.12.2019 по делу № А40-183412/19-122-1521.

[16] Решение Амурского городского суда от 24.11.2014 по делу № 12-98/2014.

[17] Постановление Арбитражного суда Московского округа от 09.11.2017 № Ф05-16382/2017 по делу № А40-5250/2017.

представляется, смешал общедоступные источники персональных данных по смыслу ст. 8 Закона о персональных данных и общедоступные персональные данные по смыслу п. 10 ч. 1 ст. 6 Закона о персональных данных. Суд сделал несколько парадоксальный и не соответствовавший действовавшему тогда закону вывод: без письменного согласия субъекта не представляется возможным утверждать, что персональные данные предоставлены именно указанным субъектом, при этом данные, сделанные общедоступными субъектом, могут содержаться только в общедоступных источниках персональных данных[18].

Во-вторых, стоит указать дело сайта *Prodoctorov.ru*[19], которое, несмотря на определенную схожесть с третьим из вышеуказанных подходов[20], вызывает интерес тем, что в основу решений судами были положены не только положения Закона о персональных данных, но и гражданского законодательства (ст. 152.2 ГК РФ). Подобная специфика обусловлена тем, что в данном деле истец обратилась в суд с требованием обязать оператора удалить ее профиль, содержащий общедоступные отзывы третьих лиц о ее профессиональной деятельности. Указанные отзывы, по ее мнению, наносили вред ее профессиональной репутации и посягали на частную жизнь. Верховный Суд, направляя дело на новое рассмотрение, в числе прочего отметил, что в подобных случаях необходимо установление баланса между конкурирующими правами — защитой частной жизни и свободой слова, в результате чего профиль истца был с сайта удален.

> Указанная позиция видится небесспорной — в частности, отнесение информации о *качестве* профессиональной врачебной деятельности истца к сфере частной жизни представляется не вполне обоснованным[21].

Конституционный Суд РФ отмечал, что в понятие «частная жизнь» включается та область жизнедеятельности человека, которая относится к отдельному лицу, касается только его и не подлежит контролю со стороны общества и государства, если она носит не противоправный характер[22].

Представляется, что широкое толкование понятия «частная жизнь», данное судами по делу *Prodoctorov.ru*, могло потенциально создать почву для злоупотреблений, связанных с желанием отдельных лиц удалить из открытого доступа негативные сведения о собственной профессиональной деятельности[23]. Вместе с тем решение ВС РФ не стало финальным для указанного дела, свою позицию по данному вопросу высказал КС РФ, о чем пойдет речь далее.

Таким образом, российская судебная практика в сфере общедоступных персональных данных носила во многом разнонаправленный характер, что послужило одной из причин для изменения законодательства.

## 3. Российское регулирование общедоступных персональных данных после 1 марта 2021 года

Регулирование в данной сфере значительным образом изменилось после принятия Закона № 519-ФЗ. В пояснительной записке к законопроекту отмечалось, что действующее регулирование «позволяет третьим лицам осуществлять сбор и последующее неконтролируемое использование указанных персональных данных на интернет-сайтах в целях, отличных от цели их первоначального распространения, а равно с ориентиром на иные целевые аудитории»[24]. Указанное не вполне верно, так как, во-первых, сам Закон о персо-

[18] См.: решение Арбитражного суда города Москвы от 05.05.2017 по делу № А40-5250/17-144-51.

[19] Определение ВС РФ от 12.11.2019 по делу № 2-2794/18.

[20] Так, Верховный Суд подчеркнул, что при сборе данных о каком-либо человеке, обработке или использовании персональных данных или публикации соответствующих материалов *способом или в объеме, который выходит за рамки того, что обычно можно предвидеть*, могут возникнуть доводы о защите частной жизни.

[21] Некоторое недоумение вызывает позиция судов о том, что данные сведения затрагивают психологическую неприкосновенность личности, в том числе право жить уединенно, не привлекая к себе нежелательного внимания (см.: апелляционное определение Воронежского областного суда от 12.03.2020 по делу № 33-1212). Вопрос о совместимости вполне обоснованного желания непривлечения к себе внимания с занятием профессиональной деятельностью, носящий общественно значимый характер, суд оставил без ответа.

[22] Определение КС РФ от 09.06.2005 № 248-О.

[23] Апелляционное определение Воронежского областного суда от 12.03.2020 по делу № 33-1212.

[24] Пояснительная записка к проекту федерального закона «О внесении изменений в Федеральный закон „О персональных данных“ в части установления особенностей обработки общедоступных персональных данных». URL: https://sozd.duma.gov.ru/bill/1057337-7 (дата обращения: 21.03.2022).

нальных данных содержит принцип недопустимости обработки персональных данных, несовместимой с целями сбора (ч. 2 ст. 5); во-вторых, из вышеприведенного анализа судебной практики следует, что она была разнородной.

Так или иначе, большая часть положений Закона № 519-ФЗ, не имеющего обратной силы, вступила в силу с 1 марта 2021 года. Законом закрепляется необходимость получения отдельного согласия на распространение персональных данных. Требования к указанному согласию установлены Роскомнадзором[25].

> Как указывали представители Роскомнадзора[26], согласие в новой форме необходимо будет получать исключительно для данных, которые будут распространяться после вступления Закона № 519-ФЗ в силу. Нельзя не отметить возможные практические трудности по применению новых требований — судя по всему, чтобы определить, когда персональные данные, разрешенные к распространению, были размещены в Интернете, Роскомнадзору необходимо будет рассматривать каждый частный случай в отдельности, запрашивая соответствующую информацию от операторов.

Из статей Закона о персональных данных было исключено понятие «общедоступные персональные данные». Так, теперь отсутствует такое правовое основание, как «обработка данных, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных либо по его просьбе» (п. 10 ч. 1 ст. 6 Закона о персональных данных). При этом сохранена ст. 8 Закона о персональных данных, посвященная общедоступным источникам персональных данных. Как и прежде, данная норма покрывает исключительно те ресурсы, которые создаются в целях информационного обеспечения (такие, как справочники и адресные книги), и не применима к разрешенным к распространению персональным данным, размещенным на иных ресурсах. В то же время с учетом разной правоприменительной практики (см. вышеприведенное дело НБКИ) и принятия Закона № 519-ФЗ, представляется необходимым заменить термин «общедоступный источник персональных данных» на «справочный источник персональных данных» как более адекватно отражающий суть указанного явления. Такое изменение терминологии поможет избежать необоснованного приравнивания всех источников, в которых содержатся персональные данные, разрешенные субъектом персональных данных для распространения, к «общедоступным источникам персональных данных» в смысле, придаваемом этому термину статьей 8 Закона о персональных данных.

В условиях сокращения доступных операторам оснований обработки персональных данных, находящихся в открытом доступе, не исключена «реанимация» относительно редко применяемого основания, а именно обработки в статистических или иных исследовательских целях (при условии обязательного обезличивания)[27], в связи с принятием в первом чтении законопроекта[28], уточняющего полномочия Роскомнадзора по утверждению требований и методов обезличивания персональных данных. Редкая применимость данного основания объясняется сложившимся рестриктивным подходом Роскомнадзора, поддерживаемого судами[29], который не позволяет применять по аналогии требования к обезличиванию персональных данных, утвержденные для государственных и муниципальных органов[30], к деятельности иных организаций, в частности коммерческих.

> Последовательная применимость данного подхода может *de facto* привести к выводу об общем запрете обезличивания персональных данных для операторов, не являющихся государственными и муниципальными органами.

[25] Приказ Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 24.02.2021 № 18 «Об утверждении требований к содержанию согласия на обработку персональных данных, разрешенных субъектом персональных данных для распространения»

[26] В рамках, в частности, сессии ответов на вопросы, которая прошла 28.01.2021 на дне открытых дверей Роскомнадзора, приуроченному к Международному дню защиты персональных данных.

[27] См.: п. 9 ч. 1 ст. 6 Закона о персональных данных.

[28] Законопроект № 992331-7 «О внесении изменений в Федеральный закон „О персональных данных“». URL: https://sozd.duma.gov.ru/bill/992331-7 (дата обращения: 21.03.2022).

[29] Решение Арбитражного суда города Москвы от 25.05.2016 по делу № А40-51869/2016.

[30] Приказ Роскомнадзора от 05.09.2013 № 996 «Об утверждении требований и методов по обезличиванию персональных данных».

Наиболее интересны в Законе № 519-ФЗ новеллы о том, что в согласии на распространение субъект персональных данных может определить перечень данных по каждой из категорий (так называемые общие[31], биометрические, специальные), а также установить условия и запреты для обработки данных как оператором, так и неопределенным кругом лиц, при этом указанные поля заполняются по желанию самого субъекта (п. 7, 8 приказа Роскомнадзора от 24 февраля 2021 года № 18). Эти требования являются несомненным вызовом для операторов персональных данных — думается, что предоставление субъекту возможности свободно (путем заполнения соответствующей графы) устанавливать условия и запреты обработки приведет к тому, что практически любое установление таковых повлечет их фактическую неисполнимость. Представим: субъект персональных данных указал, что его данные распространяются при условии выплаты ему ста долларов каждым оператором, или в том случае, если представитель оператора споет субъекту персональных данных его любимую песню. Закон не ограничивает субъекта в этой части — в связи с чем очевидно: оператор будет вынужден воздержаться от распространения персональных данных, что может нарушить права самого же субъекта. Оптимальным решением с точки зрения баланса интересов операторов и субъектов персональных данных видится предоставление субъекту возможности выбора между несколькими (не менее двух) закрытыми полями, согласие с которыми может быть подтверждено, в частности, путем проставления «галочки».

Ситуацию усугубляет и то, что закон устанавливает обязанность оператора в срок не позднее трех рабочих дней с момента получения соответствующего согласия субъекта персональных данных опубликовать информацию о наличии запретов и условий на обработку неограниченным кругом лиц персональных данных, разрешенных субъектом для распространения (ч. 10 ст. 10.1 Закона о персональных данных).

Толкование этой нормы вызывает еще большие затруднения. Потенциально существует как минимум три возможных варианта исполнения данного требования: условия и запреты будут изложены под распространенными персональными данными каждого субъекта, либо они будут изложены в политике конфиденциальности. Наконец, оператор персональных данных может создать общедоступный реестр, в котором каждый желающий сможет ознакомиться с условиями и запретами обработки персональных данных конкретного субъекта. Первый вариант толкования может привести к фактической неисполнимости указанных положений для хоть сколько-либо значительных объемов распространяемых персональных данных — администрирование «индивидуализированных» согласий повлечет несоразмерные издержки операторов, вынужденных создавать специальную систему публикации условий обработки либо отслеживать таковые вручную. Полагаем, что наличие в политике конфиденциальности соответствующего ресурса общих указаний на возможные варианты условий и запретов, которые могут быть выбраны субъектами персональных данных в согласиях, вполне достаточно для исполнения данной нормы.

Характерно, что право субъекта персональных данных на установление определенных запретов и условий обработки не применяется в случае обработки в государственных, общественных и иных публичных интересах[32], что корреспондирует положениям абз. 2 п. 1 ст. 152.2 ГК РФ[33]. При этом, как справедливо отмечает А.И. Савельев, данная формулировка говорит лишь о неприменимости запретов и условий обработки, но не всех остальных норм ст. 10.1 Закона о персональных данных[34]. Исходя из этого, субъект персональных данных вполне может отозвать свое согласие и при наличии публичного интереса в распространении его данных, что вынудит суды и Роскомнадзор действовать *contra legem*, блокируя применение данной нормы для подобных случаев.

[31] В терминологии проекта приказа Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 24.02.2021 № 18 «Об утверждении требований к содержанию согласия на обработку персональных данных, разрешенных субъектом персональных данных для распространения». Данный термин, однако, не вошел в окончательную редакцию приказа.

[32] См.: ч. 11 1 ст. 10.1 Закона о персональных данных.

[33] Схожие положения закреплены, в частности, в п. 5 ч. 1 ст. 49 Закона Российской Федерации от 27.12.1991 № 2124-1 «О средствах массовой информации», устанавливающем общественный интерес в качестве основания для распространения журналистом информации о гражданине без получения специального согласия.

[34] *Савельев А.И.* Научно-практический постатейный комментарий к Федеральному закону «О персональных данных». М., 2021. С. 244.

> В то же время при применении Закона № 519-ФЗ следует иметь в виду, что сфера его действия ограничена исключительно *первичным распространением* персональных данных в отсутствие иных правовых оснований. Закон о персональных данных содержит иные основания для обработки (в частности, распространения) персональных данных (ч. 1 ст. 6 Закона о персональных данных).

Таким образом, например, распространение, а также *вторичная* (последующая) обработка персональных данных при осуществлении журналистской деятельности (п. 8 ч. 1 ст. 10 Закона о персональных данных) не требует получения согласия по смыслу Закона № 519-ФЗ. Не требует получения указанного согласия и осуществление оператором своих прав и законных интересов (п. 7 ч. 1 ст. 6 Закона о персональных данных), в частности доведение до всеобщего сведения объекта интеллектуальных прав, неотъемлемой частью которого являются персональные данные (например, исполнение музыкального произведения с указанием имени исполнителя).

Данная позиция находит свое подтверждение в принятом уже после вступления в силу Закона № 519-ФЗ Постановлении КС РФ от 25 мая 2021 года № 22-П, поставившем точку в деле *Prodoctorov.ru*. При анализе правоотношений по распространению персональных данных Суд сослался на п. 7, 8 ч. 1 ст. 6 Закона о персональных данных, тем самым указав на то, что норма о необходимости получения специального согласия на распространение должна толковаться ограничительно и применяться лишь в случае отсутствия иных правовых оснований. Характерно, что при пересмотре данного дела по новым обстоятельствам суды уже не ссылались на распространение информации о частной жизни истца, обоснованно обращая внимание на то, что имя, фамилия, уровень образования и квалификации медицинского работника не относятся к сведениям о его частной жизни[35].

Следует учитывать и то, что распространением персональных данных является их раскрытие неопределенному кругу лиц, в этой связи в случаях, когда доступ к данным получает определенный или определимый круг лиц, Закон № 519-ФЗ применяться также не будет — например, если размещенные данные будут доступны только зарегистрированным пользователям определенного ресурса[36].

Исходя из указанного, единственный случай, когда оператору необходимо получать согласие на распространение персональных данных по смыслу Закона № 519-ФЗ, — первичное распространение в отсутствие иных правовых оснований.

Законом № 519-ФЗ также регламентирован порядок прекращения обработки персональных данных, разрешенных для распространения. Субъект вправе направить требование о прекращении обработки *разрешенных к распространению* персональных данных оператору, последний в течение трех рабочих дней обязан прекратить их обработку.

> Данную норму следует оценить в целом позитивно, как предоставляющую субъекту персональных данных механизм оперативного контроля над собственными данными. В то же время необходимо подчеркнуть, что сфера ее действия ограничена персональными данными, разрешенными к распространению по смыслу Закона № 519-ФЗ Таким образом, при наличии иных правовых оснований оператор имеет право продолжать распространение данных. Иное толкование может привести к созданию *de facto* инструмента цензуры, когда не желающее распространения определенной информации лицо будет со ссылкой на данную норму требовать удаления информации о себе из всех возможных открытых источников.

Также следует принимать во внимание возможность обращения субъектов персональных данных к российскому аналогу «права на забвение», закрепленному

[35] Апелляционное определение Воронежского областного суда от 05.08.2021 по делу № 33-4431/2021.

[36] Следует иметь в виду, что в контексте действия рекламного законодательства судами высказывалась иная позиция, которая потенциально может быть применена к правоотношениям по распространению персональных данных. Так, в постановлении ФАС Московского округа от 28.04.2010 № КА-А40/3772-10 по делу № А40-136851/09-2-871 суд отметил, что распространение информации на сайте в Интернете является рекламой, поскольку она направлена неопределенному кругу лиц, в информации отсутствует четко определенный круг лиц, она может быть доступна любому лицу, несмотря на регистрационный порядок доступа к сайту.

в ст. 10.3 Федерального закона от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации». Представляется, что если оператор персональных данных будет распространять персональные данные субъекта в отсутствие правовых оснований, то субъект в рамках процедуры, предусмотренной в обозначенной норме, может обратиться к оператору поисковой системы в целях удаления из результатов поисковой выдачи своих персональных данных (т.е. информации, распространяемой в нарушение законодательства РФ).

## 4. Европейский подход

Для надлежащей оценки Закона № 519-ФЗ представляется необходимым обратиться к европейскому опыту регулирования данной сферы[37].

Ключевым актом, регулирующим персональные данные на уровне ЕС, является Регламент Европейского парламента и Совета Европейского союза от 27 апреля 2016 года 2016/679 о защите физических лиц при обработке персональных данных и о свободном обращении таких данных, а также об отмене Директивы 95/46/ЕС (далее — *GDPR*). В *GDPR* отсутствует дефиниция общедоступных данных, при этом обработка общедоступных персональных данных, как и любых иных, запрещена без наличия правового основания (ст. 6 *GDPR*)[38]. *GDPR*, в отличие от российского Закона о персональных данных, не требует получения особого согласия на распространение персональных данных — оно должно соответствовать общим требованиям, предъявляемым к согласиям (ст. 7 *GDPR*).

В то же время положения *GDPR* содержат ряд норм, непосредственно регулирующих отношения по обработке общедоступных данных. Так, *GDPR* указывает на необходимость предоставления субъекту персональных данных информации об источнике обрабатываемых персональных данных, в том числе полученных из общедоступных источников (ст. 14 (2)*(f)*). Отдельно *GDPR* предусматривает допустимость обработки специальных категорий персональных данных, явным образом сделанных общедоступными *(manifestly made public)* субъектом персональных данных.

> *ICO*, британский уполномоченный орган по защите персональных данных[39], указывает по этому поводу, что термин «явным образом сделанный общедоступным» не определен *GDPR*, но очевидно предполагает целенаправленный поступок человека, при этом для легитимации обработки недостаточно того, что данные уже находились в открытом доступе, сам субъект персональных данных должен предпринять шаги по приданию общедоступности собственным данным.

В свою очередь, обработка персональных данных, явным образом сделанных общедоступными, должна осуществляться с учетом общих принципов и правил обработки, в частности *purpose limitation*[40].

*GDPR* известен разграничением двух особых категорий данных, а именно псевдонимизированных *(pseudonymised)* персональных данных, которые могут быть отнесены к определенному лицу с использованием дополнительной информации, при условии, что эта информация хранится отдельно и с соблюдением технических и организационных мер, гарантирующих, что персональные данные не будут отнесены к такому

[37] Учитывая общие корни регулирования, вытекающие из Конвенции о защите физических лиц при автоматизированной обработке персональных данных (*Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*, известная как *Convention 108*). Важность данного акта в качестве основополагающего для всей европейской парадигмы регулирования персональных данных неоднократно отмечалась в литературе в числе прочего применительно к действию прав и свобод человека и гражданина в контексте применения Конвенции о защите прав человека и основных свобод 1950 г. (см., напр.: *Ефремов А.А.* Новые информационные технологии в практике Европейского суда по правам человека // Прецеденты Европейского суда по правам человека. 2016. № 6. С. 10–15).

[38] В качестве основания обработки общедоступных персональных данных может выступать, в частности, законный интерес оператора (ст. 6 (1)*(f) GDPR*).

[39] What are the conditions for processing? // Information Commissioner's Office. URL: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/special-category-data/what-are-the-conditions-for-processing/ (дата обращения: 21.03.2022).

[40] См., в частности: *Recital 47 GDPR*, где отмечено, что в том случае, когда субъекты персональных данных обоснованно не ожидают вторичной обработки, т.е. обработки для цели, отличной от той, для которой данные были первоначально собраны, законные интересы субъектов персональных данных могут быть признаны превалирующими над законным интересом оператора.

лицу, и анонимизированных *(anonymised)* данных, которые персональными не являются.

Применительно к общедоступным данным это разграничение важно в контексте того, что псевдонимизация выступает одним из критериев допустимости последующей (вторичной) обработки персональных данных в целях, отличающихся от тех, для которых изначально осуществлялся их сбор (ст. 6(4) *GDPR*).

Такая последующая (вторичная) обработка персональных данных в указанном случае допускается, но цели такой обработки должны быть совместимы *(compatible)* с первоначально заявленными[41]. При проведении анализа совместимости целей во внимание могут быть приняты следующие обстоятельства:

– связь между целями, для которых были собраны данные, и целями вторичной обработки;

– контекст первоначального сбора персональных данных и разумные ожидания субъекта относительно их дальнейшего использования;

– природа данных и влияние дальнейшей обработки на субъектов;

– характер средств защиты, применяемых оператором для обеспечения справедливой обработки и предотвращения любого ненадлежащего воздействия на субъектов.

Таким образом, принцип *purpose limitation* устанавливает общий запрет обработки общедоступных данных в целях, несовместимых с первоначально закрепленными или подразумеваемыми. В этой связи лицу, желающему обрабатывать общедоступные персональные данные на основании, например, законного интереса (ст. 6 (1)*(f) GDPR*), надлежит провести тщательный анализ изначальных и предполагаемых целей обработки.

Следует также отметить наличие в *GDPR* «права быть забытым» *(right to be forgotten)*, закрепленного в ст. 17 данного акта. Так, субъект персональных данных вправе требовать от оператора удаления относящихся к нему персональных данных, осуществляемого без неоправданной задержки, в частности, в случае, если персональные данные субъекта более не являются необходимыми применительно к целям, для которых они были собраны. «Право быть забытым» было закреплено в *GDPR* под влиянием практики Европейского суда справедливости. Так, в деле «*Google* против Марио Костехи Гонсалеса»[42] гражданин Испании обратился к Национальному агентству по защите данных с требованием удалить электронную версию статьи 1998 года о продаже его дома на аукционе в счет уплаты уже погашенного им долга. Суд отказал гражданину в удалении статьи в силу законности ее публикации, вместе с тем обязав *Google Spain* удалить ссылки на данную статью из поисковой выдачи[43].

Таким образом, европейское право по большей части регулирует общедоступные персональные данные с помощью набора общих норм и принципов законодательства о персональных данных и не содержит аналогов новелл из Закона № 519-ФЗ.

## 5. Выводы

До принятия Закона № 519-ФЗ российская практика в сфере общедоступных персональных данных носила в значительной степени разнонаправленный характер, что выступило одним из поводов для вмешательства законодателя. Закон также был направлен на решение проблемы асимметрии между оператором и субъектом персональных данных с помощью предоставления последнему механизма контроля над собственными данными.

Законодательство о персональных данных, как справедливо отмечается в доктрине, призвано дать субъекту — в той степени, в которой это возможно —

[41] Opinion 03/2013 on purpose limitation // Article 29 Data Protection Working Party, 2013. URL: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf (дата обращения: 21.03.2022).

[42] Judgment of the Court (Grand Chamber) of 13 May 2014 (request for a preliminary ruling from the Audiencia Naciona, Spain, Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González (Case No. C-131/12).

[43] См. подробнее: *Войниканис Е.А.* Право быть забытым: правовое регулирование и его теоретическое осмысление // Правоведение. 2016. № 3 (326). С. 70–89.

контроль над обработкой собственных персональных данных[44]. Это обусловлено естественной связью между субъектом и данными о нем, ведь по существу личность в социальном плане может быть рассмотрена как совокупность данных о ней. Обозначенная очевидная асимметрия в отношениях между субъектом персональных данных и многочисленными операторами приводит к необходимости защиты слабой стороны правоотношений с помощью правовых механизмов законодательства о персональных данных.

Вместе с тем очевидно, что конкретный набор механизмов контроля за данными о себе, которыми должен быть наделен субъект персональных данных, зависит от степени связи между субъектом и данными о нем, а также вероятности нарушения его прав и свобод в результате обработки таких данных. Именно поэтому, например, для обработки обезличенных (псевдонимизированных) данных существуют определенные послабления, тогда как специальные категории персональных данных, представляющие собой чувствительные сведения о субъекте, обрабатываются по особым, более ограничительным для операторов правилам.

В этой связи логика Закона № 519-ФЗ, устанавливающего специальные правила для первичного распространения персональных данных, вполне обоснованна — учитывая то, что в таком случае данные о субъекте становятся доступными, в определенном смысле, *urbi et orbi*, повышение стандарта легитимации обработки и введение специальной формы согласия видится разумным. Аналогично следует оценить и возможность оперативно отозвать такое согласие.

В то же время наличие изначальных благих целей не всегда приводит к эффективности регулирования. В «Морали права» Л. Фуллер, приводя притчу о неудачной законодательной деятельности одного монарха, преисполненного самых лучших намерений, в числе причин провала реформ приводит неспособность правителя сделать законы ясными и понятными[45].

> Притча имеет прямое отношение к обсуждаемой теме: анализ положений Закона № 519-ФЗ, значительно осложняющийся многочисленными огрехами юридической техники, приводит к неутешительным выводам — ключевые нормы акта носят во многом внутренне противоречивый или трудноисполнимый характер. По справедливому замечанию А.И. Савельева, новеллы Закона № 519-ФЗ плохо вписываются в текущую терминологию и структуру Закона о персональных данных, и еще хуже — в реалии функционирования Интернета[46].

Так, возможность для субъекта персональных данных установить условия и запреты для обработки персональных данных как оператором, так и неопределенным кругом лиц, в большинстве случаев носит крайне труднореализуемый характер в связи с несоразмерными административными издержками операторов персональных данных по его исполнению.

Возможно, острота проблематики будет несколько снижена за счет использования специальной информационной системы Роскомнадзора, предназначенной для получения согласий[47].

Красноречиво отношение к Закону № 519-ФЗ и регулятора — несмотря на то, что основные положения акта вступили в силу с 1 марта 2021 года, приказ Роскомнадзора, устанавливающий требования к согласию на распространение, вступил в силу только 1 сентября 2021 года. Таким образом, до 1 сентября 2021 года в отсутствие вступивших в силу требований к согласию распространение персональных данных оказывалось в «серой» зоне, наряду с обезличиванием, осуществляемым негосударственными организациями.

Более сбалансированным представляется европейский подход, в рамках которого отношения по обработке общедоступных персональных данных

[44] *Tzanou M.* Data Protection as a Fundamental Right Next to Privacy? ‘Reconstructing’ a Not so New Right // International Data Privacy Law. Vol. 3. No. 2. P. 88–99.

[45] *Фуллер Л.* Мораль права. М., 2007. С. 53.

[46] *Савельев А.И.* Научно-практический постатейный комментарий к Федеральному закону «О персональных данных». М., 2021. С. 231.

[47] Приказ Роскомнадзора от 21.06.2021 № 106 «Об утверждении Правил использования информационной системы Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций, в том числе порядка взаимодействия субъекта персональных данных с оператором».

регулируются по большей части посредством общих норм и принципов. При этом интересы субъектов персональных данных и операторов балансируются предъявлением гибких требований к согласию на обработку персональных данных, последовательным применением принципа *purpose limitation*, а также наличием установленных в законе обстоятельств, которые в обязательном порядке должны быть приняты во внимание оператором, обрабатывающим персональные данные за пределами целей их первоначального сбора (ст. 6 (4) *GDPR*).

Вместе с тем очевидная неудачность формулировок Закона № 519-ФЗ не свидетельствует о некорректности законодательного подхода, направленного на предоставление субъектам персональных данных новых механизмов защиты своих прав. Напротив, законодательные меры, имеющие своей целью внесение большего баланса в основанные на асимметрии отношения между субъектами и операторами персональных данных, надлежит только приветствовать.

## End of Publicly Available Personal Data in Russia? To the Issue of Federal Law No. 519-FZ

This paper discusses the regulation of publicly available personal data in the context of the adoption of the Federal Law dated December 30, 2020 No. 519-FZ “On Amending the Federal Law ‘On Personal Data’”. Based on the results of the analysis of the adopted law, the author comes to the conclusion about the conceptual correctness of the attempt made by the Russian legislator to endow personal data subjects with an effective mechanism for controlling information about themselves. However, the newly implemented tool for obtaining consent for the dissemination of personal data, despite its obvious advantages reflected in increased awareness of the data subject about the processing of personal data and the ability to determine the terms of such processing face difficulties with its de facto execution, which requires the search for new solutions to this issue.

***Keywords:*** *informational law, personal data, publicly available personal data, consent to process personal data, GDPR*

### INFORMATION ABOUT THE AUTHOR

**Alexander O. Abyshko**
PhD student of the Department of Theory of Law and Intersectoral Legal Disciplines of the Faculty of Law at National Research University Higher School of Economics (e-mail: alexander.abyshko@gmail.com).

### REFERENCES

Fuller, L. The Moral of the Law. M., 2007. 308 p.

Globocnik, J. The Right to Be Forgotten is Taking Shape: CJEU Judgments in GC and Others (C-136/17) and Google v CNIL (C-507/17) in: GRUR International. 2020. Vol. 69 (4). P. 380–388.

Nissenbaum, H. Protecting Privacy in an Information Age: The Problem of Privacy in Public. Law and Philosophy 17. 1998. No. 5/6. P. 559–596.

Purtova, N. The Law of Everything. Broad Concept of Personal Data and Future of EU Data Protection Law. Law, Innovation and Technology. 2018. Vol. 10. Iss. 1. P. 40–81.

Saveliev, A.I. Scientific and Practical Article-by-Article Commentary on the Federal Law “On Personal Data” [*Nauchno-prakticheskij postatejnyj kommentarij k Federal’nomu zakonu “O personal’nyh dannyh”*]. M., 2021.

Tzanou, M. Data Protection as a Fundamental Right Next to Privacy? “Reconstructing” a Not so New Right. International Data Privacy Law. Vol. 3. No. 2. P. 88–99.

Voinikanis, E.A. The Right to Be Forgotten: Legal Regulation and Its Theoretical Understanding [*Pravo byt’ zabytym: pravovoe regulirovanie i ego teoreticheskoe osmyslenie*]. Jurisprudence [*Pravovedenie*]. 2016. No. 3 (326). P. 70–89.

**ЕВГЕНИЙ ИОСИФОВИЧ ДИСКИН**

эксперт Международного центра конкурентного права и политики БРИКС Национального исследовательского университета «Высшая школа экономики», кандидат юридических наук

# ФЕЙКОВЫЕ НОВОСТИ КАК ПОЛИТИКО-ПРАВОВОЙ ФЕНОМЕН

В статье исследуется понятие фейковых новостей как одного из феноменов цифровой трансформации в его юридическом и правовом измерениях. Автор исследует генезис феномена фейковых новостей, стремительный переход от использования данного термина в политической борьбе к юридическому закреплению и применению, несмотря на достаточно размытые критерии того, что можно считать фейком. В статье дается ответ на вопрос: является ли феномен фейковых новостей главным негативным эффектом свободы в сетевом пространстве или действующие политические силы, определяющие направления развития стран Запада, используют данный термин, создают юридические конструкции, направленные на защиту от фейковых новостей, для недобросовестной политической борьбы? Также в статье исследуется вопрос об адекватности термина «фейковые новости» для целей регулирования социальных сетей и Интернета как пространства распространения информации; даются предложения по его замене и освещаются риски, связанные со следованием текущим тенденциям, которые сложились в организации противодействия фейковым новостям.

***Ключевые слова:*** *фейковые новости, дезинформация, законодательство об обороте информации, цензура, цифровые права, социальные сети, уголовное право, конституционное право*

DOI: 10.37239/0869-4400-2022-18-3-108-120

## 1. Введение

Ранним утром 27 января 2021 года сотрудниками ФБР в маленьком курортном городке Палм Бич, штат Флорида, был арестован некто Дуглас Мэкки. В тот же день он предстал перед судом. Не столь примечательна личность этого человека, сколько примечательно то, за что он был арестован. А арестован он был

за мем, размещенный им в социальной сети *Twitter* в 2016 году (т.е. за 5 лет до ареста) в период президентских выборов, который власти США считают не только содержащим фейковую информацию, но и свидетельством наличия «заговора с целью повлиять на итоги выборов»[1]. Примечательно, что сама статья, на основании которой Мэкки предъявлены обвинения, дает суду право приговорить обвиняемого к тюремному заключению сроком до 10 лет лишения свободы[2]. Важно отметить, что и сам выбор статьи для предъявления обвинения, а также срок, который понадобился правоохранительным органам, чтобы определить подозреваемого (а это не представляло труда, ведь он жил в очень маленьком городке и зарегистрировался в социальной сети с помощью реального номера мобильного телефона), показывают экстраординарность этого случая.

Указанный пример ставит перед юристами любого государства, где соцсети оказывают значительное влияние на общественную жизнь, очень важные вопросы, которые надлежит решить в целях дальнейшего развития правового регулирования Интернета и социальных сетей: что такое фейковые новости, как и почему возник данный феномен, несут ли они общественную опасность или есть основания подвергать это сомнению?

Словосочетание «фейковые новости» (англ. *fake news*) относительно недавно вошло в русский язык, но упоминается в сетевом диалоге очень часто. Так, поисковая система *Google* говорит о 685 тыс. упоминаний русской транскрипции этого слова; англоязычная версия сайта утверждает, что в Интернете доступно 1 млрд 180 млн упоминаний данного слова.

Толковые словари русского языка на настоящий момент не содержат нормативного значения данного словосочетания. В этой связи целесообразно обратиться к языку оригинала. Кембриджский толковый словарь дает два значения слова «фейк» (англ. *fake*): 1) предмет, который создан таким образом, чтобы казаться настоящим или ценным для того, чтобы обманывать людей; 2) кто-то, кто не является тем, за кого выдает себя[3]. Кембриджский словарь содержит и определение фейковых новостей[4] (англ. *fake news*): ложные *истории, которые кажутся новостями, распространяемые через Интернет или иными способами, создаваемые для того, чтобы влиять на политические события или в качестве шутки*. По мнению С.С. Распопова и Е.Н. Богдан, «фейковые новости представляют собой сообщения, ложь в которых распознаваема и проверяема и которые намеренно сфабрикованы для введения широкой публики в заблуждение»[5]. Отметим, что общественное значение данного явления столь велико, что оно несколько раз становилось «словом года», по мнению различных СМИ[6].

Обратимся к историческому контексту появления фейковых новостей. Словосочетание «фейковые новости» вошло в современный политический лексикон в 2016 году в связи с президентскими выборами в США и Брекситом (выходом Великобритании из состава Европейского союза)[7]. Кандидат от демократической партии США Хиллари Клинтон, являясь очевидным фаворитом президентской гонки, проиграла миллиардеру Дональду Трампу, которому предсказывали поражение все ведущие мировые СМИ[8]. По результатам выборов, обе стороны обменялись обвинениями в том, что противная сторона активно использовала в своей предвыборной агитации *фейковые новости*, называя

[1] Пресс-релиз Министерства юстиции США от 27.01.2021. URL: https://www.justice.gov/opa/pr/social-media-influencer-charged-election-interference-stemming-voter-disinformation-campaign (дата обращения: 25.03.2022).

[2] URL: https://codes.findlaw.com/us/title-18-crimes-and-criminal-procedure/18-usc-sect-241.html (дата обращения: 25.03.2022).

[3] Кембриджский толковый словарь. URL: https://dictionary.cambridge.org/dictionary/english/fake (дата обращения: 25.03.2022).

[4] Кембриджский толковый словарь. URL: https://dictionary.cambridge.org/dictionary/english/fake-news (дата обращения: 25.03.2022).

[5] *Распопова С.С.*, *Богдан Е.Н.* Фейковые новости: информационная мистификация: учеб. пособие для вузов. М., 2018. С. 8.

[6] См., напр.: https://economictimes.indiatimes.com/news/politics-and-nation/fake-news-still-a-menace-despite-government-crackdown-fact-checkers/articleshow/72895472.cms?from=mdr (дата обращения: 25.03.2022).

[7] Сам феномен известен с первой трети XIX века и активно упоминается в прессе тех лет. См.: *Agrawal N.* Where fake news came from and why some readers believe it. URL: https://www.latimes.com/nation/la-na-fake-news-guide-2016-story.html (дата обращения: 25.03.2022).

[8] См., напр.: *Frank T.* With Trump certain to lose, you can forget about a progressive Clinton. URL: https://www.theguardian.com/commentisfree/2016/aug/13/trump-clinton-election-chances-moderate-policies-economy (дата обращения: 25.03.2022).

так практически все негативные утверждения в свой адрес[9].

Примечательно, что Хиллари Клинтон и представители Демократической партии США указывали на социальные сети (и их пользователей, якобы связанных с Правительством России) как на основной источник распространения фейковых новостей[10]. В свою очередь, Дональд Трамп в ходе своего президентства неоднократно называл источником фейковых новостей основные американские СМИ, включая такие крупные, как телеканал *CNN* и газету *New York Times*[11].

Данные взаимные обвинения, сопряженные с достаточно агрессивной риторикой, привели к формированию соответствующей международной повестки, а также резкой активизации борьбы с фейковыми новостями и поисками способов противодействия их распространению, в том числе путем проведения парламентских расследований в США и Великобритании[12], за которыми последовали обвинения в адрес конкретных граждан и организаций, в первую очередь российских[13]. События, произошедшие с момента избрания Дональда Трампа[14] до момента, когда он вынужден был покинуть Белый дом, дают ключ к пониманию вопроса: являются ли фейковые новости главной (или хотя бы одной из ключевых) проблемой сетевого пространства или данная повестка являлась, например, предлогом для введения широкомасштабной *гибридной цензуры*, т.е. цензуры нового типа, в которой действия крупных корпораций, политических сил и органов власти скрыто скоординированы с целью давления на своих политических оппонентов?[15]

## 2. Фейковые новости: краткий исторический экскурс

Исторический анализ показывает, что проблема ложной информации, распространяемой различными способами, не нова — она существует ровно столько же времени, сколько сама информация может влиять на какие-либо общественно-политические процессы и события.

Отметим, что словосочетанию «фейковые новости» предшествовало выражение «газетная утка», появив-

[9] Вынесенный в начало статьи пример относится именно к данном периоду. Дополнительно см. раздел 3 Доклада избирательной комиссии Австралии, в котором указывается, что фейковые новости повлияли на исход выборов в США в 2016 году и Брексит URL: https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Electoral_Matters/AECAnnualReport2017-18/Status_report/section?id=committees%2freportjnt%2f024259%2f27101 (дата обращения: 25.03.2022).

[10] См., напр.: https://www.nytimes.com/2018/12/17/opinion/russia-2016-election-influence-trump.html (дата обращения: 25.03.2022).

[11] В ходе своей первой пресс-конференции Дональд Трамп заявил корреспонденту *CNN*: «Вы и есть фейковые новости». URL: https://www.cnbc.com/video/2017/01/11/trump-to-cnn-reporter-you-are-fake-news.html (дата обращения: 25.03.2022).

[12] См. результаты парламентского расследования по Брексит. URL: https://publications.parliament.uk/pa/cm201719/cmselect/cmcumeds/1791/1791.pdf (дата обращения: 25.03.2022).

[13] Так, 16 февраля 2018 года аппарат специального прокурора США Роберта Мюллера предъявил уголовные обвинения 13 гражданам России в связи с тем, что «они участвовали в операциях, в основном предназначенных для публикации уничижительной информации о Хиллари Клинтон, чтобы очернить других кандидатов, таких как Тед Крус и Марко Рубио, поддержать Берни Сандерса и тогдашнего кандидата Дональда Трампа». Подробнее см.: https://www.justice.gov/file/1035477/download (дата обращения: 25.03.2022).

[14] Примечательно, что Трамп попытался ограничить деятельность онлайн-платформ в части цензурирования контента. Изданный 28 мая 2020 года указ президента США № 13925 озаглавлен «О предотвращении онлайн-цензуры» и содержит достаточно объемную мотивировочную часть, которую можно считать программным заявлением по данной теме. В указе прямо высказана точка зрения, что онлайн-платформы используют различные благовидные предлоги (в том числе борьба с фейк-ньюз) для введения цензуры. Однако как нормативный акт, направленный на суженное толкование раздела 230 Акта о соблюдении приличий в СМИ (*Communications Decency Act*), он был фактически саботирован федеральными властями и влияния на действия онлайн-платформ не оказал. См.: https://www.govinfo.gov/content/pkg/FR-2020-06-02/pdf/2020-12030.pdf#page=1 (дата обращения: 25.03.2022).

[15] То, о какой координации может идти речь, рассказывается в журнале *Time* в статье *Ball M*. The Secret History of the Shadow Campaign That Saved the 2020 Election, где описывается «хорошо финансируемая клика, включающая влиятельных людей из разных отраслей экономики и придерживающихся разных идеологических взглядов, которые скрытно работали вместе, чтобы влиять на восприятие, менять правила и законодательство, воздействовать на медийное освещение событий и контролировать информацию» (*a well-funded cabal of powerful people, ranging across industries and ideologies, working together behind the scenes to influence perceptions, change rules and laws, steer media coverage and control the flow of information*). URL: https://time.com/5936036/secret-2020-election-campaign/ (дата обращения: 25.03.2021).
Отметим: если отбросить сомнительный эвфемизм «спасение выборов», то описанное может рассматриваться как преступление, выраженное в «заговоре с целью повлиять на выборы».

шееся более 300 лет назад на территории, которая в настоящее время входит в состав Германии. В частности, немецкоязычные газеты в сообщениях, которые не имели подтверждения, ставили пометку из двух латинских букв *NT* — *non testatum* (с лат. «не подтверждено»). По-немецки сочетание данных букв произносилось как энте (нем. *Énte*), что означает «утка».

> Более того, само появление периодической печати в первую очередь связано с публикацией в основном никак не подтвержденных и никак не проверяемых сведений, направленных по своему воздействию на политические события.

