УДК 342.722

Правоведение. 2019. Т. 63, № 1

Цифровая трансформация: правовое измерение*

Н. А. Дмитрик

Для цитирования: *Дмитрик Н. А.* Цифровая трансформация: правовое измерение // Правоведение. 2019. Т. 63, № 1. С. 28–46. https://doi.org/10.21638/spbu25.2019.102

Правовое измерение цифровой трансформации образуют подходы к правовому регулированию общественных отношений и стоящие за ними интересы участников данного процесса — государства, бизнеса, пользователей. Так называемое информационное право как аморфный институт без собственного предмета и метода оказалось не способно противостоять вызовам цифровой трансформации. Эффективное регулирование должно осуществляться с использованием метода фактической возможности, совпадающей с правовой возможностью, т. е. субъективным правом. Вопросы персональных данных как основного «топлива» цифровой экономики обсуждаются между государством и бизнесом. Это приводит к исключению из дискуссии граждан в силу отсутствия у них ресурсов для отстаивания собственных интересов. Такие ресурсы может дать только внедрение инструментов, гарантирующих ответственность перед субъектом данных за нарушение его прав. В сфере оборота промышленных и иных неперсональных данных отсутствие регулирования является скорее благом, ускоряющим развитие рынка. Однако при этом наращивается неравенство сторон (поставщиков оборудования и его пользователей) по доступу к данным. Инструментами защиты интересов пользователей здесь должны стать право на доступ к своим данным и механизмы переносимости данных между платформами. Хотя интересы государства в цифровой сфере связаны с обеспечением собственного суверенитета, попытки связать определенные типы данных с информационными системами, находящимися на территории данного государства («локализация данных»), противоречат структуре информационных потоков, прошедших цифровую трансформацию. В этих условиях регулирование должно учитывать формирование наборов данных и сервисов мгновенно, в определенной точке сборки, что требует обеспечения свободы оборота метаданных, на основе которых осуществляется сборка. Осознанные потребности, интересы — свои и других участников отношений — помогают развивать цифровую экономику наиболее справедливым образом, втягивая все новых субъектов в состояние согласованных интересов и тем самым взаимно эффективно ограничивая интересы друг друга. Государственное регулирование в цифровой экономике, как наименее эффективное, должно осуществляться только в последнюю очередь, если достичь юридического равенства интересов не удается усилиями отдельных игроков или взаимодействием участников рынка.

Ключевые слова: большие данные, экономическая концентрация, антимонопольная политика, саморегулирование, персональные данные, интерес, цифровые платформы, цифровое неравенство.

* Данная работа выполнена согласно плану фундаментальных научных исследований в рамках государственного задания Московского государственного университета им. М. В. Ломоносова на 2019 г. (ч. 2) (перспективное направление научных исследований «Проблемы цифровой экономики», тема «Правовые вопросы формирования воли и волеизъявления в цифровой экономике у естественных (индивиды) и искусственных (ИИ) субъектов»).

Дмитрик Николай Андреевич — канд. юрид. наук, Московский государственный университет им. М. В. Ломоносова, Российская Федерация, 119991, Москва, Ленинские горы, 1; dmitric@mail.ru

Надо, чтобы за дверью каждого довольного, счастливого человека стоял кто-нибудь с молоточком и постоянно напоминал бы стуком, что есть несчастные, что, как бы он ни был счастлив, жизнь рано или поздно покажет ему свои когти, стрясется беда — болезнь, бедность, потери, и его никто не увидит и не услышит, как теперь он не видит и не слышит других.

А. П. Чехов, «Крыжовник»

Введение

Новые технологии всегда приносят с собой новые возможности. Проблема в том, что новые возможности распределяются неравномерно. О неравномерности и ее следствии — неравенстве написано и сказано много[1], и здесь нет никакого смысла повторяться. Вопрос в другом. С момента публикации отчетов Национальной администрации телекоммуникаций и информации США (National Telecommunications and Information Administration, далее — NTIA), впервые измеривших цифровое неравенство[2], прошло уже 20 лет. За это время цифровая экономика ушла далеко вперед, и если в докладах NTIA речь шла о цифровом неравенстве как угрозе, теперь неравенство, вызванное использованием технологий, — данность.

В настоящей работе, впрочем, затрагиваются не вопросы экономического неравенства: они важны, но их изучением занимается экономическая наука. Данное исследование посвящено правовому неравенству (т. е. нарушению равенства, баланса интересов), вызванному образовавшимися фактическими — в противовес юридическим — возможностями сторон правоотношений.

1. Фактические и юридические возможности

«То, что дозволено, то и юридически обеспечено»[3], — писал в 1950 г. С. Н. Братусь. Конечно же, так никогда не было, и уже вскоре после этого в определении В. П. Грибанова субъективное право предстает как «дозволенная законом мера возможного поведения управомоченного лица»[4]. Однако до сих пор субъективное право как юридическая возможность определенного — и в этом плане дозволенного — поведения существует в отрыве от фактической возможности для субъекта вести себя так или иначе. Ранее мы уже рассматривали один аспект соотношения фактического и юридического, говоря о принципе реального осуществления гражданских прав[5]. Теперь необходимо сказать о другом аспекте этого соотношения: что происходит, когда фактически доступное лицу поведение не предусмотрено (хотя и не запрещено) правом.

---

[1] Один из последних трудов ко времени написания данной статьи: Антимонопольное регулирование в цифровую эпоху / под ред. А. Ю. Цариковского, А. Ю. Иванова, Е. А. Войниканис. М.: Изд. дом Высшей школы экономики, 2018. С. 8–12.

[2] Falling Through the Net: Defining the Digital Divide. URL: https://web.archive.org/web/20100209053123/http://www.ntia.doc.gov/Ntiahome/Fttn99/ (дата обращения: 01.05.2019).

[3] *Братусь С. Н.* Субъекты гражданского права. Л.: Госюриздат, 1950. С. 11.

[4] *Грибанов В. П.* Осуществление и защита гражданских прав. М.: Статут, 2001. С. 292.

[5] *Дмитрик Н. А.* Способы осуществления гражданских прав и исполнения обязанностей с использованием сети Интернет: дис. … канд. юрид. наук. М.: МГУ им. М. В. Ломоносова, 2007. С. 17–24. — Принцип реального осуществления гражданских прав предполагает, что закрепленная в праве возможность определенного поведения должна быть фактически доступна.

В гражданском праве такая ситуация не просто допускается, она поощряется в силу принципа диспозитивности и в целом в рамках дозволительного, «правонаделительного» характера частного права. Однако, говоря о соотношении фактической и юридической возможности, нельзя забывать о том, что в правоотношении есть как минимум две стороны, при этом возможность, не мыслившаяся законодателем, может стать доступной только для одной из них.

Вернемся еще на век назад. За сто лет до С. Н. Братуся о соотношении фактических и юридических возможностей рассуждал Ф. Лассаль. Он призвал различать действительную конституцию как реальные отношения силы и юридическую конституцию как писаный документ. «Как скоро писаная конституция не соответствует действительной, между ними происходит столкновение, которого ничем нельзя предупредить и в котором писаная конституция, листок бумаги, неизбежно побеждается действительною конституцией, действительными отношениями силы, существующими в стране»[6]. Реальные отношения силы между цифровой платформой и ее пользователем сейчас как никогда входят в столкновение. Можно ли как-то предупредить победу «действительной цифровой конституции» над гарантиями и правами пользователя, предусмотренными законодательством?

