DOI: 10.29141/2218-5003-2023-14-5-3 **EDN:** PJSYEA
JEL Classification: O14, L52, O33

Усиление регулирования защиты персональных данных в России: экономические последствия и риски

А.А. Моросанова
Российская академия народного хозяйства и государственной службы при Президенте РФ, г. Москва, РФ

Аннотация. Колоссальные утечки персональных данных, происшедшие в последние годы во всем мире, подталкивают регуляторов к ужесточению контроля в сфере больших данных. Статья посвящена анализу изменений в регулировании указанной сферы в России с точки зрения возможных последствий для конкурентной среды и экономических показателей цифровых рынков. Методологическую основу исследования составили новая институциональная экономическая теория и элементы теорий экономики права и отраслевых рынков. Использовались методы сравнения структурных альтернатив, а также экономико-статистический анализ. Информационной базой работы послужили данные Росстата за 2021 г. Выявлено, что усиление регулирования в сфере персональных данных: 1) скажется на всех предприятиях, задействующих обработку больших данных; 2) в краткосрочном периоде снизит инновационную активность и инвестиционную привлекательность цифровых рынков; 3) негативно отразится на малых и средних предприятиях. Вместе с тем результаты статистического анализа свидетельствуют о том, что имеется возможность применения к рынкам больших данных отраслевого подхода, прежде всего «рамочного» регулирования. Выводы, сделанные в исследовании, могут быть учтены регулятором России при разработке или изменении правовых норм в области обращения больших данных для предотвращения негативных экономических последствий.

Ключевые слова: государственное регулирование; большие данные; персональные данные; рыночная концентрация; цифровизация; отраслевое регулирование.

Финансирование: Статья подготовлена в рамках выполнения научно-исследовательской работы государственного задания РАНХиГС.

Информация о статье: поступила 13 июня 2023 г.; доработана 17 июля 2023 г.; одобрена 27 июля 2023 г.

Ссылка для цитирования: Моросанова А.А. (2023). Усиление регулирования защиты персональных данных в России: экономические последствия и риски // Управленец. Т. 14, № 5. С. 29–46. DOI: 10.29141/2218-5003-2023-14-5-3. EDN: PJSYEA.

Strengthening personal data regulation in Russia: Economic implications and risks

Anastasia A. Morosanova
Russian Presidential Academy of National Economy and Public Administration (RANEPA), Moscow, Russia

Abstract. The enormous personal data breach of recent years is pushing regulators to tighten control over big data. The paper aims to analyse changes in big data regulation in Russia, and its possible effects on the competitive environment and economic performance of digital markets. New institutional economics theory, as well as some elements of law economics and industrial organization theory constitute the theoretical framework of the study. The research methods include comparison of structural alternatives and economic and statistical analysis. The empirical evidence covers 2021 data by Russia's Federal State Statistics Service (Rosstat). The results of the study demonstrate that strengthening regulation of personal data (1) will widely affect all businesses involved in big data processing in all sectors of the economy, (2) will reduce innovation activity and investment attractiveness of digital markets in the short term, (3) will have a negative impact on small and medium-sized businesses. The statistical analysis indicates that there is room for applying an industry-wide approach, primarily 'framework' regulation, to big data markets. The research findings can be used by the regulator when developing or altering big data legal standards to prevent adverse economic implications.

Keywords: state regulation; big data; personal data; market concentration; digitalization; industry regulation.

Funding: The article was prepared as part of the RANEPA state assignment research programme.

Article info: received June 13, 2023; received in revised form July 17, 2023; accepted July 27, 2023

For citation: Morosanova A.A. (2023). Strengthening personal data regulation in Russia: Economic implications and risks. *Upravlenets / The Manager*, vol. 14, no. 5, pp. 29–46. DOI: 10.29141/2218-5003-2023-14-5-3. EDN: PJSYEA.

ВВЕДЕНИЕ

Сфера больших данных (Big Data) – одна из самых динамично развивающихся в мире. Вместе с тем экономическое регулирование общественных отношений в этой сфере – не только актуальный, но и открытый вопрос как для политиков, так и для экспертов. С одной стороны, в связи с возникающими угрозами конфиденциальности, демократии и общественному благополучию существует спрос на усиление регулирования цифровых монополий, работающих с большими данными. С другой стороны, чрезмерное регулирование быстро развивающейся сферы может нанести значительный ущерб инновационной активности и снизить общественное благосостояние. Новые вызовы, связанные с санкционным давлением, изменением цепочек поставок, блокированием доступа к зарубежным технологиям и утечками персональных данных, заставляют пересматривать отношение к регулированию в цифровых отраслях.

Цель исследования – определить, как ужесточение регулирования персональных данных в России повлияет на сферу больших данных, конкурентную среду на цифровых рынках с учетом страновой специфики и возможности применения отраслевого подхода.

Понятие «большие данные» относительно новое для экономического регулирования, поэтому имеет множество определений. Вместе с тем любое из них включает два компонента – наборы данных и специфичные средства их обработки [De Mauro, Greco, Grimaldi, 2016; Favaretto, 2020]. Эта специфичность обусловлена тем, что «широко используемые» программные средства не могут справиться с массивами данных, а требуют «использования технологии масштабирования»[1]. Большинство исследователей признают, что основными отличительными характеристиками больших данных являются объем, разнообразие и скорость – volume, variety, velocity (3V) [Severo, Feredj, Romele, 2016]. Совокупность этих характеристик и определяет, какие данные могут относиться к «большим».

Принято считать, что сама по себе информация, даже персональная, является «общественным благом» – по сути, любая компания или иное лицо может собирать сведения беспрепятственно. Однако характеристики больших данных (3V) дают внешние эффекты, связанные с деятельностью агрегаторов информации: большие данные позволяют получать дополнительный прирост знания, а следовательно, приводят к положительному внешнему эффекту для самих компаний.

С одной стороны, компании стремятся увеличить свою эффективность, что выражается в увеличении объема данных (например, через расширение деятельности на смежных рынках и обмен информацией между платформами, создание экосистем, привлечение внимания пользователей посредством цифровых алгоритмов), а также «интернализации» информации (например, путем использования специфических собственных форматов данных). Подобные тенденции порождают «парадоксы эффективности» [Marciano, Nicita, Ramello, 2020], которые ослабляют два основных рыночных принципа: эффективность информации как общественного блага и свободу выбора потребителей. Именно это заставляет задуматься о необходимости некоторых регуляторных мер в сфере Big Data, особенно в наиболее чувствительной области – персональных данных.

Под персональными данными понимается «любая информация, относящаяся к прямо или косвенно определенному или определяемому на основании такой информации физическому лицу»[2]. Такой широкий подход является общепринятым: в нормативных документах разных юрисдикций не встречается закрытого списка типов персональных данных (например, в России имеются разногласия по поводу отнесения к ним IP-адреса)[3]. Считается, что нарушения обработки этих данных (особенно в случае утечки информации) могут потенциально нанести ущерб потребителю – как моральный, так и экономический.

С другой стороны, ужесточение регулирования (например, введение оборотных штрафов за нарушение обработки информации и возникновение «утечек») потенциально может сказаться на всех рынках больших данных, а также на смежных сферах, причем в негативном ключе.

В статье рассмотрены следующие вопросы: существуют ли альтернативные подходы к регулированию сферы персональных данных и каковы последствия их применения? Какие имеются предпосылки для изменения этого регулирования в России? Как усиление инфорсмента в сфере персональных данных может повлиять на экономические показатели на цифровых рынках, в частности на показатели экономической концентрации? Как контроль за персональными данными может сказаться на всем обращении больших данных и возможен ли отраслевой подход к их регулированию в России?

ПОДХОДЫ К РЕГУЛИРОВАНИЮ СФЕРЫ БОЛЬШИХ ДАННЫХ С ТОЧКИ ЗРЕНИЯ БЛАГОСОСТОЯНИЯ ПОТРЕБИТЕЛЯ

Самой уязвимой стороной в отношениях по поводу больших данных являются пользователи – «носители»

[1] ГОСТ Р ИСО/МЭК 20546-2021 «Информационные технологии. Большие данные. Обзор и словарь». https://docs.cntd.ru/document/1200180276.

[2] ГОСТ Р 59407-2021 «Базовая архитектура защиты персональных данных». https://docs.cntd.ru/document/1200179663.

[3] Например, в постановлении Тринадцатого арбитражного апелляционного суда от 01.06.2015 № 13АП-10709/2015 ни статический, ни динамический IP-адрес не признаны персональными данными.

персональной информации. Они не могут с уверенностью знать, как и кем используются предоставленные ими сведения. Основное регулирование в рассматриваемой сфере во всех юрисдикциях сосредоточено на защите персональных данных от потенциально вредного применения. Со стороны агрегаторов тоже имеются определенные «уязвимости», связанные со сложностью определения персональных данных. Так, часть их может являться персональными, а часть – иными характеристиками, но в совокупности все они будут считаться относящимися к пользователю. Более того, Big Data и вовсе могут не относиться к персональным, но использование метода системных отпечатков (system fingerprints) [Hupperich et al., 2018] позволяет определять «характеристики пользователей путем идентификации уникальных атрибутов системы» [Шаститко и др., 2020, с. 12] (например, IP-адрес), что еще больше размывает границы между персональными и неперсональными данными.

В литературе выделяются три различные точки зрения относительно степени и необходимости вмешательства регулятора в эту сферу в зависимости от того, какие поведенческие предпосылки закладываются при осуществлении потребительского выбора, и относительно ценности информации (табл. 1).

Рассмотрим эти подходы подробнее.