Например, предтеча современной журналистики Пьетро Арентино обрел славу публициста, по сути «вмешиваясь» в выборы папы римского в 1522 году (с его деятельностью связано возникновение слова «пасквиль», так ка его листки клеились у подножия статуи близ римской площади Пьяцца Навона, получившей в народе название «Пасквино» [итал. *Pasquino*])[16]. Другим примером, подтверждающим указанную мысль, является характеристика периодической печати в пьесе «Склад новостей» (1625 год) Бена Джонсона, где журналистика характеризовалась как «самодельщина, высосанная из пальца и не содержащая ни слога правды»[17].

Собственно, пресса не стала источником точной информации и значительно позже — в XIX веке. Так, третий президент США Томас Джефферсон в ответ на вопрос о том, как заниматься газетным делом таким образом, чтобы это приносило наибольшую пользу, сказал: «Придерживаться лишь истинных фактов и принципов. Однако я боюсь, что такой газете пришлось бы обходиться лишь малым количеством подписчиков. Печальная правда состоит в том, что никакое подавление прессы не смогло бы так основательно навредить нации, как это делает сама пресса, отчаянно предающаяся проституции в пользу лжи. Нельзя верить ничему, что напечатано в газете. Сама истина становится отравленной от одного соприкосновения с этим сосудом»[18]. Схожие сентенции можно обнаружить у М.Е. Салтыкова-Щедрина в коротком рассказе 1884 года «Обманщик-газетчик и легковерный читатель», который начинается следующими словами: «Жил-был газетчик, и жил-был читатель. Газетчик был обманщик — все обманывал, а читатель был легковерный — всему верил. Так уж исстари повелось на свете: обманщики обманывают, а легковерные верят»[19].

## 3. Фейковые новости, дезинформация и информационные войны

Правовой анализ понятия «фейковые новости» невозможен без четкого его разграничения с другими правовыми понятиями, которые связаны с оборотом и распространением информации. В частности, большой интерес представляет разграничение упомянутых выше понятий «фейковая информация» и «дезинформация».

С понятием «дезинформация» в первую очередь связывают формы ведения информационного противостояния, в том числе дезинформацию как форму ведения военных действий (информационной войны).

Вновь обратимся к толковым словарям. Малый академический словарь русского языка дает следующее определение дезинформации: *распространение (в прессе, по радио и т.п.) ложных сведений с целью ввести кого-либо в заблуждение*[20]. Юридические словари дают аналогичное определение[21].

Словарь военных терминов дает следующее определение: способ оперативной (стратегической) маскировки, заключающийся в *преднамеренном распространении ложных сведений* о своих войсках

[16] См.: *Дживелегов А.К.* Очерки итальянского Возрождения. Кастильоне. Аретино. Челлини. М., 1929.

[17] Цит. по: *Джонсон Б.* Склад новостей / пер. Т. Левита. URL: http://az.lib.ru/d/dzhonson_b/text_1625_sklad_novostey.shtml (дата обращения: 25.03.2022).

[18] Цит. по: The Letters of Thomas Jefferson 1743–1826. To John Norvell Washington, June 14, 1807. URL: http://www.let.rug.nl/usa/presidents/thomas-jefferson/letters-of-thomas-jefferson/jefl179.php (дата обращения: 25.03.2022).

[19] *Салтыков-Щедрин М.Е.* Полное собрание сочинений, 1837–1937: в 16 т. М.; Л., 1974. Т. 16. Сказки, 1869–1886. Пестрые письма, 1884–1886. С. 60–62.

[20] См.: Малый академический словарь: сост. А.П. Евгеньева. Статья «Дезинформация». М., 1957–1984.

[21] См., напр.: Энциклопедический словарь экономики и права, 2005.

(силах), их группировке, составе, вооружении, боеспособности, планах боевых действий *с целью ввести противника в заблуждение*. Дезинформация проводится в комплексе с демонстративными действиями, имитацией, скрытием[22].

> Таким образом, понятие «фейковая новость» обнаруживает сходство с понятием «дезинформация» в том виде, в котором оно становится употребительным в русском языке, потому что именно такой смысл в него вкладывают политики, общественные деятели и СМИ. В этой связи встает вопрос о том, стоит ли отождествлять эти понятия и тем самым отказаться от попыток ввести его в правовой оборот или все же четко разграничить, закрепив эти понятия нормативно, предусмотреть ответственность как за распространение фейковых новостей, так и дезинформации.

По нашему мнению, данный вопрос невозможно отделить от той общественной дискуссии, которая развернулась по поводу противодействия фейковым новостям и перешла в юридическую плоскость. Как мы уже упоминали, чрезвычайная интенсификация дискурса по данной проблеме последовала за президентскими выборами 2016 года в США. Обвинения сторон сводились к тому, что противоположная сторона применила методы скоординированного введения в заблуждение избирателей путем распространения заведомо недостоверных сведений. То есть речь на самом деле идет не столько о фейковых новостях как таковых, сколько о скоординированной кампании по дезинформации с целью повлиять на исход выборов. Если это не военные действия невоенными средствами, то нечто весьма близкое по смыслу и содержанию, учитывая то, какова цена победы в противостоянии.

Как мы уже указывали, соперничество демократической и республиканской партий перешло в том числе в юридическую плоскость путем выдвижения обвинений против Трампа и его соратников. В числе таковых были названы и граждане России, и российские юридические лица. Анализ предъявленных прокуратурой США обвинений в адрес российских граждан показывает, что американские власти усматривают общественную опасность во «вмешательстве в американскую политическую систему» путем «внесения раздоров в американское общество» и распространения «ложных сведений о кандидате от демократической партии США Хиллари Клинтон в пользу кандидата от республиканской партии Дональда Трампа»[23]. Таким образом, США де-факто перешли к уголовному преследованию лиц, которым предъявлены обвинения в проведении «кампании по дезинформации». Весьма примечательно, что менее чем через два года данные обвинения в отношении компаний «Конкорд Менеджмент» и «Конкорд Консалтинг» были сняты генеральной прокуратурой США в связи с тем, что «защита данных компаний может получить доступ к информации о том, как США противодействует иностранному влиянию»[24]. Иными словами, утверждения о вмешательстве в американскую политическую систему и многочисленные заявления прессы на этот счет остались недоказанными ввиду того, что генеральная прокуратура США оказалась неспособна провести соответствующий процесс, ограничившись голословными обвинениями в адрес обвиняемых, лишив их права на возможность доказать ложность предъявленных обвинений. Не лишним будет напомнить, что недоказанное в суде обвинение в демократическом обществе должно рассматриваться как оправдание: нет приговора — значит нет вины.

## 4. Фейковые новости в российском правовом контексте

Отметим, что проблема фейковых новостей обрела большую значимость не только за рубежом, но и в России. Например, в одном из своих последних интервью на посту премьер-министра Российской Федерации Дмитрий Медведев заявил: «Проблема эта, действительно, существует, и мир так устроен, что если раньше, во всяком случае, в период моей молодости, можно было сразу понять, откуда эта новость произошла в силу централизации источников информации, то сейчас это уяснить практически невозможно». Он до-

[22] Словарь военных терминов. М., 1988. Статья «Дезинформация».

[23] United States of America v. Internet Research Agency LLC. URL: https://www.justice.gov/file/1035477/download (дата обращения: 25.03.2022).

[24] United States of America v. Concord Management and Consulting LLC and Concord Catering motion to dismiss Concord defendants. URL: https://int.nyt.com/data/documenthelper/6818-concord-case/a2f02719179f1e9a1e6b/optimized/full.pdf#page=1 (дата обращения: 25.03.2022).

бавил, что по законам информационного жанра если какое-то сообщение начинают цитировать, то потом уже невозможно отследить первоначальный источник или это перестает быть важным. А если якобы новость процитирует какое-то количество источников, то она «становится общественно признанной и по сути близкой к достоверной при том, что таковой не является»[25].

Общественная дискуссия, посвященная целесообразности принятия пакета законов о запрете фейковых новостей в России, была достаточно накаленной. Одной из отправных точек для их разработки послужила трагедия в торговом центре «Зимняя вишня» в г. Кемерове, произошедшая в марте 2018 года. Такое мнение 15 мая 2019 года высказал глава Комитета по информационной политике Государственной Думы Российской Федерации Леонид Левин в рамках медиафорума Общероссийского народного фронта (ОНФ) «Правда и справедливость» в г. Сочи: «Рубиконом, после которого стало очевидно, что необходимо регулирование (законодательное), стала трагедия в “Зимней вишне”, когда вбрасывалась информация про несколько сотен трупов в моргах Кемерово»[26]. Здесь так же следует упомянуть, что информация о «сотнях трупов, поступивших после пожара в морги города Кемерово» распространялась злонамеренно с территории Украины, и ее автор «пранкер Евгений Вольнов» (настоящее имя Никита Кувиков) не скрывал, что сделал это в целях ведения информационной войны против Российской Федерации[27].

В результате описанных событий за последние два года в российском законодательстве появился целый ряд норм, ограничивающих распространение недостоверной информации в Интернете[28].

Действующая редакция Федерального закона от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (далее — Закон об информации) выделяет три группы субъектов, в отношении которых возникают обязанности по противодействию недостоверной информации: операторы поисковых систем, новостные агрегаторы, социальные сети.

Для указанных субъектов возникают разные обязанности:

1) на операторов поисковой системы возложена обязанность прекратить выдачу сведений об указателе страницы сайта в Интернете, которая предоставляет доступ к недостоверной информации о заявителе, требующем ее удаления;

2) на новостные агрегаторы возложена обязанность не допускать их использование в целях сокрытия или фальсификации общественно значимых сведений, распространения недостоверной общественно значимой новостной информации под видом достоверных сообщений, а также распространения информации с нарушением законодательства Российской Федерации;

3) на социальные сети возложена обязанность не допускать распространения недостоверной общественно значимой информации, распространяемой под видом достоверных сообщений, которая создает угрозу причинения вреда жизни и (или) здоровью граждан, имуществу, угрозу массового нарушения общественного порядка и (или) общественной безопасности либо угрозу создания помех функционированию или прекращения функционирования объектов жизнеобеспечения, транспортной или социальной инфраструктуры, кредитных организаций, объектов энергетики, промышленности или связи.

Нормы, действующие в отношении новостных агрегаторов, явно несколько шире, чем понятие «фейковые новости», так как здесь идет речь не только о фальсификации или распространении недостоверных сведений, но и их сокрытии, что так же представляет общественную опасность, по мнению законодателя. Отметим, что сокрытие — один из приемов дезинфор-

[25] См. подробнее: https://tass.ru/obschestvo/7196411?utm_source=yandex.ru&utm_medium=organic&utm_campaign=yandex.ru&utm_referrer=yandex.ru (дата обращения: 25.03.2022).

[26] См.: https://www.rbc.ru/society/15/05/2019/5cdc280f9a79471e7072f303 (дата обращения: 25.03.2022).

[27] URL: https://www.gazeta.ru/social/2018/03/28/11699276.shtml (дата обращения: 25.03.2021).

[28] Наиболее значимые изменения внесли Федеральные законы от 18.03.2019 № 31-ФЗ «О внесении изменений в статью 15.3 Федерального закона «Об информации, информационных технологиях и о защите информации» (законопроект № 606593-7), от 15.10.2020 № 341-ФЗ «О внесении изменений в статью 13.15 Кодекса Российской Федерации об административных правонарушениях» (законопроект № 606595-7), а также от 30.12.2020 № 530-ФЗ «О внесении изменений в Федеральный закон «Об информации, информационных технологиях и о защите информации» (законопроект 223849-7).

мации, так как необходимый эффект по воздействию на противника достигается целым спектром различных способов (вспомним того же троянского коня).

> По нашему мнению, определение, данное в Законе об информации, имеет больше сходства с понятием дезинформации, чем с определением фейковых новостей. Исходя из анализа выявленных на сегодняшний день фейковых новостей, можно сделать вывод, что далеко не все они создаются с целью злонамеренного введения общества в заблуждение и не всегда ставят задачу нанести вред общественно значимым интересам.

В этой связи необходимо обратить внимание на такое явление, как розыгрыш, — это тоже форма намеренного введения в заблуждение, но в сатирических целях, т.е. у авторов нет задачи нанести обществу вред. Ярким примером такого рода является деятельность так называемого информационного агентства «Панорама», вымышленные новостные сообщения которого имеют яркий сатирический характер, но нередко в силу невнимательности и поспешности журналистов и редакторов попадают на страницы не только мелких, но и ведущих российских СМИ в качестве уже вполне реальных новостей[29]. При этом, естественно, новость теряет сатирический характер и превращается в фейковую, однако не в силу прямого умысла ее автора, а ввиду утери контекста при ее дальнейшей перепечатке. На мой взгляд, фейковой ее делает не сама сущность сообщения, а то, что она была помещена в обычное СМИ, без указания источника новости, что придает ей видимость абсолютно реальной, скрывает ее среди информационного потока.

> Очевидно, что фейковые сообщения, созданные в качестве сатиры и юмора, не могут считаться общественно опасной деятельностью и на них должны полностью распространяться гарантии, установленные ст. 29 Конституции Российской Федерации, в частности свобода мысли и слова, а также право свободно передавать, производить и распространять информацию любым законным способом.

Это прямо следует из положений ч. 3 ст. 55 Конституции. В этой связи Конституционный Суд в своем Постановлении от 20 декабря 1995 года № 17-П указал следующее: «Гарантируя права и свободы человека и гражданина и обеспечивая их защиту, государство одновременно вправе устанавливать в федеральном законе ограничения прав и свобод в целях обеспечения обороны страны и безопасности государства (часть 3 статьи 55 Конституции Российской Федерации), в том числе предусматривать уголовную ответственность за деяния, умышленно совершенные в ущерб основным ценностям конституционного строя. При этом правомерное осуществление гражданином своих конституционных прав и свобод не может рассматриваться как нанесение ущерба суверенитету Российской Федерации, обороне страны и безопасности государства и влечь для него неблагоприятные правовые последствия»[30]. Таким образом, вряд ли использование гражданами своего права на самовыражение в форме создания сатирических новостей (тем более если это прямо указано на сайте, публикующем такие новости) может рассматриваться как ущерб основным ценностям конституционного строя.

> Однако перепечатка подобных новостей без указания источника и сатирического характера изначального сообщения уже может и, на наш взгляд, должно рассматриваться как форма дезинформации и оцениваться должна с учетом содержания новости (сходства сообщения с возможно имевшими место событиями) и наличия умысла на причинение вреда защищаемым законом правоотношениям.

Заметим, что указание на сатирический характер деятельности издания не является «индульгенцией», которая дает право делать любые публикации. Напомню, что дезинформацию о трагедии в Кемерове распространял самоназванный «пранкер», т.е. человек, декларирующий свою информационную деятельность в качестве юмористической.

В таком случае очевидно, что преследоваться должна скорее дезинформация, т.е., по сути, то, что объявле-

[29] Достаточно наглядно данную тенденцию иллюстрирует новостное сообщение о начале выпуска водки крепостью в 39 градусов, которое разместило на своем сайте популярное сетевое издание *Lenta.ru*. URL: https://lenta.ru/news/2019/01/13/na_svyatoe_pokusilis/ (дата обращения: 25.03.2022).

[30] Постановление КС РФ от 20.12.1995 № 17-П «По делу о проверке конституционности ряда положений пункта „а“ статьи 64 Уголовного кодекса РСФСР в связи с жалобой гражданина В.А. Смирнова» // СПС «КонсультантПлюс».

но противоправной деятельностью в соответствии с ч. 8 ст. 10.4 Закона об информации. Формулировки ст. 207.1 «Публичное распространение заведомо ложной информации об обстоятельствах, представляющих угрозу жизни и безопасности граждан» и 207.2 «Публичное распространение заведомо ложной общественно значимой информации, повлекшее тяжкие последствия» Уголовного кодекса Российской Федерации по своему смыслу больше схожи с дезинформацией, так как дезинформация исторически связана с приемами информационной войны, т.е. нанесения реального вреда, сравнимого с проведением теракта[31].

## 5. История советского права и ее уроки

В части понимания процесса развития контроля государства над распространяемой информацией интерес представляют исторические параллели с советским уголовным правом в аспекте введения административной и уголовной ответственности за распространение гражданами, говоря языком современного законодательства, фальсифицированных общественно значимых сведений, распространения недостоверной общественно значимой новостной информации под видом достоверных сообщений.

В РСФСР, а потом и в СССР уголовно преследовалось распространение информации, наносившей вред общественному строю. В частности, еще УК РСФСР 1922 года содержал ст. 73, которая предусматривала наказание сроком до 6 месяцев тюремного заключения за измышление и распространение в контрреволюционных целях ложных слухов или непроверенных сведений, могущих вызвать общественную панику, возбудить недоверие к власти или дискредитировать ее[32].

Примечательно, что при всем разнообразии так называемых контрреволюционных преступлений, предусмотренных УК РСФСР 1926 года, в дальнейших редакциях данная статья исчезла, в частности Постановление ЦИК СССР от 25 февраля 1927 года «Положение о преступлениях государственных (контрреволюционных и особо для Союза ССР опасных преступлениях против порядка управления)» уже не содержит такого состава преступления. Однако к уголовному преследованию за распространение слухов очень быстро вернулись в начале Великой Отечественной войны. Указом Президиума Верховного Совета СССР от 6 июля 1941 года была введена уголовная ответственность за подобные преступления. Названный указ гласил: «Установить, что за распространение в военное время ложных слухов, возбуждающих тревогу среди населения, виновные караются по приговору военного трибунала тюремным заключением на срок от 2 до 5 лет, если это действие по своему характеру не влечет за собой по закону более тяжкого наказания»[33].

Таким образом, максимальный срок наказания за распространение слухов повышался сразу в 10 раз, по сравнению с максимальной санкцией, предусмотренной ст. 73 УК РСФСР 1922 года. Однако, нужно принять во внимание, что действие данного указа во времени было ограничено периодом военного положения (во всяком случае, номинально)[34].

---

[31] Этот вывод подтверждается и тем, что упомянутый ранее фейк о сотнях погибших в Кемерове не был распространен из хулиганских побуждений, а был, по сути, близок по своей направленности к террористическому акту, так как был направлен на дезорганизацию спасательных служб и правоохранительных органов, создание паники, массовых беспорядков, нападений на представителей органов власти, «скрывающих правду от народа», — указанные последствия описаны в ст. 205 УК РФ: «Совершение… действий, устрашающих население и создающих опасность гибели человека, причинения значительного имущественного ущерба либо наступления иных тяжких последствий, в целях дестабилизации деятельности органов власти или международных организаций либо воздействия на принятие ими решений…».

[32] Цит. по: СПС «КонсультантПлюс».

[33] URL: http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=ESU&n=6643#09760909659724064 (дата обращения: 25.03.2022).

[34] Фактически данная норма была упразднена лишь в 1959 году. См.: Указ Президиума ВС СССР от 13.04.1959 «О признании утратившими силу законодательных актов в связи с введением в действие Основ уголовного законодательства, Законов об уголовной ответственности за государственные и за воинские преступления, Основ законодательства о судоустройстве, Положения о военных трибуналах и Основ уголовного судопроизводства». URL: http://www.consultant.ru/cons/cgi/online.cgi?rnd=82A96EF19D1D34C685EB03484F86A8D8&req=doc&base=ESU&n=17321&dst=100098&fld=134&REFFIELD=3&REFDST=1&REFDOC=6643&REFBASE=ESU&stat=refcode%3D16876%3Bdstident%3D100098%3Bindex%3D3#1q8rr039h3 (дата обращения: 25.03.2022).

В дальнейшем при реформировании уголовного законодательства в конце 50-х годов от прямого упоминания слухов или непроверенных сведений в УК отказались. Статья 70 УК РСФСР 1960 года была сформулирована значительно шире по смыслу и была озаглавлена «Антисоветская агитация и пропаганда». В частности, под страхом лишения свободы на срок от 2 до 5 лет запрещалась «агитация или пропаганда, проводимая в целях подрыва или ослабления Советской власти либо совершения отдельных особо опасных государственных преступлений, распространение в тех же целях клеветнических измышлений, порочащих советский государственный и общественный строй, а равно распространение либо изготовление или хранение в тех же целях литературы такого же содержания».

Но такое положение просуществовало относительно недолго. Уже 16 сентября 1966 года УК РСФСР был дополнен ст. 190.1 «Распространение заведомо ложных измышлений, порочащих советский государственный и общественный строй»[35].

Отметим, что применение упомянутых статей являлось репрессивным инструментом, но уже не столь массовым как в 1930-е годы — с 1956 по 1987 год по 70-й статье УК РСФСР было осуждено 6543 человека, а по ст. 190.1 УК РСФСР — 1609 человек. Необходимо упомянуть и о том, что после прихода к власти Л.И. Брежнева число осужденных по ст. 70 УК РСФСР неуклонно снижалось: большая часть осужденных пришлась на 4 года — с 1956 по 1960 год (Брежнев стал Первым секретарем ЦК КПСС 14 октября 1964 года), когда были осуждены 4676 человек. За следующие пять лет было осуждено 1072 человека, а в пятилетку с 1971 по 1976 год — 276 человек[36]. Таким образом, применение данной статьи кратно снижалось.

Статья 190.1 была исключена из УК РСФСР полностью Указом Президиума Верховного Совета РСФСР от 8 апреля 1989 года «О внесении изменений и дополнений в Уголовный и Уголовно-процессуальный кодексы РСФСР». В свою очередь, ст. 70 была фактически заменена другой статьей, принципиально другого содержания, озаглавленной «Призывы к свержению или изменению советского государственного и общественного строя», она вводила уголовную ответственность за «публичные призывы к свержению советского государственного и общественного строя или к его изменению способом, противоречащим Конституции СССР, либо к воспрепятствованию исполнения советских законов в целях подрыва политической и экономической систем СССР, а равно изготовление с целью распространения или распространение материалов такого содержания». Отмена указанной статьи была связана с желанием прекратить практику подавления инакомыслия и борьбы с «посягательством» граждан на руководящую идеологическую роль КПСС (отметим, что руководящая роль КПСС была отменена лишь 14 марта 1990 года с внесением соответствующих поправок в Конституцию СССР).

Учет описанного контекста очень важен, так как в отечественном законодательстве уголовное преследование «слухов и измышлений» было неразрывно связано с преследованием граждан по политическим мотивам и борьбой с нарушением монополии КПСС и подконтрольной ей прессе на распространение информации.

В этой связи обращает внимание то, что идея уголовного и административного преследования за фейковые новости, которая появилась на фоне скандальных президентских выборов 2016 года в США, при рассмотрении ее в контексте развития отечественного уголовного законодательства в XX веке обнаруживает немало сходства между уголовным преследованием за «внесение раздоров в американское общество»[37] и уголовным преследованием за «агитацию или пропаганду, проводимую в целях подрыва или ослабления Советской власти». Как уже отмечалось выше, обвинения во внесении раздоров и распространении фейковых новостей, якобы ставшие причиной победы Трампа, судебную проверку не выдержали, так и оставшись голословными[38]. Таким образом, имеет

[35] Указ Президиума Верховного Совета РСФСР от 16.09.1966. URL: https://base.garant.ru/1306638/ (дата обращения: 25.03.2022).

[36] Справка Пятого управления КГБ СССР № 5/5 – 167 от 04.03.1988 в ЦК КПСС о количестве лиц, осужденных по ст. 70 и 190-1 УК РСФСР. Цит. по: *Семичастный В.Е.* Спецслужбы СССР в тайной войне. М., 2016.

[37] Цит. по: United States of America v. Elena Alekseevna Khysyaynova. URL: https://apps.npr.org/documents/document.html?id=5011321-Khusyaynova-Complaint (дата обращения: 25.03.2022).

[38] С учетом того, что вторые для себя выборы Дональд Трамп проиграл, перспективы судебного разбирательства относи-

право на существование точка зрения, что имело место политическое сведение счетов проигравшей выборы партии, т.е. обвинения носили политический характер.

> Как показывает советская история, власти тем сильнее прибегали к уголовному преследованию подобных деяний, чем больше был необходим контроль за информационным пространством и подавление любых альтернативных точек зрения. И наоборот, чем увереннее чувствовали себя власти, считая обстановку в государстве стабильной, тем меньше уголовных дел заводилось по подобным статьям.

Подтверждение данного умозаключения можно найти в последних инициативах, которые звучат из-за океана. 2 февраля 2021 года в газете *New York Times* вышла статья под заголовком «Как администрация Трампа может помочь разрешить наш кризис с реальностью» (*How the Biden Administration Can Help Solve Our Reality Crisis*)[39]. В этой статье автор перечисляет различные обвинения в адрес оппозиционных к президенту Байдену средств массовой информации и онлайн-групп, которых он обвиняет в циркуляции «безосновательных теорий заговора», после чего обозначает вопрос, который стоит перед администрацией Байдена: как объединить страну, в которой миллионы людей предпочитают создавать свою версию реальности? Опрос экспертов привел к весьма озадачивающему мнению: Байден должен создать специальный орган *(task force)*, который возглавит «царь реальности» *(reality tzar)*. Автор, видимо, предчувствовал расширение зрачков читателей и поэтому заявил, что «безусловно это звучит немного как антиутопия, но давайте выслушаем экспертов». Интересно, что все опрошенные являются экспертами по противодействию терроризму, что автоматически ставит вопрос: неужели в США стало так много радикально настроенных граждан, что нужно создавать целый орган, который ни много ни мало будет контролировать реальность? Судя по самой статье, наибольшую озабоченность у редакции издания вызывает то, что далеко не все американцы убеждены в легитимности новой президентской администрации, подозревая, что злоупотребления на выборах представляют собой умело сконструированный нарратив *(false election fraud narrative)*. Все описанное начинает напоминать борьбу с *«клеветническими измышлениями, порочащими советский государственный и общественный строй»*, т.е. подавлением инакомыслия под предлогом явно раздутого вреда от фейковых новостей, а ведь, как мы уже выяснили, новости никогда особой точностью и не отличались.

> Учитывая сказанное, необходимо критически воспринимать мировой опыт преследования авторов фейковых новостей, принимая во внимание исторический и политический контекст подобных действий. Ни в коем случае нельзя забывать о гарантируемых Конституцией России правах на свободу мысли и слова, праве свободно получать, производить и распространять информацию.

Особенно важно определить, какие общественные отношения необходимо защитить путем расширения круга лиц, привлекаемых к ответственности за фальсификацию общественно значимых сведений, распространение недостоверной общественно значимой новостной информации под видом достоверных сообщений.

Необходимо напомнить, что закрепленная в Законе об информации формулировка уже является весьма неоднозначной, на что, в частности, обращал внимание Совет при Президенте Российской Федерации по развитию гражданского общества и правам человека[40]. Так, эксперты Совета отметили, что легального определения понятий «фальсификация общественно значимых сведений» и «недостоверная информация» в настоящее время не существует. В Законе

тельно выборов предыдущих становятся весьма туманными — актуальность данной повестки для обеих политических партий явно утеряна.

[39] *Roose K.* How the Biden Administration Can Help Solve Our Reality Crisis. URL: https://www.nytimes.com/2021/02/02/technology/biden-reality-crisis-misinformation.html (дата обращения: 25.03.2022).

[40] Экспертное заключение Совета при Президенте Российской Федерации по развитию гражданского общества и правам человека на проект Федерального закона № 223849-7 «О внесении изменений в Федеральный закон «Об информации, информационных технологиях и о защите информации». URL: http://www.president-sovet.ru/presscenter/news/read/4610/ (дата обращения: 25.03.2022).

об информации соответствующие определения не даны. Следует согласиться с выводами Совета о том, что необходимо руководствоваться Постановлением Пленума ВС РФ от 24 февраля 2005 года «О судебной практике по делам о защите чести и достоинства граждан, а также деловой репутации граждан и юридических лиц». Пунктом 9 указанного Постановления определено, что предметом судебного рассмотрения могут быть «утверждения о фактах, соответствие действительности которых можно проверить… Не соответствующими действительности сведениями являются утверждения о фактах и событиях, которые не имели места в реальности во время, к которому относятся оспариваемые действия». Справедливо замечание и о том, что определение общественно значимой информации весьма сложно отделить от оценочных суждений.

Представляется, что дальнейшее нормативное регулирование данных правоотношений должно, безусловно, быть лишено тех недостатков, на которые указал Совет при обсуждении поправок в Закон об информации.

> Необходимо избежать ситуации, когда практическое применение соответствующих норм приведет к административному произволу и установлению цензуры, что прямо запрещено ч. 5 ст. 29 Конституции Российской Федерации.

Тем более что к этому движутся те страны, которые обычно высоко ставились в различных рейтингах свободы Интернета и превозносившие собственные гарантии свободы слова.

Тем не менее нельзя переходить и в другую крайность — отмахиваться от проблемы и связывать ее только с авторитарными инстинктами власти. Развитие процессов информатизации российского общества, повышение роли социальных сетей как источника информации сопровождается активным переходом социально значимых дискуссий в виртуальное пространство. В социальных сетях ведутся аккаунты президента и премьер-министра, членов Правительства, губернаторов, депутатов Федерального Собрания и других представителей власти. В таком виде социальные сети начинают представлять собой не просто более развитые аналоги чатов, распространенных на ранних этапах развития Интернета, а во многом общественно-политические площадки, важность которых для нормального диалога власти и общества постоянно возрастает.

> Устраняться от необходимости регулирования обращения информации в Интернете на основании того, что существует риск перехода к ограничению свободы слова и введению цензуры, в том числе с учетом приведенного контекста, на наш взгляд, нецелесообразно.

Неоднократно упомянутая ситуация с «Зимней вишней» — яркий пример того, что отсутствие механизмов наказания за подобные действия может многократно усилить негативный эффект от какой-то чрезвычайной ситуации, повлечь беспорядки, гибель людей, посеять панику.

## 6. Основные выводы

Дабы избежать указанных рисков, необходим ответственный и взвешенный подход к законотворчеству, не допускающий расширительного или двоякого толкования соответствующих норм. Необходимо четко ставить цель — зачем вводится то или иное регулирование, каких результатов мы хотим достичь, вводя тот или иной пакет норм: создать «царя реальности» и авторитарный контроль за пользователями Интернета, которых мы рассматриваем как потенциальных экстремистов, или делаем всё, чтобы предупредить трагедию, не дать преступникам использовать трагические события в своих целях.

В этом смысле вопрос терминологии — с чем должен бороться законодатель, с фейк-ньюз или с дезинформацией — становится далеко не таким абстрактным. Оголтелая борьба «цифровых гигантов» с фейк-ньюз логически приводит к тому, что заместитель Председателя Совета Безопасности России Дмитрий Медведев назвал «призраком цифрового тоталитаризма, который постепенно заполняет собой общество»[41], что несовместимо с принципами и гарантиями, заложенными в Конституции России. Отметим, что отрицать существование фейковых сообщений и их негативное влияние на общество бессмысленно,

[41] Дмитрий Медведев: Америка 2.0. После выборов. URL: https://tass.ru/opinions/10470467 (дата обращения: 25.03.2022).

однако нужно четко разграничивать дезинформацию и фейки, взвешивать негативные последствия их распространения.

> Самую большую угрозу правам и законным интересам граждан несет именно дезинформация, главным отличием которой является злой умысел распространяющего либо безразличие к негативным последствиям.

В отношении лиц, занимающихся дезинформацией, ставящих цель нанести ущерб обществу, государство должно применять весь спектр санкций, включая уголовное преследование дезинформаторов, блокировку распространения информации, автоматизированное пресечение повторного распространения совместно с мерами цифрового просвещения для тех, кто подвергся воздействию дезинформации.

К фейк-ньюз, которые мы определяем как недостоверную или частично недостоверную информацию, распространяемую ввиду заблуждения под видом достоверной, нужен более гибкий подход. Во-первых, необходим общественный контроль деятельности новостных агрегаторов, социальных сетей и аудиовизуальных сервисов, направленной на борьбу с фейками с целью прекратить злоупотребления, несовместимые с конституционными гарантиями свободы слова[42]. Во-вторых, необходимо активное участие общества и государства в формировании внутренней политики новостных агрегаторов, СМИ, социальных сетей, аудиовизуальных платформ по борьбе с фейками и дезинформацией, особенно в части контроля их соответствия нормам законодательства и исключения тенденций по их превращению в цензоров. В-третьих, необходимо создать такие механизмы взаимодействия упомянутых субъектов и государства, в которых государство (действуя прозрачно и в рамках закона) могло бы в режиме реального времени контролировать и направлять борьбу с дезинформацией, включая выявление и преследование правонарушителей в момент совершения деяния. Описанный подход позволит снизить риски повторения «информационных терактов», подобных случаю в Кемерове, и одновременно будет сдерживать цифровую цензуру, в которую очевидным образом скатываются крупнейшие интернет-платформы.

Развитие правового регулирования сейчас находится на той стадии, когда основные санкции за дезинформацию в законодательстве есть, однако это не решает проблемы как таковой. К сожалению, у государства пока отсутствует концептуальное понимание взаимосвязи описанных процессов, их сущностное разграничение и необходимость ухода от реактивного подхода (в логике «нам написали заявление — мы возбудили дело») к активному, когда государство, действуя рука об руку с институтами гражданского общества, направляет действия интернет-платформ, пресекает преступления описанного характера или серьезно ограничивает их последствия. К сожалению, пока движения в этом направлении не наблюдается.

[42] Например, можно обязать соцсети раскрыть алгоритмы фильтрации контента и оценить получаемые результаты с точки зрения ущемления свободы слова и права распространять не запрещенную законом информацию, чтобы исключить такие вопиющие случаи, как бан за упоминание фамилии «Хохлов» и подобные инциденты массового характера. Также давно назрел вопрос о необходимости предоставить возможность пользователям обжаловать решения социальных сетей и аудиовизуальных сервисов по блокировке и удалению контента с участием в рассмотрении жалоб представителей государства.

## Fake-News as a Political and Legal Phenomenon

What this article deals with is the phenomenon of “fake news” in its legal and political interpretation during digital transformation. Author examines genesis of the “fake news”, rapid shift from political use of this term to legal enshrinement, application despite quite vague criteria of the legal understanding of what is, and what is not “fake news”. The article answers the question — is the phenomenon of “fake news” the worst outcome of the global internet freedom or it is a useful legal tool for the Western political elites in their unfair political struggle? The articles also examines adequacy of the term “fake news” as a framework for the regulation of the social networks and internet as platform for sharing information, gives propositions of other terms for such use, assesses risks of following current trends in combating fake news.

***Keywords:*** *Fake news, disinformation, information law, censorship, digital rights, social media, criminal law, constitutional law*

## INFORMATION ABOUT THE AUTHOR

**Evgenii I. Diskin**
Expert of the BRICS Competition Law and Policy Centre, Higher School of Economics (HSE), Candidate of Juridical Sciences (e-mail: ediskin@hse.ru).

## REFERENCES

Ball, M. The Secret History of the Shadow Campaign That Saved the 2020 Election. Time Magazine. February 4, 2021. URL: https://time.com/5936036/secret-2020-election-campaign.

Dzhivelegov, A.K. Essays of the Italian Renaissance. Castiglione. Aretino. Cellini [*Ocherki ital'yanskogo Vozrozhdeniya. Kastil'one. Aretino. Chellini*]. Moscow, 1929. 353 p.

Frank, T. With Trump Certain to Lose, You Can Forget about a Progressive Clinton. The Guardian. August 13, 2016. URL: https://www.theguardian.com/commentisfree/2016/aug/13/trump-clinton-election-chances-moderate-policies-economy.

Frolov, D.B. Information Warfare: the Evolution of Forms, Means and Methods [*Informatsionnaya voyna: evolyutsiya form, sredstv i metodov*]. Sociology of Power [*Sociologiya vlasti*]. 2005. No. 5. P. 121–146.

Makarov, V.E. Political and Social Aspects of Information Security: Monograph [*Politicheskie i sotsial'nye aspekty informatsionnoy bezopasnosti: Monografiya*]. Moscow, 2015. 351 p.

Medvedev, D.A. America 2.0. After Elections [*Amerika 2.0. Posle vyborov*]. Tass, January 16, 2021. URL: https://tass.ru/opinions/10470467.

Raspopova, S.S., Bogdan, E.N. Fake news: Information hoax: Textbook for universities [*Feykovye novosti: Informatsionnaya mistifikatsiya: Uchebnoe posobie dlya vuzov*]. Moscow, 2018. 112 p.

Roose, K. How the Biden Administration Can Help Solve Our Reality Crisis. New York Times. February 2, 2021. URL: https://www.nytimes.com/2021/02/02/technology/biden-reality-crisis-misinformation.html.

Saltykov-Shchedrin, M.E. Complete Works [*Polnoe sobranie sochineniy*], 1837–1937: In 16 vols. Moscow; Leningrad, 1974. Vol. 16. Tales [*Skazki*], 1869–1886. Motley Letters [*Pestrye pis'ma*], 1884–1886.

The Letters of Thomas Jefferson 1743–1826. To John Norvell Washington, June 14, 1807. URL: http://www.let.rug.nl/usa/presidents/thomas-jefferson/letters-of-thomas-jefferson/jefl179.php.

DOI: 10.37239/0869-4400-2022-18-3-121-143

**МИХАИЛ БОРИСОВИЧ ЖУЖЖАЛОВ**

старший юрист юридической фирмы «Томашевская и партнеры»

**РОМАН МИХАЙЛОВИЧ ЯНКОВСКИЙ**

партнер юридической фирмы «Томашевская и партнеры», доцент факультета права Национального исследовательского университета «Высшая школа экономики», кандидат юридических наук

# Санкции и контрсанкции: с чем мы столкнулись в этот раз?

В 2022 году российская экономика столкнулась с новыми санкциями, количество и объем которых существенно превысил введенные ранее. Помимо санкций, введенных государствами, множество крупных иностранных компаний объявили о планах прекратить работу в России. Как с правовой точки зрения устроены новые ограничения и какие правовые меры предпринимаются, чтобы ограничить полученный экономикой ущерб?

Из всех правовых институтов «санкционное право», пожалуй, развивается сейчас динамичнее всего. У России исторически больше связей с западным миром, чем у Кубы в 1962 году или у Ирана в 1979 году, и мы видим, как юридическая мысль всего мира активно работает, чтобы эти связи разорвать. Введенные в первую очередь в 20-х числах февраля санкции в основном расширили списки подвергшихся ограничениям лиц, существующие еще с 2014 года (следовательно, использовался существующий предмет и механизмы санкций). Но затем было изобретено и введено множество новых видов санкций, например запреты на использование воздушного пространства. Перспективным трендом (если можно так выразиться) становятся запреты на импорт из России: вначале это были нефть и газ, затем рыба, икра и алкоголь, продукция металлургической промышленности… — возможности здесь воистину неисчерпаемы.

Мы систематизировали результаты этого творческого процесса, чтобы по возможности понять, могут ли быть пределы у «санкционного» нормотворчества (похоже, что нет). Также мы изучили ответные меры, введенные Россией, в частности новый громкий законопроект о «внешнем управлении» офисами иностранных фирм в России.

## 1. Какие санкции уже действовали к 2022 году?

Традиционно выделяется несколько видов санкций.

1. Персональные, которые вводятся в отношении конкретных лиц. Как правило, это запрет на пребывание в стране, сотрудничество с ее гражданами и организациями, а также заморозка принадлежащих лицу активов. Такие санкции не обязательно носят карательный характер: так, в Великобритании распространена практика предоставления лицензий на завершение деятельности в стране, по истечении которых блокируются любые активы и трансакции[1].

[1] См., напр.: лицензия ПАО «Сбербанк России», выданная до 24.06.2022: General Licence: Correspondent Banking Relationships & Processing Sterling Payments in relation to Energy INT/2022/1277877 / Office of Financial Sanctions Implementation HM Treasury, 01.03.2022. URL: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/

**Mikhail B. Zhuzhzhalov,**
Senior Associate at Tomashevskaya & Partners (e-mail: m.zhuzhzhalov@mail.ru).

**Roman M. Yankovskiy,**
Partner of Tomashevskaya & Partners, Associate Professor, Faculty of Law, National Research University "Higher School of Economics", Candidate of Juridical Sciences (e-mail: roman.yankovskiy@gmail.com).

**Sanctions and Counter-Sanctions: What are We Facing This Time?**

2. Секторальные, которые распространяются на отдельные группы трансакций. Это финансовые санкции, санкции в области нефтедобычи, энергетики и прочие группы разного масштаба.

3. Вторичные — этот специфический вид санкций нацелен на тех, кто активно взаимодействует с лицами и странами, включенными в санкционные списки. Жертвы вторичных санкций «заражаются» санкционным режимом последних и на них распространяется запрет на взаимодействие.

Примечательно, что формально обязанности из санкций падают не на лиц, оказавшихся под санкциями, а на тех, кто с ними сотрудничает, т.е. на граждан и организации юрисдикций, вводящих санкции.

Какие из этих санкций были введены после событий 2014 года?

1. Персональные: запрет на пребывание в странах, заморозка активов.

2. Инвестиционные: запрет инвестировать в долговые инструменты, ценные бумаги и прочие инструменты с длительным сроком обращения (как правило, от 30 дней), выпущенные российскими органами государственной власти, а также прямо поименованными лицами.

3. Экспортные: запрет на поставки в Россию вооружения и товаров двойного назначения, т.е. тех, которые могут использоваться в военных целях или при производстве вооружения.

Важно понимать, как определялись списки лиц, на которых распространялись санкции. По общему правилу, такие списки были закрытыми: санкции распространялись на непосредственных фигурантов списка и их подконтрольных лиц[2]. В некоторых случаях санкционные акты содержали критерии, при которых список мог пополняться (например, туда вносятся лица, поставлявшие в Крым оборудование, способствовавшее энергетическому обособлению полуострова от Украины)[3]. Однако на лиц за пределами списка санкции не распространялись, и в некоторых случаях это позволяло проводить операции в обход санкций, используя новые или не попавшие в список компании. Хотя такое поведение никогда не было полностью легально, наказание грозило самым откровенным нарушителям.