Пока что мы можем наблюдать полнейшую правоту Ф. Лассаля и выводов, сделанных им более полутора веков назад. Реальные отношения силы находятся во власти цифровых платформ, поставщиков информационных продуктов и сервисов, а отнюдь не пользователей и даже не государств. Вот лишь несколько примеров из исследований разных аспектов цифровой экономики. «Для пользователя технические средства, как правило, носят абсолютный характер: он не обладает необходимыми знаниями, чтобы попытаться их обойти»[7]. «Концентрация в цифровой экономике, дополненная сетевыми эффектами или издержками на смену поставщика услуг, приводит к антиконкурентному поведению. Но интернет-фирмы ставят в тупик традиционное антимонопольное законодательство, поскольку они не ведут себя как традиционные монополии»[8]. Получается, что процесс концентрации доступными им средствами не могут остановить ни пользователи, ни государство. Возможность концентрации обусловлена синергетическим эффектом от совпадения четырех технологий: облачных вычислений, мобильности, социальных сетей и больших данных. Пользователи растущего количества мобильных устройств производят все больше контента, который удобно и дешево хранить на облачных сервисах. Облачные сервисы помогают делиться контентом между пользователями разных мобильных платформ, независимо от государств и их границ. Рост объемов контента делает привлекательными все новые мобильные устройства и платформы и требует все новых облачных хранилищ. Накапливаемые данные «приземляются» на социальные сети, делая доступным анализ информации из таких сетей и управление ею с использованием технологий больших данных. В свою очередь, накапливаемые данные используются для рекламы и повышения пользовательской ценности все новых мобильных сервисов и платформ[9].

---

[6] *Лассаль Ф.* О сущности конституции (речь, произнесенная в одном берлинском бюргерском окружном собрании в 1862 г.) // Войтович В. Ю. Теоретические основы сущности конституции: учеб. пособие. Ижевск: Удмуртский университет, 2012. С. 21.

[7] *Кувыркова А. Ю.* Осуществление исключительных интеллектуальных смежных прав: дис. … канд. юрид. наук. М.: МГУ им. М. В. Ломоносова, 2010. С. 54.

[8] Digital Dividends: World development report 2016. URL: http://www.worldbank.org/en/publication/wdr2016 (дата обращения: 01.05.2019).

[9] См. об этом: *Прохоров А. М., Коник Л. Г.* Цифровая трансформация. Анализ, тренды, мировой опыт. М.: АльянсПринт, 2019. С. 22–25.

Этот процесс, предоставленный сам себе, может только наращивать концентрацию, но никак не снижать ее[10].

В деле нахождения баланса интересов сторон информационного правоотношения особенно плохо показало себя так называемое информационное право. Стыдливая формула «информационное право по методам правового регулирования является комплексной отраслью третьего уровня классификации»[11] прикрывает фактическое отсутствие собственного метода, который позволил бы решать задачи, стоящие перед правом как социальным регулятором в информационной сфере. «Специфика методов информационного права — сочетание конституционного регулирования, административных способов обеспечения особенностей информационной деятельности, привлечение всего арсенала контрольных, принудительных, карательных мер в процессе обеспечения соблюдения законодательства и реакции государства на правонарушения — объясняет и проблему места информационного права в системе права в целом»[12]. Точнее не скажешь. Информационное право, понимаемое таким образом, не смогло и не сможет противопоставить какие-либо правовые методы фактическим возможностям контролировать доступ к информации, имеющимся у цифровых платформ, — этот фактор действительно в полной мере определяет место информационного права в системе других отраслей права.

Совершенно иные горизонты открывает понимание метода информационного права (точнее, права информационных технологий) как метода фактической возможности, своего рода lex informatica правовых норм. «Если в правовом режиме содержание норм определяется законом и судебными решениями, в lex informatica правила поведения определяются техническими возможностями и практикой применения технологий»[13]. Что не допускается техникой, то и невозможно.

Метод фактической возможности не является новым для права, но пока его применение не консолидировано в рамках одной отрасли или даже института. Данный метод активно используется в авторском праве и смежных правах в рамках технических средств защиты авторского права, не только подменяя собой лицензионный договор, но и добавляя в содержание исключительного права новое правомочие (на доступ к произведению или объекту смежных прав)[14]. Фактическая возможность — метод регулирования в системах, где требуется авторизация для совершения юридически значимых действий. Например, отношения по регистрации доменных имен, где правила формируются регистраторами, часто основываются на методе «все действия, совершенные под номером договора и паролем заказчика, признаются совершенными лично заказчиком»[15]. Здесь принципиально не только указание на ту или иную возможность поведения в договоре

---

[10] Согласно докладу Всемирного банка Digital Dividends, концентрация возможности управления доступом к информации является главным риском цифровой трансформации.

[11] *Елин В. М., Жарова А. К.* К вопросу о методологии информационного права // Право и государство: теория и практика. 2013. № 4. С. 135. — В приведенной цитате авторы ссылаются на работу: *Бачило И. Л., Лопатин В. Н., Федотов М. А.* Информационное право. СПб.: Юридический центр Пресс, 2005. С. 75.

[12] Там же.

[13] *Войниканис Е. А.* Право интеллектуальной собственности в цифровую эпоху: парадигма баланса и гибкости. М.: Юриспруденция, 2013. С. 54.

[14] См. об этом: *Дмитрик Н. А.* Способы осуществления гражданских прав… С. 131; *Koelman K. J., Helberger N.* Protection of Technological Measures // Copyright and Electronic Commerce. Legal Aspects of Electronic Copyright Management. The Hague: Kluwer Law International, 2000. P. 189.

[15] См. п. 8.15 Правил регистрации доменных имен в доменах .RU и .РФ, утв. Координационным центром национального домена сети Интернет. URL: https://cctld.ru/files/pdf/docs/rules_ru-rf.pdf (дата обращения: 15.04.2020).

или локальном правовом акте (правилах), но и фактическое использование логина и пароля, что приводит к формированию фикции, основанной на фактической, а не юридической возможности определенного поведения. Метод фактической возможности используется в регулировании самых разных правоотношений и не только в виде программного кода: например, в транспортной сфере этот метод образуют транзитные зоны в аэропортах, турникеты на станциях и в подвижном составе, развязки и шлагбаумы и т. п.

Говоря о перспективах метода фактической возможности, важно упомянуть несколько вещей.

Во-первых, не любой алгоритм является регулятором, но только тот, за которым законодатель признал правомочие регулировать общественные отношения (т. е. формировать на конкретном уровне те абстрактные возможности, которые закреплены в виде субъективных прав). И технические средства защиты авторского права, и действия под логином (паролем) пользователя, и турникеты применяются в соответствии с тем или иным правовым актом (законом, локальным актом или договором). Lex informatica — это логика, делегированная правом технике.

Во-вторых, метод фактической возможности как метод права требует крайне аккуратного применения, поскольку он регулирует столь же значимые отношения, что и право. Можно предложить в качестве рамок для данного метода его познаваемость, предсказуемость и доверие к нему со стороны пользователей[16]. В частности, он не допускает «шапкозакидательских» законов, про которых уже на стадии разработки эксперты говорят, что реализовать их не получится. Метод фактической возможности предполагает тщательную оценку его воздействия, разработку соответствующей технической и технологической базы, тестирование, оценку затрат на внедрение — и только после этого применение.