Рыночный подход. В данном случае конфиденциальность информации и защита персональных данных являются рациональным выбором индивидов и вопросом субъективных предпочтений. Индивид рационально выбирает степень защиты своих данных и ресурсы, посредством которых он может предоставлять ту или иную информацию. Поэтому такие отношения должны оставаться между потребителем и поставщиком товаров/услуг. Некоторые экономисты подчеркивают, что есть только «небольшая группа потребителей, чувствительных к конфиденциальности» [Haucap, 2019, p. 4], и лишь они могут пострадать в случаях утечек и иных нарушений.

Так как речь идет о рациональном выборе, а рынок может удовлетворять любые запросы о желаемом уровне безопасности, то защита персональной информации не попадает под цели антимонопольного регулирования. Потребительское благосостояние трактуется исключительно с точки зрения эффективности рынка, то есть не предполагает необходимости защиты информации. Несмотря на достаточно сильную теоретичность, данный подход учитывается в аргументации при принятии управленческих и судебных решений, например в США.

Если потребители ценят сохранность своих данных, то это породит спрос на сервисы, обеспечивающие высокую степень защиты или полную конфиденциальность. Однако подобное поведение не наблюдается повсеместно, что получило название «парадокс конфиденциальности» (privacy paradox) [Marthews, Tucker, 2019]: участники опросов выражают обеспокоенность насчет конфиденциальности своих данных, но это расходится с выявленными реальными предпочтениями. Например, в поисковой системе DuckDuckGo, которая не собирает персональные данные, не происходило расширения аудитории при значимых информационных поводах (например, при введении компанией Google новой политики по увеличению категорий собираемых данных или раскрытии информации о том, что эти данные на цифровых коммерческих платформах используются государственными органами США для слежения за населением). По мнению некоторых экономистов, это свидетельствует о том, что реальный спрос на безопасность персональных данных завышен [Athey, Catalini, Tucker, 2017].

«Парадокс конфиденциальности» не будет парадоксом, если учитывать иные факторы влияния на поведение потребителей – асимметрию информации, неравенство в переговорной силе, отсутствие видимых рыночных альтернатив (об этом подробнее будет сказано далее).

Вместе с тем в России запрос на анонимность, конфиденциальность и сохранность данных имеет свою специфику. С 2022 г. резко возросло число пользователей VPN-сервисов[1], прежде всего из-за стремления получить доступ к ушедшим с российского рынка социальным сетям и сервисам [Мороса-

[1] По количеству загрузок VPN-приложений в 2022 г. Россия вышла на третье место в мире (см.: Global VPN Adoption Index. https://atlasvpn.com/vpn-adoption-index).

Таблица 1 – Подходы к регулированию сферы персональных данных
Table 1 – Approaches to personal data regulation

Подход	Предпосылки	Цена информации	Роль регулятора
Рыночный	Рациональное поведение	Справедливая	Регулирование не нужно
Информационный	Ограниченно рациональное поведение, асимметрия информации, разница в переговорной силе	Компании «платят» потребителю неполную цену за информацию	Помощь в раскрытии информации для потребителей. Норма о «переносимости данных»
Регуляторный	Ограниченно рациональное поведение, асимметрия информации (потребитель практически не осведомлен ни о качестве, ни о цене), разница в переговорной силе, ограниченность выбора со стороны потребителей	Цену информации невозможно измерить, особенно отдельно для каждого индивида	Необходим контроль за действиями, потенциально наносящими вред благосостоянию потребителей

нова, 2022]. Сервисы VPN, подменяя IP-адрес, дают пользователю анонимность, а в какой-то степени и защиту персональных данных, так как их затруднительно идентифицировать. При этом речь идет именно о сокрытии информации от государственных органов, а не от коммерческих цифровых платформ и самих VPN-сервисов, для которых передаваемые данные являются открытыми (однако отдельный вопрос здесь – насколько эту открытость осознают пользователи).

Роскомнадзор блокирует доступ к VPN-сервисам, не соблюдающим российское законодательство, прежде всего обязательство хранить персональные данные граждан РФ на серверах внутри страны (а это, по сути, противоречит основному функционалу VPN – предоставлению места на зарубежном сервере). Поэтому «парадокс конфиденциальности» в случае России звучит так: пользователи предпочитают небезопасное с точки зрения государства хранение своих данных в угоду избирательной конфиденциальности, анонимности по отношению к государственным органам и доступу к заблокированным сервисам.

Информационный подход. Согласно данному подходу потребители делают ограниченно рациональный выбор, решая, с какими компаниями можно контактировать, а с какими не стоит. В этом его отличие от рыночного подхода, где выбор осуществляется полностью информированными людьми [Kemp, 2020]. Между потребителями и компаниями существует асимметрия информации: первые не в полной мере осведомлены о ценности своих данных и качестве их защиты, а также не обладают переговорной силой (например, не вправе изменять условия договора, пользовательского соглашения или вынуждены принимать настройки cookies). У информации о каждом клиенте есть цена, которую он готов заплатить за бесплатный доступ к сервисам или повышение качества предоставляемых услуг. Однако существует вероятность, что потребителю «не доплачивают» – компании не возмещают истинную стоимость персональной информации. Здесь кроется первая причина критики «парадокса конфиденциальности»: если пользователь не осведомлен об истинных характеристиках благ, то свой выбор он будет осуществлять на основе других «видимых» характеристик трансакции, предположительно на основе соотношения выгод (объема и качества услуг, популярности сервиса и пр.) и издержек (экономии сил и времени).

Регулятор должен продумывать меры, которые помогут лучше ориентироваться на рынке, в частности помощь в распространении информации о том, какие компании и в каком объеме собирают и используют персональные данные, каким компаниям передают информацию. Еще одним примером необходимого регулирования в рамках данного подхода является внедрение нормы о «переносимости данных» – предоставление пользователю возможности по собственному желанию перенести данные с одного цифрового сервиса на другой. Такая норма была внедрена в Евросоюзе в рамках Общего регламента по защите данных (General Data Protection Regulation (GDPR))[1], в России подобного права нет.

Однако и этот подход имеет определенные сложности реализации. Прежде всего, даже полностью раскрытая информация о способах использования больших данных может быть слишком сложной в качестве основы для принятия решения потребителем, может быть не понята им или неверно истолкована. Также существуют трудности с измерением уровней обеспечиваемых каким-либо сервисом безопасности и сохранности данных. Пользователям, как и регулятору, сложно судить, какой из сервисов действительно заботится о правомерном использовании данных, а какой может пренебрегать некоторыми правилами. Более того, соблюдение даже высокого уровня защиты не всегда способно уберечь от целенаправленных вредительских действий (как атаки со стороны, так и действий собственных сотрудников), а также от технических и человеческих ошибок.

Стоит отметить, что сложность измерения уровня защиты информации может сказаться и на оценке результативности регулирования в этой сфере. Например, введение Реестра учета инцидентов в области персональных данных[2] в 2023 г. само по себе увеличит число зарегистрированных случаев утечек, но будет ли это означать, что компании ослабили защиту информации? Вероятнее всего, нет. Экономисты признают сложность измерения успешности политики по кибербезопасности [Marthews, Tucker, 2019], поэтому вопрос выбора критериев оценки является отдельным вопросом в рамках разработки и инфорсмента данных мер.

В соответствии с этим подходом регулятору рекомендовалось внедрять «механизм компенсации “истинной” ценности персональной информации» [Acquisti, Taylor, Wagman, 2016]. Но предположение о том, что такой механизм в принципе возможен, подвергается критике, что приводит к формулированию следующего подхода.

Регуляторный подход. Сбор и использование персональных данных – это не столько уплачиваемая потребителями цена, «сколько объективная стоимость, возлагаемая на потребителей в процессе цифровых транзакций» [Kemp, 2020, p. 632]. Самая главная проблема, которая накладывает отпечаток на благосостояние потребителей, – это то, что вся информация об использовании персональных данных представля-

[1] General Data Protection Regulation: Right to data portability. Art. 20. https://gdpr-info.eu/art-20-gdpr/.

[2] Согласно ч. 10 ст. 23 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» для учета информации об инцидентах, поименованных в ч. 3.1 ст. 21 этого закона, Роскомнадзор будет вести реестр учета инцидентов в области персональных данных.

ет собой «черный ящик» – у потребителей нет совершенно никаких сведений о том, какой доход приносит компании каждое дополнительное «знание». Еще один эффект заключается в том, что ценность представляют именно агрегированные, массовые данные, к которым можно применить методы анализа информации, поэтому практически невозможно рассчитать «индивидуальную» цену информации.

Если следовать подходу экономического анализа права [Shavell, 2004], то можно получить следующий парадокс: утечка большого количества персональных данных будет общественно эффективным деянием, так как ценность агрегированных данных для любого нового владельца окажется выше суммарных потерь каждого индивида. Но не стоит забывать, что, во-первых, не все персональные данные являются «большими», а во-вторых, любая персональная информация потенциально может быть использована злоумышленниками для иных целей. Это объясняет отсутствие четкого механизма возмещения ущерба тем пользователям, чьи сведения были скомпрометированы (вне зависимости от того, входили ли они в массив «больших данных» или были «отдельными»). На сегодняшний момент бремя доказательства ущерба лежит на самом потребителе в рамках индивидуального или коллективного иска: нужно предоставить явные подтверждения того, что факт утечки принес какие-либо издержки.