## 2. Санкции после событий 2022 года

С 23 февраля[4] началось активное расширение действующих списков и их синхронизация между странами[5]. Однако стали вводить и новые виды санкций.

file/1057865/GENERAL_LICENCE_correspondent_banking_energy_INT.2022.1277877.pdf (дата обращения: 21.03.2022 ).

[2] Так называемое «правило 50%» (50% *rule*): санкции распространяются на лиц, более чем 50% акций или долей которых (в сумме) владеют фигуранты санкционного списка.

[3] См., напр.: решение Европейского суда общей юрисдикции по делу № T-721/17 *Topor-Gilka v. Council*.

[4] Дата введения первых санкций обусловлена разницей часовых поясов России и западных стран.

[5] Например, список организаций, попавших под экспортные санкции в Японии 01.03.2022, собран из перечня, опубликованного для тех же целей в США 25.02.2022,

Инвестиционные санкции расширились до финансовых: добавились ограничения деятельности банков и российской банковской системы в целом. Были введены санкции против ЦБ и Минфина России. Активы ряда банков (ВТБ, «Открытие» и др.) были полностью заморожены, а их операции — приостановлены на территории ЕС, Великобритании и США[6]; те, кому повезло больше («Сбер»), получили запрет на отдельные операции (например, открытие корреспондентских и транзитных счетов в США)[7].

Экспортные санкции начали превращаться в тотальные эмбарго, иногда включающие персональную или финансовую составляющую, например запрет на продажу предметов роскоши, который 11 марта ввели США и 15 марта ввел ЕС.

Появились импортные санкции — запрет на ввоз определенных российских товаров. Этот вид санкций введен впервые, и неясно, до каких пределов он будет расширяться.

Санкции против отдельных лиц по-прежнему применяются на основе открытых (хотя и сильно расширенных) списков, однако с развитием практик обхода санкций следует ожидать их «генерализации» — введения запрета на сотрудничество с российскими государственными учреждениями и организациями, отвечающими установленным признакам. Многие компании уже поспешили ограничить сотрудничество с нашим государством или даже уйти с рынка, не дожидаясь официального запрета.

Надо сказать, что иностранный бизнес опасается не только нормативных ограничений, но и репутационных последствий сотрудничества с нашей страной. Эти риски, вероятно, будут также учитываться зарубежными компаниями при формировании политик комплаенса. Другими словами, канселинг России станет вполне реальным фактором риска для зарубежных компаний и экспортеров, а также основой для будущих «генеральных» санкций.

Меняется и концептуальная основа санкций. Санкции 2014 года зачастую были направлены на отдельных лиц, чтобы ограничить их влияние или подтолкнуть к правильному (с точки зрения стран, вводящих санкции) поведению[8]. В отличие от них, нынешние санкции явно исходят из признания угрозой самой России в лице любых ее представителей и вообще всего, что

---

а санкции Швейцарии полностью повторяют санкции ЕС (персональные, финансовые и экспортные). См.: Verordnung vom 4. März 2022 über Massnahmen im Zusammenhang mit der Situation in der Ukraine. URL: https://www.fedlex.admin.ch/eli/cc/2022/151/de (дата обращения: 21.03.2022).

[6] США включили в *SDN* (*special designated persons* — список лиц, которым блокируются все активы и счета, хотя в случае с банками такая санкция не затрагивает активы их клиентов) ПАО ВТБ (Банк), АО «ФК «Открытие», АО «АКБ Новикомбанк» и ПАО «Совкомбанк». Первые два попали под аналогичные санкции в ЕС, Соединенном Королевстве и многих других странах.

[7] Так называемый список *CAPTA*, созданный 24.02.2022, в который включено ПАО «Сбербанк России» и его дочерние компании (Директива *OFAC* № 2).

[8] См.: часть (4) преамбулы к Решению Совета ЕС № 2014/145/CFSP; часть (6) преамбулы к Решению Совета ЕС № 2014/512/CFSP; часть (2) преамбулы к Регламенту Совета ЕС № 833/2014.

из России исходит. Это меняет масштаб санкций: вводятся «тотальные» санкции, не ограниченные «нежелательными» лицами или отраслями. С учетом высокого уровня координации между странами из самых разных регионов[9] можно называть новый подход скоординированной блокадой, направленной на причинение нашей стране максимального экономического урона.

## 3. Российские контрмеры

Масштаб экономических проблем, с которыми столкнулась наша страна, подтверждается характером принятых контрмер. Они не являются ответными санкциями в привычном смысле и приняты, очевидно, для защиты организаций и граждан.

Например, запрет выплаты дивидендов представителям недружественных юрисдикций[10] в значительной мере направлен на поддержку отечественных эмитентов; аналогичную цель преследует временный порядок исполнения обязательств по ценным бумагам и долговым инструментам[11]. Запрет на вывоз определенных видов товаров призван предотвратить возможный дефицит и не дать вывезти ценное оборудование; он не ограничивается недружественными юрисдикциями[12]. Запрет на сделки с ценными бумагами и недвижимостью[13] также выглядит в большей степени как мера по стабилизации цен на рынке ценных бумаг и недвижимости хотя бы потому, что сделки с долями в обществах с ограниченной ответственностью, в отличие от акций, не были запрещены[14].

Больше похожи на ответные санкции такие меры, как закрытие воздушного пространства, а также оглашенный 15 марта запрет на въезд в Россию иностранных деятелей, наиболее активно действовавших против России.

Серьезную реакцию вызвали объявления ряда иностранных компаний (в том числе ряда международных юридических фирм) об уходе из России. Возможные социальные последствия потребовали срочных контрмер: Генеральная прокуратура сообщила, что оценит такие действия на предмет фиктивного или преднамеренного банкротства, а также нарушений трудового законодательства[15]. Как следствие, формулировки компаний сменились с закрытия на «приостановку» деятельности с продолжением выплаты заработной платы сотрудникам до сокращений или увольнений.

---

[9] К санкциям присоединяются, помимо европейских стран, Страны Содружества (Канада, Австралия, Новая Зеландия, ряд стран, расположенных на островах Карибского моря), Дальнего Востока (Япония, Сингапур, Тайвань, Южная Корея).
[10] Указ Президента РФ от 28.02.2022 № 79; предписание ЦБ РФ от 28.02.2022.
[11] Указ Президента РФ от 05.03.2022 № 95.
[12] Указ Президента РФ от 08.03.2022 № 100, Постановления Правительства РФ от 06.03.2022 № 302 и от 09.03.2022 № 312.
[13] Указы Президента РФ от 28.02.2022 № 79 и от 01.03.2022 № 81.
[14] Письмо ФНП от 02.03.2022.
[15] Генпрокуратура проверит компании, объявившие об уходе с российского рынка // ТАСС. 2022. 14 марта. URL: https://tass.ru/proisshestviya/14035547 (дата обращения: 21.03.2022).

## 4. «Национализация» иностранных компаний

Вслед за этим в публичных источниках появился законопроект «О внешней администрации по управлению организацией», который, вероятно, скоро будет готов к внесению в Государственную Думу. Фактически законопроект вводит форму национализации закрывающихся иностранных предприятий: суд вправе на три месяца передать предприятие во внешнее управление «ВЭБ.РФ», а банк — Агентству по страхованию вкладов. Управляющий проводит меры по предупреждению банкротства, инвентаризацию и оценку имущества, а затем перепродает предприятие новому владельцу. Задача последнего — в течение года вести деятельность и не сокращать более трети сотрудников.

Новая процедура похожа на внешнее управление при банкротстве, но прямо к процедурам несостоятельности не отнесена. Это порождает вопрос — как будет работать оспаривание сделок и привлечение руководства компании к субсидиарной ответственности.

Основания введения процедуры крайне расплывчаты. Используются две новые категории:

1) фактическое прекращение управления организацией;

2) необоснованное прекращение деятельности (в текущей редакции — «действия, которые *могут* привести к необоснованному прекращению деятельности, ликвидации, банкротству»).

Эти основания поясняются в самом тексте (который, к слову, из-за обилия подобных разъяснений напоминает акты высших судов). Так, о *фактическом прекращении управления* может свидетельствовать не только отсутствие действующего исполнительного органа (типичная ситуация для дедлока), но и прекращение деятельности других органов, включая учредителей (несмотря на то, что участия в текущем управлении они принимать и не должны). Свидетельствовать о прекращении управления может, в частности, то, что учредители покинули Россию, и в их отсутствие произошло существенное уменьшение стоимости имущества организации или она стала неспособна исполнять свои обязательства.

О *необоснованности прекращения деятельности* свидетельствует, в частности, то, что в отсутствие «очевидных экономических оснований» расторгнуты договоры, «имеющие существенное значение для… деятельности» организации, либо направлено уведомление о сокращении более трети работников.

## 5. Ищем компромисс с иностранными инвесторами

Очевидно, законопроект ориентирован на ситуации, когда единственной причиной ухода иностранной компании из России является указание или рекомендация глобального офиса. Однако мы наблюдаем и другие ситуации: некоторые компании прекращают бизнес в России безотносительно

позиции зарубежного руководства, а некоторые (например, международные юридические и аудиторские компании) — фактически переносят его в новые, параллельные структуры под российским брендом. Откровенно говоря, цели распустить коллектив не преследует ни одна международная компания. Они стремятся, напротив, сохранить команду с поправкой на объективное уменьшение объема работы. Многие сообщают о переводах ценных сотрудников в иностранные офисы. Как правоприменительные органы будут относиться к такому мнимому «сокращению штата», не влекущему массовых увольнений, — большой вопрос, потому что закон не делает скидки на такие ситуации.

В качестве компромисса озвучено (но пока не формализовано в нормативных актах) такое решение: глобальные компании передают права участия доверенным лицам в России с сохранением менеджмента и коллектива сотрудников и с возможностью обратного выкупа в будущем[16]. При этом продажа акций[17] резидентами недружественных России юрисдикций[18] ограничена — необходимо получить разрешение Правительственной комиссии[19]. Она, очевидно, столкнется с потоком запросов и будет использовать свои полномочия (включая полномочие выдавать генеральные разрешения[20]).

**ВЛАДИМИР БОРИСОВИЧ РУМАК**

старший юрист
ООО «ДСЛ-Сервис»

**Vladimir B. Rumak**
Senior Lawyer at
DSL-Service (e-mail:
attorney@dslservice.ru).

**On the Eve of Severe Trials**

## В канун тяжелых испытаний

Согласно третьему закону Ньютона любое действие рождает противодействие. Немудрено, что многочисленные экономические санкции, наложенные на Россию чемпионскими темпами[21] в конце февраля — начале марта 2022 года, породили закономерный ответ[22].

Как это обычно бывает, действовали российские власти методом кнута и пряника. Кнут предназначался больше для иностранцев, ведущих бизнес в Рос-

---

[16] См.: Белоусов назвал варианты действий для зарубежных компаний в России // РБК. 2022. 4 марта. URL: https://www.rbc.ru/politics/04/03/2022/6221be509a7947fc551ccf9c (дата обращения: 21.03.2022).

[17] Продажа долей в уставном капитале указанным запретом не охвачена. См.: письмо ФНП от 02.03.2022 № 1176/03-16-3.

[18] Перечень установлен Распоряжением Правительства РФ от 05.03.2022 № 430-р.

[19] Указы Президента РФ от 28.02.2022 № 79 и от 01.03.2022 № 81.

[20] Пункт 16 Порядка согласования сделок Правительственной комиссией, утвержденного Постановлением Правительства РФ от 06.03.2022 № 295. См. пример такого разрешения в выписке из протокола от 10.03.2022 № 7. URL: https://minfin.gov.ru/ru/document/?id_4=135719 (дата обращения: 21.03.2022).

[21] По некоторым подсчетам, количество введенных в отношении россиян санкций с 22 февраля по состоянию на 8 марта приблизилось к рубежу 3000, и их число стремительно растет. См.: Россия возглавила рейтинг стран с самым большим количеством санкций // РИА Новости. 2022. 8 марта. URL: https://ria.ru/20220308/sanktsii-1777111282.html (дата обращения: 21.03.2022).

[22] Оговорюсь, что данный раздел Хроники ограничен описанием экономических контрсанкций, за скобками находится большой пласт законов, ужесточающих меры ответственности в общесоциальной сфере, которые являются предметом отдельного анализа.

сии, а пряник — для российских бизнесменов и отечественных бенефициаров российских же активов.

Первый упреждающий удар был нанесен по валютным операциям: в соответствии с Указом Президента РФ от 28 февраля 2022 года № 79 российских участников внешнеторговых контрактов обязали в трехдневный срок возвращать 80% валютной выручки, а вывод валюты за рубеж фактически запретили (сейчас идут переговоры о том, чтобы эти ограничения были либерализованы[23]).

На следующий день в одночасье были заморожены сделки в отношении недвижимости и ценных бумаг с гражданами и организациями, имеющими отношение к «иностранным государствам, совершающим недружественные действия»[24]. Таким образом, любые попытки реализации основных российских активов со стороны недружественных иностранцев без специального разрешения компетентных органов были пресечены на корню. Вывоз наличной иностранной валюты в размере, превышающем 10 тыс. долларов, был также запрещен.

Подобного развития событий, кажется, мало кто мог представить: если к разного рода торговым эмбарго отечественный бизнес привык, то такого рода тотальный запрет стал скорее холодным душем (впрочем, справедливости ради стоит сказать, что в сравнении с мерами, принятыми в некоторых «недружественных иностранных государствах», ответ этот выглядел чем-то само собой разумеющимся[25]). Целый день еще нотариусы сомневались, могут ли они заверять хотя бы сделки с долями и прочим имуществом, которое не было поименовано в запретительном Указе. Федеральной нотариальной палате даже пришлось выпускать специальное разъяснение, чтобы успокоить бдительных коллег и напомнить им о существовании в гражданском праве России принципа диспозитивности[26]. Помогло это слабо — удостоверять такого рода сделки нотариусы все еще опасаются.

На смену первой волне запретов последовали посулы, правда не всем, а только предпринимателям из *IT*-отрасли, отток которых за рубеж государство воспринимало особенно остро. Меры поддержки бизнеса высоких технологий поручено было разработать нешуточные: от грантов, налоговых льгот и трехлетнего освобождения от проверок контролирующих органов до отсрочки от призыва на военную службу, о которой в связи с последними событиями молодым программистам сложно не думать[27]. Следом законодатель

---

[23] URL: https://www.vedomosti.ru/business/news/2022/03/11/913077-poslableniya-za-narusheniya-valyutnogo-kontrolya (дата обращения: 21.03.2022).
[24] Указ Президента РФ от 01.03.2022 № 81.
[25] Принятые за рубежом имущественные ограничения в отношении российских бизнесменов стали столь повсеместными, что удостоились такой оценки от официального представителя Кремля как «бандитизм на международном уровне». См.: Песков назвал бандитизмом санкции против бизнесменов за встречу с Путиным. URL: https://www.rbc.ru/politics/16/03/2022/6231b5f49a794756412dc765 (дата обращения: 18.03.2022).
[26] Письмо ФНП от 02.03.2022 № 1176/03-16-3.
[27] См.: Указ Президента РФ от 02.03.2022 № 83.

освободил вообще весь бизнес от всех плановых проверок до конца года[28]. Правда, прокурорского надзора эти послабления не коснулись, да и внеплановые проверки никто не отменял, а для них как раз поводов появляется все больше, например в целях проверки повышения цен, которые в текущих условиях грозят расти непрерывно и неизбежно[29]. Как в этом случае будут балансировать российские власти — остается только гадать. Впрочем, к такому балансированию российский бизнес вполне привычен.

Далее вновь последовали запреты. Очередным холодным душем стал порядок исполнения обязательств перед кредиторами — иностранными лицами, так или иначе связанными с «недружественными государствами»[30]. Обязательства в сумме более 10 млн руб. перед таковыми впредь могут исполняться путем зачисления денежных средств на специальные счета в российских банках[31]. Таким образом, Президент фактически обогатил способы исполнения обязательств, предусмотренные ст. 327 ГК РФ, еще одним.

Похожим образом (т.е. императивно) был решен вопрос с исполнением обязательств авиакомпаний, которым иностранные лизингодатели враз велели вернуть все находящиеся в лизинге самолеты, чем едва не поставили на грань существования всю авиаотрасль России. Впрочем, исполнить эти обязательства российские авиакомпании не смогли бы, даже если бы очень захотели: в условиях, когда воздушное пространство за рубежом оказалось закрыто для нас, а российское воздушное пространство — для иностранцев, организовать возврат самолетов оказалось просто невозможно. Российские власти и здесь нашли оригинальный выход: возможность исполнения обязательств авиакомпаний планируется поставить под четкий правительственный контроль[32].

Порцию антисанкционного креатива успели выдать даже суды. В профессиональном юридическом сообществе широко обсуждаемым стало решение Арбитражного суда Кировской области по делу № А28-11930/2021, в котором суд отказал в удовлетворении исковых требований правообладателю мультфильма «Свинка Пеппа» только на том основании, что истец является резидентом недружественного государства — Великобритании. Сего факта оказалось достаточно для того, чтобы сделать вывод о злоупотреблении правом со стороны истца[33]. Если это решение устоит в вышестоящих инстанциях, можно

---

[28] Статья 5 Федерального закона от 03.03.2022 № 46-ФЗ.

[29] См., напр.: ФАС проверит «Детский мир» из-за роста цен на детское питание и подгузники // Интерфакс. 2022. 5 марта. URL: https://www.interfax.ru/business/826586; ФАС проверит повышение цен продавцом бытовой техники «Технопарк-Центр» // РИА Новости. 2022. 10 марта. URL: https://ria.ru/20220310/tseny-1777415392.html; ФАС начала проверять цепочки поставок сахара в розницу // Интерфакс. 2022. 17 марта. URL: https://www.interfax.ru/russia/829677. Дата обращения: 21.03.2022.

[30] Перечень таких стран уже определило Правительство РФ. В него вошли США, страны ЕС, Великобритания, Украина, Канада, Австралия, Япония, Республика Корея, Тайвань (Китай), Швейцария, Норвегия и еще с дюжину небольших государств. См.: Распоряжение Правительства РФ от 05.03.2022 № 430-р.

[31] См.: Указ Президента РФ от 05.03.2022 № 95.

[32] См. ст. 11 Федерального закона от 14.03.2022 № 56-ФЗ.

[33] Свинка Пеппа не вышла гражданством // Коммерсантъ. 2022. 14 марта. URL: https://www.kommersant.ru/doc/5252458 (дата обращения: 21.03.2022).

даже не гадать, как с учетом принципа взаимности будут относиться к российским бизнесменам в иностранных судах. Впрочем, судьба российских исков за рубежом наши власти в сложившейся ситуации, видимо, мало волнует.

Наконец, подоспели и соответствующие изменения в гражданское законодательство, правда, не в сам ГК, а в переходные положения[34]. Разработчики объяснили это временным характером вводимых ограничений[35]. Законопроект предлагает ввести разного рода возможности реагирования контрагентов на невозможность исполнения обязательств ввиду санкций: от освобождения от ответственности за неисполнение до одностороннего отказа от исполнения либо прекращения обязательств. При этом законодатель предусматривает и вариативность способов исполнения, например возможность размещения дополнительных акций в пользу иностранного займодавца вместо возврата займа. При этом для пособников санкций применение этих новых дивных гражданско-правовых возможностей исключено вовсе. Для российских пользователей иностранной интеллектуальной собственности законопроект также принес хорошие новости: действие санкций признано обстоятельством, автоматически продлевающим лицензионные соглашения с правообладателями, которые теперь не смогут быть расторгнуты по инициативе последних.

Несмотря на все эти заградительные меры рисков для российского бизнеса, активно пользующегося офшорами, с каждым днем становилось все больше. Спасательным кругом могла стать очередная амнистия капитала, позволяющая добиться хоть какой-то предсказуемости в управлении активами в рамках одной юрисдикции, и она не заставила себя долго ждать[36]. Воспользовавшиеся ею бизнесмены будут освобождены от ответственности за несоблюдение валютного законодательства в части репатриации выручки по внешнеторговым контрактам (т.е. валюты, полученной от нерезидентов и не возвращенной на счета банков — резидентов РФ в установленный срок), а также за неуплату таможенных пошлин и налогов, если занесут указанные активы в декларацию, подаваемую в порядке амнистии капитала. Срок подачи деклараций при этом установлен с 14 марта 2022 года по 28 февраля 2023 года.

Пожалуй, этот четвертый (и рискну предположить, что заключительный) этап амнистии капитала станет самым результативным: российские власти, столько лет пытавшиеся подобрать ключ к сердцам покинувших родную гавань бизнесменов, теперь обречены на успех, ведь перед бенефициарами российских активов стоит простой выбор — возвращение или перспективы фактической потери бизнеса. Обращает на себя внимание тот факт, что перечень имущества, декларирование которого предусмотрено Законом об амнистии,

---

[34] См. Законопроект № 92282-8. URL: https://sozd.duma.gov.ru/bill/92282-8 (дата обращения: 21.03.2022).

[35] См. об этом: Павел Крашенинников делает невозможное возможным // Его законопроект прекращает обязательства, конвертирует долги в акции и продлевает интеллектуальные права // Закон.ру. 2022. 22 марта. URL: https://zakon.ru/discussion/2022/03/22/pavel_krasheninnikov_delaet_nevozmozhnoe_vozmozhnym__ego_zakonoproekt_prekraschaet_obyazatelstva_kon (дата обращения: 21.03.2022).

[36] Федеральный закон от 09.03.2022 № 48-ФЗ.

кроме традиционных денежных средств и финансовых активов[37] пополнился необычными объектами в виде наличных денежных средств и транспортных средств. В отношении первых обязанности по декларированию обычно несут чиновники, ну а вторые по понятным причинам были внесены на фоне повального снятия с регистрации яхт и самолетов российской бизнес-элиты в офшорных юрисдикциях.

При этом интригует параллельное принятие пакета мер ответственности за незаконное обогащение чиновников[38], — подобные инициативы ранее Государственной Думой отвергались[39].

Понятно, что в условиях, когда «железный занавес [между Россией и Западом] уже опустили»[40], а гарантии собственности по всему миру претерпевают небывалые испытания, можно ожидать чего угодно: в таких случаях даже введение внешнего управления активами, брошенными в спешке ушедшими с российского рынка иностранными компаниями, выглядит как благо[41].

**АЛЕКСАНДР ПЕТРОВИЧ ЕВСЕЕВ**

доцент департамента систем судопроизводства и уголовного права Национального исследовательского университета «Высшая школа экономики», кандидат юридических наук

## Приглашение на казнь

Кажется, Иосиф Бродский заметил, что его главная тема — время и то, что оно делает с человеком. Сказанное справедливо и для государственно-правовой жизни. Иногда бывает, что политик, начинавший как западник и либерал, с течением времени становится (или, по крайней мере, хочет казаться)

---

[37] В вопросе возврата финансовых активов есть свои подводные камни. К примеру, до сих пор непонятно, как российские власти обеспечат возвращение активов в виде криптовалюты. Для амнистии капитала необходимо перевести их на счета российских банков, в то время как действующее российское регулирование совершать криптовалютные банковские операции пока не позволяет. Несмотря на высокую популярность криптовалюты среди российского населения, Центробанк видит в ней больше угроз, нежели возможностей (см.: https://www.cbr.ru/Content/Document/File/132241/Consultation_Paper_20012022.pdf; дата обращения: 21.03.2022), а Правительство только в начале февраля подошло к концепции легализации криптовалюты (см.: Правительство представило концепцию легализации оборота криптовалют в РФ. Обобщение // Интерфакс. 2022. 8 февр. URL: https://www.interfax.ru/business/820959; дата обращения: 18.03.2022).

[38] Федеральным законом от 06.03.2022 № 44-ФЗ предусмотрено, что обнаружение на счетах чиновников, а также их супругов и несовершеннолетних детей имущества, превышающего их трехлетний заработок, может повлечь прокурорскую проверку.

[39] См., напр.: Госдума отклонила законопроект о наказании за незаконное обогащение // Коммерсантъ. 2018. 17 янв. URL: https://www.kommersant.ru/doc/3522407; В УК РФ могут ввести статью о незаконном обогащении // ИПП «Гарант.ру». 2019. 22 июля. URL: https://www.garant.ru/news/1283292/ (дата обращения: 21.03.2022). Во втором случае речь шла о внесении руководителем фракции «Справедливая Россия» Сергеем Мироновым в Госдуму законопроекта № 757818-7, который так и не прошел первое чтение.

[40] Слова Олега Дерипаски, сказанные на Красноярском экономическом форуме 3 марта. См.: Дерипаска спрогнозировал трехлетний кризис в России // Интерфакс. 2022. 3 марта. URL: https://www.interfax.ru/business/825949 (дата обращения: 21.03.2022).

[41] Такой законопроект уже готовится к внесению в Государственную Думу. См. об этом: ЦБ согласовал проект о внешнем управлении активами покидающего РФ иностранного бизнеса // Интерфакс. 2022. 16 марта. URL: https://www.interfax.ru/business/829556 (дата обращения: 21.03.2022).

**Alexander P. Evseev**
Associate Professor of the School of Court Proceedings and Criminal Law of the Faculty of Law at National Research University "Higher School of Economics", Candidate of Juridical Sciences (e-mail: apevseyev@gmail.com)

**An Invitation to Execution**

почвенником и консерватором. Можно сколь угодно долго повторять слова, приписываемые У. Черчиллю, «тот, кто в юности не был революционером, у того нет сердца; тот, кто остался им в старости, у того нет ума», но факт остается фактом — надежда российских либералов конца нулевых интеллигентнейший Д.А. Медведев дал решительный крен вправо. Свидетельством этому его недавние высказывания о целесообразности восстановления в России смертной казни, которая, по его словам, «активно применяется в США и Китае»[42]. В конце прошлого года аналогичную мысль применительно к умышленным убийствам высказывал и Председатель КС РФ В.Д. Зорькин[43], особым либерализмом никогда не отличавшийся.

Помимо прочего, третий президент заявил, что приостановка членства России в Совете Европы и ПАСЕ — «неплохой повод, наконец, хлопнуть дверью и забыть об этих бессмысленных богадельнях навсегда»[44].

Оставим в стороне манеру, в которой эти идеи были сформулированы, — свойственную, скорее, соседу по лестничной клетке, нежели крупному федеральному чиновнику. Обратимся лучше к их сути. Хотя, как писал Н.А. Бердяев, «ужас, который сейчас происходит, нельзя обсуждать с юридической точки зрения, как-то неуместно аргументировать против смертной казни, да и слишком элементарный это вопрос»[45].

Итак, в крохотном посте Д.А. Медведева сконцентрированы сразу несколько утверждений: 1) смертная казнь — «важный институт для предотвращения особо тяжких преступлений в стране»; 2) она применяется в двух «сверхдержавах» — США и Китае; 3) Совет Европы со всеми своими институциями нам не указ — «бессмысленные богадельни» (слово «богадельня» вообще частый гость медведевского лексикона; вспомним знаменитое «Газпром» — это не богадельня», относящееся к газовым переговорам с Украиной в теперь уже далекие, своего рода «вегетарианские времена»).

Сразу отметим: в США смертная казнь может назначаться как федеральными судами (около 2% от общей массы смертных приговоров), так и судами штатов (98%). Дело в том, что Северная Америка — страна вертикального дуализма, который проявляется в одновременном наличии на каждой территории государства двух не пересекающихся между собой типов судов: федеральных и соответствующего субъекта федерации[46]. Поэтому практика применения смертной казни на федеральном уровне и в каждом из 50 штатов крайне неоднородна.

---

[42] URL: https://meduza.io/news/2022/02/26/horoshaya-vozmozhnost-vosstanovit-ryad-vazhnyh-institutov-tipa-smertnoy-kazni-medvedev-o-sanktsiyah-protiv-rossii (дата обращения: 21.03.2022).
[43] *Зорькин В.Д.* Конституционное правосудие: процедура и смысл. СПб., 2021. С. 80.
[44] URL: https://meduza.io/news/2022/02/26/horoshaya-vozmozhnost-vosstanovit-ryad-vazhnyh-institutov-tipa-smertnoy-kazni-medvedev-o-sanktsiyah-protiv-rossii (дата обращения: 21.03.2022).
[45] Смертная казнь: за и против / сост. О.Ф. Шишов, Т.С. Парфенова. М., 1989. С. 201.
[46] См.: Судоустройство и правоохранительные органы: учебник / под ред. Л.В. Головко. М., 2022. С. 172.

Так, до президентуры Д. Трампа в последний раз смертная казнь («протокол смертельной инъекции») приводилась в исполнение по приговору федерального суда в 2003 году, еще при президенте-республиканце Дж. Буше-младшем. Однако Трамп, прозорливый популист и демагог, в конце своего президентского срока решил сыграть на этой теме в надежде получить дополнительные голоса избирателей. В июне 2020 года генеральный прокурор США У. Барр, выполняя прямое указание президента, распорядился привести в исполнение приговоры федеральных судов в отношении четырех детоубийц, а затем в расписание казней, намеченных до конца года, были внесены имена еще семи осужденных федеральными судами, в том числе одной женщины, осужденной за убийство и киднеппинг, хотя казнь женщин в стране не проводилась уже около 70 лет[47]. Всего же в последние шесть месяцев правления Трампа были казнены 13 человек — самый высокий показатель применения высшей меры за последние 120 лет. Впрочем, как известно, выиграть выборы ему это не помогло.

На региональном уровне смертная казнь никогда не применялась или отменена в 23 штатах, формально сохраняется в 24 штатах, причем в 11 из них на практике она не используется: в Калифорнии — с 2006 года, Нью-Хэмпшире — с 1939, Канзасе — с 1965, Вайоминге — с 1992, Колорадо и Орегоне — с 1997, Пенсильвании — с 1999, Монтане, Неваде и Северной Каролине — с 2006, Кентукки — с 2008 года[48]. При этом данные штаты пытаются отказаться от нее и как от гипотетической возможности. Например, в 2019 году от нее отказался Нью-Хэмпшир, в котором фактически не казнили с рузвельтовских времен, и заменил смертную казнь пожизненным заключением без права помилования (к слову сказать, с точки зрения стандартов ЕСПЧ такой вид наказания ущемляет «право на надежду» и квалифицируется как вид пытки — см. постановление по делу *Винтер против Соединенного Королевства*). Еще в трех штатах действуют моратории на смертные приговоры, наложенные губернаторами.

С Китаем (первое место в мире по числу казней) ситуация выглядит сложнее. Как и подобает закрытой азиатской стране, Поднебесная не публикует официальную статистику о количестве вынесенных и приведенных в исполнение смертных приговоров. *Amnesty International*, международная неправительственная организация, постоянно мониторящая эту тему, с 2009 года даже перестала публиковать оценочные данные о применении смертной казни в Китае, предполагая, однако, что количество таких приговоров составляет более тысячи в год (впрочем, не так уж и много по меркам полуторамиллиардной страны). Таким образом, возникает вопрос: можно ли американский и китайский кейсы ставить на одну доску, как это делает Д.А. Медведев? Очевидно, что нет. В первом из них смертная казнь фактически не применяется, а во втором — соответствующие данные засекречены, что само по себе вызывает вопросы.

---

[47] См.: *Квашис В.Е.* О новых тенденциях и перспективах института смертной казни в США // Общество и право. 2020. № 4. С. 9.

[48] URL: https://www.pewresearch.org/fact-tank/2019/03/14/11-states-that-have-the-death-penalty-havent-used-it-in-more-than-a-decade/ (дата обращения: 21.03.2022).

Впрочем, «хватит о дальнем береге». Обратимся к опыту царской России, давно и по праву считающейся у нас эталоном законопослушания и хороших манер ее подданных. В этой связи не будем апеллировать к истории, когда для казни народовольцев по всей России не могли сыскать палача. Не станем мы и упоминать глубокую традицию аболиционизма, представленную именами Л.Н. Толстого, Ф.М. Достоевского, И.С. Тургенева, В.Г. Короленко, других представителей русской интеллигенции, с которыми невозможно спорить, а можно только, как писал дореволюционный юрист В.Д. Набоков, отец будущего писателя В. В. Набокова, «зажать уши и зажмурить глаза…». Просто обратимся к сухой статистике.

Пореформенная Россия сохранила смертную казнь за государственные преступления. С 1866 по 1895 год, т.е. почти за 30 лет, суды вынесли 137 смертных приговоров, из которых в исполнение были приведены всего лишь 44, а 93 заменены вечной или срочной каторгой[49]. По подсчетам М.Н. Гернета, даже после подавления революции 1905 года в тот год было реально казнено лишь 10 человек, годом позже — 144[50]. Правда, по приговорам военно-полевых судов в 1906–1907 годах были казнены уже 683 человека[51].

Показательна статистика послевоенных лет (1950–1990 годы). В общей структуре примененных судами мер наказания смертная казнь составляла 0,1%, а в 1985–1989 годах — 0,04% (в абсолютных величинах от 770 смертных приговоров в 1985 году до 276 в 1989-м)[52]. При этом, как свидетельствует статистика, в советские годы к смертной казни приговаривали в основном за три вида преступлений: умышленное убийство при отягчающих обстоятельствах, измена Родине и бандитизм (почти никогда — за изнасилование при особо отягчающих обстоятельствах). С 1963 года, после дела Рокотова и Файбишенко, ни за фальшивомонетничество, ни за нарушение правил о валютных операциях смертная казнь не назначалась.

Как видим, отказ государства от данной формы реакции на преступление или сведение ее к минимуму — *объективная* и *необратимая* тенденция, наблюдаемая как в общемировом масштабе (за исключением традиционно менее развитой в правовом отношении Азии), так и в рамках нашей страны.

Возвращаясь в день сегодняшний, нельзя не отметить, что в Конституции РФ 1993 года смертная казнь рассматривалась сугубо в качестве «исключительной меры наказания за особо тяжкие преступления против жизни», да и то с оговоркой касательно предоставления обвиняемому права на рассмотрение его дела судом с участием присяжных заседателей (ч. 2 ст. 20). Дело в том, что в то время общественное сознание еще не было готово принять полную отмену смертной казни. По данным социологического опроса, проведенного ВЦИОМ в 1994 году, 37% респондентов высказались за сохранение смерт-

---

[49] См.: *Яковлева З.* О смертной казни в СССР // Социалистическая законность. 1991. № 4. С. 45.
[50] См.: Смертная казнь: за и против. С. 144.
[51] См. там же.
[52] См.: *Яковлева З.* Указ. соч. С. 44.

ной казни в законодательстве, а еще 24% предложили расширить сферу ее применения[53]. По этой причине создателям Конституции смертная казнь виделась как временная исключительная мера «впредь до ее отмены», т.е. на ограниченный переходный период. Однако там, где не способен сказать свое слово народ и даже конституционный законодатель, должен вмешаться Конституционный Суд, что, собственно, он и сделал дважды.

Первый раз — в 1999 году, установив, что до тех пор, пока во всех субъектах РФ не созданы суды присяжных, смертная казнь не может назначаться по приговору суда. Иное ставило бы наших граждан в неравные условия и противоречило бы принципу правовой определенности. Второй — десятью годами позже, когда было принято Определение КС РФ № 1344-О-Р, в котором тот указал, что мораторий на смертную казнь нельзя в сложившихся условиях рассматривать как временную меру, поскольку и после введения суда присяжных во всех субъектах смертная казнь не может применяться, в связи с чем законодатель должен исключить эту санкцию из уголовного законодательства как фактически устаревшую, противоречащую международным обязательствам и недействующую.

Так что Европейский суд здесь ни при чем. Это — прямо и недвусмысленно сформулированная правовая позиция отечественного органа конституционной юрисдикции, преодолеть которую в состоянии лишь сам КС РФ. Нарушить же ее — означает тем самым расписаться в том, что решения КС РФ не имеют никакой юридической силы.

Можно привести еще массу аргументов против смертной казни, например: само ее наличие или отсутствие никак не влияет на динамику преступности; во многом эта мера носит, скорее, символическое значение по принципу «око за око», нежели реально помогает бороться с преступностью; смертная казнь отнюдь не смягчает общественные нравы, скорее наоборот. Российский ученый-юрист И.Я. Фойницкий вспоминал, как во Франции, где наиболее деятельно работала гильотина, этот инструмент в виде игрушки был едва ли не в каждом доме: дети для забавы гильотинировали птиц, собак, кошек и т.п.[54] Кроме того, всегда существует риск судебной ошибки.

Но дело даже не в этом. Русская власть издревле стремилась извлечь пользу из подсознательного влечения народа к человеческому жертвоприношению и продолжает играть на данной чувствительной струне сегодня. Но не таков русский человек. Вспомним мудрые слова Н.С. Таганцева: «Русский народ не пойдет за теми, кто зовет на погромы и разрушения. Но если бы эта вера моя оказалась неосновательной, ложной, то и тогда я позволил бы себе одно: обратиться к Всеблагому Подателю жизни, чтобы он взял и меня отсюда, из этой юдоли вражды и ненависти, но никогда не пойду в тот стан, который требует крови и жертв»[55].

---

[53] См.: *Дубин Б.* Цена жизни и границы права: россияне о смертной казни, российском законе и суде // Вестник общественного мнения. 2007. № 6. С. 18.
[54] Смертная казнь: за и против. С. 269.
[55] Там же. С. 161.

**ГЕННАДИЙ АЛЕКСАНДРОВИЧ ЕСАКОВ**

доктор юридических наук, профессор, ведущий научный сотрудник сектора уголовного права, уголовного процесса и криминологии Института государства и права Российской академии наук

**Gennady A. Esakov**

Leading Research Fellow of Criminal Law, Criminal Procedure and Criminology Department at the Institute of State and Law of the Russian Academy of Sciences, Doctor of Juridical Sciences, Professor (e-mail: gesakov@gmail.com)

**Criminal Legislation of the [Special Operation] Time**

# Уголовное законодательство [спецоперационного] времени*

Чрезвычайные времена требуют экстренных решений. И вот Государственная Дума извлекла из пыльных запасников седьмого созыва два законопроекта, № 464757-7 и № 1197680-7, меняющие соответственно УК РФ и КоАП РФ. Как бы забыв о требованиях регламента, которые запрещают менять концепцию законопроекта при его принятии во втором чтении, по сути проигнорировав требование ст. 8 Федерального закона от 13 июня 1996 года № 64-ФЗ о необходимости отзыва ВС РФ (который, конечно, на исходную версию законопроекта давал отзыв, но мы же ведь понимаем, что по существу своему это был отзыв на иной проект и иную концепцию), Дума приняла законопроекты во всех оставшихся чтениях утром. В тот же день отправила их в Совет Федерации с тем, чтобы ближе к ночи с 4 на 5 марта уже подписанные законы, № 31-ФЗ и № 32-ФЗ, были опубликованы на портале *pravo.gov.ru* и вступили в силу.

Оговоримся, что дата их вступления в силу неясна: в пользу «с 4 марта» говорит Обзор по отдельным вопросам судебной практики, связанным с применением законодательства и мер по противодействию распространению на территории Российской Федерации новой коронавирусной инфекции (*COVID-19*) № 1 (утв. Президиумом ВС РФ 21 апреля 2020 года), вопрос 14, и Постановление Президиума ВС РФ от 27 сентября 2006 года по делу № 443П06. В пользу «с 5 марта» — Определение ВС РФ от 26 июля 2010 года по делу № 86-Д10-3 и Постановление КС РФ от 24 октября 1996 года № 17-П. Нам импонирует вторая точка зрения просто потому, что утром 4 марта еще никаких законов и в помине не было[56].

В уголовном законе появились три новых статьи. Статья 207.3 УК РФ, или публичное распространение заведомо ложной информации об использовании Вооруженных Сил РФ. Сразу можно сказать, что страшилки в виде 15 лет лишения свободы по ч. 3 этой статьи так и останутся, видимо, страшилками просто потому, что представить себе удовлетворительную конструкцию тяжких последствий (например, нарушение планов деятельности Вооруженных Сил РФ, дезорганизация финансово-хозяйственной ситуации, крупные экономические потери и т.п.), причинной связи и неосторожности (и тем более умысла) в связи с деянием крайне проблематично.

Что же касается ч. 1 и 2 статьи, то очевидным прообразом здесь стали «коронавирусные» ст. 207.1 и 207.2 УК РФ. Соответственно, к ним применимы

---

* Пока эта заметка готовилась к печати, Государственная Дума вновь с отступлением от своего регламента в ускоренном режиме готовится принять два законопроекта, № 9712-8 и 9732-8, расширяющие область наказуемых по ст. 207.3 и 280.3 УК РФ действий. В принципе, уже проще восстановить ст. 70 УК РСФСР 1960 г. в ее исходной редакции, чем плодить такое множество отдельных норм.

[56] Для исторической справки по этому вопросу сошлемся еще на решение Сената № 1910/22 по вопросу о применении закона 6 июня 1909 года об усилении ответственности за похищение лошадей и крупного домашнего скота и определение ВС СССР от 29.10.1947 по делу Старикова и Усольцева.