В-третьих, построение ответа на вызовы цифровой трансформации на основе методов права информационных технологий не означает фактического закрепления status quo. Наоборот, использование государством технических возможностей должно восстановить баланс интересов, нарушенный неравномерной доступностью новых технологий. Совершенно иную картину мы, к сожалению, видим во многих сферах деятельности: правовые и технические инструменты пытаются использовать для того, чтобы закрепить новый, дискриминационный баланс интересов сторон, отдав фактический приоритет интересам сильной стороны в правоотношении (обычно — цифровой платформе). Это касается прежде всего тех элементов процесса цифровой трансформации, которые превращают индустриальную экономику в цифровую, т. е. в экономику данных: персональных и промышленных данных, а также трансграничного обмена такими данными.

2. Персональные данные и цифровая трансформация

Персональные данные стали передовой борьбы за цифровую экономику в России, да и во всем мире. Российский Центр компетенций по нормативному регулированию цифровой экономики разработал два и планирует разработать еще шесть законопроектов, изменяющих правовой режим персональных данных[17]. В Беларуси в срочном порядке разработан и внесен в Палату пред-

[16] См. подробнее об этом: *Дмитрик Н. А.* Пределы правового регулирования в цифровую эпоху // Информационное общество. 2018. № 3. С. 47–58.

[17] См. раздел «Оборот данных» Портала Центра компетенции по нормативному регулированию цифровой экономики. URL: http://sk.ru/foundation/legal/p/03.aspx (дата обращения: 01.05.2019).

ставителей закон о персональных данных[18] (ранее отдельного законодательного акта по вопросам обработки персональных данных в республике не было). В рамках Евразийского экономического союза (далее — ЕАЭС) разрабатывается Соглашение об обороте данных в Союзе (в том числе о защите персональных данных)[19]. Знаменитыми стали Общий регламент ЕС по защите персональных данных (General Data Protection Regulation, далее — GDPR)[20] и закон Калифорнии о приватности пользователей[21]. Немного менее заметным, но не менее значимым событием стало признание Евросоюзом Японии государством, обеспечивающим адекватный уровень защиты персональных данных. Перечень документов и связанных с ними событий можно продолжать долго, и это только подчеркивает значимость вопроса о правовом режиме персональных данных в контексте цифровой экономики.

В России основная дискуссия сосредоточилась вокруг вопросов об общедоступных данных, о возможности использования обезличенных данных, а также о порядке получения согласия на обработку персональных данных. Центральной площадкой для дискуссии стал уже упоминавшийся Центр компетенций по нормативному регулированию цифровой экономики (далее — Центр компетенций), который, как следует из его статуса, в большей степени агрегировал интересы бизнеса. Бизнес же оценивает предусмотренный российским законодательством порядок работы с персональными данными как административный барьер. В созданном Центром компетенций реестре[22] указаны следующие барьеры: необходимость получения множественных согласий субъекта данных; неопределенность в соотношении персональных данных и больших данных, которая «ставит вопрос о необходимости получения согласия субъекта на обработку больших и пользовательских данных»; невозможность передачи данных, составляющих банковскую тайну, даже с согласия пользователя третьим лицам; невозможность дачи согласия на обработку биометрических данных представителем и т. д. Интерес бизнеса заключается в упрощении (или отмене) согласия на обработку персональных данных в рамках технологий больших данных, т. е. профайлирования и обогащения данных с целью извлечения из них пользы. Данный интерес немного по-разному преломляется применительно к двум основным видам пользовательских данных в контексте больших данных: общедоступным и обезличенным.

Общедоступные данные — или, в терминологии ст. 8 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»[23] (далее — Закон о персональных

---

[18] Информация о законопроекте доступна на сайте Палаты представителей Национального собрания Республики Беларусь. URL: http://house.gov.by/ru/zakony-ru/view/o-personalnyx-dannyx-661/ (дата обращения: 01.05.2019).

[19] Разработка данного соглашения предусмотрена решением Высшего Евразийского экономического совета от 11.10.2017 № 12 «Об Основных направлениях реализации цифровой повестки Евразийского экономического союза до 2025 года». URL: https://www.garant.ru/products/ipo/prime/doc/71708158/ (дата обращения: 10.04.2020).

[20] Regulation (EU) 2016/679 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. URL: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:32016R0679 (дата обращения: 10.04.2020). — Регламент является одним из документов, реализующих стратегию единого цифрового рынка ЕС (Digital Single Market).

[21] California Consumer Privacy Act of 2018. URL: http://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375 (дата обращения: 10.04.2020).

[22] Официальный сайт СКОЛКОВО. URL: http://sk.ru/news/m/wiki/21074.aspx (дата обращения: 01.05.2019).

[23] Здесь и далее, если не указано иное, нормативно-правовые акты и судебная практика приводятся по СПС «КонсультантПлюс». URL: http://www.consultant.ru (дата обращения: 10.04.2020).

данных), «данные из общедоступных источников персональных данных» — являются естественным сырьем для формирования больших данных. Эти данные можно автоматически собирать, комбинировать, при необходимости — обновлять или отслеживать обновления. В докладе Центра компетенцией барьером для бизнес-интересов указывается «правовая неопределенность для компаний, работающих с общедоступными персональными данными». «Поисковые “роботы” не умеют определять: являются ли данные персональными; кому они принадлежат, кто их разместил и зачем. Нет ответа на вопрос: можно ли использовать данные для обучения алгоритмов поиска или создания технологий?»[24] В докладе делается справедливое замечание об изменении позиции Роскомнадзора по вопросу использования данных из общедоступных источников. До 2016 г. данные в социальных сетях Роскомнадзор считал возможным использовать для любых целей. С 2016 г. Роскомнадзор стал исходить из того, что данные в социальных сетях общедоступны, но для их использования в целях, отличных от размещения, требуется согласие. Суды, как следует из рассматриваемого материала, считают данные в социальных сетях не общедоступными, поскольку нельзя достоверно подтвердить, что данные были сделаны общедоступными субъектом персональных данных либо по его просьбе, как того требует п. 10 ч. 1 ст. 6 Закона о персональных данных[25].

В рассматриваемом докладе как соответствующие интересам бизнеса изложены две возможные концепции регулирования. Первая — «концепция двух ключей», в соответствии с которой социальная сеть или иная площадка, на которой пользователи размещают свои данные, обеспечивает получение согласий от пользователей и контролирует последующее использование третьими лицами размещаемых данных, обеспечивая на это согласие пользователей (как субъектов персональных данных) и собственное согласие (как субъекта интеллектуальных прав). Вторая концепция предполагает свободный (без получения согласия) сбор персональных данных из общедоступных источников и их накопление (этап «сырых данных»), при этом получение согласия требуется только в случае использования этих данных (этап использования).

Что касается обезличенных данных, то они во многих случаях являются результатом применения технологий больших данных, итоговым продуктом, оптимизированным под использование в конкретной области: в рекламе, банками, страховыми компаниями. Производственная цепочка тем самым состоит из трех звеньев: сырые данные (например, данные из общедоступных источников) — профайлы (агрегированные и структурированные данные) — обезличенные данные (применяемые для оптимизации деятельности в разных сферах). Проблеме обезличенных данных посвящен разработанный Центром компетенций законопроект[26] о внесении изменений в Закон о персональных данных и в Федеральный закон от 27.06.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (далее — Закон об информации). Разработанным за-

[24] Концептуальные развилки по подготовке проекта федерального закона в части установления порядка и правил доступа к общедоступным данным. URL: http://sk.ru/foundation/legal/m/sklegal03/22418/download.aspx (дата обращения: 01.05.2019).

[25] Имеется в виду дело об оспаривании ненормативного акта управления Роскомнадзора по ЦФО Национальным бюро кредитных историй, где Верховный суд РФ высказал именно такую позицию. См. карточку дела. URL: http://kad.arbitr.ru/Card/eb1907d9-be95-4b0e-85c7-0481aef89b31 (дата обращения: 01.05.2019).