«Парадокс конфиденциальности» не является парадоксом и по второй причине (первая рассмотрена выше), которая кроется в структуре и функционировании цифровых рынков, прежде всего в наличии цифровых платформ и экосистем. Действующие на этих платформах косвенные сетевые эффекты могут сильно влиять на выбор потребителя и даже выступать «блокирующим» фактором. Указанный выбор не основывается на качестве предлагаемой защиты данных, а зачастую связан с тем, что потребитель не видит иных альтернатив. Простота переноса личных данных с одного сервиса на другой в рамках одной экосистемы также подталкивает к определенному выбору, в то время как механизм использования этих данных экосистемой остается для пользователей полной тайной. Помимо прямого вреда для их благосостояния методы сокрытия сведений компаниями могут серьезно препятствовать конкуренции.

Отправной точкой для введения регулирования ex ante сферы больших данных во многих странах является защита персональных данных. Экономическое регулирование всех типов больших данных – фронтир для регуляторов во всех юрисдикциях. Но, несмотря на чувствительность персональных данных, видна разница в практических подходах: например, в США нет каких-либо общих норм по контролю за этой сферой, имеются лишь отдельные отраслевые стандарты. В России наблюдается стремление к усилению инфорсмента по защите персональных данных (стремление к регуляторному подходу), но должным образом не задействованы механизмы подхода информационного. Регуляторный подход имеет свои преимущества в достижении информационной безопасности, однако не лишен рисков, связанных с негативными экономическими последствиями.

УСИЛЕНИЕ РЕГУЛИРОВАНИЯ СФЕРЫ ПЕРСОНАЛЬНЫХ ДАННЫХ В РОССИИ

В 2022 г. в России произошли колоссальные утечки персональных данных: согласно исследованию «Лаборатории Касперского»[1], всего за прошлый год зафиксировано 168 фактов утечек, содержащих 290 млн пользовательских данных. 64 % от всего их объема «утекли» в результате кибератак на крупные для своих сфер бизнесы: «Яндекс.Еда», СДЭК, «Ростелеком», «Билайн» и «Теле2», «Гемотест» и др.[2]

Основное регулирование сферы обращения данных в России происходит на основании федерального закона «О персональных данных»[3]. На сегодня в нормативных актах нет такого понятия, как «утечка персональных данных». Действия (а вернее бездействие) компании, у которой были украдены такие данные, рассматриваются в соответствии с ч. 1 ст. 13.11 КоАП РФ «Обработка персональных данных в случаях, не предусмотренных законодательством Российской Федерации в области персональных данных, либо обработка персональных данных, несовместимая с целями сбора персональных данных…». Максимальный штраф за нарушение этих норм составляет 100 тыс. руб. для юридических лиц (за повторное нарушение – 500 тыс. руб.). В частности, за одну из самых масштабных утечек персональных данных «Яндекс.Еду» оштрафовали на 60 000 руб.[4]

Получается, что компанию, скомпрометировавшую свои данные, привлекают к ответственности за «недопустимую обработку» данных, а не за необеспечение кибербезопасности (при этом ч. 6 ст. 13.11 КоАП РФ оговаривает соблюдение некоторых условий по сохранности данных, но «без использования средств автоматизации», а подобных требований для «цифровых средств» в законодательстве нет). Важно подчеркнуть, что здесь действует «правило небрежности» – несмотря на то, что утечки информации зачастую случаются из-за намеренных действий

[1] Значимые утечки данных: аналитический отчет (2023) // Лаборатория Касперского. https://go.kaspersky.com/ru-data-leakage-report-2022.

[2] Курашева А. (2023). Путин поручил разобраться с оборотными штрафами за утечки данных к июлю // Ведомости. 13 января. https://www.vedomosti.ru/technology/articles/2023/01/13/959007-putin-oborotnimi-shtrafami.

[3] О персональных данных: федеральный закон от 27.07.2006 № 152-ФЗ.

[4] Фадеичев С. (2022). Суд оштрафовал «Яндекс.Еду» на 60 тыс. рублей из-за утечки данных // ТАСС. https://tass.ru/proisshestviya/14435979.

некой третьей стороны («взлома» и подобных действий), наказание несет компания, которая не обеспечила сохранность данных (а в законодательстве никак не установлены даже минимальные требования по ее обеспечению). Кроме того, как уже подчеркивалось, отсутствует механизм компенсаций для самих потребителей – взысканные штрафы не идут на оплату ущерба пострадавшим пользователям.

Нельзя не обратить внимание на тот факт, что даже максимальный штраф, который может получить компания за данное нарушение, является мизерной суммой для крупных участников рынка (а именно они ответственны за большую часть скомпрометированных данных). В то же время затраты на обеспечение кибербезопасности для малых и средних предприятий составляют 38 тыс. долл, а для крупных – 375 тыс. долл. в год[1]. Такое несоответствие создает смещенные стимулы для компаний: экономической выгоды от обеспечения защиты информации попросту нет, механизм репутации здесь работает лишь отчасти из-за высокой рыночной власти цифровых компаний и «парадокса конфиденциальности». Последнее явление (не относящееся, по сути, к парадоксам) присутствует на рынке: пользователей не смущают утечки информации по ряду рассмотренных причин и/или в силу отсутствия альтернатив, и они продолжают обращаться к привычным сервисам.

В России информация об «утечке» персональных данных из двух крупных платформ – «Яндекс. Лавки» и СДЭК – не повлияла на их финансовые показатели и объем аудитории. Об этом косвенно можно судить по возрастающему тренду товарооборота по всем сервисам электронной коммерции «Яндекса» (рис. 1) и числу пользователей «Яндекс.Маркета», входящего в единую экосистему (рис. 2) (чертами на обоих рисунках помечены даты появления информации об утечках).

У компании СДЭК наблюдались две крупные утечки информации в 2022 г., но число запросов «СДЭК отслеживание»[2], в отличие от запроса «Почта России отслеживание», даже возросло после объявления о незаконном доступе к персональным данным в сети (рис. 3).

Приведенные примеры лишь частично иллюстрируют данный феномен, но показывают устойчивость

[1] См.: В следующие три года российские компании планируют увеличить бюджет на кибербезопасность на 14 % // Лаборатория Касперского. https://www.kaspersky.ru/about/press-releases/2023_v-sleduyushie-tri-goda-rossijskie-kompanii-planiruyut-uvelichit-byudzhet-na-kiberbezopasnost-na-14.

[2] Запрос «СДЭК отслеживание» является вторым по популярности после запроса «СДЭК» и позволяет определить тех, кто воспользовался сервисом, а не инфоповодом об утечке персональных данных.

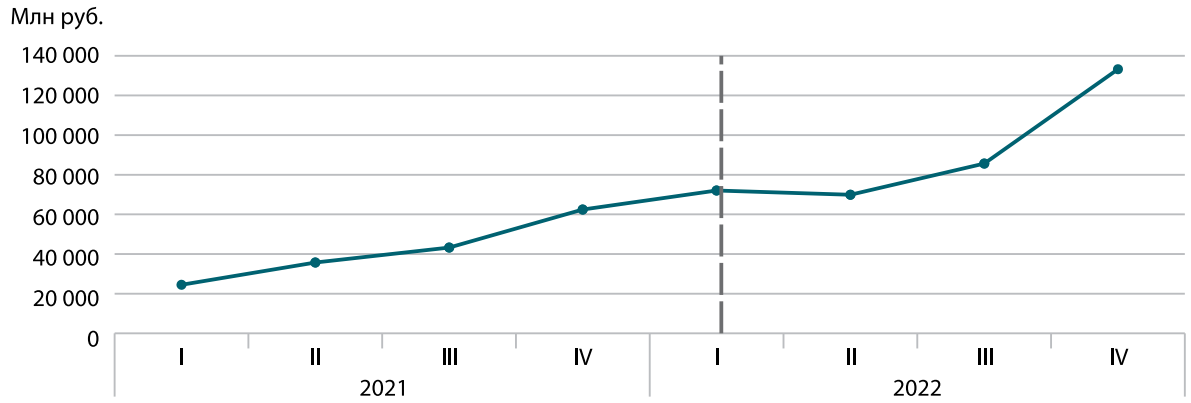

Рис. 1. Товарооборот сервисов электронной коммерции «Яндекса» в ценах I квартала 2021 г., 2021– 2022[1]

Turnover of Yandex e-commerce services (GMV) in Q1 2021 prices, 2021–2022

[1] Рис. 1, 2 составлены по: Финансовые результаты ООО «Яндекс». https://ir.yandex.ru/financial-releases.