разъяснения, данные в «короновирусном» обзоре № 2 (утв. Президиумом ВС РФ 30 апреля 2020 года), в частности:

1) под *заведомо ложной информацией* следует понимать такую информацию (сведения, сообщения, данные и т.п.), которая изначально не соответствует действительности, о чем достоверно было известно лицу, ее распространявшему. Характер такой информации может быть самый разнообразный: о боевых операциях, потерях, пленных, нарушениях норм международного гуманитарного права и т.д. Можно предположить, что заведомая ложность будет устанавливаться на практике исходя из одного лишь факта несоответствия информации официально распространяемой Вооруженными Силами РФ или иными органами государственной власти (главное, отличать здесь официальную позицию, на соответствие которой будет проверяться распространяемая обвиняемым информация, от личной позиции того или иного должностного лица)[57];

2) распространение заведомо ложной информации должно быть под видом *достоверной*. О придании ложной информации вида достоверной могут свидетельствовать, например, формы, способы ее изложения (ссылки на компетентные источники, высказывания публичных лиц и пр.), использование поддельных документов, видео- и аудиозаписей либо документов и записей, имеющих отношение к другим событиям. По своей форме информация может преподноситься, к примеру, в виде утверждений или слухов, но за исключением оценочных суждений и личного мнения;

3) размещение лицом в Интернете, в частности на своей странице или на странице других пользователей, материала, содержащего ложную информацию (например, видео-, аудио-, графического или текстового), созданного им самим или другим лицом (в том числе так называемый репост), может быть квалифицировано по данной статье только в случаях, когда установлено, что лицо действовало с прямым умыслом, сознавало, что размещенная им под видом достоверной информация является ложной, и имело цель довести эту информацию до сведения других лиц;

4) распространение заведомо ложной информации следует признавать *публичным*, если такая информация адресована группе или неограниченному кругу лиц и выражена в любой доступной для них форме (например, в устной, письменной, с использованием технических средств). Вопрос о наличии признака публичности распространения информации суды должны разрешать с учетом места, способа, обстановки и других обстоятельств. При этом следует учитывать: публичный характер распространения заведомо ложной информации может проявляться в использовании для этого средств массовой информации, информационно-телекоммуникационных сетей, в том числе мессенджеров (*WhatsApp*, *Viber* и др.), в массовой рассылке электронных

[57] В судебной практике по ст. 207.1 УК РФ заведомая ложность отрицания коронавируса иногда по сути презюмируется исходя из общеизвестности факта эпидемии коронавируса (определение Седьмого кассационного суда общей юрисдикции от 09.11.2021 по делу № 77-4915/2021).

сообщений абонентам мобильной связи, распространении такой информации путем выступления на собрании, митинге, распространения листовок, вывешивания плакатов и т.п. Что касается размещения информации в социальных сетях, то здесь не имеет юридического значения закрытый характер группы, которой рассылается информация или которая имеет доступ к такой информации. Однако по смыслу уголовного закона не может признаваться публичным распространение информации близким лицам.

Статья 280.3 УК РФ сконструирована достаточно сложно и неопределенно. Понятие дискредитации в ней противоположно в целом понятию оправдания в ст. 205.2 УК РФ и может быть определено как заявление о признании использования Вооруженных Сил РФ в соответствующих целях неправильным, не нуждающимся в поддержке или повторении, сомнения в нужности или целесообразности их использования, ссылки на неправомерность такого использования, указания на неэффективность использования[58]. К дискредитации относится также отрицание наличия целей использования Вооруженных Сил РФ в конкретных ситуациях, а равно использование таких наименований, как «война», «агрессия», «геноцид» и других подобных терминов, означающих международные преступления. Частный случай дискредитации приведен в диспозиции — это публичные призывы к воспрепятствованию использования Вооруженных Сил РФ в соответствующих целях, т.е. адресованные неограниченному кругу лиц или органам власти предложения или требования пресекать либо прекратить такое использование (призывы при этом необязательно должны быть успешными). Раскрытые выше признаки публичности и распространения (поскольку дискредитация может выражаться и в распространении информации) в полной мере приложимы и к этому составу преступления.

Судебная практика по новой ст. 20.3.3 КоАП РФ уже дает яркие оригинальные примеры трактовки аналогичной административной нормы[59]: это не просто банальное «нет…» (о да, у нас появилось свое *N*-слово!) на листе бумаги, в социальных сетях, но и те же слова, вытоптанные на снегу и даже просто обозначенные (как то сочли правоохранительные органы) на листе бумаги звездочками, лист бумаги с заповедью «не убий», ношение одежды цветов флага сопредельного государства, воскресные проповеди священников. В этом году в Вербное воскресенье, когда в римско-католических церквях будут читать Страсти от Луки, оглашать в церкви главу 22 (стихи 49–51) Евангелия от Луки, видимо, будет рискованно. А уж про литургию Великого четверга в православии с ее Евангелием от Матфея (глава 26, стих 52) даже думать боязно!

---

[58] Для сравнения можно привести приговор по ст. 207.1 УК РФ, где размещение призывов, направленных неограниченному кругу граждан независимо от их возраста, места работы и состояния здоровья, выходить на улицу вопреки установленным запретам, фотографировать себя на улице и выкладывать эти фотографии в соцсетях в знак протеста с режимом изоляции, а также публичное отрицание пандемии коронавируса было расценено в том числе как дискредитация законной деятельности органов государственной и исполнительной власти (определение Седьмого кассационного суда общей юрисдикции от 09.11.2021 по делу № 77-4915/2021).

[59] Приводимые примеры взяты исключительно из средств массовой информации и потому могут быть неточны; на портале ГАС «Правосудие» к моменту написания этой заметки полных текстов решений еще не было.

Первая часть статьи требует административной преюдиции (ст. 20.3.3 КоАП РФ), тогда как вторая предполагает уголовную ответственность сразу, но при условии наступления определенных в диспозиции последствий. Здесь таится своего рода подводный камень: исходя из сложившейся административной практики, в качестве призывов могут рассматриваться и призывы к организации массовых мероприятий против такого использования. В случае если такие мероприятия в итоге проходят и влекут последствия (например, массовые нарушения общественного порядка, общественной безопасности, помехи функционированию или прекращение функционирования объектов жизнеобеспечения, транспортной или социальной инфраструктуры), действия по призывам к ним могут квалифицироваться как преступление по ч. 2 статьи без предшествующей административной преюдиции («неудачные» призывы к массовым мероприятиям прямо предусмотрены ч. 2 ст. 20.3.3 КоАП РФ).

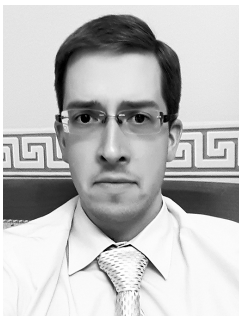
Проще в сравнении с двумя предшествующими новыми нормами сформулирована ст. 284.2 УК РФ, также требующая административной преюдиции по ст. 20.3.4 КоАП РФ. Наказуемое деяние представляет собой предложение, адресованное за рубеж, о введении санкций. При этом состав преступления имеет место независимо от того, являлось ли такое предложение успешным (т.е. были введены санкции или нет).

Призывы не обязательно должны быть публичными, т.е. могут содержаться и в частной переписке. При их распространении в Интернете для установления признаков состава преступления можно ориентироваться на высказанные выше суждения.

Один из самых небесспорных моментов в связи с распространением информации и призывов в Интернете связан с толкованием судебной практикой времени совершения преступления. Размещение материалов в Интернете (в том числе репост) рассматривается как своего рода длительное преступление (именовать его «длящимся» исходя из чистоты терминологии некорректно), не ограниченное временем размещения материала. Поэтому срок давности для привлечения к уголовной ответственности за это преступление (ст. 78 УК РФ) начинает течь или с момента удаления материала из публичного доступа в Интернете, или с момента обнаружения противоправных действий сотрудниками правоохранительных органов. Эта правовая позиция была сформулирована в Постановлении ВС РФ от 13 августа 2021 года по делу № 81-АД21-9-К8, вынесенному в связи с размещением в Интернете информации, выражающей в неприличной форме, которая оскорбляет человеческое достоинство и общественную нравственность, явное неуважение к обществу, государству, официальным государственным символам Российской Федерации, Конституции РФ или органам, осуществляющим государственную власть в Российской Федерации (ч. 3 ст. 20.1 КоАП РФ)[60].

[60] Аналогичный подход встретился в судебной практике по ст. 298.1 УК РФ, когда размещение клеветнических материалов на портале *pravo.ru* имело место до введения в УК РФ указанной статьи. Однако суд счел, что «поскольку клеветнические комментарии, которые оставались размещенными на информационном портале в интернете и продолжали быть доступными просмотру неограниченному кругу лиц, выявлены… в период действия ст. 298.1 УК РФ, ряд тождественных действий ФИО1 верно оценены

Данный подход не является бесспорным с точки зрения понимания времени совершения преступления в ч. 1 ст. 9 УК РФ, однако именно он создает риски привлечения к уголовной или административной ответственности по новым нормам всех тех, кто разместил соответствующие посты в Интернете, в том числе до 5 марта с.г., и не удалил их вплоть до настоящего дня.



**ПАВЕЛ ДМИТРИЕВИЧ БЛОХИН**

доцент юридического факультета Национального исследовательского университета «Высшая школа экономики», кандидат юридических наук

**Pavel D. Blokhin**

Associate Professor of the Faculty of Law at National Research University "Higher School of Economics", Candidate of Juridical Sciences (e-mail: pavel.blokhin@ksrf.ru)

**Constitutional Court, Unfair Competition and Economics of Law**

## Конституционный суд, недобросовестная конкуренция и экономика права

Еще в начале 1990-х годов талантливый ученый-конституционалист А.А. Белкин положил начало такому жанру правовых исследований, как комментарий к практике КС РФ. Предметом интереса автора были преимущественно решения по вопросам государственного строительства (федеративного устройства, разделения властей и пр.). Причем анализ этих решений не ограничивался формально-догматическим методом, а в большой степени опирался на общественно-политический контекст[61]. В последующие десятилетия, как представляется, этот жанр получил некоторое развитие ввиду того, что в фокусе внимания ученых все чаще оказываются решения по вопросам гражданского права и смежных дисциплин; в связи с этим к известным ранее методам анализа добавляются сравнительно-правовой, экономико-правовой и иные[62]. Напротив, вопросы антимонопольного права, среди которых немалое место занимает проблема недобросовестной конкуренции, долгие годы не ставились перед КС РФ. Соответственно, не было и возможности проследить, в какой степени экономико-правовые (или иные) соображения могут быть востребованы при решении такого рода споров. Опубликованное в феврале этого года Постановление по делу о проверке конституционности ст. 14.8 и 51 Федерального закона «О защите конкуренции» в связи с жалобой общества с ограниченной ответственностью «Медэксперт»[63] дает шанс восполнить этот пробел.

Фабула данного дела состояла в следующем: заявитель был признан нарушившим законодательство о защите конкуренции в связи с участием в электронном аукционе, поскольку в представленной им лицензии был указан иной адрес, чем тот, по которому ему предстояло оказывать медицинские услуги заказчику. Заявителю было предписано перечислить в федеральный бюджет

---

судом как единое преступление, а довод осужденной об отсутствии состава преступлений обоснованно признан ошибочным» (апелляционное постановление Курского областного суда от 25.02.2015 по делу № 22-169/2015. URL: https://clck.ru/dgy2u; дата обращения: 21.03.2022).

Эта правовая позиция в полной мере применима к ситуациям с новыми статьями уголовного закона в случае обвинений, основанных на постах в Интернете, размещенных до 5 марта с.г., но доступных и после этой даты.

[61] См.: *Белкин А.А.* Комментарии к решениям Конституционного Суда Российской Федерации 1992–1993. СПб., 1994.

[62] См., напр.: *Лоренц Д.В.* Экономический анализ позиций Конституционного Суда РФ относительно защиты права собственности // Законодательство и экономика. 2016. № 1.

[63] Постановление КС РФ от 17.02.2022 № 7-П.

сумму средств, полученных им в результате частичного исполнения заключенного контракта и оказания упомянутых услуг.

Вследствие этого в жалобе ставились два взаимосвязанных и при этом вполне самостоятельных правовых вопроса. Во-первых, является ли одной из форм недобросовестной конкуренции (перечень которых в законе является открытым) участие некоторого лица в электронном аукционе на оказание медицинских услуг в отсутствие у него надлежащим образом оформленной лицензии на осуществление медицинской деятельности? Во-вторых, должно ли лицо, в отношении которого антимонопольным органом установлен факт недобросовестной конкуренции, перечислить по предписанию последнего в федеральный бюджет всю сумму дохода от исполнения контракта, или оно вправе учесть произведенные им расходы?

Следует отметить, что, хотя и предмет рассмотрения по делу (п. 1.4 мотивировочной части), и конституционно-правовое истолкование оспоренного регулирования (пункт 1 резолютивной части) в значительной степени предопределены описанными выше обстоятельствами дела (электронный аукцион; лицензия), правовые позиции в мотивировочной части решения охватывают более широкий круг обстоятельств, так как используют в ряде случаев обобщающие категории (осуществление закупок; разрешение, позволяющее осуществлять деятельность по исполнению контракта). В то же время, по-видимому, не охватываются этими позициями иные составы антимонопольных правонарушений, такие, например, как злоупотребление доминирующим положением, поскольку они не являлись и не могли являться предметом оценки Суда по данному делу.

В отношении первого вопроса правовая позиция КС РФ изложена в п. 3.2 мотивировочной части и состоит в следующем: «…*статья 14.8 Федерального закона «О защите конкуренции» не предполагает, что участие хозяйствующего субъекта в электронном аукционе и исполнение заключенного по его результатам контракта в отсутствие у него надлежаще оформленной лицензии, позволяющей осуществлять соответствующую деятельность, должно быть признано недобросовестной конкуренцией, если такое несоответствие требованиям законодательства может быть установлено комиссией по осуществлению закупок в рамках исполнения ею своих обязанностей при обычной внимательности и осмотрительности, а хозяйствующий субъект не совершил каких-либо действий (бездействия), специально направленных на сокрытие этого несоответствия*». Тем самым КС РФ, по существу, вплотную подошел к тому, чтобы признать: недобросовестная конкуренция в рассматриваемой форме, в отличие от некоторых иных составов антимонопольных нарушений, может иметь место лишь при наличии умышленной формы вины[64]. В итоге Суд сделал обоснованный (в частности, положениями конкурентного законо-

[64] Следует признать, что в литературе высказывались несовпадающие точки зрения по вопросу о необходимости установления и учета формы вины при привлечении к ответственности в антимонопольном праве (см., напр.: *Корчак Н.Н.* Доктрина «поведенческого подхода» вины при установлении субъективных условий ответственности в сфере конкуренции // Lex Russica. 2013. № 11).

дательства и законодательства о государственных закупках) вывод о том, что иной подход означал бы нарушение принципа справедливости (соразмерности) при ограничении свободы экономической деятельности.

Безусловно, несоответствие хозяйствующего субъекта требованиям, установленным заказчиком в соответствии с законом (к лицензии, сертификату, членству в СРО и пр.), должно влечь неблагоприятные правовые последствия вне зависимости от того, вызвано ли такое несоответствие злонамеренностью или деловым просчетом. Эти последствия состоят как в отклонении заявки на участие в торгах такого субъекта[65], так и, в случае если контракт с ним все же был заключен и начал исполняться, в привлечении к ответственности, например за занятие предпринимательской деятельностью с нарушением условий разрешения (лицензии)[66]. Однако те последствия, которые лежат в плоскости антимонопольного регулирования, могут наступать лишь при соблюдении условий, очерченных КС РФ и процитированных выше.

Представляется, что иной подход не отвечал бы экономико-правовым представлениям о том, какое распределение рисков между участниками закупочных процедур является экономически эффективным. Возложение установленной ст. 14.8 Закона о защите конкуренции ответственности на потенциального исполнителя за любые дефекты разрешительной документации, в том числе носящие формальный характер, лишало бы добросовестного (в широком, гражданско-правовом смысле) субъекта стимула участвовать в закупках под угрозой признания его недобросовестным (в автономном, антимонопольном значении) конкурентом. Так, из имевшихся в деле материалов следовало, что ООО «Медэксперт» уведомляло заказчика ФГБОУ «МарГУ» о намерении оказывать ему медицинские услуги по месту нахождения последнего с использованием мобильной бригады[67]. При этом сведения об адресе осуществления медицинской деятельности, указанные в лицензии общества, были доступны как закупочной комиссии, так и его конкурентам в соответствующем открытом реестре.

Одновременно у закупочной комиссии, создаваемой заказчиком, уменьшался бы стимул ответственно и добросовестно исполнять свои обязанности по отбору исполнителя. Это приводило бы к тому, что несоответствие его предъявляемым требованиям выявляется уже после заключения контракта и начала его исполнения. Так, хотя в анализируемом деле все три члена закупочной комиссии были признаны нарушившими порядок осуществления закупок, они были освобождены от ответственности, поскольку данное административное правонарушение признано малозначительным, не повлекшим серьезной угрозы обществу[68].

---

[65] Часть 1 и подп. «а» п. 1 ч. 5 ст. 49 Федерального закона от 05.04.2013 № 44-ФЗ «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд».
[66] Статья 14.1 КоАП РФ.
[67] См., в частности: решение Верховного суда Республики Марий Эл от 16.01.2019 по делу № 7р-18/2019.
[68] См. там же.

При этом предложенный КС РФ подход, напротив, лишает стимулов именно хозяйствующих субъектов, заведомо не соответствующих требованиям заказчика, принимать участие в торгах и пытаться скрыть такое несоответствие, в частности сообщив заведомо недостоверные сведения в заявке или приложив к ней подложные документы. Общественная вредность таких действий очевидна: несоответствие требованиям в этом случае намного сложнее обнаружить, а закупочная комиссия и конкуренты вынуждены затрачивать больше сил для выявления такого недобросовестного лица.

В отношении второго вопроса КС РФ в п. 4 мотивировочной части сформулировал следующую правовую позицию: «*…не исключается возложение на нарушителя законодательства о защите конкуренции при определенных исключающих иной подход обстоятельствах (в частности, если в результате недобросовестной конкуренции причинен значительный, явный и прямой ущерб хозяйствующим субъектам — конкурентам или соответствующее деяние носило грубый характер) обязанности перечислить в федеральный бюджет в качестве «дохода, полученного от монополистической деятельности или недобросовестной конкуренции» все полученное от совершения такого деяния*». Из изложенной позиции можно сделать вывод о том, что Суд фактически устранил существовавшую правовую неопределенность понятия «доход», отказавшись понимать под таковым прибыль (доходы минус обоснованные и документально подтвержденные расходы).

Такое понимание, следует признать, не лишено оснований: в отличие от ныне действующего регулирования Закон РСФСР «О конкуренции и ограничении монополистической деятельности на товарных рынках» (в редакции от 25 мая 1995 года) говорил о перечислении в федеральный бюджет именно «прибыли», полученной вследствие антимонопольного нарушения, — вероятно, отказавшись от этой терминологии, законодатель выразил тем самым свою политическую волю. В тех же случаях, когда законодатель желает «очистить» доходы от понесенных расходов, он может прямо указать на это в соответствующих положениях.

Между тем отсутствие неопределенности нормы в затронутом заявителем контексте не означает безусловной соразмерности (справедливости) предусмотренного ею правоограничения. Для оценки этого обстоятельства, как представляется, может быть полезным определение экономико-правовой природы данного ограничения. В науке считается общепризнанным, что меры ответственности, в том числе и имущественной, могут преследовать компенсационную (восстановительную) или штрафную (карательную) цели или обе сразу. Для ответственности в виде возмещения убытков характерны свойства адресности (возмещение осуществляется в пользу того лица, которому нанесен имущественный вред) и эквивалентности (возмещение призвано максимально полно восстановить нарушенную имущественную сферу потерпевшего). Для ответственности в виде штрафа, в том числе административного, эти свойства нехарактерны, поскольку вне зависимости от фигуры потерпевшего штраф уплачивается в бюджет бюджетной системы РФ, а величина такого штрафа обычно не связана с величиной ущерба. Промежуточное положение занимает сверхкомпенсационная ответственность, аналогичная

статутным убыткам *(statutory damages)*, которая, хотя взыскивается в пользу пострадавшей стороны, лишь условно связана с размером причиненного вреда; последняя выполняет, таким образом, как восстановительную, так и карательную функцию.

Предусмотренная ст. 51 Закона о защите конкуренции мера имеет выраженные штрафные признаки. Вне зависимости от того, кто являлся заказчиком товаров (работ, услуг) и понес ущерб в связи с необходимостью расторжения контракта и проведения новых закупочных процедур, доход нарушителя от недобросовестной конкуренции поступает в федеральный бюджет и притом не имеет целевого назначения. Что же касается конкурента правонарушителя, который получил бы право заключить контракт, не будь совершен акт недобросовестной конкуренции, то возмещение ему убытков осуществляется в порядке гражданского судопроизводства[69]. Штрафной характер рассматриваемой меры подтверждается и тем, что лицо, перечислившее в бюджет незаконный доход, освобождается от привлечения к административной ответственности[70].

Между тем КС РФ неоднократно признавал применительно как к административным штрафам[71], так и к компенсации за нарушение исключительных прав[72], что справедливость и соразмерность мер штрафного характера допущенному правонарушению требует учета судом «тяжести содеянного, размера и характера причиненного ущерба, степени вины правонарушителя и иных существенных обстоятельств, обусловливающих индивидуализацию при применении тех или иных мер государственного принуждения», не исключая и «материального положения ответчика». В противном случае такая санкция перестает выполнять свою основную функцию — общей и специальной превенции и рискует превратиться в инструмент подавления экономической инициативы[73]. Следовательно, законодатель мог бы предусмотреть механизм, который позволял бы снизить в разумных пределах размер взыскиваемой в бюджет суммы менее величины незаконного дохода.

Приведенные правовые позиции КС РФ уже получили некоторое развитие в его практике[74]; хочется надеяться, что дальнейшему их развитию будут способствовать также и усилия ученых.

---

[69] Часть 3 ст. 37 Федерального закона «О защите конкуренции».
[70] Часть 3 ст. 51 Федерального закона «О защите конкуренции» и примечание 5 к ст. 14.31 КоАП РФ.
[71] Постановление КС РФ от 17.01.2013 № 1-П.
[72] Постановление КС РФ от 13.12.2016 № 28-П.
[73] В литературе высказывалось мнение о том, что возможность требовать с нарушителя возмещения убытков (упущенной выгоды) в пользу конкурента и одновременно взыскания дохода в пользу федерального бюджета есть двойное привлечение к одной и той же ответственности (см.: *Егорова М.А.* Гражданско-правовые последствия нарушений антимонопольного законодательства: монография. М., 2020).
[74] Определение КС РФ от 24.02.2022 № 468-О.

Объединение Корпоративных Юристов

# ЧТО НАС ЖДЕТ ЗА ГОРИЗОНТОМ: КОНФЕРЕНЦИЯ ОКЮР О ВЫЗОВАХ 2022 ГОДА

**Василий Малинин**, партнер юридической фирмы «Рустам Курмаев и Партнеры»; **Виктор Домшенко**, руководитель отдела судебной защиты Блока по правовым вопросам «Почты России»; **Полина Лебедева**, исполнительный директор, директор практики консультационных услуг в области управления юридической функцией и комплаенс-функцией *PricewaterhouseCoopers Legal* в России; **Маргарита Белякова**, руководитель направления по корпоративно-правовым вопросам «Метафракс групп»; **Александра Нестеренко**, президент ОКЮР; **Янина Станюленайте**, вице-президент по правовым вопросам «Евраз Холдинг»; **Андрей Донцов**, партнер *White&Case*; **Алла Генералова**, руководитель юридической практики «СИБУР»; **Наталья Кузьмина**, руководитель направления «АЛРОСА»; **Юлия Филиппова**, старший директор по юридическим вопросам, Центральная и Восточная Европа, *Avon*; **Анна Игнатенко**, руководитель юридического департамента фонда «Айрис»

* Релиз подготовлен пресс-службой ОКЮР.

**Вера Рихтерман**, партнер АБ ЕПАМ; **Павел Громов**, директор юридического департамента «Ашан»

**Василий Малинин**, партнер юридической фирмы «Рустам Курмаев и Партнеры»; **Виктор Домшенко**, руководитель отдела судебной защиты Блока по правовым вопросам «Почты России»

Стремительное развитие права порождает возникновение новых концепций и парадигм его понимания. Как юридическому сообществу формировать эффективный механизм развития, отвечающий правовой реальности? Вызовам 2022 года посвятила конференцию Ассоциация «Некоммерческое партнерство «Объединение Корпоративных Юристов», которая состоялась 25 февраля.

На открытии конференции **Александра Нестеренко**, президент Ассоциации, поделилась с участниками уверенностью в победе корпоративных юристов над страхами, возникающими на пути к устойчивому развитию, и напомнила: «Времена не выбирают, в них живут и побеждают».

Открывая пленарную сессию, **Екатерина Салугина-Сороковая**, генеральный директор АНО «Центр международных и сравнительно-правовых исследований», отметила, что значимость *ESG*-повестки определена изменением ценностной парадигмы в обществе, достижением определенного уровня зрелости: современный человек уделяет все больше внимания вопросам охраны окружающей среды, социальной ответственности, качества корпоративных процедур. Екатерина обозначила ландшафт нормативно-правового регулирования в сфере устойчивого развития и уделила особое внимание текущим инициативам в этой сфере.

**Сергей Ситников**, партнер, глава *ESG*-практики юридической фирмы «ЕМПП», предложил потенциальную стратегию для проведения *ESG*-трансформации компании, включая практические шаги. В их числе: назначение главы департамента устойчивого развития, проведение анализа текущего состояния на предмет учета *ESG*-факторов, определение цели устойчивого развития и подготовка *ESG*-стратегии. По мнению Сергея, важно проверить на готовность к изменениям внутренние процедуры и корпоративную политику, контрагентов, а также определить проекты, которые можно реализовать в рамках стратегии устойчивого развития и найти новые источники финансирования проектов.

Далее в своем выступлении **Руслан Васютин**, партнер *DLA Piper*, рассказал об основных механизмах и новых правилах налогообложения в России и в рамках за-

**Руслан Васютин**, партнер *DLA Piper*

**Юрий Донников**, директор юридического департамента и комплаенс *HeadHunter*

**Сергей Ситников**, партнер, глава *ESG*-практики, юридическая фирма «ЕМПП»

рубежного правового поля. В завершение выступления участники рассмотрели ключевые тенденции в подходах фискальных органов на примере конкретных кейсов. «Налоговое планирование стало управлением налоговыми рисками», — подвел итог Руслан.

**Роман Головацкий**, советник *DLA Piper*, рассказал о специфике текущего регулирования искусственного интеллекта в Российской Федерации и зарубежном законодательстве. Он указал на перспективные направления регулирования в данной сфере, в особенности на планируемый к принятию новый регламент Европейского союза — *AI Act*.

Свою точку зрения на навыки работы с *ESG* высказал **Юрий Донников**, директор юридического департамента и комплаенс *HeadHunter*. Он рассказал о формах выражения концепции устойчивого развития в контексте деятельности компании *HeadHunter* и отметил: «Согласно данным *hh.ru*, с 2019 по 2021 год наблюдается уверенный рост спроса на специальности с упоминанием *ESG*. Топ-3 отраслей в 2021 г. составляют финансовый сектор, услуги для бизнеса и информационные технологии». Также Юрий назвал сферы, на которые в настоящий

**Юлия Филиппова**, старший директор по юридическим вопросам, Центральная и Восточная Европа, *Avon*; **Маргарита Белякова**, руководитель направления по корпоративно-правовым вопросам «Метафракс групп»; **Полина Лебедева**, исполнительный директор, директор практики консультационных услуг в области управления юридической функцией и комплаенс-функцией *PricewaterhouseCoopers Legal* в России

момент направлен фокус: показатели потребления электроэнергии, социальные проекты в образовании и науке, развитие деловой репутации и добросовестной конкуренции.

**Роман Головацкий**, советник *DLA Piper*

**Полина Лебедева**, исполнительный директор, директор практики консультационных услуг в области управления юридической функцией и комплаенс-функцией *PwC* в России, осветила основные вызовы и задачи по итогу проведения ежегодного исследования юридических департаментов, которое уже 7 лет подряд проводится *PwC*. Она обозначила ключевые тенденции в развитии юридических департаментов в России и за рубежом, отметив, что российские юридические департаменты следуют лучшим международным практикам. В числе ключевых задач, стоящих перед руководителями юридических департаментов, Полина назвала автоматизацию юридических процессов, улучшение взаимодействия с внутренними клиентами, удержание ключевых работников и развитие персонала. Лучшей практикой последних лет, по ее мнению, нужно считать создание юридическими департаментами позиции *Legal Operations Officer* для концентрации и развития функционала, связанного со стратегией и повышением эффективности юридического департамента. В числе приоритетов, влияющих на мотивацию работников, Полина назвала возможность работать в дистанционном режиме, а также подчеркнула возрастающую для работников значимость возможности обучения, профессионального развития.

**Алла Генералова**, руководитель юридической практики «СИБУР»

На онлайн-выступлении **Юлия Бондаренко**, экс-директор по правовым вопросам в области науки и инноваций «Филип Моррис Продактс С.А.» (Швейцария), обозначила ряд трендов в сфере стратегического и финансового планирования за рубежом: «*Legal Operations* — это мультидисциплинарная функция, которая оптимизирует процессы оказания юридической поддержки, фокусируясь на следующих 5 направлениях:

- стратегическое планирование;
- финансовое планирование;
- отчетность и аналитика;
- управление поставщиками (консультантами);
- внедрение и адаптация новых технологий.

Несмотря на то, что в этих видах деятельности как таковых нет ничего принципиально нового, суть *Legal Operations* — постоянный фокус на ключевых процессах юридического департамента для внедрения улучшений с целью достижения большей эффективности», — объяснила Юлия.

**Татьяна Паняева**, директор юридического департамента «Нестле»

Яркую панельную дискуссию создали **Алла Генералова**, руководитель юридической практики в СИБУРе, и **Андрей Донцов**, партнер, глава практики *Corporate and M&A*

юридической фирмы *White & Case*. Они рассказали об основных трендах развития юридического департамента в вопросах усиления кадрового состава, решения бизнес-задач и выделили новые ниши для консультантов. Кроме того, в своем выступлении Алла и Андрей поделились практическим опытом, приведя в пример эффективные подходы к мотивации сотрудников. Например, рассылка с успехами коллег внутри компании или департамента.

Теме синергии работы юристов и экспертов посвятили свои выступления **Василий Малинин**, партнер юридической фирмы «Рустам Курмаев и Партнеры», и **Виктор Домшенко**, руководитель отдела судебной защиты Блока по правовым вопросам «Почты России». Они раскрыли участникам конференции специфику поиска и найма консультантов, взаимодействия с подрядчиками и особенности проведения экспертизы на примере практической составляющей юридической деятельности. Также рассказали об эффективных методах борьбы с необъективными, заинтересованными и некомпетентными экспертами на основе правовых кейсов.

Как грамотно сопровождать значимые судебные споры, соответствуя высоким стандартам профессионализма в юридической профессии, поделились **Вера Рихтерман**, партнер АБ ЕПАМ, и **Павел Громов**, директор юридического департамента «Ашан» (Россия). Они рассказали об эффективном сотрудничестве юридических департаментов и внешних консультантов в таких вопросах, как урегулирование корпоративных конфликтов, развитие уголовного направления в корпоративном споре или деле о банкротстве, урегулирование споров с государственными органами. По результатам дискуссии спикеры обозначили ключевые правила эффективного взаимодействия юридических департаментов с внешними консультантами, а также оптимальные методы отбора консультантов под запросы бизнеса во избежание типичных и зачастую фатальных ошибок.

**Дмитрий Пристансков**, статс-секретарь — вице-президент по взаимодействию с органами власти и управления «Норильского никеля», и **Владимир Таланов**, советник АБ ЕПАМ, обозначили высокие стандарты, вызванные эволюцией российского законодательства, и привели практический опыт работы над вызовами, которые возникают перед юридическими департаментами. «Сегодня мы вместе с бизнесом работаем над тем, чтобы помочь правильно структурировать российское углеродное регулирование. Важно, чтобы новые российские правила были восприняты ЕС в контексте трансграничного углеродного налога и российским товарам не пришлось платить и в России, и в ЕС при импорте», — отметил Владимир Таланов.

По итогам проведения конференции Александра Нестеренко поблагодарила участников, спикеров и модераторов, выразив уверенность в значимости проводимых встреч для развития всего юридического сообщества в условиях постоянно возникающих вызовов и быстроразвивающихся тенденций.

# К ЦИВИЛИСТИЧЕСКОЙ ТЕОРИИ СМАРТ-КОНТРАКТОВ

**ГЕОРГИЙ ВИКТОРОВИЧ ЦЕПОВ**

доцент кафедры гражданского права и процесса Национального исследовательского института «Высшая школа экономики» (СПб.), кандидат юридических наук, адвокат

**НИКИТА ВИТАЛЬЕВИЧ ИВАНОВ**

заведующий кафедрой гражданского права и процесса Национального исследовательского института «Высшая школа экономики» (СПб.), кандидат юридических наук, доцент

В статье исследуется вопрос о месте смарт-контрактов в юридической систематике. Основное отличие смарт-контракта от традиционных гражданско-правовых договоров в том, что они заключаются в электронной форме в рамках информационной системы, а их существенные условия определяют автоматическую передачу имущественных прав. Несмотря на то что условия смарт-контракта должны включать команды и данные, необходимые для его автоматического исполнения, его основным языком должен выступать язык применимого права. Самоисполнение договора — иллюзия. Для заключения и исполнения смарт-контракта необходимо выражение взаимной воли его сторонами, участие оператора информационной системы, а также наличие правил информационной системы. В децентрализованной системе функции оператора выполняют пользователи системы, объединенные в гражданско-правовое сообщество. Производители программного обеспечения должны по общему правилу нести гражданско-правовую ответственность за некачественную работу программных продуктов, используемых при заключении и исполнении автоматически исполняемых договоров.

***Ключевые слова:*** *смарт-контракт, автоматическое исполнение обязательства, информационная система, программа для ЭВМ, ответственность за недостатки программного обеспечения*

DOI: 10.37239/0869-4400-2022-18-3-149-172

---

*Pacta sunt servanda*

*(«Договоры должны соблюдаться»)*

## 1. Постановка задачи

Электронный оборот стал повседневной практикой. Многие вещи сами по себе уже не представляют ценности без обеспечивающих их функционирование

информационных систем. С появлением технологии блокчейн распространение получила криптовалюта и иные цифровые активы, а также обеспечивающие их автоматический оборот смарт-контракты.

Успех внедрения цифровых технологий объясняется не только тем, что они, устраняя людей в качестве физических исполнителей и посредников, уменьшают производственные расходы, но и тем, что снижают трансакционные издержки. Тем не менее возникают новые виды рисков и трансакционных издержек, нуждающиеся в осмыслении и преодолении.

Попытки регулирования человеческой деятельности компьютерным кодом и создание в этих целях неподконтрольных государствам и социуму глобальных информационных систем угрожают традиционным правовым системам, основным правам и свободам граждан[1]. В условиях больших массивов информации осознанный выбор становится затруднительным или невозможным, поскольку люди теряют способность контролировать не только действия сложных информационных систем, но и собственное поведение, вследствие чего становятся заложниками «цифровых» советников, поднимается вопрос о вытеснении традиционных правовых норм и стандартов микродирективами[2].

Вызовы цифровой эпохи потребовали от государства в ускоренном порядке разработать и принять законы, в значительной степени не имеющие непосредственных аналогов в прошлом[3]. Новые задачи встали и перед теоретиками права. Одна из них — выявление юридической природы смарт-контракта. Является ли он особым видом договора или служит лишь техническим инструментом для исполнения гражданско-правовой сделки? Допустимо ли заключить договор в форме программного кода? Могут ли быть программные условия смарт-контракта объектом авторских прав? На кого возлагаются обязанности по обеспечению заключения и исполнения смарт-контрактов, и кто будет нести ответственность за их ошибки? Попытаемся ответить на поставленные вопросы.

## 2. Понятие и признаки смарт-контракта

По мнению Ника Сабо, считающегося пионером исследований в рассматриваемой сфере, смарт-контракт — это «компьютеризированный трансакционный протокол, который исполняет условия договора»[4]. Позже он дал иное определение: «Смарт-контракт — это набор обещаний, определенных в цифровой форме, включая протоколы, в рамках которых стороны выполняют эти обещания»[5].

Можно выделить два основных течения в определении природы смарт-контрактов[6].

> В русле первого, технического, смарт-контракт рассматривается не как договор, а как программное средство для автоматического исполнения договора. Сформулированные сторонами условия договора подлежат трансляции в программный код смарт-контракта, исполняемый компьютером[7].

[1] См.: *Lessig L.* Code is Law. On Liberty in Cyberspace. URL: https://www.harvardmagazine.com/2000/01/code-is-law-html (дата обращения: 24.03.2022); *Kolber A.J.* Not-So-Smart Blockchain Contracts and Artificial Responsibility // Stanford Technology Law Review. 2018. Vol. 21. Iss. 2. P. 198–234.

[2] См.: *Casey A.J., Niblett A.* The Death of Rules and Standards. Indiana Law Journal. 2017. Vol. 92. No. 4. P. 1401–1447.

[3] См.: Федеральные законы от 18.03.2019 № 34-ФЗ «О внесении изменений в части первую, вторую и статью 1124 части третьей Гражданского кодекса Российской Федерации», от 02.08.2019 № 259-ФЗ «О привлечении инвестиций с использованием инвестиционных платформ и о внесении изменений в отдельные законодательные акты Российской Федерации», от 31.07.2020 № 259-ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации» (далее — Закон о цифровых финансовых активах, цифровой валюте).

[4] *Szabo N.* Smart contracts (1994). URL: http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html (дата обращения: 24.03.2022).

[5] *Szabo N.* Smart Contracts: Building Blocks for Digital Markets? (1996). URL: https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_2.html (дата обращения: 24.03.2022).

[6] Обзор концепций см.: *Федоров Д.В.* Токены, криптовалюта и смарт-контракты в отечественных законопроектах с позиции иностранного опыта // Вестник гражданского права. 2018. № 2. С. 62–70.

[7] «Умный контракт — это просто код, который работает в *Ethereum*. Он называется контрактом, потому что этот код может контролировать ценные вещи, такие как деньги (ETH) или другие цифровые активы». URL: https://ethereum.org/ru/learn/#smart-contracts (дата обращения: 24.03.2022).

При таком понимании наименование «смарт-контракт» входит в противоречие с содержанием данного термина[8].

Вне связи с договором, определяющим использование технического смарт-контракта, возникает вопрос о юридических последствиях передачи имущества посредством исполнения такого смарт-контракта. Отрицание сделочной природы технического смарт-контракта приводит к выводу, что полученное исполнение надлежит признать неосновательным обогащением (ст. 1102 ГК РФ). Если же предмет технического смарт-контракта не является объектом гражданских прав, то такой контракт вообще находится вне сферы гражданско-правового регулирования оборота имущественных благ[9].

Как видно, техническая концепция не отводит смарт-контракту места в регулировании имущественных отношений, за исключением радикального случая подмены правовых норм техническими правилами[10].

> В рамках второго, «юридического» подхода, который набирает все большую поддержку, смарт-контракт (юридический смарт-контракт[11]) рассматривается в качестве особого вида гражданско-правового договора, заключаемого в электронной форме, содержание которого в той или иной степени составляет программный код, обеспечивающий исполнение договора[12].

Высказана идея о дуализме правовой природы смарт-контракта. «С одной стороны, — пишут В.С. Белых, М.О. Болобонова, — это технологическое решение, включающее компьютерный протокол, которое

[8] В этом контексте указывают, что «смарт-контракты» не являются ни умными, ни контрактами, хотя название и прижилось. Напротив, они представляют собой механизмы, обеспечивающие выполнение соглашений с использованием программного обеспечения, а не права (*Grimmelmann J.* All Smart Contracts Are Ambiguous // Journal of Law and Innovation. 2019. Vol. 2. No. 1. P. 2).

[9] Концепция «просто код» неприемлема для целей гражданского правового регулирования оборота имущества. Применение данной концепции в российской судебной практике позволило сделать вывод, что «действующим законодательством РФ неизвестен такой способ защиты права, как обязание обеспечить возврат криптовалюты ETH 199,903438, BTC 2,14578983617, LTC 199,5696692 на цифровые кошельки контрибьюторов пропорционально размеру вклада каждого контрибьютора. Указанный способ защиты права не указан в ст. 12 ГК РФ, а значит, не является законным способом защиты права и не может быть использован, т.е. в данном конкретном случае истец лишен права на судебную защиту своих нарушенных прав» (постановление Девятого ААС от 04.02.2020 № 09АП-76537/2019, а также постановление АС Московского округа от 03.06.2020 № Ф05-7176/2020, определение ВС РФ от 14.09.2020 № 305-ЭС20-12165 по делу № А40-164942/2019). Напротив, отказ от идеи «просто код» влечет признание криптовалюты имуществом (суррогатом денежных средств), а следовательно, и признание осознанных волевых действий субъектов гражданского права по их обороту гражданско-правовыми сделками. Так, Судебная коллегия по гражданским делам ВС РФ по одному из дел отказалась считать получение средств от продажи криптовалюты в качестве неосновательного обогащения, согласившись с тем, что, «передав свое имущество (криптовалюту) взамен полученных денежных средств, П.А.С. преследовал определенную экономическую цель, заключив сделки по продаже криптовалюты», вследствие чего правовые основания для получения денежных средств у П.А.С. имелись (Определение Судебной коллегии по гражданским делам ВС РФ от 02.02.2021 № 44-КГ20-17-К7, 2-2886/2019).