[26] Портал Центра компетенции по нормативному регулированию цифровой экономики. URL: http://sk.ru/foundation/legal/m/sklegal03/22237/download.aspx; и http://sk.ru/foundation/legal/m/sklegal03/22236.aspx (дата обращения: 01.05.2019).

конопроектом устанавливается, что обезличенные данные могут использоваться любым лицом и передаваться одним лицом другому лицу, в том числе на возмездной основе. Обезличивание должно осуществляться в соответствии с требованиями и методами, установленными Роскомнадзором. Таким образом, и здесь прослеживается интерес бизнеса на устранение согласия субъекта персональных данных как барьера.

Согласие субъекта персональных данных тем не менее является краеугольным камнем защиты личной информации. Поэтому еще одним направлением нормативной работы становится построение новых механизмов получения согласия, более или менее адаптированных к цифровой реальности. В законопроектах Центра компетенции указывается, что согласие может быть дано в любой позволяющей подтвердить факт его получения форме, в том числе электронной (путем направления СМС, посредством электронной почты, заполнения формы на сайте, иными способами). В более амбициозном разработанном Минкомсвязи России законопроекте о так называемом цифровом профиле[27] предусматривается выделение цифрового профиля как особого корпуса данных, доступ к которому осуществляется в специальном порядке. В частности, если на предоставление данных требуется согласие субъекта персональных данных, оно дается субъектом в инфраструктуре цифрового профиля в форме электронного документа, подписанного усиленной квалифицированной электронной подписью или простой электронной подписью портала госуслуг. Это позволяет создать систему личных кабинетов субъектов персональных данных, где согласия на обработку могут быть удобно даны и отозваны, а также может быть получена информация о том, кто и как обрабатывает персональные данные этого субъекта. В этом плане, конечно, законопроект о цифровом профиле отражает не только интересы бизнеса, как проекты Центра компетенций, но и интересы государства, упорядочивающего и делающего более прозрачным работу с персональными данными в государственных информационных системах.

Россия — не единственная страна в мире, решающая на законодательном уровне, как обращаться с информацией о человеке в цифровой реальности. Ведущие государства осознают, что правовой режим персональной информации становится своего рода регуляторным преимуществом. Пока что первое место в этой гонке занимает Евросоюз с GDPR и связанными с ним документами стратегии цифрового общего рынка. Поскольку Регламенту было придано фактически экстерриториальное действие, его нормы распространяются по экономическим связям Европейского союза, подчиняя себе компании, работающие на европейском рынке, аутсорсеров компаний, работающих на европейском рынке, и даже разработчиков программного обеспечения для аутсорсеров компаний, работающих на европейском рынке. По заданному Европой направлению идут Индия, подготовившая в 2018 г. свой законопроект[28] о персональных данных, сопоставимый по объему с GDPR, и Япония, чей правовой режим обработки персональных данных, несмотря на серьезные отличия в режиме обезличенных данных (они могут передаваться оператором третьим лицам без согласия субъекта)[29], был признан Евросоюзом адекватным. Однако победоносное шествие GDPR и его

[27] Федеральный портал проектов нормативных правовых актов. URL: https://regulation.gov.ru/projects#npa=89871 (дата обращения: 01.05.2019).

[28] The Personal Data Protection Bill, released on 27 July 2018. URL: https://meity.gov.in/writereaddata/files/Personal_Data_Protection_Bill%2C2018_0.pdf (дата обращения: 01.05.2019).

[29] Linklaters Insights Data Protected Japan. URL: https://www.linklaters.com/fr-be/insights/data-protected/data-protected---japan (дата обращения: 01.05.2019).

подобий по миру омрачает тот факт, что они, похоже, не только не препятствуют концентрации, но, наоборот, стимулируют ее.

Согласно данным проекта whotracks.me, отслеживающего в реальном времени структуру рынка онлайн-рекламы и маркетинга, в том числе используемые технологии отслеживания (cookies, счетчики, кнопки и т. п.), главным бенефициаром от вступления в силу GDPR оказался Google и другие цифровые гиганты. Больше всего пострадали небольшие рекламные и иные компании, чье присутствие на рынке сократилось в диапазоне 18–31 % (июль к апрелю 2018 г.). Для сравнения, Facebook за этот же период потерял 6,5 %[30]. Объяснение этого лежит во взаимосвязи трех процессов. Во-первых, только крупные компании смогли найти ресурсы для выполнения требований и процедур GDPR. Во-вторых, небольшие компании, которые не выполнили в полном объеме новые требования, предпочли сократить рыночную активность, чтобы не подвергнуться штрафам. В-третьих, Google использовал эту ситуацию, чтобы убедить крупных клиентов перейти с платформ небольших провайдеров с непонятным статусом выполнения требований GDPR на платформу Google. Приведенное наблюдение подтверждают также сводные данные по количеству используемых средств отслеживания в Евросоюзе и США. В Евросоюзе оно сократилось на 3,4 % (июль к апрелю 2018 г.), в то время как в США оно выросло на 8,3 %[31], что соответствует обычному росту данного рынка. Таким образом, введение усиленных правил защиты персональных данных привело лишь к повышению концентрации на рынке и увеличению количества технологий отслеживания.

Как минимум, это говорит о том, что любая формализация правил работы с персональной информацией приводит к охране по форме, а не по сути. Любая замена одного формального требования на другое (бумажного согласия на цифровое) не повышает защиту интересов субъектов персональных данных. Выполнение формальных требований лучше всего удается самым большим компаниям, для остальных же это становится барьером для развития или даже для выхода на новый цифровой рынок.

Также нельзя не обратить внимание, что как минимум в России дискуссия о защите персональных данных ведется между бизнесом и государством. Однако ни бизнес, ни государство не являются субъектами персональных данных; они ведут дискуссию не о себе, а о других. Накладываясь на формальный, бюрократический подход к защите, это приводит к дискуссии, по сути, об удобной процедуре защиты персональных данных, закрывающей риски безопасности (для государства) или имущественных потерь (для бизнеса). Но никак не к дискуссии о защите интересов субъектов персональных данных.

Интерес же субъектов персональных данных заключается по крайней мере в том, чтобы им не был причинен вред обработкой платформами персональных данных. Если защищать данный интерес, необходимо иметь в виду условия (или причины) возникновения вреда, вызванного незаконной обработкой персональных данных, и формы такого вреда. Причины возникновения вреда всегда обусловлены тем, что персональная информация связана контекстом ее использования. Как указывает Хелен Ниссенбаум, информация о человеке раскрывается в определенном контексте, связана правилами и нормами этого контекста и может использоваться только в этом контексте[32]. Например, фотография

[30] Study: Google Is the Biggest Beneficiary of the GDPR. URL: https://cliqz.com/en/magazine/study-google-is-the-biggest-beneficiary-of-the-gdpr (дата обращения: 01.05.2019).

[31] Ibid.

[32] *Nissenbaum H.* Privacy as contextual integrity // Washington Law Review. 2004. Vol. 79, no. 3. P. 119–158.

с дружеской вечеринки, посланная в группу этих друзей в мессенджере, остается в контексте дружеского общения и не может причинить какого-либо вреда. Та же фотография, на которой изображен друг-чиновник, опубликованная в журналистском расследовании, может стоить этому человеку должности и даже свободы. Связанность информации о человеке определенным контекстом означает не просто его право давать или не давать согласие на использование информации. Это свобода человека внутри контекста: свобода общения с людьми, входящими в контекст, и свобода от общения с людьми, в него не входящими. Нарушение этой свободы, т. е. произвольное перемещение информации между контекстами, причиняет вред.