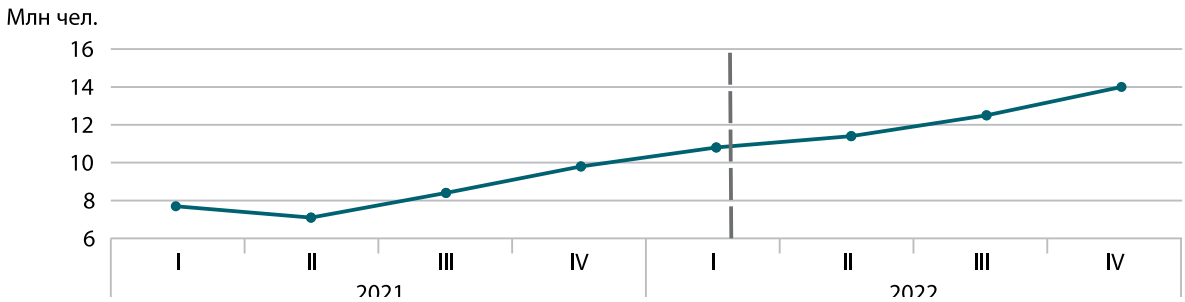

Рис. 2. Количество активных покупателей на «Яндекс Маркете», 2021– 2022

Fig. 2. Number of active buyers on Yandex.Market, 2021–2022

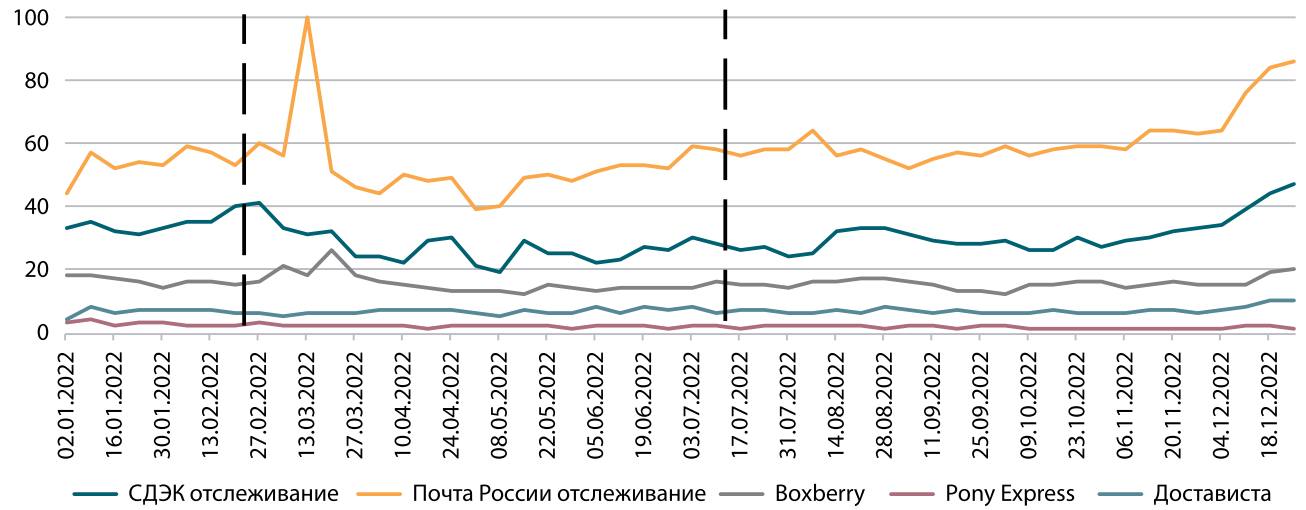

Рис. 3. Индексы популярности поисковых запросов крупных сервисов доставок в РФ за 2022 г.[1]

Fig. 3. Popularity indices of search queries for large delivery services in Russia, 2022

потребительских предпочтений. Возможно, даже новые, только пришедшие на платформы пользователи полагают, что «второй раз это не повторится», хотя делают это, как показывает практика, напрасно (так, «утечки» с сервиса СДЭК случались неоднократно).

Смещенные стимулы компаний по обеспечению защиты информации были замечены регулятором. Роскомнадзор с 1 марта 2023 г. изменил порядок уведомлений об утечках и составил Реестр учета инцидентов в области персональных данных с возможной передачей данных в ФСБ, а Минцифры разрабатывает проект закона, согласно которому должны быть введены оборотные штрафы (от 1 до 3 % годового оборота) за повторное нарушение ФЗ «О персональных данных» (в зависимости от объема и значимости этих данных) и фиксированный штраф за первичное нарушение (но «вилка» суммы штрафа будет увеличена). На данный момент неясно, по каким критериям будет оцениваться значимость утекших данных и кто будет осуществлять «маркировку», так как законопроект находится на стадии разработки и публично не обсуждался.

Можно наблюдать, что исходной точкой в ужесточении регулирования в сфере больших (персональных) данных является защита информации с точки зрения потребителя, что теоретически должно повысить его благосостояние. Сложность определения индивидуальной ценности информации со стороны третьих лиц не позволяет рассчитать наносимый ущерб (и сопоставить предельный ущерб и предельный размер наказания). Это объясняет, почему в рассматриваемой сфере целесообразно вводить регулирование персональных данных согласно «правилу собственности» (как, например, GDPR), а не «правилу ответственности» (но именно этот подход свойствен России).

Однако, как будет подробнее рассмотрено далее на опыте Евросоюза, применение жестких мер предосторожности способно неблагоприятно повлиять на структуру рынков, а это, в свою очередь, тоже может сказаться на благосостоянии потребителей, но уже негативно.

[1] Источник: Google.Trends.

ВЛИЯНИЕ GDPR НА РЫНОЧНУЮ КОНЦЕНТРАЦИЮ

Опыт Евросоюза, который в 2018 г. внедрил GDPR, свидетельствует о том, что в краткосрочной и среднесрочной перспективе усиление регулирования в сфере больших данных приводит к негативным экономическим последствиям. В частности, согласно результатам изучения влияния на инновации количество сделок относительно венчурных инвестиций B2C упало на 17,6 %, а B2B – на 10,8 % [Jia, Ginger, Wagman, 2019]. Изменился и их характер – инновации стали преимущественно адаптивными, уменьшилось число прорывных [Blind, Niebel, Rammer, 2022], произошел частичный отказ от сделок на уровне стартапов [Martin et al., 2019].

В период 2018–2020 гг. снизились доходы не только в области электронной коммерции (на 13,3 %) [Goldberg, Johnson, Shriver, 2021], но и в иных отраслях: компании, попавшие под регулирование, испытали снижение прибыли на 8 % и снижение продаж на 2 % (исключением являются крупные технологические компании) [Godinho de Matos, Adjerid, 2019; Arcuri, 2020; Chen, Frey, Presidente, 2022]. В целом влияние GDPR на показатели компаний зависит, прежде всего, от их готовности к соответствующим мерам, которая является важным конкурентным преимуществом[2]. При этом GDPR сказался не только на европейских рынках, но и рынках вне ЕС: есть мнение, что этот закон послужил более существенным ограничивающим фактором в цифровых отраслях США, чем внутреннее законодательство страны [Koski, Valmari, 2020].

[2] Cisco. Maximizing the value of your data privacy investments. https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/dpbs-2019.pdf.

Особого внимания в контексте данной работы требуют исследования, посвященные влиянию GDPR на уровень концентрации в различных отраслях. Большинство исследователей данной области сходятся во мнении, что введенный нормативный акт повысил уровень концентрации на цифровых рынках (прежде всего рынках рекламы, аналитики и социальных сетей [Johnson, Shriver, Goldberg, 2022], а также веб-технологий [Peukert et al., 2022]), так как он негативно сказался на малых и средних компаниях [Kemp, 2020; Zhuo et al., 2020; Geradin, Karanikioti, Katsifis, 2021].

Можно выделить следующие причины, по которым крупные компании если не выиграли, то смогли после введения GDPR минимизировать потери эффективнее, чем малые и средние компании [Geradin, Karanikioti, Katsifis, 2021]:

- затраты на внедрение защиты создают дополнительные барьеры для входа (или даже приводят к выходу некоторых компаний). Для крупных компаний-платформ работает эффект масштаба – удельный вес издержек от необходимости внедрения защиты меньше, чем у «нишевых», небольших компаний;
- доверие на рынке возрастает к крупным платформам, поскольку действует «эффект бренда» – убеждение, что крупные компании могут позволить услуги лучших специалистов и закупку/разработку качественного программного обеспечения, поэтому они являются «надежными» контрагентами для работы с большими данными. В целом репутационные и экономические риски действительно подталкивают крупные фирмы к обеспечению высокого уровня зашиты, но обратное не является верным: мелкие и средние предприятия могут разработать или использовать средства, также обеспечивающие надежную кибербезопасность;
- крупным платформам проще получить согласие пользователя. Эта ситуация схожа с описанной в предыдущем пункте, но со стороны потребителя, и особенно заметна для экосистем: пользователь, предоставив данные единожды, приобретает возможность доступа к множеству сервисов, предоставляемых компанией;
- крупные платформы неохотно делятся данными из-за возросших рисков. Вследствие невозможности качественно измерить уровень технической защиты данных они отказывают в доступе к ним сторонним предприятиям, так как это действие может повлечь юридическую и экономическую ответственность.

Особо стоит подчеркнуть, что эффекты от усиления регулирования не являются схожими в разных отраслях экономики [Adjerid et al., 2016]. Степень, в которой личная информация должна быть защищена или раскрыта, чтобы максимизировать индивидуальное или общественное благосостояние, не является универсальной: «оптимальный баланс конфиденциальности и раскрытия информации очень сильно зависит от контекста и меняется от сценария к сценарию» [Acquisti, Taylor, Wagman, 2016, p. 484].

Введение оборотных штрафов за утечку персональных данных в России несопоставимо по масштабу с изменениями, обусловленными внедрением GDPR в Европе. Однако изменения в законодательстве, связанные с требованием о внесении факта утечек в реестр, а также ожидаемой величины штрафа (в любом выражении – в абсолютном за первое нарушение или в относительном за повторное), вносят корректировку в стимулы компаний по соблюдению норм кибербезопасности. По сути, регулятор меняет две характеристики, влияющие на ожидаемую полезность правонарушителя (согласно экономической теории права Г. Беккера [Becker, 1968]), увеличивая вероятность наказания и ответственность за правонарушение (и для игроков, которым не свойствен риск, первый фактор оказывается важнее).

Однако стоит указать, что здесь в расчет не берутся два существенных аспекта: 1) смещение стимулов к усилению кибербезопасности сопряжено с большими издержками по ее соблюдению (особенно для малых предприятий), а именно это согласно опыту ЕС и приводит к негативным экономическим эффектам; 2) подобные меры не оказывают никакого воздействия на самих киберпреступников, поэтому частота попыток взлома (в том числе успешных) может оказаться даже выше, несмотря на все усилия компаний-агрегаторов по сохранности данных и поиску надежных контрагентов.