[10] Не случайно организаторы проекта *Ethereum*, по-видимому, забыв о лукавой концепции «…просто код, который работает в *Ethereum*», придают смарт-контрактам функцию по регулированию имущественных отношений, рассматривая смарт-контракты как компьютерные программы, которые хранятся на блокчейне и позволяют преобразовывать традиционные контракты в цифровые параллели. Смарт-контракты оцифровывают соглашения, превращая условия соглашения в компьютерный код, который автоматически выполняется при выполнении условий контракта. URL: https://ethereum.org/ru/smart-contracts (дата обращения: 24.03.2022). Функция смарт-контракта как регулятора имущественных отношений отчетливо видна при анализе правового положения децентрализованной автономной организации *(DAO)* «Основа *DAO* — это умный контракт. Контракт определяет правила организации и хранит капитал группы. Как только контракт будет запущен на *Ethereum*, никто не сможет изменить правила, кроме как голосованием. Если кто-то попытается сделать что-то, что не предусмотрено правилами и логикой кода, он потерпит неудачу. Управление капиталом также определяется умным контрактом. Это означает, что никто не может тратить деньги без одобрения группы». URL: https://ethereum.org/ru/dao/ (дата обращения: 24.03.2022). Общая концепция «децентрализованной автономной организации» — это концепция виртуальной организации, имеющей определенный набор членов или акционеров, которые, возможно, с большинством в 67% имеют право тратить средства организации и изменять ее код. URL: https://ethereum.org/ru/whitepaper/ (дата обращения: 24.03.2022).

[11] Отмечается, что термин «умный юридический контракт» все чаще используется, чтобы подчеркнуть технико-юридические качества контракта, подлежащего исполнению по закону и часто, хотя и не всегда, выраженного в форме «умного контракта» (*Hunn P.G.* Smart Contracts as Techno-Legal Regulation // Journal of ICT Standardization. 2019. Vol. 7. Iss. 3. P. 273).

[12] См.: *Hunn P.G.* Smart Contracts as Techno-Legal Regulation. Journal of ICT Standardization. 2019. Vol. 7. Iss. 3. P. 269–286; *Allen J.G.* Wrapped and Stacked: “Smart Contracts” and the Interaction of Natural and Formal Languages // European Review of Contract Law. 2018. Vol. 14. Iss. 4. P. 307–343.

может не являться соглашением, с другой стороны — соглашение сторон в электронной форме, имеющее юридическую силу»[13]. Тем не менее далее указанные авторы не вполне последовательно придерживаются выдвинутой ими же дуалистической концепции, отмечая, что «правовая природа смарт-контракта может быть различной». И определяют его и как техническое средство, которое может обеспечить исполнение отдельных положений классического договора, и как самостоятельный договор, способ выражения вовне внутренней воли сторон сделки (форму договора)[14], что означает описание термином «смарт-контракт» разных явлений.

Также предложено паллиативное решение: смарт-контракт рассматривается как объективно существующий цифровой феномен, определяемый через набор присущих ему функций — формы гражданско-правовой сделки, способа обеспечения исполнения обязательства, способа исполнения обязательства, надлежащего самоисполнения гражданско-правового обязательства. При этом перспективным указывается построение цивилистической теории смарт-контракта через призму такого родового признака, как способ исполнения обязательства[15]. Однако «паллиативное решение» едва ли пригодно для научных целей и правоприменительной деятельности, поскольку не соответствует принципу правовой определенности.

Напротив, в целях отграничения смарт-контракта от иных договоров, заключаемых в электронной форме, предпринята попытка сузить его определение, связав исключительно с технологией блокчейн. Такого подхода придерживается, в частности, А.И. Савельев, который определяет смарт-контракт как «договор, существующий в форме программного кода, имплементированного на платформе блокчейн, который обеспечивает автономность и самоисполнимость условий такого договора по наступлении заранее определенных в нем обстоятельств». «При этом, — пишет А.И. Савельев, — следует особо подчеркнуть, что смарт-контракт как таковой имеет смысл лишь постольку, поскольку в нем фигурирует криптовалюта, которая выступает в качестве цифрового актива, циркулирующего в рамках блокчейна (или цифровой манифестации такого актива) и/или встречного предоставления»[16]. Встречаются и иные интерпретации[17].

Как видно, отмеченные разногласия имеют не только терминологический характер, но и затрагивают сущность изучаемого явления. Какой же подход наиболее полно и точно соответствует назначению

[13] См.: *Белых В.С., Болобонова М.О.* Проблемы правового регулирования смарт-контрактов в России // Правовое регулирование экономических отношений в современных условиях развития цифровой экономики: монография / отв. ред. В.А. Вайпан, М.А. Егорова. М., 2019. С. 104.

[14] См.: *Белых В.С., Болобонова М.О.* Указ. соч. С. 108, 110, 113.

[15] *Захаркина А.В.* Смарт-контракт в условиях формирования нормативной платформы экосистемы цифровой экономики Российской Федерации // Вестник Пермского университета. Юридические науки. 2020. Вып. 1 (47). С. 78–79. По мнению А.А. Волоса, «наиболее комплексным, включающим в себя все особенности смарт-контракта представляется подход, в соответствии с которым смарт-контракт, не выступая самостоятельным или отдельным видом договора, тем не менее предопределяет гражданско-правовое договорное правоотношение, которое обладает специфическими чертами. При этом в зависимости от конкретной ситуации смарт-контракт может выступать и в качестве иных указанных выше категорий» (*Волос А.А.* Гражданско-правовая сущность смарт-контракта // Юрист. 2019. № 7. С 27). В другой своей работе данный автор дает несколько иное определение: «Смарт-контракт — это особая форма договора, а также совокупность специфических порядков и способов заключения договора, осуществления прав и исполнения обязанностей сторон, прекращения договорных отношений» (*Волос А.А.* Смарт-контракты и принципы гражданского права // Российская юстиция. 2018. № 12. С. 7).

[16] *Савельев А.И.* Некоторые правовые аспекты использования смарт-контрактов и блокчейн-технологий по российскому праву // Закон. 2017. № 5. С. 99.

[17] См.: *Ефимова Л.Г., Сиземова О.Б.* Правовая природа смарт-контракта // Банковское право. 2019. № 1. С. 27–28. Давая характеристику умному контракту, применяемому при использовании технологии блокчейн, А.Ю. Чурилов отмечает, что он «…состоит из трех основных частей — „ядра“ (программного кода), в котором содержатся условия будущего договора; файла договора, находящегося в системе блокчейн; баланса счета пользователя» (*Чурилов А.Ю.* Использование технологии блокчейн: платежная система, «умные» контракты, принятие коллегиальных решений, хранение информации // Право в сфере Интернета: сб. ст. / рук. авт. кол. и отв. ред. д.ю.н. М.А. Рожкова. М., 2018 С. 153). По мнению Риккардо де Кария, децентрализованный смарт-контракт может быть определен как любое соглашение в цифровой форме, которое: а) написано в виде компьютерного кода (т.е. является частью софта); б) запускается на платформе блокчейн или с использованием иной аналогичной технологии распределенного реестра (поэтому децентрализованный); в) автоматически исполняется без необходимости вмешательства человека (поэтому является умным) (*De Caria R.* The Legal Meaning of Smart Contracts // European Review of Private Law. 2018. Vol. 26. Iss. 6. P. 737). См. также: *O'Shields R.* Smart Contracts: Legal Agreements for the Blockchain // North Carolina Banking Institute. 2017. Vol. 21. Iss. 1. P. 177–194.

юридического смарт-контракта? Действительно ли смарт-контракты немыслимы вне платформы блокчейн и использования криптовалюты и «представляют собой качественно новое явление, бросающее вызов классическим доктринам договорного права»[18], или же все-таки укладываются в традиционную цивилистическую систематику?

> Прежде всего отметим, что едва ли целесообразно обозначать термином «смарт-контракт» исключительно способ исполнения договора. В таком случае произойдет удвоение сущности, поскольку сторонам потребуется согласовать не только условия основного договора, но и условия смарт-контракта (распорядительного договора), определяющие способ исполнения основного договора.

Нет никакой необходимости ограничивать смарт-контракт технологией распределенного реестра (платформой блокчейн)[19]. Несмотря на ажиотаж последних лет по внедрению систем распределенного реестра, пока нет объективных данных об их тотальном превосходстве над централизованными системами[20]. Огромные энергетические затраты, необходимые для поддержания работы крупных открытых децентрализованных систем[21], а также организационные проблемы и риски[22] скорее свидетельствуют об обратном. Не случайно рассматривается переход от системы *proof-of-work* к системе *proof-of-stake*, что существенно обособит статус посредников, от которых, как принято считать, система распределенного реестра и была призвана избавить пользователей[23].

> Прозрачность данных распределенного реестра противоречит интересу сторон смарт-контракта в сохранении тайны его содержания. Вместе с тем использование анонимности как средства преодоления негативных последствий открытого реестра входит в конфликт с основами правопорядка.

Так, для заключения договора стороны — субъекты гражданского права должны согласовать взаимную волю, для чего им необходимо знать минимально необходимую юридически значимую информацию друг о друге, даже если с субъективной точки зрения каждого из них личность контрагента не имеет существенного значения[24]. Допустив анонимность, придется смириться с тем, что под логином стороны смарт-контракта сможет скрываться не только ограниченное в правоспособности или недееспособное лицо, но и автономная информационная система, которая генерирует «оферты» или «акцепты». Очевидно, что такая ситуация имеет мало общего с заключением гражданско-правового договора: достоверно определить, чью волю в данном случае транслирует компьютерная программа и на что направлена воля ее пользователя (реальное заключение договора или обман контрагента), будет затруднительно.

---

[18] *Савельев А.И.* Некоторые правовые аспекты использования смарт-контрактов и блокчейн-технологий по российскому праву. С. 101.

[19] Неслучайно п. 2 ст. 1 Закона о цифровых финансовых активах, цифровой валюте не связывает выпуск, учет и обращение ЦФА исключительно с информационными системами на основе распределенного реестра.

[20] Эффективность систем распределенного реестра нельзя переоценивать. Во-первых, информация имеет двуединую природу: нематериальную и физическую. Запись, хранение и стирание информации требует энергии. Во-вторых, в децентрализованных системах количество организационных связей увеличивается с каждым новым участником в геометрической прогрессии, что влечет увеличение трансакционных издержек. На данное обстоятельство обращает внимание Р. Познер: «…в большинстве случаев издержки трансакций возрастают с увеличением числа сторон — и весьма быстро, — пишет он, — показательна формула, определяющая число связей, необходимых для вступления в соглашение всех $n$ членов множества: $n(n-1)/2$» (*Познер Р.* Экономический анализ права. Т. 1. СПб., 2004. С. 68).

[21] Годовое потребление электроэнергии для майнинга биткойнов, по данным Кембриджского центра альтернативных финансов (на дату обращения), составляет 136,98 ТВтч, что больше потребления электроэнергии многими странами. См.: https://ccaf.io/cbeci/index (дата обращения: 24.03.2022); Энергии, затрачиваемой на годовой майнинг криптовалюты, хватило бы на то, чтобы все чайники Великобритании кипятились 27 лет. URL: URL: https://www.ixbt.com/news/2021/02/12/set-bitcoin-za-god-potrebljaet-bolshe-chem-niderlandy-jetogo-hvatilo-by-chtoby-pitat-vse-chajniki-velikobritanii-27-let.html (дата обращения 24.03.2022).

[22] См.: *Хвостик Е.* Мошенники освоили блокчейн // Коммерсант. 2021. 8 мая. URL: https://www.kommersant.ru/doc/4801843?from=main_5 (дата обращения: 24.03.2022).

[23] См.: https://ethereum.org/en/developers/docs/consensus-mechanisms/pos/ (дата обращения: 24.03.2022).

[24] Допустим, на рынке два незнакомых друг с другом лица обменяли товар на деньги. Сами стороны могут считать, что между ними был заключен и исполнен договор купли-продажи. Однако объективировать свои отношения для третьих лиц и государства как продавца и покупателя определенного товара они смогут лишь при условии раскрытия установленных законом данных о себе и совершенной ими сделке.

Договорное правоотношение в принципе немыслимо вне правовой системы: «…при свершении любых действий — как непосредственно направленных на удовлетворение своих интересов, охраняемых законом, так и вынуждающих к определенному поведению обязанное лицо — управомоченный связан как с обязанными лицами, так и с государством»[25]. При отсутствии идентификации сторон договора законный оборот имущественных благ невозможен, поскольку гражданские права и обязанности могут признаваться правопорядком только у субъекта гражданского права. Государство вправе и должно знать субъектов договорных отношений для защиты прав и законных интересов третьих лиц (супругов, кредиторов), а также публичных интересов, в том числе для целей привлечения их к имущественной ответственности.

Именно поэтому п. 1 ст. 19 ГК РФ устанавливает правило о том, что гражданин приобретает и осуществляет права и обязанности под своим именем, включающим фамилию и собственно имя, а также отчество, если иное не вытекает из закона или национального обычая. Использование псевдонима допускается в случаях и в порядке, предусмотренных законом. Юридическое лицо имеет свое наименование (п. 1 ст. 54 ГК РФ), под которым и выступает в гражданском обороте (п. 1 ст. 48 ГК РФ). Приведенные нормы устанавливают порядок осуществления гражданской правоспособности в целях правовой определенности, без которой не может быть реализован и принцип свободы договора (ст. 421 ГК РФ)[26].

Не случайно поэтому норма абз. 2 п. 1 ст. 160 ГК РФ предусматривает, что для признания формы сделки, совершенной с помощью электронных либо иных технических средств, необходимо не только воспроизведение на материальном носителе в неизменном виде содержания сделки, но и *достоверное определение лица, выразившего волю*.

В том же русле следует Закон о цифровых финансовых активах, цифровой валюте[27], устанавливая в качестве базового правила, что для признания лица обладателем цифровых финансовых активов (ЦФА) *оно должно быть включено в реестр пользователей информационной системы*, который должен вестись *оператором* информационной системы по специальным правилам[28]. В частности, в реестр пользователей должны быть внесены сведения о пользователе информационной системы[29]. На оператора информационной системы, в которой осуществляется выпуск ЦФА, возлагается обязанность по обеспечению восстановления доступа обладателя ЦФА к записям информационной системы по требованию обладателя ЦФА, если такой доступ был им утрачен, а также обеспечения внесения (изменения) записей о ЦФА на основании вступившего в законную силу судебного акта, исполнительного документа и т.п.[30] На оператора информационной системы, в которой осуществляется выпуск ЦФА, как и на оператора обмена, возлагаются обязанности по хранению информации о сделках с ЦФА в течение не менее пяти лет с даты их совершения[31].

[25] *Толстой Ю.К.* К теории правоотношения. Л., 1959. С. 43.

[26] Отсутствие достоверных данных о стороне договора вносит существенную неопределенность относительно самого факта заключения договора. Заблуждение стороны в отношении лица, с которым она вступает в сделку, установлено законом в качестве основания для оспаривания сделки (см.: подп. 4 п. 2 ст. 178 ГК РФ). В судебной практике встречается позиция о том, что подписание договора неустановленным лицом служит основанием для признания его незаключенным. См.: Определение ВС РФ от 03.08.2020 № 302-ЭС20-10072 по делу № А74-19726/2018. Ранее, в Постановлении Президиума ВАС РФ от 06.11.2012 № 8728/12 по делу № А56-44428/2010 применительно к редакции ст. 168 ГК РФ, действовавшей до вступления в силу Федерального закона от 07.05.2013 № 100-ФЗ «О внесении изменений в подразделы 4 и 5 раздела I части первой и статью 1153 части третьей Гражданского кодекса Российской Федерации» (до 01.09.2013), была сформулирована правовая позиция о том, что «договор, заключенный неустановленным лицом, не отвечает требованиям закона, поэтому является ничтожным согласно статье 168 Гражданского кодекса независимо от признания его таковым судом». См. также: Определение ВС РФ от 25.12.2019 № 307-ЭС19-24592 по делу № А26-7433/2018.

[27] Возможность использования смарт-контрактов для оборота ЦФА предусмотрена ч. 2 ст. 4 Закона о цифровых финансовых активах, цифровой валюте: «Записи о цифровых финансовых активах вносятся или изменяются… в силу действия, совершенного в рамках сделки, предусматривающей исполнение сторонами возникающих из нее обязательств при наступлении определенных обстоятельств без направленного на исполнение обязательств отдельно выраженного дополнительного волеизъявления сторон путем применения информационных технологий в соответствии с правилами информационной системы, в которой учитываются цифровые финансовые активы».

[28] См.: ч. 7 ст. 4, ст. 8 Закона о цифровых финансовых активах, цифровой валюте.

[29] См.: п. 1 ч. 2 ст. 8 Закона о цифровых финансовых активах, цифровой валюте.

[30] См.: ч. 1, 2 ст. 6 Закона о цифровых финансовых активах, цифровой валюте.

[31] См.: ч. 4 ст. 6, ч. 10 ст. 10 Закона о цифровых финансовых активах, цифровой валюте.

> Несмотря на то, что смарт-контракты начинают активно внедряться в финансовом секторе, нет смысла искусственно сужать определение смарт-контракта, основываясь на его предмете — цифровой валюте, ЦФА[32].

Цифровые активы обладают экономической ценностью тогда, когда связаны с потребляемыми людьми благами. Поэтому ощутимый полезный экономический эффект от смарт-контрактов можно ожидать при их использовании не только и не столько в финансовом, сколько реальном секторе экономики (купле-продаже товаров, перевозке и т.п.). Идея широкого применения договора такого рода заложена в абз. 2 ст. 309 ГК РФ[33].

Высказана идея, что одно из ключевых отличий смарт-контракта от обычного договора — его машинный язык («код — договор»). Так, по мнению А.И. Савельева, «тот факт, что условия договора изложены в форме программного кода, не имеет сам по себе юридического значения, поскольку договорное право допускает различные способы формализации договоренности сторон. Главное, чтобы они допускали возможность установления факта достижения согласия конкретными сторонами по конкретным условиям»[34]. При этом возможность использования компьютерного кода в качестве языка договора выводится из принципа свободы договора[35].

Однако с приведенным тезисом нельзя согласиться как с объективной, так и с субъективной точки зрения.

Объективный характер выбора языка договора объясняется тем, что «всякий язык — это сосуд, в котором отливаются, сохраняются и передаются идеи и представления народа»[36], в том числе идеи о праве и справедливости. Язык является неотъемлемым элементом человеческой культуры в целом и правовой системы в частности.

«Жить в обществе и быть свободным от общества нельзя»[37]. Гражданско-правовой договор как общественное явление не существует сам по себе, вне правовой системы, поэтому используемая им терминология должна соответствовать языку объективного права[38]. В противном случае ни стороны, ни суд, ни иные правоприменительные органы не смогут определить его необходимые элементы[39], непонятый и непринятый обществом (государством) «договор» останется «вещью в себе». Поэтому выбор языка договора не может быть произвольным и должен происходить в соответствии с применимым правом[40].

---

[32] Об опасности для государства и общества выпуска и оборота частных криптовалют, являющихся суррогатами денежных средств, см. доклад Банка России «Криптовалюты: тренды, риски, меры». М., 2022. URL: https://www.cbr.ru/Content/Document/File/132241/Consultation_Paper_20012022.pdf (дата обращения: 24.03.2022).

[33] Как указывалось ранее, термин «смарт-контракт» противоречив, определяется по-разному, однако повсеместно используется в деловой практике. При понимании условности данного наименования сам по себе спор о наименовании приобретает схоластический характер. Напротив, признаки данного *договора* («юридического смарт-контракта») имеют принципиальное значение.

[34] *Савельев А.И.* Некоторые правовые аспекты использования смарт-контрактов и блокчейн-технологий по российскому праву. С. 107.

[35] См. также: *Федоров Д.В*. Токены, криптовалюта и смарт-контракты в отечественных законопроектах с позиции иностранного опыта // Вестник гражданского права. 2018. № 2. С. 63.

[36] *Гердер И.Г*. Идеи к философии истории человечества. М., 1977. С. 297.

[37] *Ленин В.И.* Партийная организация и партийная литература // ПСС В.И. Ленина. 5-е изд. Т. 12. М., 1968. С. 104.

[38] В соответствии с п. 43 Постановления Пленума ВС РФ от 25.12.2018 № 49 «О некоторых вопросах применения общих положений Гражданского кодекса Российской Федерации о заключении и толковании договора» условия договора подлежат толкованию в системной взаимосвязи с основными началами гражданского законодательства, закрепленными в ст. 1 ГК РФ, другими положениями ГК РФ, законов и иных актов, содержащих нормы гражданского права (ст. 3, 422 ГК РФ).

[39] Поэтому невозможно составить договор о передаче цифровых активов на древнеегипетском языке: в нем просто не найти выразительных средств, соответствующих реалиям XXI века.

[40] Согласно ст. 8 Закона РФ от 25.10.1991 № 1807-1 «О языках народов Российской Федерации» в сферах общения, подлежащих правовому регулированию в соответствии с данным законом, право выбора и использования языка общения гражданами РФ определяется законодательством РФ и субъектов РФ. Пунктом 2 ст. 22 данного Закона установлено, что делопроизводство в сфере обслуживания и коммерческой деятельности ведется *на государственном языке Российской Федерации и иных языках, предусмотренных договорами между деловыми партнерами.* По смыслу данного Закона речь идет *о человеческом языке*. См. также: ст. 68 Конституции РФ, Федеральный закон от 01.06.2005 № 53-ФЗ «О государственном языке Российской Федерации». О значении языка для юридических целей см.: *Белов С.А., Кропачев Н.М.* Что нужно, чтобы русский язык стал государственным? // Закон. 2016. № 10. С. 100–112; *Белов С.А., Кропачев Н.М., Ревазов М.А*. Судебный контроль за соблюдением норм современного русского литературного языка // Закон. 2017. № 3. С. 103–115;

Субъективная сторона выбора языка договора связана с необходимостью осознания сторонами своих действий и преследуемых целей[41]. Реализация принципа свободы договора прежде всего выражается в самой возможности сторон заключить договор, для чего требуется выразить свою волю и согласовать ее с волей контрагента[42], что невозможно без использования понятного для них обеих языка: речь является формой выражения воли и мысли[43].

> Поэтому *язык гражданско-правового договора* — это хотя и формализованный (юридический), но *язык человеческого общения*, на котором по объективным правилам выражается воля сторон.

По крайней мере, существенные условия должны быть понятными сторонам договора, чтобы договор считался заключенным[44]. Нарушение языковых правил влечет искажение передачи информации. Поэтому в случае, если зафиксированная формула не соответствует воле стороны, договор может быть оспорен при наличии существенного заблуждения (ст. 178 ГК РФ).

В отличие от языка права *язык программирования не служит средством общения между людьми.* Это *формальная знаковая система, предназначенная для записи компьютерных программ*, которая определяет набор лексических, синтаксических и семантических правил, задающих внешний вид программы и действия, которые выполнит компьютер под ее управлением, и строится в соответствии с той или иной базовой моделью *вычислений* и парадигмой программирования[45].

Современные компьютерные языки не являются ни достаточно полными, ни достаточно точными для определения всех необходимых условий договора[46]. Перевод на язык программирования терминов гражданского права и умозаключений — трудная задача вследствие многозначности используемых понятий и множества логических связей, образующихся и меняющихся в процессе эволюции гражданского права[47].

*Соколова М.А.* Дефекты юридических документов: монография. М., 2016. 158 с.

[41] «Для того чтобы лицо могло совершать юридический акт, оно должно сознавать характер своего действия и те цели, на которые направлены его действия… в этом состоит одно из важнейших отличий юридических актов от юридических поступков» (*Красавчиков О.А.* Юридические факты в советском гражданском праве // *Красавчиков О.А.* Категории науки гражданского права. Избранные труды: в 2 т. Т. 2. 2-е изд. М., 2017. С. 170).

[42] «Соглашение предполагает *взаимное познание этой воли*, усвоение одним лицом содержания воли другого», — писал Г.Ф. Шершеневич (*Шершеневич Г.Ф.* Курс гражданского права. Тула, 2001. С. 397).

[43] См.: *Красавчиков О.А.* Указ. соч. С. 155. Язык определяется как «знаковая система произвольной природы, посредством которой осуществляется человеческое общение на различных уровнях коммуникации и трансляции, включая операции мышления, приобретение, хранение, преобразование и передачу сообщений (сигналов, информации, знаний) и связанные процессы... использование языка позволяет человеку производить основную часть мыслительных операций… язык выступает основным средством коммуникации и трансляции, обеспечивая извлечение (приобретение), накопление, хранение, преобразование и передачу информацию и знаний». URL: https://gtmarket.ru/concepts/7076 (дата обращения: 24.03.2022). «Значение слова, — писал Л.С. Выготский, — оказывается одновременно речевым и интеллектуальным феноменом, причем это не означает чисто внешней сопринадлежности его к двум различным областям психической жизни. Значение слова есть феномен мышления лишь в той мере, в какой мысль связана со словом и воплощена в слове, и обратно: оно есть феномен речи лишь в той мере, в какой речь связана с мыслью и освещена ее светом. Оно есть феномен словесной мысли или осмысленного слова, оно есть единство слова и мысли» (*Выготский Л.С.* Мышление и речь. Психологические исследования. М.-Л., 1934. С. 262).

[44] См.: п. 3 ст. 154, п. 1 ст. 432 ГК РФ. Согласно ст. 54 Основ законодательства Российской Федерации о нотариате нотариус обязан разъяснить сторонам смысл и значение представленного ими проекта сделки и проверить, соответствует ли его содержание действительным намерениям сторон и не противоречит ли требованиям закона. Данное положение отвечает целям обеспечения стабильности гражданского оборота, направлено на защиту интересов сторон нотариально удостоверяемого договора (см.: Определение КС РФ от 27.02.2020 № 382-О). Незнание языка применимого права в ряде случаев компенсируется возможностью заключения договора путем совершения конклюдентных действий, предоставляющих образную информацию о существенных условиях договора и понятных другой стороне (например, путем пиктограмм на торговых автоматах, на языке жестов и т.п.), возможностью использования услуг переводчика. При возникновения судебного спора он будет разрешаться в соответствии с языком применимого права.

[45] См.: https://dic.academic.ru/dic.nsf/ruwiki/1465 (дата обращения: 24.03.2022).

[46] См.: *Grimmelmann J.* Op. cit. P. 1–22. Критика понимания кода как контракта, учитывая опыт *The DAO*, приведена в работе: *Kolber A.J.* Op. cit. P. 198–234.

[47] См.: *Иванов А.А.* О глубине машинизации права // Закон. 2018. № 5. С. 35–41; *Ефимова Л.Г., Сиземова О.Б.* Указ. соч. С. 23. Как обоснованно отмечает А.Ю. Чурилов, «невозможно включить все необходимые, а применительно к некоторым договорам и существенные условия в программный код, что на практике может привести к длитель-

Достаточно вспомнить, как нелегко дать точное легальное определение понятиям разумность, добросовестность и справедливость, заботливость и должная осмотрительность, вина и непреодолимая сила и т.п.

Внедрение принципа «код — договор» посягает на свободу выбора. Рядовые пользователи информационной системы не способны без посторонней помощи не только написать, но даже понять программный код и перевести его на доступный для понимания человека язык, а тем более в разумное время[48]. Поэтому при использовании кода в качестве основного языка смарт-контракта слабая сторона потеряет свободу принятия решения, и, как следствие, отношения между сторонами утратят характер гражданско-правовых (п. 1, 2 ст. 1 ГК РФ).

Проблемы выбора, интерпретации и применения компьютерного языка уходят своими корнями в социальный пласт[49]. Компьютерный язык имеет искусственную природу: его создают люди для функционирования электронно-вычислительных систем. Они придают значение используемым в нем терминам. Кто же те люди и их объединения, которые создают компьютерные языки? Не подменяет ли их деятельность по созданию языковых правил информационных систем функции законодателя?[50] В связи с изложенным поднимается вопрос о социальном консенсусе в отношении используемого языка программирования, возможности и необходимости перехода на новые версии языка и т.п. Применительно к смарт-контрактам данная проблема приобретает критически важное значение[51].

> Анализ поставленных вопросов приводит к идее создания специального языка программирования для написания смарт-контрактов, обладающего достаточной точностью и полнотой, включающего словарь употребляемых терминов с их предсказуемым толкованием в соответствии с применимым правом[52].

В связи с тезисом «код — договор» задаются и другие вопросы. Если смарт-контракт — это только код, то где проходят его границы? Как отличить содержание собственно смарт-контракта от всего программного обеспечения, необходимого для его исполнения? Кто, как и по каким правилам определяет данные границы? Заключая смарт-контракт, соглашается ли тем самым сторона на все условия кода, включая все его пробелы и дефекты, вследствие которых данная сторона может потерять свои активы в результате соответствующих коду, но недобросовестных действий другой стороны или иных пользователей системы?[53] Поставленные вопросы заставляют усомниться в теоретической обоснованности и практической пригодности концепции «код — договор».

Итак, *компьютерный код не может выступать в качестве основного языка договора*. Тем не менее язык смарт-контракта должен быть понятен компьютеру. Следовательно, текст смарт-контракта может и должен содержать в достаточном объеме команды и данные, необходимые для исполнения его условий с учетом программного обеспечения

ным судебным тяжбам» (*Чурилов А.Ю.* Использование технологии блокчейн: платежная система, «умные» контракты, принятие коллегиальных решений, хранение информации // Право в сфере Интернета: сборник статей / рук. авт. кол. и отв. ред. д.ю.н. М.А. Рожкова. М., 2018. С. 154).

[48] Неслучайно п. 11.1 ст. 2 Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», определяя электронный документ как документированную информацию, представленную в электронной форме, указывает на такой ее признак, как *пригодность для восприятия человеком* с использованием электронных вычислительных машин. Для юридических целей восприятие должно толковаться как *осознание* содержания документа.

[49] *Grimmelmann J.* Op. cit. P. 1–22.

[50] См.: *Lessig L.* Op. cit.

[51] Как отмечает Дж. Гриммельман, мы воспринимаем как фиксированные технические факты успешный результат социального консенсуса о семантике языка программирования. Сообщество программистов и пользователей согласовывает процесс извлечения технического смысла из текста программы. Разработчики реализуют данный процесс на разных компьютерах, с разными инструментами, в разных контекстах. В большинстве случаев выполнение одной и той же программы приводит к одному и тому же результату. Когда же этого не происходит, то технический смысл рушится. «Соответствующее сообщество может переопределить *(redefine)* язык программирования таким образом, чтобы радикально изменить смысл программ, написанных на нем. Смарт-контракты на блокчейне особенно уязвимы для этого… на блокчейне способ изменить последствия контрактов — *изменить семантику…* Смарт-контракты также зависят от социальных институтов, особенно тех, которые создают и ограничивают блокчейн-сообщества» (*Grimmelmann J.* Op. cit. P. 14, 20, 22).

[52] См. на данную тему: *Allen J.G.* Wrapped and Stacked: “Smart Contracts” and the Interaction of Natural and Formal Languages // European Review of Contract Law. 2018. Vol. 14. Iss. 4. P. 307–343.

[53] См.: *Kolber A.J.* Op. cit. P. 222–223. «…Если вы согласились следовать коду в широком смысле, то вы также согласились на возможность хардфорка» (Ibid. P. 223).

информационной системы, в которой он подлежит исполнению[54]. Как видно, *язык права и компьютерный код в смарт-контракте находятся в диалектическом единстве*. В силу принципа верховенства права команды и данные должны соответствовать доступному для понимания пользователей и суда юридическому языку. Указанное означает, что для активного внедрения смарт-контрактов нужны специальные трансляторы, которые обеспечат достаточно точный перевод языка применимого права, в том числе содержащихся в объективном праве обычных условий договора, на язык компьютера и специальные конструкторы[55]. Возможность использования таких трансляторов и конструкторов приводит к выводу о целесообразности наделения оператора информационной системы, с использованием которой заключается смарт-контракт, функциями «переводчика».

Итак, какие же признаки смарт-контракта, с учетом изложенного, следует считать специфическими?

*Фундаментальным отличием смарт-контракта от традиционных гражданско-правовых договоров является то, что исполнение его сторонами вытекающих из него обязательств осуществляется при помощи информационных технологий на основании заранее сформулированных сторонами условий при наступлении определенных обстоятельств, не требующих отдельно выраженного дополнительного волеизъявления его сторон[56].*

Указанное предопределяет следующие границы применения смарт-контрактов. *Автоматическое исполнение возможно в отношении только тех договоров, условия которых можно заранее сформулировать с достаточной степенью определенности* (закрытые контракты). К таким договорам, в частности, относятся купля-продажа, подряд, отдельные виды договора возмездного оказания услуг и т.п. Напротив, трудно, если вообще возможно полностью запрограммировать и добиться автоматического исполнения открытых контрактов (агентского договора, договора доверительного управления имуществом, договора с управляющей организацией и т.п.).

> Строго говоря, термин «умный контракт» уместен лишь в тех случаях, когда в дело вступает искусственный интеллект. В остальных случаях, когда исполнение производится компьютером по жесткому сценарию, слово «смарт» не несет смысловой нагрузки и является прижившейся фигурой речи, на что и обращается внимание в литературе[57].

Кроме того, *программирование осуществимо только в отношении действий автоматов, а не людей*. Поэтому программирование условий невозможно в отношении тех обязательств, исполнение которых осуществляется непосредственно людьми. Отмеченное позволяет выделить следующие особенности смарт-контракта как гражданско-правового договора:

1) *смарт-контракт может быть заключен исключительно в электронной форме и с использованием информационной системы[58]*. Данный вывод очевиден, поскольку иные форма и способ заключения входят в противоречие с назначением смарт-контрактов. Воля сторон смарт-контракта выражается при помощи электронно-вычислительной техники, волеизъявление должно подлежать объективной проверке, его условия могут быть воспроизведены в доступном для восприятия человека виде;

2) *смарт-контракт должен содержать в качестве своих существенных условий команды и данные, которые обеспечивают его исполнение информационной системой*. Это означает, что *смарт-контракт (юридический факт)* одновременно *является и распорядительной*

[54] Можно провести аналогию между такими условиями с техническим заданием, выступающим в качестве неотъемлемой части договора подряда.

[55] В литературе отмечается: чтобы быть действительными, смарт-контракты должны быть сконструированы таким образом, чтобы соответствовать давно установленным правовым нормам, применяемым к заключению контрактов, в том числе демонстрировать явное выражение взаимного согласия сторон с условиями контракта. Этого можно было бы достичь, если бы стороны нажали кнопку, подтверждая тем самым свое согласие с условиями контракта, вместе со ссылкой на условия, сформулированные на естественном языке. Перевод смарт-контракта с компьютерного языка на естественный язык необходим и для изучения его условий судом (*O'Shields R*. Op. cit. P. 189, 190).

[56] См.: абз. 2 ст. 309 ГК РФ.

[57] См.: *Grimmelmann J*. Op. cit. P. 2.

[58] См.: *Ефимова Л.Г.* Понятие и правовые особенности электронного договора // Законы России: опыт, анализ, практика. 2019. № 7. С. 84–90.

*сделкой*. При этом распоряжение о передаче прав на имущество (программирование передачи) необходимо не только для исполнения обязательства, но и для заключения смарт-контракта.

Данный признак может позволить отличить смарт-контракт от договора розничной купли-продажи, заключаемого с использованием автоматов (ст. 498 ГК РФ), при заключении которого покупатель не согласовывает с продавцом алгоритм исполнения договора. Покупателю безразлично, какое программное обеспечение использует продавец и как оно функционирует, его интересует лишь результат — получение оплаченного товара. Риск ошибки в программировании исполнения договора, заключаемого с использованием автомата, полностью относится на продавца[59]. Напротив, риск ошибки в программировании условий исполнения смарт-контракта по смыслу применяемой юридической конструкции несут обе стороны, если иное не предусмотрено их соглашением или не вытекает из существа отношений и требований закона[60]. По этим же критериям смарт-контракт можно отграничить от использования информационных систем для исполнения отдельных обязательств (например, осуществления расчетных операций при исполнении договора банковского счета);

3) *смарт-контракт подлежит исполнению с использованием информационной системы*. Тем не менее исполнение отдельных обязательств может выходить за рамки той информационной системы, посредством которой он заключен, например заказанный покупателем товар может доставляться роботом-курьером по запрограммированному адресу. При этом может быть трудно провести четкую границу между информационными системами. В приведенном примере программно-аппаратная составляющая робота-курьера хотя и является относительно самостоятельной информационной системой[61], но должна быть связана с той информационной системой, в которой заключался смарт-контракт. Однако вместе они также образуют информационную систему;

4) *смарт-контракт не может быть заключен и исполнен без участия специального посредника — оператора информационной системы*[62].

*Существенным заблуждением является утверждение о самоисполнимости смарт-контракта.* Договор как юридический факт не может исполняться в принципе: факт либо есть, либо его нет. Существующая в рамках правоотношения юридическая обязанность — это идеальная категория, которая не может самоисполняться, воздействуя на объекты реального мира.

> Исполнение юридической обязанности осуществляется действиями обязанного лица или по его поручению действиями третьего лица. В случае со смарт-контрактом *исполнение обязанности должника происходит путем физических действий материальных объектов — автоматов, запрограммированных определенным образом.*

Таким образом, для исполнения смарт-контракта, помимо деятельности людей по определению и программированию условий исполнения, необходимы физические объекты: электронно-вычислительная техника, каналы связи, энергетические ресурсы и т.д. В ряде случаев могут требоваться записанные на материальные носители и передаваемые по каналам связи внешние данные, свидетельствующие о наступлении условий, определяющих исполнение смарт-контракта. Дефекты в работе оборудования, программного обеспечения и устройств связи, в том числе в результате действий пользователей информационной системы

[59] Согласно п. 3 ст. 498 ГК РФ, если покупателю не предоставляется оплаченный товар, продавец обязан по требованию покупателя незамедлительно предоставить покупателю товар или возвратить уплаченную им сумму.

[60] Например, риски ошибок программирования возлагаются на оператора информационной системы.

[61] См.: *Архипов В.В., Наумов В.Б.* Информационно-правовые аспекты формирования законодательства о робототехнике // Информационное право. 2017. № 1. С. 19–27.

[62] Оператор информационной системы — гражданин или юридическое лицо, осуществляющие деятельность по эксплуатации информационной системы, в том числе по обработке информации, содержащейся в ее базах данных (см.: п. 12 ст. 2 Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»). Закон о цифровых финансовых активах, цифровой валюте также добавляет еще одну категорию посредников — оператора обмена ЦФА. Оператор обмена цифровых финансовых активов может совмещать свою деятельность с деятельностью оператора информационной системы, в которой осуществляется выпуск цифровых финансовых активов (см.: ст. 10 Закона о цифровых финансовых активах, цифровой валюте).

или третьих лиц, могут повлечь невозможность исполнения смарт-контракта[63].

Оператор информационной системы как раз и является тем субъектом, в чьи обязанности должно входить обеспечение заключения и исполнения смарт-контрактов, в том числе предоставление для использования необходимого оборудования, программного обеспечения и технического обслуживания, верификации внешних данных и т.п. К функциям оператора должны относиться идентификация и аутентификация сторон договора, обеспечение конфиденциальности сведений о сторонах и условиях смарт-контракта.

Операторы обеспечивают заключение и исполнение смарт-контрактов как в централизованных, так и в децентрализованных системах. В децентрализованной системе функции оператора, по сути, выполняют все пользователи системы, объединенные в гражданско-правовое сообщество[64]. Отдельные участники децентрализованных систем могут наделяться специальными функциями, обеспечивающими работу таких систем.

Кроме того, информационная система, обеспечивающая заключение и исполнение смарт-контрактов, должна функционировать по определенным правилам, в том числе обеспечивая использование единого компьютерного протокола. Для этого правила централизованной информационной системы должны утверждаться ее оператором, а остальные пользователи должны обладать возможностью присоединиться к их действию после ознакомления с ними. Правила частично централизованной или децентрализованной информационной системы согласуются участниками гражданско-правового сообщества — пользователями системы. Применительно к децентрализованной системе проблема согласования правил и перехода на новые правила путем обновления программного обеспечения приобретает критически важное значение для целостности всей системы.

Идея о ключевом значении оператора для функционирования информационной системы, в которой осуществляется выпуск ЦФА, а также операторов обмена ЦФА нашла отражение в Законе о цифровых финансовых активах, цифровой валюте.

Так, сделки купли-продажи ЦФА, иные сделки, связанные с ЦФА, включая обмен ЦФА одного вида на ЦФА другого вида либо на цифровые права, предусмотренные законом, в том числе сделки с ЦФА, выпущенными в информационных системах, организованных в соответствии с иностранным правом, а также сделки с цифровыми правами, включающими одновременно ЦФА и иные цифровые права, совершаются через оператора обмена ЦФА. Оператор обмена обеспечивает заключение сделок с ЦФА активами путем сбора и сопоставления разнонаправленных заявок на совершение таких сделок либо путем участия за свой счет в сделке с ЦФА в качестве стороны такой сделки в интересах третьих лиц[65].

Операторы информационной системы, в которой осуществляется выпуск ЦФА, и операторы обмена ЦФА должны соответствовать специальным требованиям, установленным Законом о цифровых финансовых активах, цифровой валюте, и подлежат включению в специальные реестры, которые ведет Банк России[66]. Законом предусмотрено и обязательное наличие правил, определяющих функционирование информационной системы, в которой происходит выпуск ЦФА, а также правил обмена ЦФА[67].

На оператора информационной системы, в которой осуществляется выпуск ЦФА, Закон возлагает обязанности:

— по бесперебойности и непрерывности функционирования информационной системы;

— целостности и достоверности информации о ЦФА, которая содержится в записях информационной системы;

[63] Например, при некоторых обстоятельствах исполнение программы может зациклиться.

[64] См.: п. 103 Постановления Пленума ВС РФ от 23.06.2015 № 25 «О применении судами некоторых положений раздела I части первой Гражданского кодекса Российской Федерации».