«Конечной целью любого закона о защите данных является защита индивида от риска причинения вреда, который может быть вызван сбором, использованием и раскрытием персональной информации»[33]. Закон должен быть ориентирован не на выполнение формальных процедур, не на правила получения согласия или отсутствие необходимости его получать, а на обеспечение свободы человека внутри контекста и права каждого оставить свою информацию внутри того контекста, в котором она была получена или раскрыта. Нарушение этого права приводит к возникновению вреда, который может быть в двух формах — субъективной или объективной. Субъективный вред может выражаться в осознании человеком собственной уязвимости перед теми, кто знает о нем «слишком много», в травле, в сломанной семейной или иной личной жизни. Объективный — в том, что человека на основе вырванной из контекста информации не взяли на работу (или уволили с нее), не дали ему кредит, не продали билет на поезд, самолет или футбольный матч.

Нельзя не сказать про еще одно измерение свободы человека в цифровой экономике, также находящееся под угрозой концентрации. Под терминами «таргетирование», «повышение эффективности рекламных кампаний», «сегментирование» и всем остальным, для чего фактически используются большие данные, скрывается воздействие на нашу волю, на свободу нашего выбора. Информация о нас используется для того, чтобы управлять нами в чьих-то интересах: мы должны покупать, читать, выбирать то, что нужно рекламодателю, а не нам. Большие данные сейчас — это взлом нашей личности, добыча нашего внимания как ограниченного ресурса.

Ни один из действующих законов о защите персональных данных не защищает нас от использования платформами наших данных для управления нашей волей. Наоборот, европейский подход к защите персональных данных предполагает, что если процедурные вопросы соблюдены (есть согласие субъекта или законное основание обработки, если данные находятся в безопасности и обрабатываются транспарентно), то фактическое их использование для целей «таргетирования» является законным и, более того, справедливым. Однако по факту это приводит к еще большей концентрации: тот, кто сейчас имеет доступ к данным, предпринимает все меры, чтобы сузить поле нашего внимания только до своих товаров или информационных продуктов.

Концентрация, таким образом, выступает антагонистом не только конкуренции, но и свободы.

Нельзя сказать, что этот риск не осознается или замалчивается. Наоборот, на родине приватности, в США, осознание этого негативного фактора привело к потребности в новой политике приватности. Был принят закон Калифорнии

[33] *Gratton E.* Understanding Personal Information: Managing Privacy Risks. Canada: LexisNexis, 2013. P. 208.

о приватности пользователей, обязавший средние и крупные компании, чей бизнес связан с обработкой пользовательских данных, обеспечивать транспарентность обработки и удалять данные пользователей по их требованию. Было опубликовано заявление Марка Цукерберга, где обсуждались идеи об удалении вредоносного контента, защите выборов, переходе на новые правила защиты приватности, дающие контроль на собственной персональной информацией, а также идеи об обеспечении переносимости данных как залога конкуренции[34]. Новый подход к приватности отражает понимание связи между человеком и данными о нем в цифровых платформах, его «цифровыми двойниками». Интересы бизнеса иметь качественные, актуальные и безопасные (т. е. не создающие угрозы вреда для бизнеса) данные о своих пользователях входят в «зацепление»[35] с интересами пользователя контролировать свои данные, понимать, где они используются, и не допускать их использования во вред себе. Интересы бизнеса, понимаемые не как интересы отдельной компании, а как интересы отрасли, можно надеяться, приведут к осознанию того, что «взлом личности», отношение к человеческому вниманию как к добываемому ресурсу невыгодны. Таргетирование людей на определенные продукты, услуги, кандидатов на выборах неизбежно снижает уровень экономического и политического развития, что создает риск для всех.

Нельзя забывать и про возможности, которые дает цифровая трансформация. Формальная процедура была первейшей гарантией, и человечество тянет ее за собой с первобытного общества, строя на ней такие современные документы, как GDPR. «Процедура — это логика, вынесенная вовне, она создает для проявления разума социальный институт как своего рода “искусственный интеллект”»[36]. В цифровом обществе гарантии могут формироваться по сути, а не по процедуре, в том числе за счет использования методов фактической возможности, таких как логирование, использование реестров, мониторинг и т. п.

Однако сделать в этом направлении предстоит еще много, прежде чем государственная политика и практика ведения бизнеса в полной степени обеспечат свободу человека и связанность персональной информации контекстом ее использования. Поэтому крайне важно обеспечить участие главных заинтересованных лиц — самих граждан — в выработке этой политики и практики, в защите данных по сути, а не по форме. Говоря о России, нельзя не отметить отсутствие у граждан ресурсов для защиты своих интересов. Даже услуги судебного представительства недоступны для большинства, что говорить о лоббировании, продвижении законодательных инициатив. Здесь определенно нужен механизм, позволяющий перераспределять в пользу субъектов персональных данных ресурсы, которые могут быть использованы ими для защиты собственных интересов.

Может быть использован, в частности, опыт смежной отрасли правового регулирования, а именно законодательства об авторском праве. Установленная ст. 1301 Гражданского кодекса РФ (часть четвертая) от 18.12.2006 № 230-ФЗ компенсация, выплачиваемая в случаях нарушения исключительного права на произведение, предусматривает минимальный ее размер — от 10 тыс. до 5 млн руб., — определяемый по усмотрению суда исходя из характера нарушения.

---

[34] *Zuckerberg M*. Four Ideas to Regulate the Internet. March 30, 2019. URL: https://newsroom.fb.com/news/2019/03/four-ideas-regulate-internet/ (дата обращения: 01.05.2019).

[35] Состояние «зацепления интересов» принципиально важно для нашего исследования; о нем подробно говорится в заключительной части настоящей работы.

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

Если закрепить аналогичный механизм для сферы персональных данных, субъекту будет достаточно — например, с привлечением Роскомнадзора — доказать сам факт нарушения его прав, после чего он может рассчитывать на получение компенсации хотя бы в минимальном размере (не менее 10 тыс. руб.). За более чем десятилетний период действия норма, устанавливающая минимальный размер компенсации за нарушение исключительного права, зарекомендовала себя как эффективная, что было подтверждено, в частности, в Постановлении Конституционного суда РФ от 13.12.2016 № 28-П. Возможность получения значимой компенсации работает как механизм балансировки интересов: субъекту становится интересно защищать свои права, цифровым платформам становится неинтересно создавать для себя судебные риски, защитникам прав становится интересно инвестировать в поиск новых дел и повышение собственной квалификации, так как это окупается гонорарами. Такое зацепление интересов позволит, в свою очередь, реализовать всю ту цифровую трансформацию правовой защиты персональных данных, о которой говорилось выше.

3. Промышленные данные: цифровая трансформация в условиях неопределенности

Если для персональных данных многолетняя история их регулирования создала универсальное право на доступ к данным о себе, для неперсональных (машинных, промышленных) данных такое право отсутствует. В рамках так называемой «Индустрии 4.0»[37], т. е. цифровой трансформации промышленности, необходимость в этом праве стала достаточно актуальной. Если раньше промышленное оборудование находилось под фактическим господством его владельца как физически, так и информационно, в «Индустрии 4.0» обладание вещью и обладание данными с этой вещи оказались разделены. Особенно наглядно разделение физического и информационного господства над промышленным оборудованием проявляется в кейсе взаимодействия иностранных поставщиков смарт-оборудования и их клиентов в других странах. В силу условий договорных отношений и технологических особенностей самого оборудования его использование фактически невозможно без организации постоянного обмена данными между поставщиком и покупателем. Вследствие этого как фактически, так и юридически данные находятся в юрисдикции поставщика, а их использование регулируется законодательством страны поставщика оборудования.