Согласно исследованию VK Cloud[1], около 69 % компаний в России привлекают сторонних специалистов для работы с большими данными. По информации Росстата, доля внутренних сотрудников, задействованных для анализа этих данных, несколько больше – от 42 до 68 % в зависимости от отрасли[2] (рис. 4), но тем не менее каждая из отраслей активно использует аутсорсинг для этих целей.

Более того, ФЗ «О персональных данных» имеет ряд недостатков, которые могут искажать поведение экономических субъектов. В частности, подчеркивается, что размытость определения понятия «оператор персональных данных» позволяет достаточно широко его трактовать [Ючинсон, 2017], и это может привести к чрезмерным наказаниям или наказаниям невиновных (по сути – ошибкам I рода с точки зрения регулятора) [Polinsky, Shavell, 1989; Шаститко, 2011]. С точки зрения самих компаний существуют стимулы к «перестраховке» – к излишним издержкам, вызванным сбо-

[1] Arenadata (2022). Технологии для работы с Big Data: готовность к использованию и основные барьеры // VK Cloud. https://mcs.mail.ru/promopage/bigdata-issledovanie/?utm_source=habr.

[2] Сведения об использовании информационных и коммуникационных технологий и производстве вычислительной техники, программного обеспечения и оказания услуг в этих сферах (итоги статнаблюдения по ф. № 3-информ) (2021) // Росстат. https://rosstat.gov.ru/statistics/science.

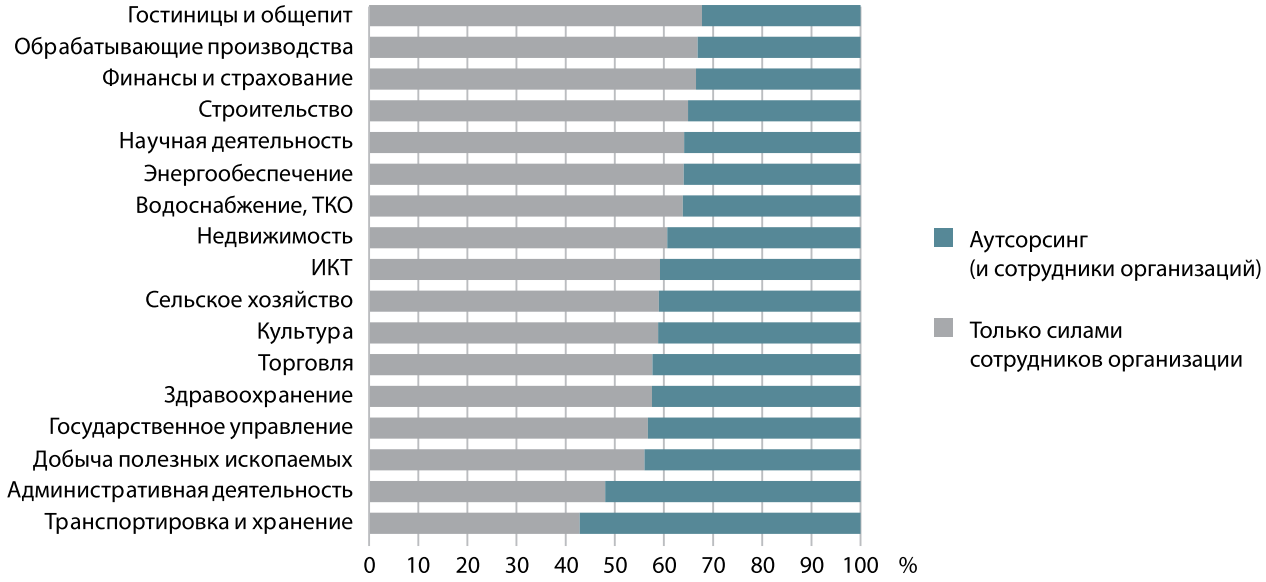

Рис. 4. Анализ больших данных в отраслях России за 2021 г.[1]

Fig. 4. Big data analysis in Russia's industries, 2021

ром и хранением данных, например связанным с файлами cookies. Учитывая эти недостатки, можно заключить, что меры по увеличению ответственности за сохранность данных способны привести к экономическим эффектам, подобным тем, с которыми столкнулся ЕС: надежными вариантами для контрактации оказываются уже действующие крупные цифровые платформы, что не дает потенциальным конкурентам возможности функционировать на рынке.

Усилить негативное влияние на экономическую концентрацию могут и ограничительные меры, связанные с санкциями. На рынке цифровой рекламы в России до 2022 г. наблюдалась активная конкуренция между зарубежными (на базе цифрового инвентаря компаний Meta и Google) и отечественными интернет-платформами. Отсутствие конкуренции «извне»[2] и предлагаемые законодательные меры способны привести к усилению экономической власти крупных российских экосистем, таких как «Яндекс», VK, «Сбер», не только на рынке рекламы, но и в смежных отраслях.

Результаты исследований о том, как влияет усиление регулирования сферы больших данных на конкуренцию, показывают, что регулятору следует принимать во внимание повышенную уязвимость малых и средних предприятий (в части их затрат на внедрение мер по защите), что должно отражаться в особом подходе к ним. Необходимо подчеркнуть – GDPR предусматривает наличие только оборотных штрафов, что предполагает соразмерность наказания величине компании.

Однако даже это приводит к разным последствиям для малых и крупных компаний (вероятно, из-за более эффективной адаптации крупного бизнеса к новым правилам). В России же предусматривается как усиление фиксированных штрафов (не зависящих от размеров компаний), так и введение штрафов оборотных, что привносит дополнительные риски для малых предприятий. Не менее важно, что значение и степень влияния больших данных отличаются в различных секторах экономики – это означает практическую невозможность применения единого универсального подхода к регулированию. Также при разработке нормативных документов необходимо учитывать, что в цифровой экономике требуется иной подход – на уровне мезоинститутов [Шаститко, 2019] (которыми являются экосистемы), так как «на уровне институциональной среды (макроинститутов) нельзя обеспечить необходимую детализацию правил, а также сохранить высокую степень адаптации к внешним шокам» [Шаститко, Курдин, Филиппова, 2023, с. 80].

ОТРАСЛЕВАЯ СПЕЦИФИКА БОЛЬШИХ ДАННЫХ

В 2020 г. примерный объем рынка больших данных в России составил 45 млрд руб.[3] В этот рынок были включены только «внешние» решения (то есть обращающиеся между компаниями) из следующих категорий: 1) вертикальные решения и услуги (например, решение по управлению грузоперевозками от «Мегафона»); 2) технологические инструменты (например, инструмент распознавания изображений Yandex Vision); 3) цифровая инфраструктура (платформа поддержки

[1] Сведения об использовании информационных и коммуникационных технологий и производстве вычислительной техники, программного обеспечения и оказания услуг в этих сферах (итоги статнаблюдения по ф. № 3-информ). (2021). // Росстат. https://rosstat.gov.ru/statistics/science.

[2] Игнатьев Д., Истомина М. (2023). Российский рекламный рынок в 2022 году снизился на 2 % // Ведомости. 27 марта. https://www.vedomosti.ru/media/articles/2023/03/27/968172-rossiiskii-reklamnii-rinok-v-2022-godu-upal.

[3] Ассоциация больших данных (2020). Стратегия развития рынка больших данных до 2024 года. https://rubda.ru/wp-content/uploads/2020/03/strategiya-bolshih-dannyh_srednyaya.pdf.

Интернета вещей от «Сбербанка»). В определение рынка не вошли элементы базовой инфраструктуры (например, серверы), так как они могут использоваться многопрофильно, и полностью «внутренние решения» компаний по обработке больших данных, поскольку они являются внутренним ресурсом.

В России нет нормативных правовых актов, регулирующих всю сферу больших данных, но в настоящее время происходит «закладывание основ» через принятие и адаптацию ГОСТов. Можно сказать, что ГОСТы выступают в качестве «рамочного регулирования», внося конкретику и обеспечивая единообразие при взаимодействии игроков рынка по поводу Big Data.

За 2020–2023 гг. было принято пять ГОСТов, четыре из которых являются переводами международных стандартов (табл. 2). Последний принятый ГОСТ 70466-2022 вызвал критику, связанную с тем, что его содержание достаточно общо и размыто и не содержит секторальных или страновых спецификаций[1].

Это свидетельствует о необходимости более адаптационного подхода к принятию нормативных документов в сфере больших данных (и всей цифровой экономики), что согласуется с главными выводами экономистов относительно проблем трансплантации институтов и мезоинститутов. Результаты такой трансплантации (в нашем случае – регулирование сферы больших данных) связаны с взаимодействием трех факторов: социокультурных характеристик (например, отношение к своим персональным данным), начальных институциональных и макроэкономических условий (наличие в стране своих крупных цифровых платформ, экосистем и пр.) и выбора технологий трансплантации (например, полное заимствование международных стандартов или частичная их адаптация) [Полтерович, 2001; Полтерович, 2006].

[1] Шпунт Я. (2022). ИИ прирастает стандартами // Comnews. 20 декабря. https://www.comnews.ru/content/223600/2022-12-20/2022-w51/ii-prirastaet-standartami.

В том, что для введения рамочного отраслевого регулирования имеется задел, можно убедиться, посмотрев на структуру больших данных по сферам экономической деятельности: какие источники используют компании и для каких целей. Согласно такому подходу, если есть принципиальные и устойчивые различия в способах использования больших данных между отраслями, значит, есть отличия и в условиях контрактации между участниками в рамках этой отрасли, а также в отношениях с государством.