[65] См.: ч. 1 ст. 10 Закона о цифровых финансовых активах, цифровой валюте.

[66] См.: ст. 5, 10 Закона о цифровых финансовых активах, цифровой валюте.

[67] См.: ст. 5, 11 Закона о цифровых финансовых активах, цифровой валюте.

— корректности реализации в информационной системе установленных оператором алгоритма (алгоритмов) создания, хранения и обновления информации, содержащейся в распределенном реестре, и алгоритма (алгоритмов), обеспечивающего тождественность указанной информации во всех базах данных, которые составляют распределенный реестр, а также (для информационных систем на основе распределенного реестра) невозможность внесения изменений в установленные оператором алгоритм (алгоритмы) иными лицами[68].

На оператора информационной системы, с использованием которой осуществляется заключение смарт-контрактов, целесообразно возложить и обязанности перед пользователями по «переводу» условий смарт-контракта с юридического языка на язык программирования, а также обратного «перевода», в том числе путем предоставления для этого сторонам смарт-контракта специальных юридических конструкторов.

> Функции смарт-контракта предопределяют и то, что к нему едва ли имеет смысл применять традиционные нормы гражданского законодательства о месте заключения договоров (ст. 444 ГК РФ).

Так, с учетом специфического способа заключения смарт-контракта едва ли целесообразно считать местом его заключения место жительства или место нахождения стороны, направившей оферту. Вместо этого логично привязать место заключения договора к виртуальному адресу (цифровому офису)[69] оферента, регистрируемому в системе.

Аналогичный подход целесообразно использовать для целей исполнения смарт-контракта при передаче цифровых активов: местом исполнения логично считать место регистрации виртуального офиса кредитора. В тех же случаях, когда исполнение смарт-контракта производится путем передачи материальных благ (например, при доставке груза), подлежат применению традиционные правила о месте исполнения обязательства (ст. 316 ГК РФ);

5) *отличительные качества смарт-контракта — существенные неизменность его условий и неизбежность исполнения*. Данные свойства очевидны при использовании технологии блокчейн.

Так, к отношениям по смарт-контракту нецелесообразно или даже невозможно, за некоторыми изъятиями, применять ряд традиционных инструментов обязательственного права, например об одностороннем отказе от исполнения договора, зачете, удержании и т.п., если только сами стороны не запрограммировали данные возможности[70].

Однако технология не должна превалировать над объективным правом.

> *Неизменность условий смарт-контракта, как и неизбежность исполнения, не могут и не должны иметь абсолютного характера, поскольку такой подход не соответствует фундаментальным принципам права[71]. Принцип юридического формализма должен уравновешиваться принципом справедливости. Более того, идея об абсолютной неизменности условий противоречит принципу надлежащего исполнения смарт-контракта.*

[68] См.: ч. 1 ст. 6 Закона о цифровых финансовых активах, цифровой валюте. Об ответственности операторов операционной системы, в которой осуществляется выпуск ЦФА, см. ст. 9 Закона.

[69] О «цифровом резидентстве» юридических лиц см.: *Вайпан В.А.* Основы правового регулирования цифровой экономики // Право и экономика. 2017. № 11. С. 9.

[70] Из необходимости участия оператора (операторов) информационной системы для обеспечения заключения и исполнения смарт-контрактов отнюдь не следует то, что операторы обладают возможностями произвольно менять правила системы. Например, в децентрализованной системе изменение правил («кода») может допускаться большинством операторов (пользователей) системы.

[71] «„Автоматизированное исполнение обязательства“ может давать сбои, что уже имело место на практике. Такое паталогическое отклонение действия от условий сделки может квалифицироваться как юридический порок действия по исполнению обязательства, поскольку оно влечет нарушение прав или законных интересов соответствующей стороны. Правопорядок не может уклониться от того, чтобы атрибутировать ненадлежащее исполнение либо с чьей-нибудь волей, либо со случаем или с непреодолимой силой. Ограничение Проектом возможности защиты прав и законных интересов сторон сделки в этих случаях не соответствует Конституции Российской Федерации и противоречит принципам гражданского права. Также надо учитывать, что пороки в модусе исполнения могут возникать не только от действий сторон сделки или третьих лиц, что выделяется в Проекте, но и от событий, не зависящих прямо или вовсе от действий людей» (Экспертное заключение Совета при Президенте Российской Федерации по кодификации и совершенствованию гражданского законодательства от 23.04.2018 № 175-2/2018 по проекту федерального закона № 424632-7 «О внесении изменений в части первую, вторую и четвертую Гражданского кодекса Российской Федерации»). URL: http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=PRJ&n=173392#022406161214113984 (дата обращения: 24.03.2022).

Так, в некоторых случаях у стороны смарт-контракта должна быть возможность потребовать изменения его условий или его расторжения и созданы механизмы, обеспечивающие их реализацию[72].

*Возможность по определенным правилам и в определенных пределах изменять условия исполнения договорного обязательства является средством достижения его исполнения*. Чем сложнее условия смарт-контракта, чем больше промежуток времени между его заключением и исполнением, тем выше вероятность того, что по объективным причинам потребуется вносить изменения в его условия.

Например, изменение данных банковского счета или идентификатора электронного средства платежа, запрограммированных в смарт-контракте, само по себе не влечет прекращения обязанности исполнения обязательства по оплате, однако для надлежащего исполнения потребуется внести коррективы в смарт-контракт.

Изменения внешних обстоятельств могут приводить и к другим тупикам «самоисполнения» «не слишком умного» контракта. Внешнее воздействие в работу информационной системы по исполнению смарт-контракта может потребоваться и в случае смерти гражданина или прекращения юридического лица — стороны смарт-контракта. Смарт-контракт невозможно исполнить на первоначальных условиях и в случае гибели его предмета.

Возникает вопрос об исполнении обязательств при дефектах функционирования информационной системы (например, повреждении данных вредоносной программой), с использованием которой был заключен и подлежал исполнению смарт-контракт, а также в результате ее блокирования со стороны государства.

Внешнее влияние необходимо и для защиты интересов третьих лиц и публичных интересов, например предъявления требований кредитора об обращении взыскания на имущество, которое является предметом смарт-контракта, и т.п.

В качестве способа разрешения коллизии между неотвратимостью исполнения на изначально сформулированных сторонами условиях и потребностью изменений правоотношения рассматривается идея обращения компьютера при определенных обстоятельствах к «оракулу» для определения правил дальнейшего исполнения смарт-контракта[73]. Реализация данной идеи ведет к цифровому арбитражу.

Итак, технические смарт-контракты, «просто коды»[74], годятся лишь для элементарных операций по обмену виртуальными объектами, не обеспечивая в условиях динамики экономической деятельности ни защиту законных интересов их сторон, ни третьих лиц, ни защиту публичных интересов. Бóльшими перспективами обладает дуалистическая концепция, в рамках которой смарт-контракт рассматривается как гражданско-правовой договор особого типа, условия которого определяются как на языке права, так и на языке программирования, а заключение и автоматическое исполнение которого осуществляется с использованием информационной системы.

## 3. Права на программное обеспечение и смарт-контракты

Поскольку смарт-контракт в том числе содержит условия (команды, данные), написанные на языке программирования, то возникает вопрос: *выступает ли программный текст объектом авторского права? На данный вопрос следует ответить положительно, однако лишь при условии, что программный текст смарт-контракта является результатом творческой деятельности* (п. 1 ст. 1259, ст. 1261 ГК РФ)[75]. Автором

[72] Вследствие несовершенства технологий, а также неопределенности будущего принцип невмешательства не следует абсолютизировать. «Не очень умные контракты в будущем могут оказаться еще более опасными: постояльцы отеля могут быть заблокированы в своих номерах, а беспилотные автомобили съезжать с мостов» (*Kolber A.J.* Op. cit. P. 199). Отмечается, что автоматическое исполнение обязательств может противоречить защитным механизмам, предоставляемыми законом потребителям, быть несовместимым с их интересами и поведением (*D'Onfro D.* Smart Contracts and the Illusion of Automated Enforcement // Washington University Journal of Law & Policy. 2020. Vol. 61. P. 173–192).

[73] См.: *Allen J.G.* Wrapped and Stacked: "Smart Contracts" and the Interaction of Natural and Formal Languages // European Review of Contract Law. 2018. Vol. 14. Iss. 4. P. 307–343.

[74] URL: https://ethereum.org/ru/learn/#smart-contracts (дата обращения: 24.03.2022).

[75] См. также: п. 80 Постановления Пленума ВС РФ от 23.04.2019 № 10 «О применении части четвертой Гражданского кодекса Российской Федерации».

и первоначальным обладателем всех авторских прав на него в указанном случае следует считать программиста, его создавшего.

В зависимости от ситуации авторами программной части смарт-контракта могут быть либо обе его стороны, либо одна из сторон, либо третье лицо, к помощи которого стороны прибегли для перевода написанного на языке права текста договора в исходный текст.

Поскольку написанные на юридическом языке условия смарт-контракта нуждаются в их переводе на язык программирования, то возникает вопрос о том, *допустимо ли такую трансляцию считать переводом в смысле создания производного объекта авторских прав* (ст. 1260, подп. 9 п. 2 ст. 1270 ГК РФ)? Такая постановка вопроса логична, если считать, что и текст гражданско-правового договора является результатом творческой деятельности его автора и, как следствие, объектом авторских прав со всеми вытекающими последствиями.

Так, если программист создает исходный текст программы для ЭВМ, которая обеспечивает заключение и автоматическое исполнение договора, основываясь на тексте, написанном юристом (например, на русском языке), то можно ли такой текст считать переводом, а программиста — автором перевода производного объекта авторских прав? От ответа на этот вопрос во многом зависит правовой режим программной части смарт-контракта как объекта авторских прав, в том числе правила его последующего использования, а также внесения в него изменений, дополнений и т.п.

> *На поставленный вопрос следует дать отрицательный ответ. При перенесении юридического содержания договора на язык программирования используются принципиально иные выразительные средства по сравнению с теми, что используются при переводе произведения с одного естественного языка на другой.*

Язык программирования предназначен для управления компьютерным устройством, а не для общения и непосредственной передачи информации другому лицу. Он подчиняется качественно иным по сравнению с человеческим языком правилам построения и в силу своей специфики не позволяет использовать охраняемые авторским правом элементы формы текста договора как своего рода литературного произведения. Программист в подобной ситуации берет из написанного юристом текста только содержание — ожидаемую от сторон договора последовательность действий, которая, как известно, авторским правом не охраняется. Что же касается формы изложения данной последовательности, то она при создании исходного текста программы новая и не будет находиться в непосредственной зависимости от фигур речи, которые были созданы юристом при вербальном формулировании условий договора.

> Признание программной части смарт-контракта объектом авторских прав влечет для сторон смарт-контракта специфические юридические риски, связанные с его исполнением.

В частности, стороны в случае утраты права на программное обеспечение, например в связи с досрочным расторжением лицензионного договора или истечением срока его действия, могут быть признаны нарушителями исключительных прав, если исполнение смарт-контракта будет происходить после указанного момента. Более того, можно представить ситуацию, когда правообладатель воспрепятствует исполнению смарт-контракта посредством предъявления требования о пресечении действия, нарушающего исключительное право[76].

Такое вторжение в сферу отношений сторон смарт-контракта хотя и может показаться, на первый взгляд, несоразмерной санкцией, в действительности таковой едва ли является. Если должник для исполнения обязательства, а кредитор для принятия исполнения используют средства, которые им не принадлежат, то они должны нести риски возможных неблагоприятных последствий. Например, если подрядчик намеревается выполнить работу по договору с помощью украденного у третьего лица инструмента, его обязательства перед заказчиком по договору подряда не смогут заблокировать виндикацию данного инструмента по иску собственника. Принципы недопустимости про-

[76] Реализация данного способа защиты исключительного права применительно к смарт-контракту, заключенному в системе распределенного реестра, проблематична. Так, блокировка государством по требованию правообладателя функционирования такой системы приведет к нарушению интересов добросовестных пользователей. Кроме того, такая блокировка затруднительна с технической точки зрения.

извольного невмешательства в частные дела и *pacta sund servanta* не должны ограничивать обладателя абсолютного имущественного права в возможности его защиты от нарушений.

В связи с дуализмом правовой природы смарт-контракта возникает и вопрос о том, кто и на каких основаниях вправе вносить изменения в программную часть смарт-контракта, в частности, при ее несоответствии тексту, сформулированному на языке применимого права, или ошибках в работе программного обеспечения[77].

При возникновении таких ситуаций у сторон смарт-контракта (если они сами не являются правообладателями) как минимум есть два варианта действий: обращение к правообладателю (например, к оператору централизованной информационной системы, если они пользовались предоставленным им транслятором юридической части смарт-контракта в его программную часть) с требованием об устранении недостатков (данный вопрос будет рассмотрен далее) либо самостоятельное их устранение.

Самостоятельные действия сторон смарт-контракта по устранению недостатков по общему правилу допустимы, поскольку лицо, которое обладает правом использования программы для ЭВМ на основании договора, обладает дополнительными правами, предусмотренными законом. В частности, если иное не предусмотрено договором с правообладателем, в силу п. 1 ст. 1280 ГК РФ пользователь вправе устранять явные ошибки в программе в целях ее использования по назначению. Кроме того, в силу подп. 3 п. 3 ст. 1280 ГК РФ лицо, правомерно пользующееся экземпляром программы для ЭВМ, вправе без согласия обладателя исключительного права на программу и без выплаты ему вознаграждения осуществить декомпилирование компьютерной программы (преобразование объектного кода в исходный текст) в целях интеграции — взаимодействия данной программы с другим программным обеспечением, которое он также использует в своей деятельности.

> Как следует из приведенных норм, проблемы с самостоятельным устранением дефектов программного обеспечения могут возникнуть в случае прекращения у соответствующей стороны смарт-контракта права использования программного обеспечения, например в связи с истечением срока действия лицензии.

На сегодняшний день лицо, не обладающее правом использования программы для ЭВМ, не пользуется правами, предусмотренными ст. 1280 ГК РФ. Как следствие, устранение ошибок в работе программной части смарт-контракта будет неправомерным по отношению к правообладателю действием, если стороны смарт-контракта по каким-то причинам утратят право использования соответствующего ПО.

При самостоятельном устранении ошибок может возникнуть и другая проблема, связанная с тем, что внесение изменений в программную часть смарт-контракта во многих случаях повлечет за собой изменение условий договора. Это, по сути, означает, что устранение ошибок по общему правилу должно согласовываться с обеими сторонами смарт-контракта. Разумеется, возможен вариант, когда стороны при заключении договора предоставят друг другу право на одностороннее изменение его условий в случае, если такие изменения обусловлены необходимостью устранения дефектов в программном обеспечении.

В заключение данного раздела следует также отметить, что в отношении технических устройств и способов, лежащих в основе функционирования программного обеспечения, обеспечивающего исполнение смарт-контракта или сопутствующих его функционированию, возможно установление патентно-правовой охраны в режиме изобретений или полезных моделей[78]. Подобное патентование возможно и в Российской Федерации, поскольку нормы п. 5 ст. 1350, п. 5 ст. 1351 ГК РФ исключают патентование программы для ЭВМ как таковой, но при этом не исключают патентование устройства, ее

[77] Примеры возможных ошибок в работе компьютерной программы, обеспечивающей заключение и исполнение смарт-контракта, см.: Smartcontracts: legal framework and proposed guidelines for lawmakers. P. 30–31. URL: https://www.ebrd.com/documents/legal-reform/pdf-smart-contracts-legal-framework-and-proposed-guidelines-for-lawmakers.pdf (дата обращения: 24.03.2022).

[78] В современной литературе отмечается принципиальная возможность патентования новых технических решений, используемых для заключения и исполнения смарт-контрактов, в странах, признающих патентование софтверных изобретений и изобретений, одним из элементов которых является программное обеспечение. См., напр.: *De Caria R.* The Legal Meaning of Smart Contracts // European Review of Private Law. 2018. No. 26 (6). P. 743.

включающую. В случае успешного патентования у патентообладателя возникнет юридическая монополия на использование подобных технических решений, которая в перспективе может стать серьезным юридическим препятствием для развития и работы централизованных и децентрализованных систем, предполагающих заключение и исполнение смарт-контрактов.

## 4. Гражданско-правовая ответственность разработчика программного обеспечения

Необходимость применения для заключения и исполнения смарт-контрактов программного обеспечения, включая программную составляющую самого смарт-контракта, заставляет задуматься и о гражданско-правовой ответственности за недостатки такого программного обеспечения (дефекты, сбои, ошибки). Очевидно, что в результате ошибок в функционировании программной части смарт-контракта его стороны не только могут не достичь поставленных ими целей сделки, но и лишаться принадлежащего им имущества.

Вопрос о гражданско-правовой ответственности разработчика программного обеспечения имеет значение как в тех случаях, когда стороны смарт-контракта самостоятельно приобретают права на использование соответствующих программных продуктов, так и тогда, когда смарт-контракт заключается сторонами при содействии оператора централизованной информационной системы. В последнем случае оператор такой системы должен иметь возможность в порядке регресса получить от разработчика программного обеспечения компенсацию за возмещенные им сторонам смарт-контракта убытки, которые были причинены в результате дефектов использованного программного обеспечения.

Указанный вопрос в принципе актуален и недостаточно исследован в отечественной и зарубежной юридической науке, а также не до конца решен в правоприменительной практике. Так, судебная практика по вопросу гражданско-правовой ответственности за недостатки программного обеспечения противоречива. Данный вопрос решается судами по-разному в зависимости от того, на каком основании пользователь приобрел право на программное обеспечение[79].

В случаях, когда программа являлась предметом заказа у автора (ст. 1288 ГК РФ) или у посредника (ст. 1296 ГК РФ), суды признают за пользователем-заказчиком право на предъявление требований в связи с недостатками программы, применяя нормы главы 37 ГК РФ о недостатках результата работы (в частности, ст. 723). Со ссылкой на общие положения о купле-продаже и нормы о поставке удовлетворяются требования пользователей и тогда, когда компьютерная программа была ими приобретена на основании договора поставки оборудования с предустановленным программным обеспечением либо на основании смешанного договора, объединяющего в себе предметы договора поставки (в отношении оборудования) и лицензионного договора (в отношении программы). При этом совершенно иначе решается вопрос о привлечении к ответственности за недостатки программного обеспечения, пользователь которого приобрел право использования по лицензионному договору. При рассмотрении дел данной категории суды со ссылкой на особый нематериальный характер программы для ЭВМ как объекта гражданских прав (результат интеллектуальной деятельности) в большинстве случаев отказывают пользователям в удовлетворении требований об устранении недостатков, возмещении убытков и т.п.[80] Редко встречается иной подход, когда требования лицензиата удовлетворяются исходя из общих положений об обязательствах, а также норм о недостатках работы, выполненной по договору подряда, которые применяются по аналогии[81]. Что касается договора об отчуждении исключительного права, то практики по делам о недостатках программного обеспечения, приобретенного пользователем по данному основанию, мы не обнаружили.

Приведенные примеры демонстрируют отсутствие в современной судебной практике единого концептуального подхода к вопросу о последствиях выявления недостатков в компьютерной программе.

[79] Обзор практики по делам данной категории см.: *Мокшанов А.* Некачественное программное обеспечение: защита интересов правоприобретателя. URL: https://zakon.ru/blog/2016/11/9/nekachestvennoe_programmnoe_obespechenie_zaschita_interesov_pravopriobretatelya (дата обращения: 24.03.2022).

[80] См.: постановления ФАС Северо-Западного Сибирского округа от 28.05.2009 по делу № А46-18259/2009; ФАС Московского округа от 30.09.2009 по делу № А40-9849/2009, от 02.07.2013 по делу № А40-111104/2012 // ИС «Картотека арбитражных дел».

[81] См.: решение Арбитражного суда г. Москвы от 25.04.2012 и постановление Девятого ААС от 03.07.2012 по делу № А40-11051/2012 // ИС «Картотека арбитражных дел».

Со сложившейся практикой по договорам заказа трудно не согласиться. И договор авторского заказа, и договор «неавторского» заказа (ст. 1296 ГК РФ) — договоры подрядного типа, поскольку их предметом выступает действие, которое предполагает объективированный результат, отделимый от личности автора (исполнителя). Ввиду отсутствия специального регулирования отношений по сдаче-приемке созданного по заказу произведения (программы для ЭВМ, базы данных) и обнаружении в созданном объекте недостатков логично применение общих положений о подряде (глава 37 ГК РФ).

Применение к отношениям из договоров купли-продажи (поставки) оборудования с предустановленным программным обеспечением норм о купле-продаже и поставке также следует признать верным решением. В подобных случаях программное обеспечение становится частью вещи, оказывающей непосредственное влияние на ее потребительские свойства. Воля сторон подобного договора направлена на отчуждение (приобретение) составной вещи, выполняющей определенные функции, в связи с чем нормы о купле-продаже (поставки) в большей степени соответствуют существу отношений, возникших между сторонами договора. Как верно отмечено в п. 39 Постановления Пленума ВС РФ от 28 июня 2012 года № 17 «О рассмотрении судами гражданских дел по спорам о защите прав потребителей», «требования граждан к качеству программного обеспечения, используемого в технически сложном товаре (например, к операционной системе, которая служит для обеспечения его функционирования), должны рассматриваться как требования к качеству товара в целом с учетом его потребительских свойств в соответствии со статьей 469 ГК РФ». Соответствующий подход был занят Судебной коллегией ВС РФ по гражданским делам при пересмотре дела № 46-КГ20-19-К6. В Определении от 15 декабря 2020 года Коллегия указала, что «…качественным следует признать такой товар, который на протяжении всего срока службы может использоваться в соответствии с конкретными целями, для которых он приобретался, в частности, должна быть гарантирована работоспособность программного обеспечения, используемого в технически сложном товаре, например операционной системы, которая служит для обеспечения его функционирования».

В то же время практика применения норм о поставке к смешанному договору, сочетающему в себе элементы купли-продажи оборудования и предоставления лицензии на программное обеспечение, представляется ошибочной. В той части, в которой отношения сторон данного договора складываются по поводу предоставления права использования программного обеспечения, они не могут подчиняться нормам о купле-продаже ни напрямую, ни по аналогии закона. Применение норм о купле-продаже непосредственно вступает в противоречие с известной нормой п. 3 ст. 421 ГК РФ, согласно которой «к отношениям сторон по смешанному договору применяются в соответствующих частях правила о договорах, элементы которых содержатся в смешанном договоре, если иное не вытекает из соглашения сторон или существа смешанного договора». При отсутствии соглашения сторон об ином их отношения в той части, в которой они являются «лицензионными», должны подчиняться нормам о лицензионном договоре. Применение норм о купле-продаже по аналогии в данном случае также не представляется правильным, поскольку содержательно данные «лицензионные» отношения от отношений по купле-продаже существенно отличаются. Договор купли-продажи предполагает перенос титула собственника: при заключении данного договора воля сторон направлена на последующее отчуждение объекта и, как следствие, переход права на него. Очевидно, что в результате заключения лицензионного договора, который не предполагает переноса титула — перехода исключительного права, возникают принципиально иные отношения, предполагающие лишь временное пользование объектом определенными способами на определенной территории.

> В ходе анализа складывающейся в другом направлении практики по лицензионным договорам прежде всего обращает на себя внимание непоследовательность судебных инстанций в решении вопроса об ответственности за недостатки программного обеспечения.

Если в отношении не только специально созданной компьютерной программы, но и ранее созданной, переданной на основании договора поставки в составе оборудования либо на основании смешанного договора отдельно от оборудования, практика идет по пути привлечения правообладателя к ответственности за недостатки, то в аналогичной ситуации правообладатель, который является стороной лицензионного договора (лицензиаром), от ответственности перед

контрагентом судами освобождается. Данный подход обосновывается спецификой предмета лицензионного договора, коим является право использования результата интеллектуальной деятельности, которое не может быть некачественным, а также отсутствием в части четвертой ГК РФ каких-либо правил о качестве программного обеспечения и последствиях обнаружения недостатков в нем.

Что касается отечественной юридической литературы последних лет, то рассматриваемый вопрос затрагивается в ней нечасто. К.И. Рябов пишет о том, что в доктрине, как отечественной, так и зарубежной, данный вопрос не имеет однозначного решения[82]. А.И. Савельев, анализируя приведенные выше судебные дела в своей работе 2013 года, поддержал подход, согласно которому лицензиар должен нести ответственность за недостатки программного обеспечения по аналогии с исполнителем, оказывающим некачественную нематериальную услугу. По мнению А.И. Савельева, «формально-догматический подход не учитывает таких особенностей компьютерной программы, как ее прикладной и функциональный характер, при котором пользователю важны не форма, а „поведение“ программы. Если компьютерная программа не может выполнить поставленную задачу, это перечеркивает все ее возможные достоинства как объекта авторского права и лишает смысла ее приобретение пользователем»[83]. В качестве дополнительного аргумента в пользу правильности этого решения ученый использовал ссылку на разработанные в 2009 году Американским институтом права Принципы договорного права в сфере программного обеспечения, в которых значительное внимание уделено гарантиям, предоставляемым в отношении компьютерной программы, в том числе гарантиям качества[84]. Однако спустя несколько лет А.И. Савельев, рассматривая вопрос об ответственности за недостатки программного обеспечения применительно к смарт-контрактам и блокчейну, занял противоположную позицию, утверждая, что «с точки зрения действующего российского права и судебной практики лицензиар программного кода не несет ответственности перед лицензиатом за ошибки или дефекты в силу закона, тем самым все риски, связанные с его использованием, лежат на пользователях — участниках блокчейн-проекта». В обоснование данного вывода автор сослался на доводы, содержащиеся в судебных актах, указанных выше (специфика предмета лицензионного договора и отсутствие в части четвертой ГК РФ норм о качестве программного обеспечения). По мнению А.И. Савельева, «можно ставить вопрос о применении аналогии закона, но основным аргументом „против“ будет противоречие положений о качестве товара или работы существу отношений по распоряжению объектами интеллектуальной собственности (особенности предмета такого рода договоров и условий охраноспособности соответствующих объектов)»[85].

Представляется, что в современных условиях и с формально-юридической, и с социально-экономической точки зрения есть все предпосылки для единообразного решения вопроса об ответственности правообладателя за некачественное программное обеспечение. Правообладатель-лицензиар, точно так же как правообладатель — автор или исполнитель по договору заказа и правообладатель — продавец по договору поставки, должен нести ответственность перед лицензиатом за недостатки, которые были выявлены в процессе использования программы. В условиях информатизации современного общества, цифровизации экономики программное обеспечение стало одним из наиболее значимых благ, необходимых для осуществления практически любой современной деятельности человека. В связи с крайне высокой степенью вовлеченности программного обеспечения в производственные и иные экономические процессы, на наш взгляд, было бы в корне неверным исключать ответственность поставщика программного обеспечения и оставлять пользователя один на один с убытками, которые могут возникнуть в связи со срывом того или иного процесса. Избирательный подход к ответственности за недостатки программного обеспечения — в зависимости от основания его приобретения

[82] *Рябов К.И.* Исключительное право на программу для ЭВМ и распоряжение им: дис. … канд. юрид. наук. СПб., 2012. С. 112.

[83] *Савельев А.И.* Актуальные вопросы судебной практики в сфере оборота программного обеспечения в России // Вестник Высшего Арбитражного Суда РФ. 2013. № 4. С. 22.

[84] *Савельев А.И.* Там же. С. 4–36. См. также: *Hillman R.A.*, *O'Rourke M.* Principles of the Law of Software Contracts: Some Highlights. URL: https://scholarship.law.cornell.edu/cgi/viewcontent.cgi?article=1191&context=facpub (дата обращения: 24.03.2022).

[85] *Савельев А.И.* Некоторые правовые аспекты использования смарт-контрактов и блокчейн-технологий по российскому праву. С. 106.

прав на него — не имеет под собой ни достаточных юридических, ни весомых социально-экономических оснований.

> В условиях действующего правового регулирования, не содержащего специальных норм по рассматриваемому вопросу, лицензиар должен отвечать за некачественное программное обеспечение на таких же условиях, на каких арендодатель и ссудодатель отвечают перед контрагентом за недостатки предоставленной во временное пользование вещью.

В связи с содержательной близостью «лицензионных» отношений и отношений, возникающих из договоров аренды и ссуды (и в том, и в другом случае предполагается временное пользование чужим благом), нормы глав 34 и 36 ГК РФ, за исключением случаев явного противоречия существу отношений, должны применяться по аналогии к лицензионному договору о предоставлении права использования программы для ЭВМ, когда этого требует пробел в правовом регулировании[86]. Вопреки встречающемуся в судебных актах и литературе утверждению, интеллектуально-правовая природа программы для ЭВМ никоим образом не препятствует применению по аналогии норм, рассчитанных на отношения временного пользования вещью. Программа для ЭВМ, которая является в большинстве случаев инструментом решения практической задачи, носит утилитарный характер. В связи с такими ее особенностями особый правовой режим результата интеллектуальной деятельности не должен при возникновении пробела в правовом регулировании препятствовать применению по аналогии норм, регулирующих отношения по поводу временного пользования вещью.

Следует также отметить, что действующее законодательство не содержит и сугубо формальных препятствий для применения аналогии закона в данном случае. Установленное в п. 2 ст. 1227 ГК РФ ограничение на аналогию закона в праве интеллектуальной собственности относится лишь к нормам раздела II ГК РФ «Право собственности и другие вещные права»[87]. Более того, целесообразность и обоснованность применения норм главы 34 ГК РФ об аренде к отношениям из лицензионного договора отмечается современными специалистами в области частного права[88].

Таким образом, при выявлении недостатков в программе для ЭВМ лицензиат, пользующийся ею на основании возмездного лицензионного договора, вправе, опираясь на аналогию закона, защищаться по правилам ст. 612 ГК РФ, согласно которым арендодатель отвечает за скрытые недостатки вещи даже в том случае, если он не знал о них в момент заключения договора. Лицензиат, которому право использования программы было предоставлено безвозмездно, вправе при обнаружении недостатков защищаться со ссылкой на положения ст. 693 ГК РФ, в соответствии с которыми ссудодатель отвечает за скрытые недостатки вещи, которые он умышленно или по грубой неосторожности скрыл от ссудополучателя при заключении договора.

Все сказанное об ответственности лицензиара за недостатки программного обеспечения может быть сведено на нет договорным условием *as is* («как есть»), которое часто включается в тексты современных лицензионных договоров. Смысл данного условия как раз сводится к тому, что лицензиар освобождается от ответственности за любые сбои и ошибки, которые могут проявиться при использовании программы лицензиатом. Однако представляется, что данное условие договора может квалифицироваться по-разному в зависимости от того, является ли договор предпринимательским или не является таковым, а также от иных обстоятельств его заключения.

Включение условия *as is* в лицензионный договор между субъектами предпринимательской деятельно-

[86] О применении норм об аренде к отношениям из лицензионного договора см.: Протокол № 19 заседания Научно-консультативного совета при Суде по интеллектуальным правам от 27.04.2018 // Журнал Суда по интеллектуальным правам. 2018. № 21. С. 6–28. URL: http://ipcmagazine.ru/official-cronicle/protocol-19-of-the-meeting-of-the-scientific-advisory-council-at-the-court-for-intellectual-property-right (дата обращения: 25.03.2022).

[87] О спорности данного законодательного решения см.: *Сергеев А.П.* Применение правил раздела II «Право собственности и другие вещные права» Гражданского кодекса РФ к отношениям интеллектуальной собственности // Закон. 2018. № 12. С. 87–95; *Иванов Н.* Доля в исключительном праве // Интеллектуальная собственность. Авторское право и смежные права. 2017. № 1. С. 26–34.

[88] См.: Протокол № 19 заседания Научно-консультативного совета при Суде по интеллектуальным правам от 27.04.2018.

сти по общему правилу следует считать допустимым, а само условие действительным и подлежащим применению. При этом необходимо учитывать по крайней мере две нормы закона, которые ограничивают действие данного условия. Во-первых, условие *as is* не должно применяться, если будет установлено, что программа была снабжена недостатками намеренно (п. 4 ст. 401 ГК РФ). Конечно, доказать и установить подобный умысел со стороны лицензиара крайне сложно, но теоретически возможно. Во-вторых, включение в договор условия *as is* может привести к отрицательным юридическим последствиям при неравенстве переговорных возможностей сторон, которое часто имеет место при заключении пользователем договора с крупными правообладателями и всегда имеет место при приобретении так называемых оберточных или коробочных лицензий. Если данное неравенство будет установлено, это приведет к возникновению у лицензиата права на изменение или расторжение договора в одностороннем порядке (п. 2, 4 ст. 428 ГК РФ, п. 10 Постановления Пленума ВАС РФ от 14 марта 2014 года № 16 «О свободе договора и ее пределах»).

При заключении лицензионного договора между лицензиаром-предпринимателем и лицензиатом – не предпринимателем (в особенности, потребителем) неравенство переговорных возможностей должно предполагаться. Учитывая важность данного условия с точки зрения имущественных последствий, которые оно может повлечь, есть основания для квалификации его как несправедливого, что дает возможность лицензиату требовать изменения либо расторжения договора, а также возмещения причиненных убытков. По крайней мере, такой подход следует, на наш взгляд, применять к возмездным лицензионным договорам, заключаемым между предпринимателем и потребителем.

Все сказанное в отношении лицензионного договора в целом должно относиться и к договору об отчуждении исключительного права на компьютерную программу. Отличия в решении вопроса о последствиях выявления недостатков в компьютерной программе применительно к данному договору состоят в том, что приобретатель исключительного права, в отличие от лицензиата, вправе защищаться со ссылкой на нормы ГК РФ о купле-продаже либо дарении, в зависимости от того, является договор об отчуждении исключительного права возмездным или безвозмездным. Близость классических договорных конструкций: купли-продажи, дарения, с одной стороны, и договора об отчуждении исключительного права — с другой, очевидна. Воля сторон договоров купли-продажи, дарения, договора об отчуждении исключительного права направлена на последующую смену правообладателя — переход имущественного права от одной стороны договора к другой.

Поскольку действующее правовое регулирование договора об отчуждении исключительного права на программу для ЭВМ не содержит каких-либо норм о качестве объекта, последствиях выявления в нем недостатков и т.п., представляется, что есть все основания для применения положений ГК РФ о купле-продаже и дарении.

Нормы о купле-продаже могут быть распространены на отношения сторон договора об отчуждении исключительного права не по аналогии закона (п. 1 ст. 6 ГК РФ), а непосредственно в силу известной отсылочной нормы, содержащейся в п. 4 ст. 454 ГК РФ. В частности, нормы о качестве проданного товара и последствиях обнаружении недостатков (ст. 469–471, 474–477 ГК РФ) должны применяться к возмездному договору об отчуждении исключительного права на программу для ЭВМ в связи с утилитарным характером программного обеспечения, который наделяет его признаками товара, обладающего определенными качественными характеристиками и подлежащего использованию по определенному назначению.

Что касается норм о дарении, то они могут быть применены в данном случае по аналогии закона (п. 1 ст. 6 ГК РФ). Как известно, нормы главы 32 ГК РФ не обязывают дарителя предоставить вещь определенного качества и не предусматривают санкции за дефекты, обнаруженные в подаренной вещи. Соответственно, если иное не предусмотрено договором об отчуждении исключительного права, при выявлении недостатков в программном обеспечении, исключительное право на которое предоставлено безвозмездно, приобретатель по общему правилу не вправе требовать их устранения и возмещения причиненных убытков. Исключение могут составлять случаи предоставления бесплатно вредоносного программного обеспечения

с целью причинить убытки приобретателю. Согласно ст. 580 ГК РФ если одаряемому будет причинен вред в связи с использованием подаренной вещи, он вправе требовать возмещения причиненных ему убытков по правилам главы 59 ГК РФ, если будет установлено, что недостатки возникли до передачи вещи, даритель знал о них, но не предупредил одаряемого. Представляется, что точно таким же должен быть подход в случае выявления приобретателем недостатков в компьютерной программе, исключительное право на которую он получил по безвозмездному договору об отчуждении исключительного права. Кроме того, в подобной ситуации приобретатель в обоснование требования о возмещении причиненных убытков может дополнительно ссылаться на общие нормы о добросовестности участников гражданских правоотношений и недопустимости злоупотребления правом (ст. 1, 10 ГК РФ).

Таким образом, пользователь программного обеспечения, в том числе предназначенного для заключения и исполнения смарт-контрактов, вправе рассчитывать на его корректную работу, исходя из заявленных правообладателем функциональных характеристик. В случае выявления в программном обеспечении недостатков пользователь вправе требовать от своего контрагента их устранения, возмещения причиненных убытков, а также применения иных санкций, исходя из норм закона, регулирующих соответствующие договорные конструкции, и условий договора, заключенного с правообладателем. Исключение могут составлять случаи договорного ограничения ответственности правообладателя (с учетом нормы п. 4 ст. 401 ГК РФ), а также включения в лицензионный договор условия *as is* («как есть»), если при этом будет соблюдено предусмотренное действующим законодательством правило о равенстве переговорных возможностей при заключении лицензионного договора.

## 5. Заключение

Итак, изложенное позволяет сделать вывод, что смарт-контракт хотя и является новой юридической категорией, обусловленной развитием цифровых технологий, но все же его нельзя считать конструкцией, «бросающей вызов классическим доктринам договорного права». Признание смарт-контракта гражданско-правовым договором влечет применение к нему, хотя и с учетом ряда особенностей, не только основных положений договорного права, но и гражданского права в целом. Производители программного обеспечения должны по общему правилу нести гражданско-правовую ответственность за некачественную работу программных продуктов, используемых при заключении и исполнении автоматически исполняемых договоров.

## Towards a Civil-Law Theory of Smart Contracts

The article examines the issue of the place of smart contracts in the legal systematization. The main difference between a smart contract and traditional civil law contracts is seen in the fact that its conclusion occurs in electronic form within information system, while its essential terms determine the automatic transfer of property rights. Despite the fact that the terms of the smart contract must include commands and data necessary for its automatic execution, the language of the applicable law should be the primary language of the smart contract. The contract cannot be self-executing, it's an illusion. For the conclusion and execution of smart contracts it is necessary not only to express the mutual will of its parties, but also the participation of the operator of the information system, as well as the existence of the rules of the information system. In a decentralized system the operator's functions are performed by the users of the system, united in the civil law community. As a general rule, software manufacturers should bear property liability for poor-quality work of software products used in the conclusion and execution of automatically executed contracts.

***Keywords:*** *smart contract, automatic execution of obligation, information system, computer program, liability for software defects*

### INFORMATION ABOUT THE AUTHOR

**Georgy V. Tsepov**
Advocate, Associate Professor at National Research University "Higher School of Economics", Candidate of Juridical Sciences (e-mail: gtsepov@hse.ru).

**Nikita V. Ivanov**
Head of the Department of Civil Law and Process at National Research University "Higher School of Economics", Associate Professor, Candidate of Juridical Sciences (e-mail: nivanov@hse.ru).

## REFERENCES


Allen, J.G. Wrapped and Stacked: “Smart Contracts” and the Interaction of Natural and Formal Languages. European Review of Contract Law. 2018. Vol. 14. Iss. 4. P. 307–343.

Arkhipov, V.V., Naumov, V.B. Informational and Legal Aspects of Drawing up Robotics Legislation [*Informatsionno-pravovyye aspekty formirovaniya zakonodatel’stva o robototekhnike*]. Information law [*Informatsionnoye pravo*]. 2017. No. 1. P. 19–27.

Belov, S.A, Kropachev, N.M., Revazov, M.A. Judicial Control over Compliance with the Norms of Contemporary Russian Literary Language [*Sudebnyy kontrol’ za soblyudeniyem norm sovremennogo russkogo literaturnogo yazyka*]. Statute [*Zakon*]. 2017. No. 3. P. 103–115.

Belov, S.A., Kropachev, N.M. What Has to Be Done to Make the russian Language National? [*Chto nuzhno, chtoby russkiy yazyk stal gosudarstvennym?*]. Statute [*Zakon*]. No. 10. P. 100–112.

Belykh, V.S., Bolobonova, M.O. Some Issues of Legal Regulation of Smart Contracts in Russia [*Problemy pravovogo regulirovaniya smart-kontraktov v Rossii*]. In Vaypan, V.A., Yegorova, M.A. (eds.) Legal Regulation of Economic Relations in Modern Conditions of Development of the Digital Economy: Monograph [*Pravovoye regulirovaniye ekonomicheskikh otnosheniy v sovremennykh usloviyakh razvitiya tsifrovoy ekonomiki: monografiya*]. Moscow, 2019. P. 97–116.

Casey, A.J. and Niblett, A. The Death of Rules and Standards. Indiana Law Journal. 2017. Vol. 92. No. 4. P. 1401–1447.

Churilov, A.Yu. The Use of Blockchain Technology: a Payment System, “Smart” Contracts, Adoption of Collegial Decisions, Storage of Information [*Ispol’zovaniye tekhnologii blokcheyn: platezhnaya sistema, “umnyye” kontrakty, prinyatiye kollegial’nykh resheniy, khraneniye informatsii*]. In Internet Law: A Collection of Articles [*Pravo v sfere Interneta: sbornik statey*] ed. M.A. Rozhkova. Moscow, 2018. P. 144–158.

De Caria, R. The Legal Meaning of Smart Contracts. European Review of Private Law. 2018. Iss. 6. P. 731–751.

D’Onfro, D. Smart Contracts and the Illusion of Automated Enforcement. Washington University Journal of Law & Policy. 2020. Vol. 61. P. 173–192.

Efimova, L.G., Sizemova, O.B. The Legal Nature of a Smart Contract [*Pravovaya priroda smart-kontrakta*]. Banking Law [*Bankovskoye pravo*]. 2019. No. 1. P. 21–30.