Такое положение не только влияет на концентрацию, но и может негативно сказываться на техническом прогрессе. Цифровая трансформация промышленности тоже основывается на данных. Данные с промышленного оборудования могут использоваться технологическими стартапами для построения и последующего тестирования математических моделей, позволяющих повысить эффективность использования оборудования. Даже 5 %-ное повышение эффективности, например, газовой турбины, имеет серьезное экономическое последствие в виде меньших расходов на ее эксплуатацию, что, в свою очередь, будет конкурентным преимуществом производителя таких турбин. Однако если данные с турбин концентрируются производителем в другом государстве, доступ к таким данным для стартапов затруднен, если не сказать невозможен. В этой ситуации также окажутся неэффективными механизмы антимонопольного регулирования, поскольку,

[37] См. портал Germany Trade & Invest (GTAI) — Агентство по внешнеэкономической деятельности Федеративной Республики Германия. URL: https://industrie4.0.gtai.de/INDUSTRIE40/Navigation/EN/Topics/industrie-4-0.html (дата обращения: 01.05.2019).

во-первых, держатель данных находится в другом государстве, во-вторых, доступ к данным в общем-то не влияет непосредственно на рынок турбин.

Понимая это, в Евросоюзе создали специальное регулирование для неперсональных данных, объявив «пятую свободу» — свободу оборота данных. Данная свобода для неперсональных данных основывается на двух механизмах. Первый из них связан с уменьшением количества требований по локализации данных, содержащихся в законодательстве государств — членов ЕС или обусловленных практикой вендоров. Таким образом, создаются условия для физического перемещения данных. Второй механизм направлен на обеспечение коммерческого перемещения данных между разными поставщиками услуг (так называемая переносимость данных). В результате свободные неперсональные данные в Европе — это данные, которые нельзя привязать ни к объекту (стране, информационной системе), ни к субъекту (поставщику услуг).

Возвращаясь к российской действительности, надо признать, что у нас оборот неперсональных данных никак не урегулирован — ни с позиций ограничения их оборота, ни с позиций обеспечения недискриминационного доступа к ним. Конечно, такие данные могут представлять собой ту или иную тайну, но это зависит от правового режима их охраны, а не от содержания данных. В какую сторону двигаться российскому регулированию (в сторону свободы оборота таких данных, создания механизмов недискриминационного доступа к ним либо в сторону ограничения свободы их оборота, например путем установления особого правового режима их обработки), пока непонятно. Однако здесь — в отсутствие опыта реализации нового Регламента ЕС — можно по аналогии опираться на негативный опыт того же Евросоюза по ограничению свободы оборота данных с помощью другого инструмента, а именно права sui generis.

Так называемое право sui generis (право особого рода), как известно, было создано более 20 лет назад Директивой 96/9/ЕС о правовой охране баз данных[38] и предоставляло составителю базы данных, который внес количественно или качественно существенный вклад в получение, проверку или представление содержания базы данных, возможность запрещать изъятие или повторное использование всего содержания базы данных или его количественно/качественно существенной части. Иначе говоря, в рамках указанной Директивы был создан механизм огораживания корпуса данных без установления в отношении них режима той или иной тайны, что позволяло защитить произведенные инвестиции[39]. Для сравнительного анализа последствий такого решения обычно используется рынок данных США, где принципиально (на основании отрицания так называемой доктрины sweat of the brow (англ. «в поте лица»), т. е. дарования правовой охраны результатам любого интеллектуального труда) не предоставляется правовой защиты данным в базах и банках данных. Исследования рынков баз данных, проводившиеся в 2001–2005 гг., не показали каких-либо преимуществ у подхода, закрепляющего исключительное право на данные в базе данных. Как указывается в обзоре эконометрических и статистических исследований[40], рынок данных в США уверенно рос как до принятия рассматриваемой директивы, так и после ее при-

[38] Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A31996L0009 (дата обращения: 01.05.2019).

[39] См. об этом: *Кувыркова А. Ю.* Осуществление исключительных интеллектуальных смежных прав. С. 21.

[40] *Maurer S. M.* Across Two Worlds: Database Protection in the United States and Europe. 2005. URL: https://www.researchgate.net/publication/228794091_Across_Two_Worlds_Database_Protection_in_the_United_States_and_Europe (дата обращения: 01.05.2019).

нятия. На основных европейских рынках (Великобритании, Германии и Франции) в годы, следующие за принятием Директивы (1998–2000), произошел разовый рост количества источников (баз и банков) данных, после чего их количество скорректировалось и продолжило расти в соответствии с трендами, существовавшими до принятия директивы.

Таким образом, любые ограничительные меры в отношении оборота неперсональных данных, в том числе путем установления прав воспрещения, как минимум не стимулируют экономического развития. Отсутствие регулирования в данной области тоже скорее соответствует интересам цифровых платформ, чем ограничивает их. Конечно, нельзя сказать, что новый Регламент ЕС по неперсональным данным является отрицанием Директивы 96/9/ЕС о правовой охране баз данных, однако совершенно точно этот Регламент учел недостатки Директивы. Свобода оборота данных сама по себе является фактором экономического роста. Отдельные ограничительные механизмы вполне возможны — они есть и в Регламенте, — но их целью должно быть не формирование легальных монополий как средства защиты (инвестиций, стабильности бизнес-процессов, технологического превосходства и т. п.), а противодействие концентрации. Иначе, как это часто бывает, цепочки данных последуют за экономическими цепочками и сконцентрируются у той компании, которая в наибольшей степени выиграет от сетевого эффекта. Следовательно, свобода оборота неперсональных данных — это не просто свобода их перемещения, но и механизм, обеспечивающий равномерность такого перемещения, равномерность доступа к ним.

Базовой гарантией здесь может стать уже упоминавшееся выше право на доступ к своим данным. Собственник высокотехнологичного оборудования должен иметь возможность доступа к данным, а в идеале — возможность переноса или даже перенаправления данных на другие платформы (например, научные платформы или в экосистемы технологических стартапов). В данной ситуации также произойдет зацепление интересов собственника оборудования и интересов исследователей и разработчиков: и те, и другие заинтересованы исследовать данные в целях повышения эффективности работы оборудования. В случае дополнения данного права механизмами создания интероперабельных форматов данных и интерфейсов обмена данными с оборудованием равномерность доступа к данным будет еще выше. Все это в совокупности будет работать против концентрации, а следовательно, обеспечивать экономический рост.

Здесь, как и при обсуждении вопроса о персональных данных, важно заметить, что достижение такого зацепления интересов необязательно находится в плоскости государственного регулирования. Важен факт осознания цифровыми платформами экономического эффекта от открытия доступа к данным: это вернется к ним алгоритмами, повышающими эффективность работы их оборудования. Важно взаимодействие разных цифровых платформ для обеспечения интероперабельности между ними. Примеры такого осознания и взаимодействия имеются, например, в сфере операционных систем и производителей сетевого оборудования и компьютерных чипов. Создание площадок для обеспечения интероперабельности, открытие данных, форматов и интерфейсов в конечном счете приводит к росту рынка и выходу его участников на смежные рынки, что, в свою очередь, позволяет пользователям получать более качественные и дешевые товары с бóльшими возможностями.