На основе официальной статистики Росстата за 2021 г. можно составить структуру используемых больших данных по целям и источникам в разрезе отраслей. С учетом этих сведений проведен корреляционный анализ распределения доли предприятий, использующих данные из восьми источников[2] на четыре цели[3] в каждой из рассматриваемых отраслей. Корреляционная матрица приведена в приложении. Выявленные группы экономических сфер обладают специфическими характеристиками по использованию больших данных (табл. 3)[4].

[2] Категории источников больших данных, которые выделяет Росстат: 1) данные, передаваемые между различным оборудованием, считываемые с цифровых датчиков или радиочастотных меток и др.; 2) данные учетных систем предприятия, таких как ERP, CRM, SCM, HRIS и аналогичные; 3) данные геолокации, получаемые в том числе с использованием портативных устройств; 4) данные веб-сайта организации; 5) данные операторов сотовой связи; 6) данные, полученные из социальных сетей; 7) дистанционное зондирование Земли; 8) иные данные.

[3] Основные цели использования больших данных, которые выделяет Росстат: 1) для продаж и маркетинга; 2) для производственного процесса; 3) для обеспечения безопасности; 4) для других целей.

[4] Группы формировались на основании коэффициента корреляции (не менее 0,97). Внутри групп все корреляции значимы на уровне 1 %. Группы 1a и 1b выделены из-за наличия незначимых корреляций, но в целом все отрасли из групп 1, 1a, 1b имеют схожую направленность. Различия подтверждаются отсутствием значимых корреляций (при p-value > 0,15).

Таблица 2 – Перечень ГОСТов по тематике больших данных в России, 2021–2023
Table 2 – Russia's national standards (GOSTs) in big data, 2021–2023

Год	ГОСТ	ISO	Примечание
2021	ГОСТ Р ИСО/МЭК 20546-2021 «Информационные технологии. Большие данные. Обзор и словарь»	ISO/IEC 20546:2019	–
2022	ГОСТ Р 59926-2021 «Информационные технологии. Эталонная архитектура больших данных. Часть 2. Варианты использования и производные требования»	ISO/IEC TR 20547-2	–
2022	ГОСТ Р 59925-2021 «Информационные технологии. Большие данные. Техническое задание. Требования к содержанию и оформлению»	Самостоятельно разработан	Отдельный раздел посвящен госзакупкам
2023	ГОСТ Р ИСО/МЭК 24668-2022 «Информационные технологии. Искусственный интеллект. Структура управления процессами аналитики больших данных»	ISO/IEC 24668:2022	Рассматриваются технологии до 2015 г. Избыточен
2023	ГОСТ Р 70466-2022 «Информационные технологии (ИТ). Эталонная архитектура больших данных. Часть 1. Структура и процесс применения»	ISO/IEC TR 20547-1	Широкая трактовка понятий. Не хватает отраслевой специфики

Таблица 3 – Использование больших данных в отраслях России
Table 3 – Application of big data in Russia's industries

№	ОКВЭД	Значимые цели	Значимые источники	Роль в обеспечении безопасности предприятия
1	Сельское, лесное хозяйство, охота, рыболовство и рыбоводство. Строительство. Добыча полезных ископаемых. Обеспечение электрической энергией, газом и паром; кондиционирование воздуха. Водоснабжение; водоотведение, организация сбора и утилизации отходов, деятельность по ликвидации загрязнений. Деятельность административная и сопутствующие дополнительные услуги . Деятельность профессиональная, научная и техническая	Производство	Геолокация. Оборудование. Сайт	Минимальная
1a	Деятельность в области здравоохранения и социальных услуг. Деятельность в области культуры, спорта, организации досуга и развлечений. Государственное управление и обеспечение военной безопасности; социальное обеспечение*	Производство. Иное	Сайт. Социальные сети. Иное	Средняя
1b	Деятельность в области информации и связи. Транспортировка и хранение. Деятельность по операциям с недвижимым имуществом	Производство. Продажи и маркетинг	Учетные системы. Сайт	Низкая
2	Торговля оптовая и розничная; ремонт автотранспортных средств и мотоциклов. Деятельность гостиниц и предприятий общественного питания	Продажи и маркетинг	Учетные системы. Сайт	Минимальная
3	Деятельность финансовая и страховая	Продажи и маркетинг. Производство	Сайт. Учетные системы	Высокая
4	Обрабатывающие производства	Продажи и маркетинг. Производство	Учетные системы. Сайт	Низкая

Составлено по: Сведения об использовании информационных и коммуникационных технологий и производстве вычислительной техники, программного обеспечения и оказания услуг в этих сферах (итоги статнаблюдения по ф. № 3-информ) (2021) // Росстат. https://rosstat.gov.ru/statistics/science

Наиболее явными специфическими методами использования больших данных обладают две отрасли: 1) финансовая и страховая деятельность; 2) обрабатывающие производства.

Финансовая и страховая деятельность лидирует по уровню использования и анализа больших данных, в том числе для целей безопасности (высокая значимость этого направления несопоставима ни с одной другой сферой). Для обрабатывающих производств характерно такое использование этих данных для двух значимых целей, но источники их получения разнятся – для продаж и маркетинга используется сайт, а для производства – преимущественно учетные системы предприятия.

Структура указанного использования очень схожа в двух сферах экономической деятельности – в торговле и гостиничном бизнесе, но сильно отличается от прочих. Основной целью являются продажи и маркетинг, однако используется не столько собственный сайт, сколько внутренние учетные системы. При этом безопасности отводится минимальная роль, что согласуется с данными «Лаборатории Касперского», в соответствии с которыми наиболее крупные утечки информации были именно из сферы ритейла[1].

Деятельность в сфере информации и связи (в которую входит ИКТ) имеет собственную, но схожую с подходом сфер транспортировки и операций с недвижимым имуществом направленность относительно Big Data. Наиболее значимой целью является производство, которое связано с логистической и информационной деятельностью.

Использование больших данных в прочих сферах имеет очень схожую структуру (группы 1, 1a). Можно выделить подгруппу «Здравоохранение. Культура. Государственное управление», где велика роль «иных целей» указанного использования, вероятно, для принятия управленческих решений.

Выявление четких самостоятельных методов использования больших данных в таких отраслях, как финансовая, информации и связи, производственная, позволяет говорить о возможности применения

[1] Значимые утечки данных: Аналитический отчет (2023) // Лаборатория Касперского. https://go.kaspersky.com/ru-data-leakage-report-2022.

к ним специфичных подходов в отношениях с государством. Эти передовые отрасли могут служить «мотором» развития сферы больших данных, разрабатывая технологии, помогающие иным отраслям. Они будут выступать за максимальное упрощение работы с большими данными и снятие регуляторных барьеров, что противоречит текущей политике в части регулирования персональной информации.

Относительная схожесть остальных отраслей в разрезе использования больших данных может послужить основой для разработки «рамочного регулирования» – через ГОСТы или иные нормативные документы, но с учетом некоторых особенностей. Так, отрасли с большим потенциалом к развитию – торговля, гостиничный бизнес и операции с недвижимостью – обладают широкими платформенными решениями и нуждаются в упрощении инвестиционной политики в этой сфере, а также в развитии собственного кадрового потенциала. Иным «отстающим» отраслям, например строительству и сельскому хозяйству, необходимы дополнительные стимулы для развития сферы применения больших данных[1], так как специфика их деятельности заключается в долгой отдаче от вложений в инновационные продукты.

Реализация рамочного регулирования возможна как с помощью саморегулируемой организации (СРО) (отрасли, в особенности «передовые», уже показывают готовность к этому через действия Ассоциации больших данных (далее – Ассоциация)), так и с помощью поддерживающих норм со стороны регулятора (в частности, шаг к этому был сделан – установление ГОСТа по госзакупкам, связанным с большими данными). Дальнейшее развитие сферы больших данных, вероятно, кроется в сочетании этих подходов (при условии добровольного участия в СРО), а граница этих подходов лежит в области применения конкретных цифровых технологий, что является отдельным аспектом дальнейших исследований.

Другим специфичным вопросом является то, насколько регулирование именно персональной информации скажется на всем рынке больших данных. Информация Росстата позволяет выделить несколько источников данных для исследования потребителей, их характеристик и поведения: 1) веб-сайт организации; 2) данные операторов сотовой связи; 3) социальные сети. Соответствующие данные (определим их как «пользовательские») нельзя однозначно отнести к персональным, так как не вся информация позволяет идентифицировать пользователя, но «персональные данные» являются непременной частью «пользовательских данных»[2]. Более того, из-за размытого определения любые категории пользовательских данных могут быть отнесены к персональным как отдельно, так и, с большей вероятностью, – в совокупности. На рис. 5 представлено разделение пользовательских и непользовательских данных по отраслям экономики, измеренное в количестве организаций, использующих эти данные.

[1] Ассоциация больших данных (2020). Стратегия развития рынка больших данных. https://rubda.ru/wp-content/uploads/2020/02/Strategiya-korotkaya-versiya.pdf.

[2] Нельзя также однозначно сказать, что иные источники не включают персональные данные. Например, источник «Данные учетных систем предприятия, таких как ERP, CRM, SCM, HRIS и аналогичных» включает данные о персонале компании, которые попадают в «персональные данные». Но открытая статистика не позволяет провести даже приблизительную оценку разделения этих данных на «персональные» и иные.