Efimova, L.G. The Concept and Legal Aspects of Electronic Contracts [*Ponyatiye i pravovyye osobennosti elektronnogo dogovora*]. Laws of Russia: Experience, Analysis, Practice [*Zakony Rossii: opyt, analiz, praktika*]. 2019. No. 7. P. 84–90.

Fedorov, D.V. Russian Draft Laws on Tokens, Cryptocurrency and Smart-Contracts Regulation From the Perspective of Foreign Experience [*Tokeny, kriptovalyuta i smart-kontrakty v otechestvennykh zakonoproyektakh s pozitsii inostrannogo opyta*]. Bulletin of Civil Law [*Vestnik grazhdanskogo prava*]. 2018. No. 2. P. 30–74.

Grimmelmann, J. All Smart Contracts Are Ambiguous. Journal of Law and Innovation. 2019. Vol. 2. No. 1. P. 2–22.

Herder, I.G. Ideas on the Philosophy of Human History. [*Idei k filosofiii istorii chelovechestva*]. Moscow, 1977. 703 p.

Hillman, R.A., O’Rourke, M. Principles of the Law of Software Contracts: Some Highlights. URL: https://scholarship.law.cornell.edu/cgi/viewcontent.cgi?article=1191&context=facpub.

Hunn, P.G. Smart Contracts as Techno-Legal Regulation. Journal of ICT Standardization. 2019. Vol. 7. Iss. 3. P. 269–286.

Ivanov, A.A. Penetration of Mechanisation in Law [*O glubine mashinizatsii prava*]. Statute [*Zakon*]. 2018. No. 5. P. 35–41.

Ivanov, N. Share in Exclusive Right. Intellectual Property [*Dolya v isklyuchitel’nom prave. Intellektual’naya sobstvennost’*]. Copyright and Related Rights [*A vtorskoye pravo i smezhnyye prava*]. 2017. No. 1. P. 26–34.

Kolber, A.J. Not-So-Smart Blockchain Contracts and Artificial Responsibility. Stanford Technology Law Review. 2018. Vol. 21. Iss. 2. P. 198–234.

Krasavchikov, O.A. Legal Facts in Soviet Civil Law [*Yuridicheskie fakty v sovetskom grazhdanskom prave*]. In the book: Krasavchikov, O.A. Categories of the science of Civil Law: Selected Works [*Kategorii nauki grazhdanskogo prava: Izbrannyye trudy*]: in 2 volumes. Vol. 2. 494 p.

Lenin, V.I. Party Organization and Party Literature [*Partiynaya organizatsiya I partiynaya literatura*] Complete collection of V.I. Lenin’s works, 5th ed. Vol. 12. Moscow, 1968. 575 p.

Lessig, L. Code is Law. On Liberty in Cyberspace. URL: https://www.harvardmagazine.com/2000/01/code-is-law-html.

O’Shields, R. Smart Contracts: Legal Agreements for the Blockchain. North Carolina Banking Institute. 2017. Vol. 21. Iss. 1. P. 177–194.

Posner, R.A. Economic Analysis of Law [*Ekonomicheskiy analiz prava*]. In 2 vol. Vol. 1. St. Petersburg, 2004. 544 p.

Ryabov, K.I. The Exclusive Right to a Computer Program and its Disposal. The dissertation for the degree of candidate of legal sciences [*Isklyuchitel’noye pravo na programmu dlya EVM I rasporyazheniye im: dissertatsiya na soiskaniye uchenoy stepeni kandidata yuridicheskikh nauk*]. St. Petersburg, 2012.

Savelyev, A.I. Actual Issues of Judicial Practice in the Field of Software Turnover in Russia [*Aktual’nyye voprosy sudebnoy praktiki v sfere oborota programmnogo obespecheniya v Rossii*]. Bulletin of the Supreme Arbitration Court of the Russian Federation [*Vestnik Verhovnogo Suda Rossijskoj Federacii*]. 2013. No. 4. P. 4–36.

Savelyev, A.I. Some Legal Aspects of Implementation of Smart Contracts and Blockchain Technologies under Russian Law

[*Nekotoryye pravovyye aspekty ispol'zovaniya smart-kontraktov I blokcheyn-tekhnologiy po rossiyskomu pravu*]. Statute [*Zakon*]. 2017. No. 5. P. 95–117.

Sergeev, A.P. Section II "Ownership and Other Property Rights as Applied to Intellectual Property Relations" [*Primeneniye pravil razdela II "Pravo sobstvennosti I drugiye veshchnyye prava" Grazhdanskogo kodeksa RF k otnosheniyam intellektual'noy sobstvennosti*]. Statute [*Zakon*]. 2018. No. 12. P. 87–95.

Shershenevich, G.F. Course of Civil Law [*Kurs grazhdanskogo prava*]. Tula, 2001. 720 p.

Sokolova, M.A. Defects of Legal Documents: Monograph [*Defekty yuridicheskikh dokumentov: monografiya*]. Moscow, 2016. 160 p.

Szabo, N. Smart Contracts: Building Blocks for Digital Markets? URL: http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_2.html.

Tolstoy, Yu.K. To the Theory of Legal Relationship [*K teorii pravootnosheniya*]. Leningrad, 1959. 88 p.

Vaypan, V.A. Legal Basis for Digital Economy [*Osnovy pravovogo regulirovaniya tsifrovoy ekonomiki*]. Law and Economics [*Pravo I ekonomika*]. 2017. No. 11. P. 5–18.

Volos, A.A. Smart Contracts and Civil Law Principles [*Smart-kontrakty I printsipy grazhdanskogo prava*]. Russian justice [*Rossiyskaya yustitsiya*]. 2018. No. 12. P. 5–7.

Volos, A.A. The Civil Law Essence of a Smart Contract [*Grazhdansko-pravovaya sushchnost' smart-kontrakta*]. Lawyer [*Yurist*]. 2019. No. 7. P. 23–28.

Vygotsky, L.S. Thinking and Speaking. Psychological Research. [*Myshleniye i rech'. Psikhologicheskoye issledovaniye*]. Moscow – Leningrad, 1934. 324 p.

Zakharkina, A.V. Smart Contracts and the Development of Regulatory Framework for the Digital Economy Ecosystem in the Russian Federation [*Smart-kontrakt v usloviyakh formirovaniya normativnoy platformy ekosistemy tsifrovoy ekonomiki Rossiyskoy Federatsii*]. Perm University Herald. Juridical Sciences [*Vestnik Permskogo universiteta. Yuridicheskiye nauki*]. 2020. No. 1. Iss. 47. P. 66–82.

**АНТОН АЛЕКСАНДРОВИЧ ИВАНОВ**

научный руководитель факультета права Национального исследовательского университета «Высшая школа экономики», профессор, кандидат юридических наук

# САМЫЙ ЛУКАВЫЙ НАЛОГ

Статья посвящена анализу налога на добавленную стоимость (НДС) исходя из понятия добавленной стоимости в том виде, в каком оно используется в экономике и гражданском праве. Особое внимание уделено роли, которую налог играет в экономике России, его экономической обоснованности и справедливости. Именно под этим критическим углом зрения рассматриваются ключевые нормы налогового права об НДС. Внимание сосредоточено на тех правилах, которые требуют корректировки.

***Ключевые слова:*** *налог, добавленная стоимость, НДС, оборот золота, упрощенные формы налогообложения*

DOI: 10.37239/0869-4400-2022-18-3-173-179

Можно не сомневаться, что самый собираемый, а значит, и самый деструктивный для экономической жизни налог одновременно и самый лукавый. И это налог на добавленную стоимость (НДС)! Вы спросите, в чем его лукавство? А в том, что он в максимальной степени искажает обычные житейские понятия, чтобы искусственно повысить собираемость. Тому есть немало примеров, но начнем с самого простого.

Считается, что НДС облагает налогом добавленную стоимость, т.е. такую, которая у конкретного налогоплательщика увеличилась по сравнению со стоимостью того блага, которое он приобрел у другого лица. Значит, была одна стоимость, стала другая — и с разницы надо заплатить налог. На первый взгляд, выглядит справедливо, насколько вообще справедливыми являются налоги — механизм принудительного отъема государством денег у налогоплательщиков.

Если же стоимость не добавлена — нет и НДС, поскольку разница нулевая. Но тут есть одна уловка, связанная с методикой расчета: сумма налога образуется как разница между НДС уплаченным и полученным. Если эта разница положительная, налицо сумма налога к уплате. При нулевой или отрицательной разнице никакого налога нет, поскольку нет и добавленной стоимости. Правда, некоторые операции освобождены от уплаты НДС, и положительная разница все равно образуется.

Возьмем в качестве примера куплю-продажу золотых слитков. Их особенность состоит в физической неизменности. Золото — всегда золото. Так что никаких добавлений нет. Напротив, если слитки повреждены, это снижает их цену, пусть и несущественно. А НДС есть, поскольку покупка слитков у банка облагается этим налогом, а обратная продажа банку — нет. Между тем продается один и тот же предмет. По справедливости, государство при обратной продаже золотого слитка должно возвращать НДС, уплаченный ранее при его покупке, либо вообще не брать его при покупке, как происходит в обычных операциях с золотыми монетами (формально наличными деньгами). Вот и налицо лукавство.

Разумеется, рыночная цена золота меняется, в современных условиях нельзя вести речь о «золотом стандарте», когда само золото — деньги[1]. Но очевидно, что от самого гражданина данный процесс не зависит, он просто держит в руках один и тот же предмет. Текущая цена его может падать или повышаться по сравнению с ценой приобретения, соответственно возникают «–» или «+», которые в текущем режиме не учитываются. А вот когда золотой слиток продается, НДС берется со всей цены без учета ее изменений и без права на вычет.

Так же происходит и с другими сделками купли-продажи с участием граждан, но последние обычно потребляют приобретенные блага, а не перепродают их, и вопрос о возврате НДС не встает. Когда же продаются использованные (подержанные) вещи, ясно, что к ним добавлено то, как и в случае с золотом, что возникло под влиянием рыночной конъюнктуры. А так налицо физический износ (нечто убавленное). Рассчитать НДС при таких обстоятельствах затруднительно. В этом смысле золотые слитки — удачный пример, поскольку они неизменны. Даже земельные участки и иное недвижимое имущество физически меняются[2].

Внимание, вопрос! Нельзя ли воспользоваться тем, что сделки с золотыми слитками — яркий пример лукавства НДС, и поставить перед судами вопрос о возврате после продажи налога, уплаченного при покупке слитка — с учетом процента его физического износа.

> Мотивировка простая: нарушены правила о том, что у налога должны быть разумные экономические основания[3], которых в нашем случае, увы, нет. Никакая стоимость, связанная с усилиями людей, при продаже золотых слитков не добавляется, налицо лишь несправедливое изъятие, установленное законом[4].

Теперь о другом аспекте НДС. Ничего плохого в том, чтобы облагать налогом добавленную стоимость и определять сумму к уплате как разницу между НДС полученным и уплаченным, *a priori* нет. Нужно же как-то формализовать этот налог, с тем чтобы он одинаково взимался в различных ситуациях. Все-таки равенство налогообложения — конституционный принцип. Разумеется, некоторые различия в зависимости от категорий налогоплательщиков допустимы, но они не должны быть чрезмерными[5].

В случае с облагаемыми НДС операциями с золотыми слитками и не облагаемыми НДС операциями с золотыми монетами (деньгами) разница неоправданно высока. И те и другие объекты изменяют свою стоимость

[1] См. подробнее: *Bretton Woods system*. URL: https://en.wikipedia.org/wiki/Bretton_Woods_system (дата обращения: 21.03.2022).

[2] Аналогом золота в этом смысле являются ценные бумаги. То, что к ним добавлено (или убавлено), очень сильно зависит от рыночных цен. Неслучайно подоходный налог от операций с ценными бумагами взымается в особом порядке.

[3] Постановления КС РФ от 12.11.2020 № 46-П, от 22.06.2009 № 10-П; Президиума ВАС РФ от 08.10.2013 № 3589/13, от 08.12.2009 № 11715/09.

[4] Неслучайно недавно было принято решение отменить НДС на операции с золотыми слитками. URL: https://www.tinkoff.ru/invest/news/772140 (дата обращения: 21.03.2022).

[5] Так, в Постановлении КС РФ от 23.12.1999 № 18-П взнос во внебюджетные фонды в размере 20,6% от заработка (дохода) для нотариусов, глав крестьянских (фермерских) хозяйств и адвокатов признан неконституционным, поскольку государственные трудовые пенсии данных категорий не соответствуют размерам взносов.

в зависимости от рыночных условий, что учитывается в цене. Довесок в виде НДС не имеет разумного экономического смысла с точки зрения неизменности объектов соответствующих сделок, к которой обладатели ничего не добавляют. И механизм, который приводит к несправедливому налогообложению, состоит в освобождении от налога одних операций и взимании его при других, по сути таких же.

Однако это не единственное проявление лукавства НДС, когда добавленной стоимости нет, а налог есть. Точнее, облагается налогом и та стоимость, которая не добавлена, а перешла к конкретному плательщику от иного лица. Обратимся к другой, намного более значимой для общества сфере — к оплате труда. Действительно, труд добавляет стоимость к товару, но он же и уменьшает значительную часть этой стоимости при выплате зарплаты и отчислений в социальные фонды.

> Между тем НДС взимается таким образом, как будто все, что принес труд, является добавленной стоимостью. На самом деле это не так. Добавленной является лишь та часть стоимости, которая уменьшена на величину выплаченной зарплаты и отчислений в социальные фонды.

Работодатели и работники (граждане) — разные субъекты права. Первые платят НДС, вторые — нет. А поскольку суммы налога к уплате не уменьшаются на виртуальные начисления НДС при выплате зарплаты работникам и платежей в социальные фонды, объектом налогообложения в этой части перестает быть добавленная стоимость. Объектом становится в значительной мере стоимость убавленная, поскольку никакого вычета из НДС к уплате не производится. К тому же такой порядок налогообложения ставит в заведомо невыгодное положение тех работодателей, у кого большие затраты на труд[6]. А ведь они как раз и развивают национальное производство[7].

Может возникнуть вопрос: а что, труд вообще не создает добавленной стоимости? Создает, но лишь в той части, в которой эта стоимость присваивается работодателем, т.е. за вычетом заработной платы работников и отчислений в социальные фонды. Добавленную стоимость создает и предпринимательский труд, и та доля труда работника, которую присваивает себе работодатель. Все остальное стоимость уменьшает, и лишь только вследствие особенностей обложения НДС увеличивает его налоговую базу. На самом деле в той части, в которой оплачивается труд работников и производятся отчисления в социальные фонды, НДС вообще не должен взиматься.

Тем более это очевидно применительно к отчислениям в социальные фонды, где вообще имеет место двойное налогообложение, что сейчас скрыто, поскольку эти отчисления — формально не налог. Зато когда был единый социальный налог (ЕСН), с одной и той же суммы удерживался и НДС, и ЕСН — классическое двойное налогообложение. Да и сейчас мало что изменилось, поскольку отчисления в социальные фонды столь же обязательны, как и налоги. К тому же они делаются в пользу работников (кроме, пожалуй, отчислений на социальное страхование, которые имеют двойственную природу). Никакой пользы для работодателей — плательщиков НДС они не предоставляют.

> Именно поэтому у нас такая высокая нагрузка на труд, одна из самых высоких в мире, когда к обязательным отчислениям добавляется еще и налог на добавленную стоимость, тогда как исходя из экономической природы этого налога он должен уменьшаться в части выплаты зарплаты и отчислений в социальные фонды.

Тогда налоговая нагрузка работодателей была бы существенно ниже, а перенос обязательных отчислений на работников способствовал бы обелению теневой зарплаты гораздо эффективнее, чем все меры по борьбе с обналичиванием денег и их отмыванием. Причем даже если в отношении подоходного налога и обязательных платежей работодатель по-прежнему оставался бы налоговым агентом.

Кстати, точно такая же логика применима и в отношении специальных налоговых режимов, которые включают в свой состав освобождение от уплаты НДС. Хорошенькое «освобождение»: государство ис-

---

[6] См. подробнее: раздел «Налоги» доклада Президенту Российской Федерации от 2020 года «Реестр системных проблем российского бизнеса». URL: http://doklad.ombudsmanbiz.ru/2020/3.pdf (дата обращения: 21.12.2021).

[7] Не потому ли у нас экономика приобрела чисто сырьевой уклон, причем на экспорт отправляется главным образом непереработанное сырье. Порядок начисления НДС этому в немалой степени способствует.

ходя из своих соображений перекладывает бремя по уплате налога на контрагента, не освобожденного от уплаты НДС, облегчая участь того, кому предоставлен льготный режим. А в чем тут добавленная стоимость? В особенностях определения налоговой базы, если стоимость, по сути, не добавляется? Ведь добавляется она лишь тому, кто находится на специальном налоговом режиме, и то не всегда. А последний-то от НДС освобожден!

По справедливости, плательщик НДС должен уменьшать сумму налога к уплате на виртуальную сумму, которую он списал бы, будь получатель денег плательщиком НДС. Тогда льготный режим, который предоставляется государством, был бы по-настоящему справедливым. Преимущество получает один налогоплательщик, а второй ничего не теряет. *Win-Win!* Существующий же сейчас порядок лишь дискриминирует малый бизнес, пользующийся специальными налоговыми режимами, поскольку плательщики НДС стараются выбирать тех контрагентов, платежи которым уменьшают их НДС к уплате[8].

И наконец, про НДС в ином, сущностном аспекте. Это косвенный налог, который рассчитывается в виде разницы между налогом, полученным от контрагентов «в цене» товара или услуги (сейчас по общему правилу по ставке 20%), и налогом уплаченным, в свою очередь, за приобретенные товары и услуги (обычно по той же ставке). Если налога получено больше, чем уплачено, разница подлежит уплате в бюджет. Отрицательная разница возмещается в случаях и в порядке, предусмотренных законом, причем далеко не всегда.

Изначально не имело значения, кому была уплачена сумма с НДС. Главное, что она уплачена. Такова природа косвенного налога, которой воспользовались злостные неплательщики, в результате чего возникла существующая система обналичивания денег. Конкретное лицо переводило сумму с НДС кому-то и считало себя свободным от каких-либо обязательств. А уплатил ли получатель налог в бюджет, плательщика не волновало. Подобного рода злоупотребления начиная с середины 90-х годов прошлого века приобрели столь массовый характер, что резко снизили поступления в бюджет не только НДС, но и других налогов[9]. Обналичка избавляла бизнес от всех напастей.

Справедливости ради нужно отметить, что в момент появления НДС налоги, при их полной уплате, поглощали до 90% всех доходов, а то и больше. Это вместе с гиперинфляцией, которую допустило государство, полностью лишало налогоплательщиков стимулов к своей деятельности. Поэтому они обратились к обналичке не от хорошей жизни, а вынужденно. Но как часто бывает, то, что делается по принуждению, может потом понравиться и стать методом ведения предпринимательской деятельности, от которого никто не готов отказаться.

Обналичка давала огромную массу неучтенных денег, благодаря которым все — и работодатели, и работники — максимизировали свой доход за счет неуплаченных налогов. Не остались внакладе и чиновники, которые незаконно участвовали в предпринимательской деятельности или получали взятки. Неучтенная наличка подпитывала их многочисленные потребности. Поскольку борьбой с обналичиванием занимались правоохранительные органы, очень скоро они стали крышевать соответствующую деятельность, а то и сами ею заниматься[10]. Система выкристаллизовалась, а бюджет серьезно пострадал.

Борьба с обналичкой велась, но с переменным успехом. Как только пресекалась определенная схема ухода от налогов, на ее место становилась новая, на расшифровку и поиск методов борьбы с которой уходило время. Напоминало это соревнование между замка́ми и взломщиками: чем сложнее становились

[8] См.: *Егорова Н.* «Ограничители» для применения УСН в 2017 г. // Информационный бюллетень «Экспресс-Бухгалтерия». 2016. № 30. С. 13.

[9] См. подробнее: отчет Евразийской группы по противодействию легализации преступных доходов и финансированию терроризма «Структурный анализ финансовых потоков, связанных с обналичиванием, направленных на совершение правонарушений и отмывание преступных доходов». URL: https://eurasiangroup.org/files/TYPOLOGY%20REPORTS/WGTYP_2017_11_rev_1_rus.pdf (дата обращения: 21.03.2022); исследование Банка России «Структура сомнительных операций и секторы экономики, формировавшие спрос на теневые финансовые услуги». URL: https://cbr.ru/today/resist/resist_sub/2021_1/ (дата обращения: 21.03.2022).

[10] Как работает «налоговая крыша» в ДЭБ МВД. URL: https://newsland.com/user/4297694390/content/kak-rabotaet-nalogovaia-krysha-v-deb-mvd/4107230 (дата обращения: 21.03.2022).

первые, тем изощреннее действовали вторые. Пока не пришло понимание, что без лишения НДС свойства косвенного налога проблему не решить.

На самом деле, конечно, есть более цивилизованный, хотя и намного более долгий путь — сделать уплату налогов категорическим нравственным императивом для подавляющего большинства людей. Однако на этом пути так много препятствий, и главное из них — низкое качество государственного управления. Изменять себя государство было не готово, поскольку это предполагало использование множества механизмов эффективного общественного контроля: переход к реальной демократии, сменяемость власти, независимость судей, свобода СМИ. Поэтому был использован другой, более быстрый метод — эрозия, а точнее, фактическая отмена косвенного порядка взимания НДС.

Тогда-то и появились доктрины недобросовестного налогоплательщика[11], затем необоснованной налоговой выгоды[12], которая есть лишь более-менее причесанный вариант первой доктрины, наконец, ст. 54.1 НК РФ. В мои задачи не входит анализ того, какая же доктрина заложена в ней. Хорошо, что там нет слова «недобросовестность», хотя кое-что из конструкции злоупотребления гражданскими правами туда попало, несмотря на то что последняя существует в рамках дозволительного, а не предписывающего регулирования. Я имею в виду положение о том, что экономия на налогах не должна быть единственной или основной целью использования налогоплательщиком той или иной операции. Здесь заимствование из германского *BGB* для меня очевидно[13].

Что касается критерия реальности операции (ее фактического совершения), то оно вытекает из запрета мнимых и притворных сделок российским ГК.

> Но главное, что привнесено сейчас в налоговое законодательство, — возложение на налогоплательщика риска неуплаты в бюджет НДС его контрагентами, как бы далеко от него они ни отстояли, через ряд презумпций, закрепленных в законе и вопреки (что важно!) косвенному порядку уплаты НДС.

Если конкретный налогоплательщик перевел сумму НДС своему контрагенту, формально он выполнил свою обязанность и больше государству ничего не должен. Иное возможно, если по правилам уголовного законодательства будет доказано, что он являлся соучастником неуплаты налога вместе с конкретным неплательщиком.

По смыслу ныне действующей ст. 54.1 НК РФ и сложившейся правоприменительной практики доказывать факт совершения налогового преступления не нужно, а можно просто опровергнуть платеж и доначислить недоимку в сумме уплаченного вместе с ним НДС, пени и штраф по принципу объективного вменения. В итоге НДС из косвенного налога превращается в прямой. Но у нас уже есть один прямой налог — налог на прибыль, и он также позволяет исключать определенные затраты при определении налоговой базы исходя из оценочных суждений о том, что они не относятся к экономически обоснованным и необходимым.

Налоговые базы по НДС и налогу на прибыль тем самым сближаются, и чем больше будет доначислений НДС при неуплате его контрагентами, без установления факта соучастия в неуплате налогов, тем сильнее станет их отождествление (слияние в одну базу). А раз так, то возникает конституционная проблема двойного налогообложения одной и той же базы при помощи разных налогов. Очевидно, такой подход противоречит идее экономического основания налога. Один из налогов — или НДС, или налог на прибыль — становится излишним. В противном случае нужно четко разграничивать их налоговые базы. Во время последней дискуссии о замене НДС на налог с продаж указанное обстоятельство, скорее всего, учитывалось[14].

---

[11] Определение КС РФ от 25.07.2001 № 138-О «По ходатайству Министерства Российской Федерации по налогам и сборам о разъяснении Постановления Конституционного Суда Российской Федерации от 12 октября 1998 года по делу о проверке конституционности пункта 3 статьи 11 Закона Российской Федерации „Об основах налоговой системы в Российской Федерации“».

[12] Постановление Пленума ВАС РФ от 12.10.2006 № 53 «Об оценке арбитражными судами обоснованности получения налогоплательщиком налоговой выгоды».

[13] § 226 BGB. URL: https://www.gesetze-im-internet.de/bgb/__226.html (дата обращения: 21.03.2022).

[14] См. подробнее: Дворкович пообещал отмену НДС. URL: https://www.bfm.ru/news/17276 (дата обращения: 21.03.2022; Мишустин не поддержал идею замены НДС налогом с про-

Неслучайно изменения в ст. 54.1 НК РФ были внесены по модели злоупотребления гражданскими правами, т.е. как предполагающие переоценку тех или иных операций *post factum*, по результатам действий третьих лиц, а не самого налогоплательщика. Прямое исключение ряда платежей с НДС из числа тех, что уменьшают сумму данного налога к уплате, со всей очевидностью показало бы однотипность регламентации НДС и налога на прибыль, а значит, и их тождества. Риск признания их неконституционными вырос бы, именно поэтому для меня самый лукавый налог — это НДС.

Выше были рассмотрены разные ситуации, связанные с начислением и уплатой НДС, и показана, надеюсь, их противоречивость. Если эти суждения убедили не всех, постараюсь еще раз обосновать, почему именно НДС — самый лукавый налог.

Во-первых, потому что его название «налог на добавленную стоимость», с одной стороны, и механизм его начисления и взыскания в отдельных случаях, с другой стороны, не имеют ничего общего. Одним названием маскируются, по сути, разные в экономическом и правовом смысле механизмы и, следовательно, разные налоги. НДС, таким образом, представляет собой условное понятие, значение которого нужно устанавливать в зависимости от тех ситуаций, в которых он применяется. Во-вторых, потому что НДС выполняет функцию пополнения бюджета, но при этом создает чрезмерные перекосы в развитии экономики, что явно не соответствует природе налога. В-третьих, налог на добавленную стоимость используется как превращенная форма ответственности за неуплату налогов другими лицами при отсутствии состава правонарушения со стороны плательщика. Это противоречит сути правового принуждения.

Анализ лукавого НДС начался с вопроса об обложении им операций с «живыми» золотыми слитками, более широко — операций по продаже гражданам товаров, в цену покупки которых был включен НДС. При их перепродаже гражданами НДС не возмещается и не возвращается, даже если стоимость данных товаров вовсе не изменилась. Цепочка передачи добавочной стоимости рвется. И если при экспорте сумма НДС возмещается в силу прямого указания закона, в обычной ситуации так не происходит.

> Иными словами, НДС в экономическом смысле становится налогом с продаж. Их одновременное существование влечет двойное налогообложение.

Далее было отмечено, что в значительном числе случаев налог на добавленную стоимость превращается в свою противоположность — в налог на убавленную стоимость, что сильно дифференцирует условия деятельности разных с экономической точки зрения субъектов налогообложения. Выплаты работникам и отчисления в социальные фонды, облагаясь НДС, непропорционально повышают налоговую нагрузку на тех, у кого доля расходов на оплату труда высока (сфера производства и услуг). Напротив, те, у кого эта доля мала (например, экспортеры сырья), оказываются в привилегированном положении. Экономика развивается однобоко.

Если же используются особые налоговые режимы для предприятий сферы производства и услуг (упрощенная система, единый сельскохозяйственный налог и т.п.), предполагающие освобождение от НДС, то последний, по идее, никуда не исчезает. Он остается на последнем лице в цепочке перед льготником, по сути, дополнительно обременяя его. Добавленная стоимость уменьшается, а налог остается. Более того, если такой льготник снова вступает в цепочку отношений, облагаемых НДС, налог не восстанавливается, а пропадает безвозвратно. В итоге у плательщиков НДС значительно снижается желание работать с малыми и средними предприятиями на льготном режиме, бизнес которых в итоге страдает.

> Наконец, НДС, который изначально был оборотным налогом, судебная практика, а вслед за ней и Налоговый кодекс превратили в прямой налог и тем самым отождествили с налогом на прибыль. В итоге у них в значительной мере совпала налоговая база, что свидетельствует о двойном налогообложении.

Переложение на «живого» плательщика НДС, который не был уплачен третьим лицом, не превращается в меру ответственности, поскольку не предполагает

даж. URL: https://www.interfax.ru/business/703258 (дата обращения: 21.03.2022).

установления состава правонарушения. В этом смысле подобное переложение ничем не отличается от непризнания затрат в целях обложения налогом на прибыль, поскольку там тоже не предполагается выявления каких-либо правонарушений.

Кстати, вывод о том, что не подлежит вычету НДС, уплаченный по операции, не относящейся к деятельности, которую ведет налогоплательщик, также противоречит природе оборотного налога и представляет собой некорректное заимствование правил, применяемых при исчислении налога на прибыль. Здесь значение должна иметь не природа проведенной транзакции, а лишь сам факт уплаты НДС в составе платежа. И ссылка на то, что природа НДС иная, просто нужно как-то реагировать на налоговые нарушения третьих лиц, не срабатывает. Именно лукавый характер этого налога, т.е. его сущность, позволяет так действовать. Изменение порядка исчисления и (или) уплаты НДС, конечно, даст кое-что, но не отменит главного: добавленная стоимость и прибыль экономически очень близки.

Отсюда следует вывод: без отказа от НДС не получится создать внутренне непротиворечивую систему налогообложения. Вопрос в том, какие налоги придут ему на смену, сколько потеряет бюджет и выиграет общество. И здесь понадобятся усилия экономистов, юристов и, наконец, самих налоговиков.

## The Most Wily Tax

This article is devoted to the analysis of value added tax (VAT) through the notion of added value in economics and civil law. The main focus of the study is directed at the role of VAT in the economy of Russia, its economic reasonableness and fairness. The author offers critical view on the main norms of Russian tax law concerning VAT especially those which is to correct.

***Keywords:*** *tax, added value, VAT, gold circulation, simplified tax regimes*

### INFORMATION ABOUT THE AUTHOR

**Anton A. Ivanov**
Head of Private Law Department at National Research University Higher School of Economics, Candidate of Juridical Sciences, Professor (e-mail: a.ivanov@hse.ru).

### REFERENCES

Egorova, V.A. “Limiters” for the application of the simplified tax system in 2017 [*«Ogranichiteli» dlya primeneniya USN v 2017 godu*]. Bulletin Board “Express-Accounting” [*Informatsionnyi byulleten’ «Ehkspress-Bukhgalteriya»*]. 2016. No. 30. P. 12–14.

**АЛЕКСЕЙ СЕРГЕЕВИЧ ФИЛЯШИН**

аспирант юридического факультета МГУ имени М.В. Ломоносова, кафедра уголовного процесса, правосудия и прокурорского надзора

# УГОЛОВНО-ПРОЦЕССУАЛЬНАЯ ПОЛИТИКА *CRIME CONTROL* В США, ЕЕ КОНТЕКСТ И ИДЕОЛОГИЯ

В статье исследуется контекст и основные события «уголовно-процессуальной контрреволюции», произошедшей в доктрине, законодательстве и судебной практике США в конце 1970-х – начале 1980-х годов. Автор отмечает, что доминирование либеральных юристов в школах права и юридическом сообществе в целом потребовало от консервативных юристов, тяготеющих к политике контроля преступности, переосмыслить свою аргументацию и создать новые доктрины, которые позволят обосновать необходимые им жесткие политико-правовые меры уголовно-процессуального характера — сокращение процессуальных гарантий обвиняемых в ходе производства обысков и допросов. Одна из таких доктрин — ранняя версия экономического анализа права, укладывавшаяся в консервативный нарратив, утверждающий, что требования справедливого процесса связывают руки правоохранителям и способствуют крупнейшему в американской истории разгулу преступности. В целом же созданная консервативными интеллектуалами и судьями доктрина тяготела не к догматическим, а к политико-прагматическим аргументам, вызвав как очередной виток политизации американского права, так и впоследствии консервативную реакцию на такую политизацию в виде современного ориджинализма. Другим парадоксальным следствием «уголовно-процессуальной контрреволюции» стало одновременное сокращение функциональной дистанции с действующими в Англии на тот момент правилами *common law* и в то же время ее концептуальное увеличение благодаря новаторским аргументам консерваторов.

***Ключевые слова:*** *уголовный процесс США, crime control, уголовно-процессуальная политика, экономический анализ права, правило Миранды, ориджинализм*

DOI: 10.37239/0869-4400-2022-18-3-180-192

## 1. Введение и методологические соображения

1960-е годы в истории уголовного судопроизводства Соединенных Штатов отмечены противостоянием двух ярко выраженных тенденций. Первая из них — становление основ системы процессуальных гарантий, привычных для современного американца или исследователя, в первую очередь защиты от необоснованных обысков и правила Миранды. Вторая — начало колоссального роста преступности, ставшего симптомом масштабного социального кризиса, и усиливающееся недовольство населения неспособностью федерального правительства каким-либо образом совладать с ним. Критика бездействия такого рода со стороны консерваторов породила обширный пласт правовых аргументов, призванных обосновать необходимость в более жестком по отношению к обвиняемым регулировании, и позже, в 1970-е годы, эти аргументы были приняты на вооружение федеральными судами, в первую очередь Верховным судом США. Интеллектуальное противостояние консерваторов и их либеральных оппонентов в сфере правовой доктрины заставило и первых, и вторых активнее прибегать к достижениям или риторике других социальных наук, чтобы завоевывать влияние, что серьезным образом сказалось на «ландшафте» американской процессуалистики. Конечно, с учетом роли англоязычного знания современного мира этот процесс не мог ограничиться Северной Америкой, и ученые других стран стали всё активнее и активнее выходить за пределы привычной юридической догматики. На фоне общего интеллектуального восхищения, однако, часто забывается, что многие из аргументов, впервые выдвинутые американскими учеными и судьями, были порождениями своего времени, и сформулированы в ходе вполне конкретных политических дебатов, которые захватили американские суды во второй половине XX века. В настоящей статье я постараюсь воссоздать этот социально-политический контекст, покажу, что оригинальные идеи американских юристов могут быть корректно поняты и использованы только с его учетом и что такие тенденции могут вызывать реакцию, выражающуюся в возвращении к более традиционным приемам юридического мышления.

## 2. Социальный и политический контекст

Чтобы корректно адресовать проблему политического климата, необходимо поначалу отвлечься от собственно права и сделать небольшой экскурс в политическую науку. Для специалистов никогда не было секретом, что суды на самом деле активно участвуют в политике. Одной из первых англоязычных работ, подчеркивающих зависимость судебной системы от электоральных стимулов, была статья Роберта Даля *Decision-Making in a Democracy: The Supreme Court as a National Policy-Maker*[1]. Даль показал, что «Верховный суд неизбежно является частью господствующего политического альянса. Как элемент политического руководства этого альянса, суд, конечно, поддерживает его основные политические действия»[2]. Более современные работы, например *The Supreme Court and the American Elite* Лукаса Пове-младшего, только подтверждают этот тезис[3]. Электоральные стимулы оказывают на Верховный суд США серьезное влияние, поскольку доминирующая политическая коалиция назначает судей в ходе политической процедуры сенатских слушаний, ориентируясь в том числе на их политические взгляды. Тем не менее, как пишет Стивен Телес[4], классическая теория влияния электоральных циклов недостаточно хорошо объясняет судейскую политику. Он отмечает: это связано с тем, что к 1950-м годам политическая система США, в которой господствовали ориентированные на выборы партии, эволюционировала в ту, где господствуют широкие надпартийные коалиции. Такие коалиции включают не только партии, но и разнообразные институты и группы влияния, позволяющие коалиции успешно добиваться своего даже тогда, когда выборы проиграны, например аналитические центры *(think tanks)*, фонды и даже университеты. Именно эти организации и люди оказывают огромное влияние на курс, которому следуют суды, поскольку, как утверждает Чарльз Эпп[5], суды, в отличие от других ветвей власти, ограничены в своей способности самостоятельно выбирать те вопросы, которые им следует решить. Иначе говоря, чтобы федеральный суд мог использовать свое полномочие *judicial review* или пересмотреть прецедент, необходимо, чтобы до него вообще дошло нужное дело — значит, стороны активно должны

---

1 *Dahl R.* Decision-Making in a Democracy: The Supreme Court as a National Policy-Maker // Journal of Public Law. 1957. Vol. 6. P. 279–295.

2 Ibid. P. 279.

3 *Powe Jr.L.* A. The Supreme Court and the American Elite, 1789–2008. Harvard University Press, 2009.

4 *Teles S.M.* The Rise of Conservative Legal Movement. Princeton University Press, 2008. P. 9–21.

5 *Epp C.R.* The Rights Revolution. Chicago, University of Chicago Press, 1998. P. 3. Цит. по: *Teles S.M.* The Rise of Conservative Legal Movement. P. 11.

обжаловать его. Чтобы вынести информированное политическое решение, ему нужны аргументы, которые стороны озвучивают в прениях, а другие заинтересованные в исходе дела лица, например органы власти, общественные или коммерческие организации или даже неравнодушные профессора права — в направляемых ими в суд заключениях *amicus curiae*. Собственная позиция судьи, в конце концов, тоже формируется в ходе образования в школах права, профессора которых склонны занимать вполне определенные политические позиции. Таким образом, большая правящая коалиция включает не только тех, кто принимает решения, но и тех, кто снабжает последних казусами, аргументами, интеллектуальными ресурсами и пр. Участие этих людей жизненно необходимо, чтобы осуществлять нужный политический курс, и потому важно понимать, каким образом они формируют и распространяют идеи, которые позже ложатся в основу судебных решений.

«Новый курс» Рузвельта стал настоящим торжеством американского либерализма. Сформированная в годы его президентства политическая коалиция укрепилась настолько хорошо, что не разрушилась, когда к власти пришли более консервативные политики, а продолжила успешно существовать. Особенно успешно это проявилось именно в праве, что касается не только правосудия, но и юридического образования и науки. Школы права в 1950-е и 1960-е годы были настоящим заповедником либерализма, который стал своего рода научным и профессиональным мейнстримом, проповедовавшим эгалитаризм и лояльно относившимся к судейскому активизму; найти консерваторов в этой среде было действительно непросто. В то же время Верховный суд США впервые в своей истории оказался под контролем либеральных юристов (одним из них стал Главный судья Эрл Уоррен — соответственно, этот период в истории суда называется «суд Уоррена»), и это немедленно было использовано участниками коалиции для реформы уголовного процесса.

К концу 1940-х годов федеральный уголовный процесс оставался лишенным более-менее четких доктрин, а право штатов существовало независимо от федеральных конституционных требований. Суд Уоррена же смог изменить эту ситуацию. В 1961 году в деле *Мapp v. Ohio*[6] он при помощи довольно хитрого интерпретационного приема имплементировал IV Поправку в право штатов — отныне те требования производства обысков и арестов, которые были установлены федеральными судами, стали обязательны для полицейских департаментов по всей стране. Поскольку в федеральном процессе существовало правило об исключении доказательств, а в праве многих штатов — нет, это стало означать, что незаконные действия сотрудников полиции по всей стране стали влечь угрозу аннулирования полученных доказательств. В 1967 году позиции судей в деле *Katz v. United States*[7] создали последовательную доктрину «разумного ожидания неприкосновенности», установившую взамен неопределенного набора казуистичных правил, не определявшего, когда же именно подлежит применению поправка, ясный принцип: обыском считается любое нарушение неприкосновенности частной жизни. Это серьезно расширило круг действий, попавших под такое регулирование. В 1963 году решением по делу *Gideon v. Wainwright*[8] штаты были обязаны предоставлять защитника тем, кто не может позволить пригласить его самостоятельно, в 1964 году в *Escobedo v. Illinois*[9] судьи разрешили защитнику присутствовать на полицейских допросах. В 1966 году в легендарном деле *Miranda v. Arizona*[10] суд постановил, что в судебном разбирательстве не могут быть использованы сведения, сообщенные на допросе, если перед этим лицу не были разъяснены его конституционные права. Объем процессуальных прав, которым обладали в досудебном производстве обвиняемые на территории США, был расширен существенно.

Что касается политического и социального фона, то 1960-е годы в США, безусловно, были годами кризиса. За десятилетие количество зарегистрированных насильственных преступлений выросло на 126%[11]. Криминологи Джон Клегг и Аданер Усмани[12] предлагают следующее объяснение ситуации. Крах системы издольщины в середине XX века привел к тому, что черное население начало массово мигрировать в промышленные города севера в поисках работы, однако рабочие места в них

[6] Mapp v. Ohio, 367 U.S. 643 (1961).

[7] Katz v. United States, 389 U.S. 347 (1967).

[8] Gideon v. Wainwright, 372 U.S. 335 (1963).

[9] Escobedo v. Illinois, 378 U.S. 478 (1964).

[10] Miranda v. Arizona, 384 U.S. 436 (1966).

[11] См.: *Eisen L.-B.*, *Roeder O.* America's Faulty Perception of Crime Rates / Brennan Center for Justice. URL: https://www.brennancenter.org/our-work/analysis-opinion/americas-faulty-perception-crime-rates (дата обращения: 27.03.2022).

[12] *Clegg J.*, *Usmani A.* The Economic Origins of Mass Incarceration // Catalyst. 2019. Vol. 3. No. 3. P. 9–53.