4. Трансграничный оборот персональных и неперсональных данных во время и после цифровой трансформации

Философия поствестфальского государства похожа на воздушный шар: государство с его границами и суверенитетом внутри них работает оболочкой, поддерживая внутреннее давление. Потеря границ в таком государстве окажется потерей государственности. Формирование Европейского союза в такой философии по опасности похоже на переборку тоннеля метро на больший диаметр: приходится по блокам разбирать внутренние оболочки государств и складывать из них внешнюю обделку союза, притом что замена каждого блока грозит прорывом и, как следствие, утратой и большого, и маленьких тоннелей.

Постсоветские страны живут в этом же измерении. Государственность наших стран во многом опирается на границы как барьеры для свободного перемещения людей, товаров, услуг, капиталов между ними, что позволяет оправдывать национальные правопорядки внутри государства. Достаточно поздно осознанное «пятое измерение», т. е. информационное пространство, государства пытаются огородить в той же логике. Согласно Указу Президента Республики Беларусь от 01.02.2010 № 60 «О мерах по совершенствованию использования национального сегмента сети Интернет»[41], государственные органы и организации, юридические лица и индивидуальные предприниматели обязаны использовать информационные сети, системы и ресурсы национального сегмента сети Интернет, размещенные на территории Республики Беларусь. Согласно ст. 12 Закона Республики Казахстан от 21.05.2013 № 94-V «О персональных данных и их защите»[42], хранение персональных данных осуществляется в базе, которая хранится на территории Республики Казахстан. Аналогичное положение, пусть и в более размытой формулировке, содержится в ч. 5 ст. 18 российского Закона о персональных данных. Многочисленные территориальные ограничения хранения данных содержатся и в российском Законе об информации. В частности, технические средства информационных систем, используемых государственными органами, органами местного самоуправления, государственными и муниципальными унитарными предприятиями или государственными и муниципальными учреждениями, должны размещаться на территории РФ.

Как уже отмечалось выше, по крайней мере в части неперсональных данных Евросоюз пошел по пути уменьшения количества территориальных ограничений, поскольку счел их препятствием для экономического роста. Фактически любые ограничения места хранения информации (так называемое требование о локализации) в условиях глобального Интернета лишь усугубляют положение тех организаций, которые находятся в данном государстве и вынуждены подчиниться таким требованиям. Глобальные игроки, в отношении которых требования о локализации невозможно принудительно исполнить, лишь получают конкурентное преимущество. На момент написания настоящей работы ни одна из «большой четверки» западных цифровых платформ (Google, Apple, Amazon и Facebook) не локализовала свои данные ни в одной из стран ЕАЭС, введших требования о локализации. Следовательно, любые ограничения оборота данных, в том числе требования о локализации, существующие в законодательстве государства, только ухудшают положение его собственных предпринимателей по сравнению с возможностями глобальных цифровых платформ и приводят к увеличению, а не к уменьшению концентрации.

---

[41] Национальный правовой Интернет-портал Республики Беларусь. URL: http://www.pravo.by/document/?guid=3871&p0=P31000060 (дата обращения: 01.05.2019).

[42] Информационная система «Юрист». URL: https://online.zakon.kz/Document/?doc_id=31396226 (дата обращения: 01.05.2019).

Сетевые эффекты подсказывают совершенно иной метод локализации потоков данных внутри государства или межгосударственного союза. Чем дробить одну информационную среду на множество локальных, имеющих экспоненциально меньшую ценность, лучше увеличивать интероперабельность локальных цифровых пространств. Ценность электронного документа, который можно использовать в юридически значимых целях лишь в России, согласно закону Меткалфа о зависимости ценности сети от количества ее пользователей, в четыре раза меньше, чем если бы его можно было использовать на территории всех стран ЕАЭС. Сопоставимое снижение ценности данных возникает в силу несовместимости правовых режимов отдельных видов информации (ноу-хау, банковской тайны, тайны связи, иной конфиденциальной информации) в наших странах. И напротив, выстраивание совместимых правовых режимов тайн, совместимых систем требований к защите информации не только повысит ценность соответствующих видов информации, но и увеличит «переговорный вес» евразийского цифрового пространства в отношении глобальных цифровых платформ. Таким образом, построение интероперабельной цифровой среды — это основной путь для того, чтобы заставить глобальные платформы играть по нашим правилам в наших странах.

Здесь важен еще один момент. До настоящего времени национальное законодательство наших стран — об информации, о государственных и иных информационных ресурсах, об интеллектуальной собственности — реализует статический подход к информации, ее накоплению и использованию. Субъектами отношений являются операторы персональных данных, операторы информационных систем, изготовители баз данных и иные подобные субъекты, которые, по мнению государства, собрали определенный массив данных и получают выгоду, контролируя его. Отсюда в регулировании возникает логика огораживания, как для частных, так и для государственных массивов информации. Однако цифровая трансформация предполагает иную логику. Как известно, самый большой сервис такси в мире не владеет ни одним автомобилем, самый большой сервис по предоставлению мест для проживания не владеет недвижимостью и т. д. Цифровая трансформация превращает профессионального контрагента в «точку сборки», где нужные пользователю здесь и сейчас данные превращаются в информационный продукт, актуальный на момент сборки (заказ такси, бронирование апартаментов и т. п.). Тем важнее для формирования цифровой среды вопрос интероперабельности, причем на первое место здесь выступает доступность метаданных. Метаданные, с одной стороны, дают возможность находить и упаковывать необходимые сведения в информационный продукт, с другой — не приводят к концентрации критических массивов информации у цифровых платформ. Данные остаются там, где они есть, цифровые платформы лишь управляют их сборкой под конкретный запрос. Такое построение информационной цепочки архитектурно препятствует концентрации и, следовательно, поощряет более равномерный доступ к данным, способствуя экономическому росту.

Заключение

Пока что, к сожалению, цифровая экономика выступает своего рода Воландом из романа Булгакова «Мастер и Маргарита»: с сожалением смотрит на наши законы, не желая подчиняться им — и имеет для этого все возможности, поскольку существует по собственным закономерностям высшего порядка.

Взаимодействие аналогового мира с цифровой экономикой нельзя построить с позиций силы. Эти миры, наверное, могут уничтожить друг друга, но для того,

чтобы сосуществовать, им надо договариваться на равных, без предварительных условий, согласовывая собственные свободные воли.

Свобода — ключевая характеристика цифрового измерения. Это мир, посетить который может каждый, но без привилегий или предубеждений, связанных с расовой принадлежностью, экономической или военной мощью, правом рождения[43]. «Моральный закон есть условие, единственно при котором мы можем осознать свободу... Но если не было бы свободы, то не было бы в нас и морального закона»[44]. Никакой закон, навязанный для цифровой экономики извне, не будет работать в ней эффективно. Поэтому правовое измерение цифровой экономики — это измерение интересов ее участников с целью нахождения баланса между ними и путей устранения правового неравенства, вызванного доступностью или недоступностью новых технологий. Но интерес, как известно, — это осознанная потребность[45], поэтому и правовое измерение цифровой экономики — это осознание ее акторами своих потребностей, осознание соотношения своих интересов и интересов контрагентов и добросовестное, без предубеждения и без навязывания, согласование этих интересов.

Е. В. Войниканис, приходя к схожим выводам, говорит о балансе интересов как ключевом принципе регулирования цифровой среды и неотъемлемой части новой правовой парадигмы[46]. Но такой тезис может запутать. Баланс интересов — это не компромисс и не «равномерное распределение прав и обязанностей между сторонами». Еще менее можно характеризовать баланс интересов как длительное состояние — не бывает длительных состояний у стремительно развивающейся цифровой экономики.