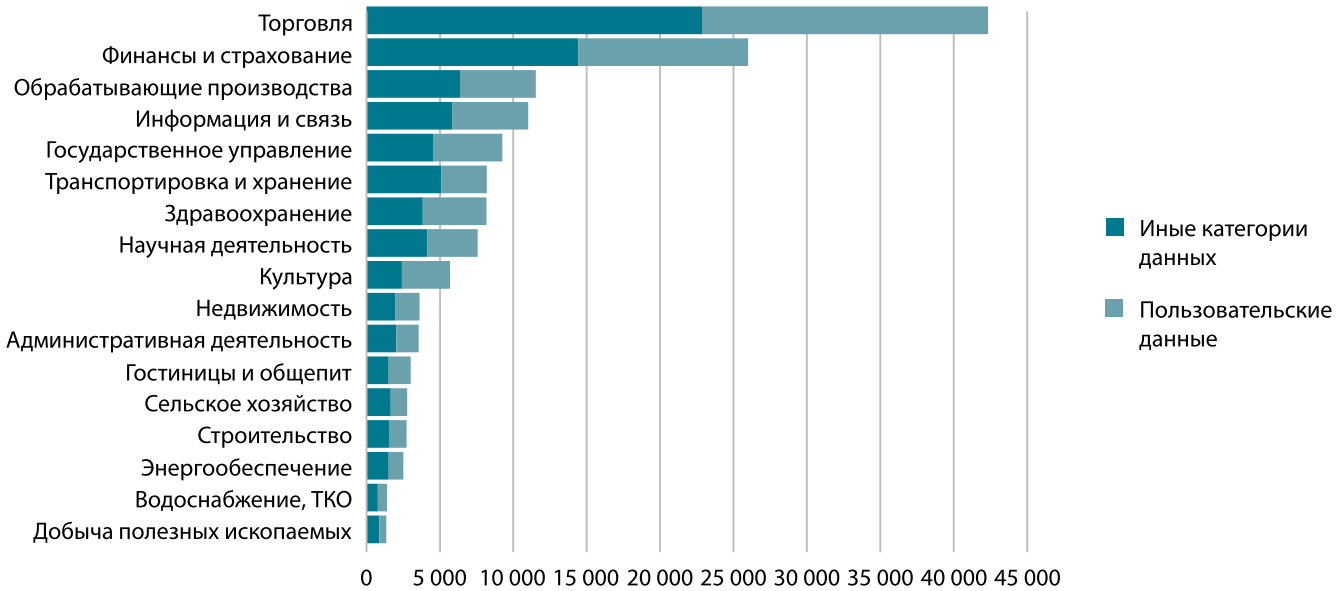

Рис. 5. Пользовательские и иные данные в отраслях экономики РФ, количество компаний, 2021[3]

Fig. 5. User and non-user data by industry in Russia, number companies, 2021

[3] Сведения об использовании информационных и коммуникационных технологий и производстве вычислительной техники, программного обеспечения и оказания услуг в этих сферах (итоги статнаблюдения по ф. № 3-информ) (2021) // Росстат. https://rosstat.gov.ru/statistics/science.

Можно наблюдать, что компании работают с пользовательскими и непользовательскими данными примерно в равной пропорции во всех отраслях (а в социальных отраслях, таких как государственное управление, здравоохранение и культура, данные первого типа даже преобладают). Это означает, что усиление регулирования в области персональных данных коснется широкого спектра компаний и большого объема данных.

Если посмотреть на цели использования пользовательских и непользовательских данных (рис. 6), то можно сделать следующие выводы:

- в разрезе одной отрасли эти цели имеют примерно схожий профиль, с той лишь оговоркой, что пользовательские данные применяются больше в сферах маркетинга и продаж, а также для управления персоналом [Попов, 2019];
- указанное использование имеет отраслевую специфику.

Это означает, что эффект от введения регулирования лишь в части пользовательских данных может сказаться шире, на всей области Big Data. Об этом предупреждает и Ассоциация, заявляя, что любые ограничения этого рынка сильно отражаются на потенциале развития.

Члены Ассоциации разработали Стратегию развития рынка больших данных до 2024 г., которая предусматривает несколько сценариев в зависимости от принимаемых государством мер. Базовый сценарий предполагает увеличение вклада больших данных в ВВП на 1,2 % (по сравнению с 2019 г.). Однако даже он предусматривает ряд регуляторных мер, имеющих достаточно радикальный характер. В частности, изменения в политике персональных данных, которые должны, по мнению Ассоциации, произвести «умеренный эффект», включают позволение компаниям обрабатывать персональную информацию для выполнения широкого круга целей (введение единого согласия пользователя на все способы обработки и цели). Для более «агрессивного эффекта» требуются поощрение обмена отраслевыми данными внутри и между отраслями через саморегулируемые стандарты [Савельев, 2015] и упрощенный обмен информацией с государством.

Как мировые, так и российские тенденции в области регулирования персональных данных свидетельствуют об ужесточении контроля. По всей видимости,

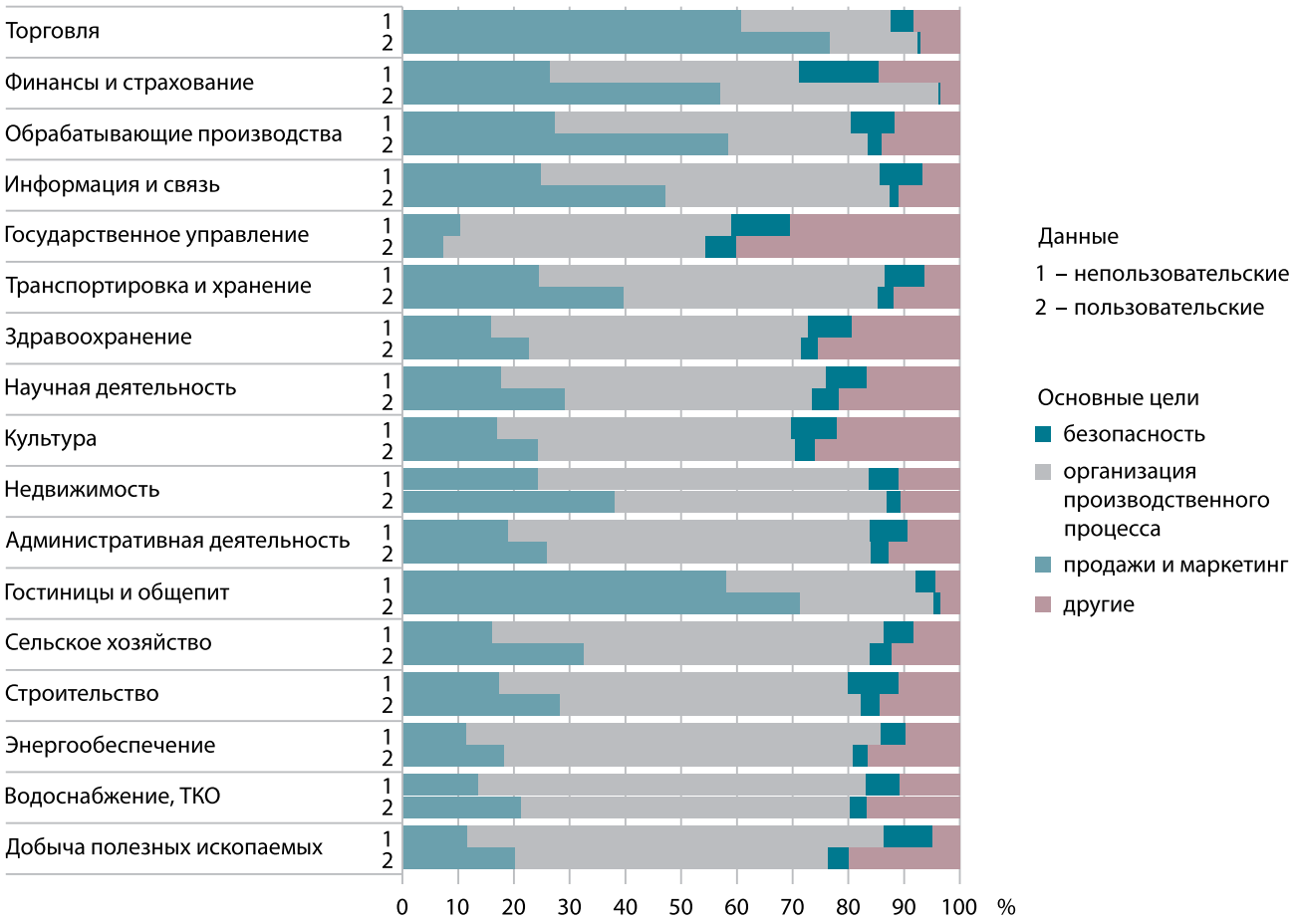

Рис. 6. Цели обработки пользовательских и непользовательских данных в российских отраслях экономики, 2021[1]

Fig. 6. Purposes of user and non-user data processing by industry in Russia, 2021

[1] Сведения об использовании информационных и коммуникационных технологий и производстве вычислительной техники, программного обеспечения и оказания услуг в этих сферах (итоги статнаблюдения по ф. № 3-информ) (2021) // Росстат. https://rosstat.gov.ru/statistics/science.

в этой части не следует ждать поддержки государством свободного обращения и упрощения режима обмена. Это означает, что сценарий «агрессивного» развития отрасли практически неосуществим, так как регулирование персональных данных оказывает сильное влияние на весь рынок больших данных по двум причинам:

- персональные данные не имеют четкой «спецификации» – в рамках одной отрасли цели использования пользовательских и непользовательских данных отличаются незначительно;
- размытое определение понятия «персональные данные» подталкивает компании к перестраховке, так как многие категории информации потенциально могут попасть под регулирование.