уже были заняты другими мигрантами. Белое население городов начало массово переезжать в пригороды, что повлекло уменьшение городских бюджетов и, как следствие, социальных сервисов и в результате вылилось в массовую криминализацию городского черного населения. Все это вместе с антивоенными протестами и расовыми бунтами создавало у публики чувство угрозы, чем успешно воспользовались консерваторы. Впервые нарратив «закона и порядка», апеллировавший к неспособности администрации либерального президента Линдона Джонсона совладать с домашними угрозами, был использован кандидатом в президенты от Республиканской партии Барри Голдуотером в ходе кампании 1964 года, и после этого обрел растущую популярность.

Важной частью нарратива «закона и порядка» была критика суда Уоррена. Сам Голдуотер, например, заявлял, что борьба с преступностью должна начаться с федеральных судов[13], которые, по его словам, должны были отменить решения, связывающие руки прокурорам (речь, вероятно, шла в первую очередь о решениях по делам Эскобедо и Миранды)[14]. Рональд Рейган, избираясь губернатором Калифорнии, тоже сделал «закон и порядок» важной частью своей кампании — и точно так же, как и Голдуотер, он возлагал ответственность за связавший руки полиции Верховный суд[15]. Не только политики в своих выступлениях делали такие заявления. Когда Линдон Джонсон, обеспокоенный ростом популярности «закона и порядка» и ростом преступности, собрал в 1965 году комиссию, целью которой было выработать устраивающее его компромиссное объяснение, семеро членов комиссии во главе с президентом Американской ассоциации юристов Льюисом Пауэллом составили приложение к ее итоговому докладу под названием «Дополнительный отчет о конституционных ограничениях», представляющий собой довольно алармистскую критику решений Верховного суда в сфере предварительного расследования — в основном решения по делу Миранды. «Если решение большинства в деле Миранды будет полноценно внедрено в практику, то это может означать буквально уничтожение института досудебного допроса — на улице, на месте преступления, и в полицейском участке — поскольку такого допроса не может быть без присутствия защитника, пока задержанное лицо каким-либо образом не откажется от права от него, — предостерегали авторы. — <…> Для того чтобы работать эффективно и, в частности, сдерживать преступное поведение, суды должны решительно осуждать виновных — точно так же, как и оправдывать невиновных. Ограничения, которые препятствуют разумному достижению этой цели, не оказывают обществу хорошую услугу»[16]. Уже позже, после победы Никсона на выборах, подобную позицию озвучивал помощник Генерального прокурора США (и будущий судья и затем Главный судья Верховного суда) Уильям Ренквист, который в одном из меморандумов указывал на следующие негативные стороны практики суда Уоррена: «…(а) строгие ограничения, касающиеся производства полицейских допросов на ранних стадиях процесса, даже когда такие допросы проводятся без использования принуждения; (б) добровольные признания и заявления обвиняемого исключаются в ходе судебного разбирательства даже тогда, когда они относимы и убедительно доказывают его вину…»[17]. Ренквист даже предлагал создать специальную комиссию для пересмотра существующих ограничений, однако это предложение не было принято президентом[18].

Впрочем, как пишет Майкл Фламм, после выборов 1968 года политический накал вокруг роста уличной преступности сошел на нет. По его мнению, это связано как с объективной неспособностью остановить его усилиями федерального правительства (рост продолжился вплоть до 1990-х годов), так и с тем, что политически его было намного удобнее использовать для критики оппонентов, а не для построения позитивной повестки. Тем не менее консервативные судьи, назначенные в федеральные суды Никсоном, Фордом и позже Рейганом, никуда не исчезли и продолжили курс, направленный на сокращение прав обвиняемых.

[13] Remarks at the Mark Hopkins Hotel, July 16, 1964, Box 10, PCF, Goldwater MSS, AHF. Цит. по: *Flamm M.W.* Law and Order: Street Crime, Civil Unrest, and the Crisis of Liberalism in the 1960s. N.Y., Columbia University Press, 2005.

[14] *White T.H.* The Making of the President: 1964. Harper Collins, 1965. P. 125.

[15] "Crime", 1966, RNC Series-Film, Audio-Visual Department, JFK Library. Цит. по: *Flamm M.W.* Law and Order. P. 74.

[16] Congressional Record: Proceedings and Debates of the 90th Congress Second Session. Washington, DC, US Government Printing Office. Vol. 114. Part 10. P. 13123–13126.

[17] Адресованное главному юристу Белого дома Джону Дину *"Summary of Memorandum Re: Constitutional Decisions Relating to Criminal Law"*, 1 апреля 1969 года, и приложение к нему. Dean, Box 24, WHSF. Цит. по: *McMahon K.J.* Nixon's Court: His Challenge to Jusicial Liberalism and Its Political Consequences. The University of Chicago Press, 2011. P. 191.

[18] Ibid. P. 190–191.

## 3. Интеллектуальные истоки

Одним из важных интеллектуальных течений в юридической мысли США 1970-х годов стал экономический анализ права. Он зародился в Чикаго интеллектуальными усилиями Аарона Директора, начавшего преподавать в школе права курс антимонопольного права, которое первоначально и было основным предметом критики экономистов. Чуть позже к движению присоединились другие именитые экономисты, такие как Рональд Коуз и Гэри Бекер (оба будущие лауреаты Нобелевской премии по экономике), и юристы, например Ричард Познер и Гвидо Калабрези[19]. Присутствие последних помогло укрепить репутацию чикагской школы — ведь до этого, как замечает Стивен Телес, все, что выходило из Чикаго, считалось чистой идеологией. Познер же был клерком у достаточно либерального судьи Верховного суда США Уильяма Бреннана, а Калабрези — профессором в мейнстримной либеральной школе права Йельского университета, что некоторым образом снижало барьер, существовавший между чикагскими экономистами и либеральным юридическим сообществом[20].

Основной своей задачей ранние представители направления видели критику институтов и политики, поддерживаемых юридическим мейнстримом того времени, например агрессивного антимонопольного регулирования. Для этого они использовали инструментарий, представляемый экономической наукой того времени — в первую очередь несложные модели. В 1968 году Гэри Бекер пишет свою легендарную статью *Crime and punishment: an economic approach*[21], в которой анализирует уголовное право и преступное поведение при помощи анализа издержек и выигрышей *(cost-benefit analysis)*. В конце 1972 года выходит первое издание книги Ричарда Познера «Экономический анализ права», ставшей чрезвычайно популярной[22]. Экономический анализ довольно быстро привлекает к себе внимание консервативных фондов, обеспокоенных судьбой американского бизнеса в перегруженной регуляциями, как считали их руководители, экономике. Средства этих фондов активно использовались консервативными интеллектуалами для того, чтобы популяризовать эту научную дисциплину, — наиболее показательным примером успешного проекта такого рода можно назвать Экономический институт для федеральных судей, созданный профессором Генри Манне при финансовой поддержке консервативных фондов (например, Фонда Олина) и ориентированный на обучение федеральных судей основам микроэкономики. С 1976 по 1990 год обучение на этих двухнедельных курсах прошло 40% всего федерального судейского корпуса[23].

> Как показал проведенный анализ решений посещавших программу федеральных судей Эллиота Эшема, Дэниела Чена и Суреша Найду, ее участники были более склонны использовать экономические термины в решениях[24].

Экономический анализ, конечно, распространялся не только среди судей, но и среди профессоров — через аналогичные курсы, которые и были прообразом судейских[25], а также путем увеличивающегося рекрутинга консервативных профессоров в мейнстримные школы права, в первую очередь, школы права университетов Лиги плюща[26]. Сторонники экономического анализа занимали и посты в органах исполнительной власти, например выпускник Чикагского университета Роберт Борк, который исполнял обязанности Генерального прокурора при Никсоне, затем стал Генеральным солиситором и, наконец, судьей федерального апелляционного суда по округу Колумбия. Таким образом, экономический анализ права послужил для консерваторов тем, чего им ранее не хватало: 1) набором политических рекомендаций, которым их не могли снабдить мейнстримные юристы; 2) интеллектуальным инструментом в борьбе за свое влияние.

---

[19] *Меркуро Н.*, *Медема С.* Экономическая теория и право: от Познера к постмодернизму и далее. М., 2019. С. 166–180.

[20] *Teles S.M.* The Rise of Conservative Legal Movement. P. 96–101.

[21] *Becker G.S.* Crime and Punishment: An Economic Approach // Journal of Political Economy. 1968. Vol. 76. No. 2. P. 169–217.

[22] *Posner R.A.* Economic Analysis of Law. Boston, Little, Brown and Company, 1973.

[23] *Butler H.N.* The Manne Programs in Economics foe Federal Judges // Case Western Reserve Law Review. 1999. Vol. 50. P. 352.

[24] *Ash E.*, *Chen D.L.*, *Naidu S.* Ideas Have Consequences: The Impact of Law and Economics on American Justice. March 24, 2021. URL: https://www.law.nyu.edu/sites/default/files/ash-chen-naidu-2021-03v1.pdf (дата обращения: 27.03.2022).

[25] *Teles S.M.* The Rise of Conservative Legal Movement. P. 105–108.

[26] Ibid. P. 181–219.

По своей сути экономический анализ права представлял приложение к юридическим дисциплинам методологии теоретической макроэкономики, в первую очередь ценовой теории *(price theory)* и теории рационального агента[27]. Несмотря на то, что Николас Меркуро и Стивен Медема называют в качестве еще одного краеугольного камня методологии чикагской школы экономического анализа права убежденность в том, что критерием, по которому оценивается регулирование, является экономическая эффективность, мне кажется более верным считать стремление к оценке эффекта частью более общей нормативной консеквенциалистской предпосылки, на которую вообще опирается экономика как дисциплина в своей нормативной части. Чтобы лучше понять методологические проблемы ранних работ чикагской школы, необходимо сказать, что устройство экономической науки (и сообщества) в 60-х и 70-х годах прошлого века существенно отличалось от того, которое мы видим сейчас.

> Если сейчас, как пишут Роджер Бэкхаус и Беатрис Шерье, наиболее престижными в экономике являются эмпирические работы (или, по крайней мере, работы, содержащие в себе эмпирический элемент), то 50 лет назад в дисциплине абсолютно господствовали теоретики-неоклассики, центральной задачей которых было построение моделей, что касалось и микроэкономики тоже[28].

Это было связано со многими причинами, не только с общим престижем теории, но и с тем, что, как утверждают Джона Гелбах и Джонатан Клик, до 1990-х годов методы анализа данных были развиты достаточно плохо и предоставляли широкий простор для достаточно произвольных выводов — рандомизированные и естественные эксперименты появились в инструментарии дисциплины достаточно поздно[29]. Надо добавить, что эмпирическая неполнота исследований касается не только анализа данных, но и простых методов социологии — наблюдения, включенного наблюдения и пр. Стандартная «чикагская» публикация 1960–1980 годов, таким образом, обычно включает описание проблемы, построение модели, анализ следующих из нее выводов и ряд политических рекомендаций; в них почти никогда не исследуются практики, существующие на самом деле (например, специфичные ведомственные стимулы, которые действуют на агентов, и т.д.). Из этого следует, что ряд существенных для построения модели условий остаются скрытыми от исследователя и от читателя такой публикации, следующие из нее выводы не тестируются — но политические рекомендации в разделе «заключение» уже даны.

Отдельную проблему представляет собой консеквенциалистская нормативная предпосылка, на которую опирается экономическая наука в целом. Поскольку экономика — дисциплина, изучающая распределение ограниченных ресурсов, это почти неизбежно приводит к следующему: ее фундаментальной установкой становится утверждение о том, что действия агентов должны оцениваться относительно того распределения, которое является их результатом. Соответственно, экономисты практически всегда принимают одну из версий этой консеквенциалистской философии и, исходя из нее, строят свои политические рекомендации. В случае с ранним, «чикагским» экономическим анализом права эта установка обычно выражалась через так называемый принцип эффективности Калдора – Хикса, который кратко может быть сформулирован как «выгоды выигравших от распределения должны быть гипотетически способны компенсировать потери проигравших».

> Важно заметить, что представители движения, такие как сам Ричард Познер, предприняли серьезные усилия, чтобы доказать: эффективность — достаточный критерий для оценки действий агентов в правовой системе и в то же время критики альтернативных идей, например тех, в которых ключевым этическим принципом выступает автономия личности[30].

[27] *Меркуро Н.*, *Медема С.* Экономическая теория и право: от Познера к постмодернизму и далее. С. 180–189.

[28] *Backhouse R.E.*, *Cherrier B.* The Age of Applied Economist: The Transformation of Economics since the 1970s // History of Political Economy. 2017. Vol. 49 (Supplement). P. 1–33.

[29] *Gelbach J.B.*, *Klick J.* Empirical Law and Economics in: Parisi F. (ed.) The Oxford Handbook of Law and Economics: Vol. 1: Methodology and Concepts. Oxford University Press, 2017. P. 30–32.

[30] *Posner R.A.* The Economics of Justice. Harvard University Press, 1980. P. 60–76, 98–99.

Подобная нормативная предпосылка выглядит интуитивно уязвимой к критике, и не случайно. Работы моральных философов, таких как Элизабет Энском[31] или Джон Финнис[32], предоставляют нам ряд сильных аргументов против консеквенциалистской позиции такого рода, как теоретических, среди которых, например, невозможность интерсубъективных сравнений, так и практических.

Конечно, далеко не все экономисты настаивали на жесткой версии консеквенциалистской посылки даже в 1970-х годах и допускали, что эффективность — лишь один из ряда моральных принципов. Однако то, что тезисы иного рода мы видим у Познера — наиболее влиятельного теоретика экономического анализа эпохи, говорит о многом. В итоге «чикагская» версия экономического анализа образца 1960–1980 годов, серьезно повлиявшая, как мы увидим ниже, на уголовный процесс эпохи *crime control*, во всяком случае концептуально, оказывается, по крайней мере в части, достаточно уязвимой и с позиции собственно экономической методологической рефлексии, и с позиции ее нормативных предпосылок.

Но что сделало реализацию чаяний консерваторов возможной? Дело в том, что во время президентства Никсона в Верховном суде освободилось сразу четыре места: с поста Главного судьи ушел Эрл Уоррен; в 1969 году в результате скандала ушел Абэ Фортас; в 1971-м умер Хьюго Блэк — после его смерти из пяти судей, составивших большинство в *Miranda v. Arizona*, в суде остался лишь один — Уильям Бреннан. В том же году умер Джон Маршалл Харлан. Ричарду Никсону, таким образом, выпала редкая возможность назначить за свое президентство сразу четырех судей, что радикально изменило баланс в Верховном суде, — с тех пор назначенные либеральными президентами судьи уже никогда не будут составлять в нем большинство. При их назначении, как указывает Кевин МакМахон, Никсон учитывал их отношение к «закону и порядку»[33]. Суд, получивший название «суд Бёргера» (в честь нового Главного судьи), таким образом, был намного более консервативным, чем предыдущий, и сам по себе был склонен относиться к правам обвиняемых с намного большим скептицизмом. Активное участие новой консервативной коалиции в «снабжении» его идеями, делами и аргументами позволило ему инициировать пересмотр или сужение ряда ключевых доктрин и сформировать прецеденты, которые оказывают влияние на практику Верховного суда и сегодня и о которых пойдет речь ниже.

## 4. Контроль преступности: консервативная волна

Давление консерваторов, опирающихся на популярность у белого электората идеи «закона и порядка», возымело успех еще до разгрома либеральной коалиции. В 1968 году склонявшийся вправо Конгресс принял *Omnibus Crime Control and Safe Streets Act* (Сводный закон о контроле преступности и обеспечения безопасности на улицах)[34] — вероятно, первую серьезную законодательную меру в рамках политики жесткого контроля преступности. Первоначальная версия титула III закона, написанная либеральной администрацией Линдона Джонсона, предусматривала имплементацию в федеральный статут правил, установленных Верховным судом в двух делах 1967 года — *Katz v. United States* и *Berger v. New York*[35]. В первом из них суд, отвергнув раннее установленный в *Olmstead v. United States* прецедент[36], постановил, что, поскольку IV Поправка защищает неприкосновенность частной жизни, прослушивание переговоров, вторгающееся в это право, также считается обыском и требует получения ордера суда, основанного на достаточном основании *(probable cause)*. Второе дело касалось прослушивания переговоров без процессуальных гарантий. Тем не менее Конгресс отнесся недружелюбно к тому, что билль предусматривал, что с ходатайством о прослушивании переговоров в суд мог обратиться только Генеральный прокурор США и только в делах, касающихся национальной безопасности[37], и включил в число обладателей такого полномочия его помощников, прокуроров штатов и окружных

[31] *Anscombe G.E.M.* Modern moral philosophy // Philosophy. 1958. Vol. 33. No. 124. P. 1–19.
[32] *Finnis J.* Natural Law and Natural Rights. 2nd ed. Oxford University Press, 2011. P. 111–118.
[33] *McMahon K.J.* Nixon's Court. P. 190.
[34] Omnibus Crime Control and Safe Streets Act of 1968 (Pub.L. 90–351, 82 Stat. 197).
[35] Berger v. New York, 388 U.S. 41 (1967).
[36] Olmstead v. United States, 277 U.S. 438 (1928).
[37] *Flamm M.W.* Law and Order. P. 136–137.

прокуроров[38], установив, что прослушивание может осуществляться по достаточно широкому кругу дел — в том числе по таким классическим насильственным и корыстно-насильственным преступлениям, как убийство и разбой[39].

> Конгресс не ограничился простым переиначиванием инициативы президента, касающейся прослушивания, и добавил в акт положения, отсутствующие ранее, — Титулом II Акта он просто-напросто отменил действие решения *Miranda v. Arizona*, разрешив федеральным судам принимать любые признания и показания в качестве доказательств, если они были сделаны добровольно, в том числе если им не разъяснялись их конституционные права[40].

Фактически федеральная судебная практика должна была вернуться к тесту «совокупности обстоятельств» или «добровольности», которым Верховный суд следовал ранее. Такой радикальный шаг закономерен, если вспомнить, насколько распространена была критика этого прецедента среди консервативных политиков ранее — именно он был главной атакой консерваторов. Несмотря на то, что закон касался лишь федеральных судов и округа Колумбия, не распространяясь на штаты, всё так же обязанные следовать позиции, изложенной в *Miranda*, принятие этого положения, впоследствии известного как § 3501 Кодекса Соединенных Штатов, стало серьезным ударом по правам обвиняемых и первой серьезной победой политики *crime control*.

Достаточно важно понимать: поскольку § 3501 касался лишь федерального права, Верховный суд продолжил регулярно пересматривать решения судов штатов, руководствовавшихся правилами *Miranda* — формирование судебной практики не прекратилось. Консервативный настрой нового судебного большинства ярко проявился в деле *Harris v. New York*[41] уже в 1970 году. Дело касалось довольно специального вопроса о том, могут ли данные без разъяснения о правах показания быть использованы не для того, чтобы обосновать обвинение, а для того, чтобы поставить под сомнение достоверность показаний обвиняемого. Решение Главного судьи Бёргера, указавшего, что это возможно, нанесло серьезный удар по позиции Суда в *Miranda*. Дело в том, что, как указывает Джоффри Стоун[42], позиция Суда в *Miranda* была сконструирована так, чтобы создать ясное правило для разрешения как можно большего числа дел. Позиция Бёргера же представляла собой отвержение этого правила и, по сути, означала, что 60-страничное решение суда в *Miranda* представляла собой простое отвлеченное рассуждение, не имеющее обязательной силы. В 1974 году в *Michigan v. Tucker*[43] Верховный суд занял еще более агрессивную позицию, сформулировав решение так, будто дело Миранды просто продолжало предыдущую линию прецедентов, основанных на принципе добровольности. Больше того, в самом решении судья Ренквист неоднократно называл требования *Miranda* «профилактическими стандартами» или «процедурными гарантиями». Выбор такого языка довольно важен: он символизирует то, что в 1970-х суд вполне соглашался с позицией Конгресса, считавшего, что он имеет право федеральным законом установить иное правило, если оно касается «процедурных гарантий», а не Конституции непосредственно. Несмотря на то, что в итоге суд занял иную позицию в *Dickerson v. United States*, аннулировав § 3501 и признав требования *Miranda* конституционными[44], впоследствии Верховный суд неоднократно возвращался к линии *crime control*, постепенно продолжая сокращать их объемы.

Хороший примером того, как политические настроения эпохи стали определять практику Верховного суда, — знаменитое дело *Terry v. Ohio*[45]. Фабула дела была таковой: опытный детектив, патрулировавший улицу, заподозрил, что компания молодых людей, прохаживающихся по ней, планирует ограбление магазина. Он остановил их и ощупал их карманы, обнаружив в них оружие; за его скрытое ношение заявитель и был осужден. Как указывает Барри Фридман, перед судом Уоррена встала непростая

[38] Omnibus Crime Control and Safe Streets Act of 1968, sec. 802.
[39] Ibid.
[40] Omnibus Crime Control and Safe Streets Act of 1968, sec. 701.
[41] Harris v. New York, 401 U.S. 222 (1971).
[42] *Stone G.* The Miranda Doctrine in the Burger Court // Supreme Court Review. 1977. Vol. 99. P. 107-108.
[43] Michigan v. Tucker, 417 U.S. 433 (1974).
[44] Dickerson v. United States, 530 U.S. 428 (2000).
[45] Terry v. Ohio, 392 U.S. 1 (1968).

задача. Во-первых, общественное мнение было настроено к нему крайне недружелюбно, шла предвыборная гонка, в апреле был убит Мартин Лютер Кинг, а за несколько дней до вынесения итогового решения — бывший генеральный прокурор, сенатор Роберт Кеннеди. Во-вторых, полицейский детектив явно действовал, не удовлетворяя конституционному стандарту достаточного основания — он руководствовался своей интуицией, но оказался прав. По словам Фридмана, всё это крайне сужало возможности для вынесения приемлемого решения[46]. Судьи не могли решить дело в пользу Терри без политических последствий; судьи не могли решить дело в пользу штата Огайо, понизив планку стандарта достаточного основания, потому что это стало бы универсальным правилом для всех обысков, уничтожив роль стандарта как процессуальной гарантии. Итогом стало необычное решение, принятое восемью голосами против одного, и опирающееся на довольно необычное истолкование IV Поправки.

> Автор решения, Главный судья Уоррен, указал, что вторую часть поправки, которая требует выдавать ордера лишь при наличии достаточного основания, необходимо читать в контексте первой части, запрещающей произвольные обыски вообще. Обыск, произведенный в отношении Терри, был, по мнению Суда, вполне обоснованным — «разумный человек имел бы основание считать, что [Терри] был вооружен и что это представляло угрозу безопасности сотрудника полиции во время расследования его подозрительного поведения».

В итоге суд, по сути, создал дополнительный, более низкий стандарт для обысков такого рода — стандарт разумного подозрения *(reasonable suspicion)*. Важно иметь в виду, что решение было тесно связано с фактическими обстоятельствами дела — обыск производился для обеспечения безопасности сотрудника полиции, а не для обнаружения доказательств. Но, как опять же указывает Фридман, последствия решения по делу Терри в долгосрочной перспективе оказались достаточно неожиданными[47]. Полицейские департаменты по всей стране массово начали обыскивать людей на основании нового стандарта, причем указание на то, что такой обыск может быть произведен для обеспечения безопасности, не было воспринято. В результате при помощи так называемых обысков Терри полиция стала искать не только оружие, но и наркотики. Это привело к появлению в некоторых городах, например Нью-Йорке, к созданию программ массовых уличных обысков (так называемые *stop-and-frisk*), сомнительная легальность которых стала причиной для подачи ряда исков в федеральные суды[48]. Консервативные же судьи, назначенные в Верховный суд впоследствии, лишь расширили действие доктрины Терри[49].

В такой обстановке обновленный в начале 1970-х состав суда начал пересматривать в духе *crime control* и практику об обысках. Первым из таких дел стало *United States v. Calandra* 1974 года[50]. Текст решения большинства написал Льюис Пауэлл-младший, имя которого мы уже вспоминали выше в связи с приложением к докладу президентской комиссии. Каландра был допрошен федеральным большим жюри на основании доказательств, полученных в результате обыска в помещении его предприятия. На вопросы он отвечать отказался, утверждая, что обыск был неправомерным, и заявил ходатайство об исключении. Перед Верховным судом встал вопрос: может ли свидетель отказаться давать показания перед большим жюри на таком основании? Суд ответил на этот вопрос отрицательно.

В ходе прений представитель Соединенных Штатов Луи Клейборн высказал аргумент, который, вероятно, можно считать провозвестником эпохи, все более и более апроприирующей экономические аргументы или риторику. Он указал: «…единственное возможное обоснование для этого (судебного рассмотрения ходатайства об исключении доказательства. — *А.Ф.*) — небольшой дополнительный сдерживающий эффект *(deterrent effect)*»[51]. Вероятно, аргумент федерального правительства показался убедительным для судьи Пауэлла, и его мотивировка во многом

[46] *Friedman B.* Unwarranted: Policing Without Permission. N.Y., Farrar, Straus and Giroux, 2017. P. 145–149.
[47] Ibid. P. 150.
[48] См., напр.: Floyd, et al. v. City of New York, et al., 959 F. Supp. 2d 540 (S.D.N.Y. 2013).
[49] Hiibel v. Sixth Judicial District Court of Nevada, 542 U.S. 177 (2004), Heien v. North Carolina, 574 U.S. 54 (2014).
[50] United States v. Calandra, 414 U.S. 338 (1974).
[51] Oral argument — October 11, 1973. URL: https://www.oyez.org/cases/1973/72-734 (дата обращения: 27.03.2021).

строится именно на исследовании «сдерживающего эффекта».

> Как постановил суд, исключение доказательств является средством, созданным судом для сдерживания злоупотреблений полиции, а не конституционным правом. В случае с допросом свидетеля большим жюри сдерживающий эффект слишком мал, чтобы оправдать его использование.

Сложно сказать уверенно, является ли решение Пауэлла результатом усвоения терминологии экономического анализа, для которого характерно оперирование термином «сдерживающий эффект» — в конце концов, Верховный суд использовал понятие «сдерживание» и раньше, в решениях по таким делам, как *Alderman v. United States*[52] или *Elkins v. United States*[53]. Тем не менее именно в решении по делу Каландры эта терминология использована наиболее часто и наиболее системно. Даже если предположить, что судья Пауэлл просто опирался на язык предыдущих решений, решение по делу Каландры можно рассматривать как очередной шаг суда в сторону от более догматической и более деонтологической позиции (в соответствии с которой исключение доказательств необходимо для обеспечения честности суда *[judicial integrity]*) к консеквенциалистской позиции (в соответствии с которой исключение доказательств должно быть применимо лишь постольку, поскольку его результатом станет сдерживание полиции). В любом случае решение судьи Пауэлла создало прецедент, который позже будет ключевым для решения аналогичных дел, например в *United States v. Janis* в 1976 году[54]. Той же логике Верховный суд последовал и в *Stone v. Powell*[55] — решение примечательно тем, что его также писал судья Паэулл. В дополнение к термину «сдерживающий эффект» там появляется и более откровенный экономизм «социальные издержки» *(social cost)*, что подтверждает гипотезу: в основе решения могли лежать экономические аргументы или оно по меньшей мере испытало влияние дискурса *law & economics*.

Следующим прецедентом в этой линии стала позиция суда в *United States v. Leon* 1983 года[56], которая эксплицитно являет собой прорывной пример применения экономического анализа права к уголовному процессу. Фактическая сторона дела Леона была таковой: полиция произвела обыск, основанный на ордере, который впоследствии суд признал не имеющим достаточного основания. Тем не менее, как постановил суд, сотрудник полиции, производя обыск, действовал добросовестно *(in good faith)*. Вопрос о том, существует ли основанное на добросовестности исключение из правила об исключении доказательства, и встал перед Верховным судом.

В деле Леона использование экономического анализа сторонами совершенно очевидно. Показательна речь Генерального солиситора Рекса Ли в прениях: «Из прецедентов этого суда следует с ясностью, что, поскольку наивысшей и, возможно, единственной целью правила об исключении доказательства является сдерживание, это правило применяется только в тех ситуациях, когда выигрыши сдерживания превышают издержки исключения сильных доказательств. <…> Предельные доказательственные издержки превышают предельный выигрыш от сдерживания, который был бы результатом применения правила об исключении доказательств в этом процессе»[57]. Из слов Ли ясно следует: он рассматривал предыдущие решения суда именно в свете своеобразного анализа выигрыша и издержек, которым, по его мнению, и должны были руководствоваться судьи, разрешая дело.

> Поскольку сдерживающий эффект в отношении лица, заблуждающегося насчет правомерности своих действий, был бы небольшим, издержки исключения доказательств превышали бы выигрыши. Дело должно быть решено в пользу Соединенных Штатов. Судья Уайт, автор решения большинства, встал именно на эту позицию.

В решении сказано: «…этот вопрос должен быть решен путем взвешивания издержек и выигрышей

[52] Alderman v. United States, 394 U.S. 165 (1968).
[53] Elkins v. United States, 364 U.S. 206 (1960).
[54] United States v. Janis, 428 U.S. 433 (1976).
[55] Stone v. Powell, 428 U.S. 465 (1976).
[56] United States v. Leon, 468 U.S. 897 (1984).
[57] Oral argument — January 17, 1984. URL: https://www.oyez.org/cases/1983/82-1771 (дата обращения: 27.03.2021).

воспрепятствования использованию обвинением вполне достоверных вещественных доказательств, полученных на основании ордера, выданного незаинтересованным и нейтральным магистратом, который, в конце концов, оказался порочным». Он указал на то, что с исключением доказательств связаны «существенные социальные издержки». Таким образом, исключение доказательств, важнейшее средство правовой защиты от неправомерных обысков, было подчинено логике, основанной на анализе результатов его применения.

Конечно, монополия такого подхода внутри консервативного крыла не могла продержаться долго. Уже в 1980-е оно пополнилось без преувеличения легендарным Антонином Скалиа, ставшим пионером совершенно новой теории применения Конституции — ориджинализма[58].

> Несмотря на то, что ориджинализм, конечно же, не подразумевал простого возвращения к юридической догматике прошлого, он вполне сознательно пытался очистить практику Верховного суда от рассуждений, основанных на более прагматическом анализе социальных последствий предстающих перед ним правовых ситуаций, и заменить их достаточно строгим телеологическим толкованием конституционного текста.

Уже в первом решении, касающемся обысков, судья Скалиа разошелся с описанной нами доктриной. Например, в деле *Arizona v. Hicks* 1987 года[59] он проигнорировал возражение судьи Пауэлла о том, что прецедент, требующий считать несложные физические манипуляции с объектами обыском (и, соответственно, требовать наличия достаточного основания), может «сдержать добропорядочного сотрудника полиции от законного получения необходимых для осуждения виновного доказательств»[60]. Скалиа отметил, что выбирает «следовать основанному на тексте традиционному стандарту достаточного основания»: «Более чем возможно, что в данных обстоятельствах не существует ни одного эффективного средства (получить доказательства — *А.Ф.*) помимо обыска <…> но нет ничего нового в осознании того, что Конституция иногда оставляет без внимания преступные деяния меньшинства ради защиты неприкосновенность частной жизни большинства»[61]. Ориентированная на грамматическое и телеологическое толкование мысль Скалиа, тяготеющая к более традиционной догматике, продолжает вдохновлять ряд консервативных судей и сейчас — спустя пять лет после его смерти в 2016 году.

## 5. Заключение

Изучив решения Верховного суда Бёргера, мы можем убедиться, что 1970-е годы — достаточно важная поворотная точка в американском процессе. Назначенные Никсоном консервативные судьи стали сворачивать достижения своих предшественников, не только возвращаясь к более старой доктрине (в случае с допросами), но и применяя совершенно новую (как в случае с обысками), основанную на совсем других предпосылках. Важно, что этот поворот заложил основы для целых линий прецедентов, продолжающихся вплоть до сегодняшнего дня. Несмотря на то, что после 1970-х состав Верховного суда стал намного более сложным и в нем появились обладатели невиданных доселе убеждений (например, ориджиналисты), достижения процессуальной контрреволюции продолжают жить и использоваться для решения новых дел. Конечно, это серьезно изменило характер самой доктрины, в том числе в компаративном ключе.

Американский уголовный процесс в части регулирования досудебного производства стал серьезно отличаться от английского, пожалуй, еще в начале XX столетия. Поворот к судебной политике *crime control*, в основе которого порой лежало представление о том, что Верховный суд слишком сильно отклонялся от традиционных правил *common law*, смог уменьшить это расхождение: например, в Англии

[58] Ориджинализм — доктрина конституционной интерпретации, которая требует толковать Конституцию на основании первоначального значения содержащихся в ней принципов и норм, т.е. с учетом исторического контекста и телеологически.
[59] Arizona v. Hicks, 480 U.S. 321 (1987).
[60] Ibid. (Особое мнение судьи Пауэлла.)
[61] Ibid. (Решение большинства.)

не существовало правила, аналогичного *Miranda*[62], и постепенная ликвидация императивного исключения доказательств приблизила американское регулирование к английскому. Это касается и неправомерных обысков, где английские судьи имели большую дискрецию и учитывали, решая вопрос об исключении, действуют ли сотрудники полиции добросовестно или нет[63].

Но важно иметь в виду, что в последнем случае аргументы, использованные судьями в США, не имели ничего общего с аргументами, которые использовали английские судьи.

> Например, если в английских делах исключение доказательств до сих пор контролируется по большей части принципом справедливости («будет ли процесс несправедливым в отношении обвиняемого, если доказательства не будут исключены?»), то используемый в ряде американских дел анализ выигрышей и издержек относится к принципиально другому роду аргументации и в итоге ложится в основу принципиально отличных от английских решений.

Хотя консервативный суд Бёргера мог бы просто отвергнуть позиции своих предшественников в делах об обысках и вернуться к тому способу обоснования судебных решений, который господствовал ранее в *common law*, он предпочел опереться на своего рода внеправовой анализ, ориентирующийся в первую очередь на изучение социальных последствий. Это, с одной стороны, на время серьезно обеднило доктрину судебного большинства, из которой, например, исчезли рассуждения о справедливости, характерные, как я указал выше, для английских судов. С другой стороны, такая позиция, опирающаяся, по крайней мере отчасти (даже пусть и декларативно), на достижения современной экономической теории, выглядела достаточно солидно, чтобы конкурировать с более привычными американским юристам либеральными теориями, преподаваемыми в школах права, и позволила консерваторам найти достаточно убедительный способ политически обосновать более жесткую модель уголовной политики.

[62] См.: R v. Voisin [1918] 1 KB 531 — одно из ключевых решений, регулирующих этот вопрос до принятия Акта о полиции и доказательствах в уголовном процессе *(PACE)* 1984 года.
[63] См.: Fox v. Chief Constable of Gwent [1986] AC 281.

## "Crime Control Turn" and American Law of Criminal Procedure: Context and Ideology

This paper focuses on what is known as the "conservative turn" of the late 1960s–1980s in American criminal procedure. This shift, strongly associated with the ubiquitous "law and order" rhetoric and policies of the time, couldn't be possible without the strong support of conservative intellectuals, whose theories and doctrines have strongly impacted federal courts' reasoning in landmark "crime control" cases. The author concludes that the conceptual framework of "crime control" turn in criminal procedure can not be characterized simply as a return to older common law standards and actually follows the general trend of middle-century American jurisprudence, that is, the transition from a dogmatic to more pragmatic and policy-based approach (informed, e.g., by economics). The policy-based theories and tests adopted by the courts, paradoxically, caused a conceptual drift of American criminal procedure away from its English sister, while increasing the courts' discretionary powers in search and seizure cases.

***Keywords:*** *US criminal procedure, crime control, law and order, due process, law and economics, Miranda rule, originalism, conservative legal movement*

### INFORMATION ABOUT THE AUTHOR

**Aleksei S. Filiashin**
Department of Criminal Process, Justice and Public Prosecutor Supervision at the Law Faculty of Lomonosov Moscow State University, PhD student (e-mail: a.filyashin@ya.ru).

### REFERENCES

Eisen, L.-B., Roeder, O. America's Faulty Perception of Crime Rates. Brennan Center for Justice. URL: https://www.brennancenter.org/our-work/analysis-opinion/americas-faulty-perception-crime-rates.

Anscombe, G.E.M. Modern Moral Philosophy. Philosophy. 1958. Vol. 33. No. 124. P. 1–19.

Ash, E., Chen, D.L., Naidu, S. Ideas Have Consequences: The Impact of Law and Economics on American Justice. March 24, 2021. URL: https://www.law.nyu.edu/sites/default/files/ash-chen-naidu-2021-03v1.pdf.

Backhouse, R.E., Cherrier, B. The Age of Applied Economist: The Transformation of Economics since the 1970s. History of Political Economy. 2017. Vol. 49 (Supplement). P. 1–33.

Becker, G.S. Crime and Punishment: An Economic Approach. Journal of Political Economy.1968. Vol. 76. No. 2. P. 169–217.

Butler, H.N. The Manne Programs in Economics for Federal Judges. Case Western Reserve Law Review. 1999. Vol. 50. P. 351–420.

Clegg, J., Usmani, A. The Economic Origins of Mass Incarceration. Catalyst. 2019. Vol. 3. No. 3. P. 9–53.

Dahl, R. Decision-Making in a Democracy: The Supreme Court as a National Policy-Maker. Journal of Public Law. 1957. Vol. 6. No. 2. P. 279–295.

Epp, C.R. The Rights Revolution. Chicago, University of Chicago Press. 1998. 342 p.

Finnis, J. Natural Law and Natural Rights (2nd ed.). Oxford University Press. 2011. 494 p.

Friedman, B. Unwarranted: Policing Without Permission. New York, Farrar, Straus and Giroux. 2017. 448 p.

Gelbach, J.B., Klick, J. Empirical Law and Economics in: Parisi F. (ed.) The Oxford Handbook of Law and Economics: Volume 1: Methodology and Concepts. Oxford University Press. 2017. P. 29–59.

McMahon, K.J. Nixon's Court: His Challenge to Jusicial Liberalism and Its Political Consequences. The University of Chicago Press. 2011. 360 p.

Posner, R.A. Economic Analysis of Law. Boston, Little, Brown and Company. 1973. 415 p.

Posner, R.A. The Economics of Justice. Harvard University Press. 1980. 432 p.

Powe, Jr.L.A. The Supreme Court and the American Elite, 1789–2008. Harvard University Press. 2009. 421 p.

Stone, G. The Miranda Doctrine in the Burger Court. Supreme Court Review. 1977. Vol. 99. P. 99–169.

Teles, S.M. The Rise of Conservative Legal Movement. Princeton University Press. 2008. 360 p.

White, T.H. The Making of the President: 1964. Harper Collins. 1965. 480 p.

Merkuro, N., Medema, S. Economic Theory and Law: from Posner to Postmodernism and Beyond [*Jekonomicheskaja teorija i pravo: ot Poznera k postmodernizmu i dalee*]. Moscow, 2019, 648 p.

# В АПРЕЛЬСКОМ НОМЕРЕ

**Главная тема:** **Должностные преступления**

## Среди авторов номера:

**Г.А. Есаков**

К концепции единых служебных преступлений

*Каковы различия между преступлениями, предусмотренными главами 23 и 30 УК РФ, и не стоит ли эти главы объединить?*

**П.С. Яни**

Преподаватель в межсессионный период — не субъект получения взятки

*Не во всех случаях преподаватель может быть субъектом должностных преступлений: при определенных условиях он не должен считаться должностным лицом.*

**В.А. Алексеев**

Новое в законодательстве о недвижимых вещах: критический комментарий

*Автор анализирует цели и возможные последствия внесения изменений в ГК РФ, касающихся регулирования отношений в сфере недвижимости.*

## Темы ближайших номеров

МАЙ Толкование права

ИЮНЬ Гражданско-правовые сообщества

ЗАКОН
ИЗДАТЕЛЬСКАЯ ГРУППА

**Учредитель:**

**ООО «Издательская группа «Закон»**

**РЕДАКЦИЯ И ИЗДАТЕЛЬСТВО:**

Главный редактор:
**Александр Верещагин**
avere@igzakon.ru

Директор издательства:
**Владимир Багаев**
bagaev@igzakon.ru

Шеф-редактор:
**Ирина Шмарко**
shmarko@igzakon

Выпускающий редактор:
**Елена Пятикрестовская**

Корректор:
**Татьяна Казакова**

Компьютерная верстка:
**Мария Гранкина**

Распространение:
**Ринат Якупов**
rinat@igzakon.ru

Фотография на обложку:
**Алексей Мунтян**

Подписной индекс **39001**
в Объединенном каталоге
«Пресса России»
и в каталоге Агентства «Роспечать»

Редакция не несет ответственности
за достоверность сведений,
содержащихся в рекламных материалах.

Отпечатано
в ООО «БукиВеди»

Перепечатка материалов
журнала «Закон»
допускается только
с письменного
согласия издателя.

Подписано в печать 29.03.2022

Формат 84x108 1/16
Бумага офсетная № 1
Офсетная печать
Объем 11.5 печ. л.
Тираж 2000 экз.
Цена свободная

Регистрационный ПИ № ФС77-72467 от 20.03.2018

zakon.ru/senat

# ПОЛНОЕ СОБРАНИЕ СЕНАТСКИХ РЕШЕНИЙ

## ПО ЧАСТНОМУ ПРАВУ

## 1866-1917

ВПЕРВЫЕ
В ОТКРЫТОМ ДОСТУПЕ:

- все сборники решений Гражданского Кассационного Департамента
- указатели сенатской практики
- аннотации к тысяче наиболее ярких дел

Специальный раздел
на портале «Закон.ру»

**zakon.ru/senat**

ЗАКОН
ИЗДАТЕЛЬСКАЯ ГРУППА

Составитель: Александр Верещагин, доктор права Эссекского университета (Великобритания), главный редактор журнала «Закон».

При поддержке
Университета Дмитрия Пожарского.