Использование права как социального регулятора в цифровой экономике, ее правовое измерение могут состояться, только если состоялось то самое зацепление интересов, о котором несколько раз говорилось выше. Когда, по Канту, акторы цифровой экономики осознают свою свободу как следствие морального закона в себе. Когда приватность становится конкурентным преимуществом не только бизнеса, но и правопорядка того или иного государства. Когда суверенитет государства основывается на свободе оборота данных как базисе его технологического превосходства. Когда действующие лица цифровой экономики осознают свою и чужую свободу как связанность контекстом общения.

Осознанные потребности, интересы — свои и других участников отношений — помогают развивать цифровую экономику наиболее справедливым образом, втягивая все новых субъектов в состоявшееся зацепление интересов и тем самым взаимно эффективно ограничивая интересы друг друга. Сейчас мы можем не замечать этого, но однажды зацепленные интересы продолжают работать, обеспечивая устойчивость нашего, в том числе цифрового, мира. Это правила дорожного движения, стандарты электросвязи, международные системы расчетов, механизмы шифрования трафика, в конце концов, сам Интернет как сверхустойчивая система, которую никто не может контролировать.

Статья поступила в редакцию 14 июня 2019 г.;
рекомендована в печать 20 декабря 2019 г.

---

[43] "We are creating a world that all may enter without privilege or prejudice accorded by race, economic power, military force, or station of birth" (A Declaration of the Independence of Cyberspace by John Perry Barlow. URL: https://www.eff.org/ru/cyberspace-independence (дата обращения: 01.05.2019)).

[44] *Кант И.* Критика практического разума. М.: Эксмо, 2015. С. 14.

[45] *Грибанов В. П.* Осуществление и защита гражданских прав. С. 240.

[46] *Войниканис Е. А.* Право интеллектуальной собственности... С. 554.

Digital transformation: The legal dimension*

Nikolay A. Dmitrik

For citation: Dmitrik, Nikolay A. 2019. Digital transformation: The legal dimension. *Pravovedenie* 63 (1): 28–46. https://doi.org/10.21638/spbu25.2019.102 (In Russian)

The legal dimension of digital transformation is being formed by approaches to the legal regulation of social relationships backed by the interests of its actors: states, businesses and users. The so-called information law as an amorphous institution without its own subject and method was not able to meet the challenges of digital transformation. Effective regulation should be carried out using the method of de facto possibility coinciding with the legal possibility, i. e. subjective right. The issues of personal data as the main "fuel" of the digital economy are discussed between the state and business. This leads to the exclusion of citizens from the discussion due to their lack of resources to defend their own interests. Such resources may be provided only by the introduction of instruments that guarantee responsibility to the data subject for violation of his or her rights. In the area of industrial and other non-personal data, the lack of regulation is more of a factor for the acceleration of market growth. However, there is growing inequality between parties (equipment suppliers and users) in access to data. The right to access one's own data, as well as the mechanisms of data portability between platforms, should be the tools to protect the interests of users here. Although the interests of the state in the digital sphere are related to ensuring its own sovereignty, attempts to ground certain types of data on information systems located on the territory of the state ("data localization") contradict the structure of information flows that have undergone a digital transformation. Under these conditions, regulation should take into account the formation of data sets and services online, at a certain point of assembly, which requires freedom of circulation of metadata on the basis of which the assembly is carried out. The perceived needs and interests help to develop the digital economy in the most equitable way, drawing new subjects into the state of agreed interests and, thus, effectively limiting each other's interests. Governmental regulation being less efficient should be applied as a last resort, only if legal equality cannot be achieved by the efforts of various participants or interaction of market players.

Keywords: big data, economic concentration, antitrust policy, self-regulation, personal data, interests, digital platforms, digital divide.

References

Bachilo, Illaria L., Lopatin, Vladimir N., Fedotov, Mikhail A. 2005. *Information law*. St. Petersburg, Iuridicheskii tsentr Press. (In Russian)

Bratus', Sergei N. 1950. *Subjects of civil law*. Leningrad, Gosurizdat Publ. (In Russian)

Dmitrik, Nikolay A. 2018. Limits on legal regulation in the digital age. *Informatsionnoe obshchestvo* 3: 47–58. (In Russian)

Dmitrik, Nikolay A. 2007. *Ways of exercising civil rights and executing duties with the use of the Internet.* PhD in law thesis. Moscow, Lomonosov Moscow State University. (In Russian)

Elin, Vladimir M., Zharova, Anna K. 2013. On the methodology of information law. *Pravo i gosudarstvo: teoriia i praktika* 4: 133–144. (In Russian)

Gratton, Eloïse. 2013. *Understanding Personal Information: Managing Privacy Risks*. Canada, LexisNexis.

Gribanov, Veniamin P. 2001. *Implementation and protection of civil rights*. Moscow, Statut Publ. (In Russian)

Kant, Immanuil. 2015. *Critique of Pure Reason*. Rus. ed. Moscow, EKSMO Publ. (In Russian)

* This article was prepared in accordance with the fundamental scientific research plan within the framework of state order of Lomonosov Moscow State University 2019 (part 2) (perspective direction of legal studies "Problems of digital economy", topic "Legal issues related to formation and expression of will in digital economy by natural (individuals) and artificial (AI) subjects").

Koelman, Kamiel J., Helberger, Natalie. 2000. Protection of Technological Measures. *Copyright and Electronic Commerce. Legal Aspects of Electronic Copyright Management*: 165–228. The Hague, Kluwer Law International.

Kuvyrkova, Anastasia Iu. 2010. *Exercise of exclusive intellectual and related rights.* PhD in Law thesis. Moscow, Lomonosov Moscow State University. (In Russian)

Lassal', Ferdinand. 2012. On the essence of the Constitution (speech delivered in a Berlin burgher district Assembly in 1862). *Voitovich V. Iu. Teoreticheskie osnovy sushchnosti konstitutsii: ucheb. posobie.* Izhevsk, Udmurt University Publ. (In Russian)

Maurer, Stephen M. 2005. *Across Two Worlds: Database Protection in the United States and Europe*. Available at: https://www.researchgate.net/publication/228794091_Across_Two_Worlds_Database_Protection_in_the_United_States_and_Europe (accessed: 01.05.2019).

Muskhelishvili, Nikolai L., Sergeev, Viktor M., Shreider, Iulii A. 1996. Value reflection and conflicts in a divided society. *Voprosy filosofii* 11: 24–36. (In Russian)

Nissenbaum, Helen. 2004. Privacy as contextual integrity. *Washington Law Review* 79 (3): 119–158.

Prokhorov, Aleksandr M., Konik, Leonid G. 2019. *Digital transformation: analysis, trends, world experience*. Moscow, Al'iansPrint. (In Russian)

Tsarikovskii, Andrei Iu., Ivanov, Aleksei Iu., Voinikanis, Elena A. (eds). 2018. *Antitrust regulation in the digital age*. Moscow, Higher School of Economics Publ. (In Russian)

Voinikanis, Elena A. 2013. *Intellectual property law in the digital age: a paradigm of balance and flexibility*. Moscow, Iurisprudentsiia Publ. (In Russian)

Zuckerberg, Mark. 2019. *Four Ideas to Regulate the Internet*. March 30, 2019. URL: https://newsroom.fb.com/news/2019/03/four-ideas-regulate-internet/ (accessed: 01.05.2019).

Received: June 14, 2019
Accepted: December 20, 2019

Nikolay A. Dmitrik — PhD in Law, head of laboratory for legal informatics and cybernetics, Law faculty of Lomonosov Moscow State University, 1, Leninskie Gory, 119991, Moscow, Russian Federation; dmitric@mail.ru