Особые тенденции обращения больших данных в разрезе отдельных отраслей говорят о специфике, которая должна приниматься во внимание регулятором. В рамках наиболее специфичных отраслей можно не только принимать отраслевые ГОСТы по указанному обращению, но и применять методы саморегулирования[1], особенно в части «непотребительских» данных.

ЗАКЛЮЧЕНИЕ

Отправной точкой для введения регулирования сферы больших данных, как правило, служит наиболее чувствительная сфера – персональных данных. Ни на практике, ни в теории нет единого подхода к необходимости и степени вмешательства регулятора – это зависит от восприятия реального ущерба, наносимого потребителям при несанкционированном использовании данных.

С одной стороны, существует «парадокс конфиденциальности», который свидетельствует о том, что спрос на защиту информации со стороны пользователей не является высоким. В России этот парадокс имеет свою специфику, связанную с мотивацией применения VPN-сервисов. С другой стороны, методы сокрытия информации цифровыми компаниями не дают возможности сделать осознанный выбор пользователю, который практически всегда не знает, какую персональную информацию компания собирает, как анализирует и передает ли третьим лицам.

Регуляторам в сфере больших данных в России следует принимать во внимание следующие аспекты.

Существует возможность сочетания регуляторного и информационного подходов. Информационный подход представляет собой помощь со стороны регулятора в раскрытии информации о целях и способах использования персональных данных и предоставлении пользователю права переносить их на другие платформы, но в России он практически не применяется. Такой подход менее эффективен с точки зрения обеспечения защиты данных, чем регуляторный, но лишен и его недостатков, обозначенных далее.

Ужесточение контроля персональных данных несет негативные экономические последствия. Юридические и экономические недоработки ФЗ «О персональных данных», санкционное давление и отсутствие зарубежных конкурентов, а также общая специфика цифровых рынков (наличие косвенных сетевых внешних эффектов, доверие к крупным компаниям, более эффективное внедрение мер кибербезопасности у экосистем, связанное с эффектом масштаба) могут привести к ситуации, подобной опыту ЕС. Внедрение GDPR показало, что усиление регулирования влечет не только снижение инновационной активности, падение финансовых показателей (что особенно характерно для малых и средних предприятий), но и повышение уровня экономической концентрации на цифровых и смежных рынках (при этом GDPR предусматривает наличие только оборотных штрафов). В России же предполагается как усиление фиксированных (не зависящих от размеров компаний), так и введение оборотных штрафов. Кроме того, уже введены меры, влияющие на вероятность наказания компаний за утечку информации (введение реестра), что привносит дополнительные риски для малых предприятий из-за чрезмерного регулирования.

Наличие отраслевых особенностей использования больших данных в российских секторах экономики диктует необходимость установления разных отношений этих секторов с государством. Проведенный анализ показал разницу подходов к сбору, анализу и использованию больших данных среди различных секторов экономики в России. «Передовые» отрасли (финансы, ИКТ, обрабатывающие производства) могут выступать драйверами для внедрения технологий больших данных в прочие секторы, и именно они настаивают на снижении регуляторного давления со стороны государства и создании рамочного регулирования (через специфические стандарты) с помощью действий СРО.

Усиление контроля только за персональными данными скажется достаточно широко – на всей сфере больших данных, всех отраслях экономики (как цифровых, так и реального сектора) и рынке труда. Стратегически важным направлением является поддержка IT-специалистов, обладающих специфическими отраслевыми знаниями, и компаний, взращивающих таких работников.■

[1] Ассоциация больших данных разработала собственный кодекс, в котором оговорены основные принципы добросовестного обращения с данными. По версии самой ассоциации, саморегулирование является наиболее подходящей альтернативой развития сферы больших данных. Однако Минцифры считает, что этого недостаточно для обеспечения безопасности данных.

Приложение. Корреляционная матрица показателей использования больших данных (целей и источников) по отраслям в РФ
Appendix. Correlation matrix of big data use indicators (goals and sources) by industry in Russia

	Сельское хозяйство	Строительство	Администрирование	Добыча	Наука	Электроэнергия	Водоснабжение	Здравоохранение	Культура	Недвижимость	Транспорт	Информация и связь	Госуправление	Финансы	Производство	Торговля	Деятельность гостиниц
Сельское хозяйство	1																
Строительство	0,996	1															
Администрирование	0,986	0,994	1														
Добыча	0,980	0,989	0,995	1													
Наука	0,977	0,987	0,993	0,995	1												
Электроэнергия	0,959	0,974	0,985	0,995	0,991	1											
Водоснабжение	0,967	0,981	0,992	0,998	0,994	0,999	1										
Здравоохранение	0,938	0,958	0,975	0,985	0,988	0,995	0,993	1									
Культура	0,926	0,949	0,967	0,978	0,983	0,990	0,988	0,999	1								
Недвижимость	0,965	0,950	0,931	0,901	0,907	0,862	0,880	0,836	0,820	1							
Транспорт	0,910	0,886	0,840	0,814	0,812	0,762	0,780	0,719	0,698	0,964	1						
Информация и связь	0,807	0,765	0,715	0,674	0,679	0,610	0,634	0,562	0,537	0,915	0,963	1					
Госуправление	0,787	0,826	0,858	0,891	0,891	0,927	0,914	0,948	0,956	0,620	0,480	0,278	1				
Финансы	0,188	0,186	0,152	0,096	0,117	0,033	0,066	0,026	0,029	0,323	0,406	0,435	–0,129	1			
Производство	0,198	0,137	0,066	0,006	0,029	–0,081	–0,049	–0,123	–0,146	0,416	0,556	0,724	–0,414	0,627	1		
Торговля	–0,561	–0,612	–0,661	–0,712	–0,699	–0,769	–0,747	–0,797	–0,811	–0,343	–0,193	0,032	–0,944	0,294	0,678	1	
Деятельность гостиниц	–0,461	–0,513	–0,552	–0,617	–0,596	–0,679	–0,651	–0,701	–0,715	–0,222	–0,105	0,130	–0,882	0,346	0,731	0,976	1

Составлено по: Сведения об использовании информационных и коммуникационных технологий и производстве вычислительной техники, программного обеспечения и оказания услуг в этих сферах (итоги статнаблюдения по ф. № 3-информ) (2021) // Росстат. https://rosstat.gov.ru/statistics/science

Примечание. Полужирным шрифтом выделены показатели, где p-value < 0,01. Ячейки окрашены согласно градиенту: от наименьшей отрицательной корреляции (красный) до наибольшей положительной корреляции (зеленый).

Источники

Моросанова А.А. (2022). Социальные сетевые медиа и цифровые платформы в новых условиях: quo vadis? // Вестник Московского университета. Серия 6, Экономика. № 4. С. 39–63. https://doi.org/10.38050/01300105202243.

Полтерович В.М. (2001). Трансплантация экономических институтов // Экономическая наука современной России. № 3. С. 24–50.

Полтерович В.М. (2006). Стратегии институциональных реформ. Перспективные траектории // Экономика и математические методы. Т. 42, № 1. С. 1–19.

Попов Е.В. (2019). Экономические институты цифровизации хозяйственной деятельности // Управленец. Т. 10, № 2. С. 2–10. DOI: 10.29141/2218-5003-2019-10-2-1.

Савельев А.И. (2015). Проблемы применения законодательства о персональных данных в эпоху «Больших данных» (Big Data) // Право. Журнал Высшей школы экономики. № 1. С. 43–66.

Шаститко А.Е. (2011). Ошибки I и II рода в экономических обменах с участием третьей стороны-гаранта // Журнал Новой экономической ассоциации. № 10. С. 125–148.

Шаститко А.Е. (2019). Мезоинституты: умножение сущностей или развитие программы экономических исследований? // Вопросы экономики. № 5. С. 5–25. DOI: 10.32609/0042-8736-2019-5-5-25.

Шаститко А.Е., Курдин А.А., Филиппова И.Н. (2023). Мезоинституты для цифровых экосистем // Вопросы экономики. № 2. С. 61–82. DOI: 10.32609/0042-8736-2023-2-61-82.

Шаститко А.Е., Маркова О.А., Мелешкина А.И., Морозов А.Н. (2020). Ценообразование на основе больших данных: предметное поле проблемы // Вестник Московского университета. Серия 6, Экономика. № 6. С. 3–22. DOI: 10.38050/01300105202061.

Ючинсон К.С. (2017). Большие данные и законодательство о конкуренции // Право. Журнал Высшей школы экономики. № 1. С. 216–245. DOI: 10.17323/2072-8166.2017.1.216.245.

Acquisti A., Taylor C., Wagman L. (2016). The economics of privacy. *Journal of Economic Literature*, vol. 54, no. 2, pp. 442–492. https://doi.org/10.1257/jel.54.2.442

Adjerid I., Acquisti A., Telang R., Padman R., Adler-Milstein J. (2016). The impact of privacy regulation and technology incentives: The case of health information exchanges. *Management Science*, vol. 62, no. 4, pp. 1042–1063. https://doi.org/10.1287/mnsc.2015.2194

Arcuri M.C. (2020). General Data Protection Regulation (GDPR) implementation: What was the impact on the market value of European financial institutions? *Eurasian Journal of Business and Economics,* vol. 13, no. 25, pp. 1–20. https://doi.org/10.17015/ejbe.2020.025.01

Athey S., Catalini C., Tucker C. (2017). The digital privacy paradox: Small money, small costs, small talk. *NBER Working Papers 23488*. National Bureau of Economic Research, Inc.

Becker G.S. (1968). Crime and punishment: An economic approach. *Journal of Political Economy*, no. 76, pp. 169–217.

Blind K., Niebel C., Rammer C. (2022). The impact of the EU General Data Protection Regulation on innovation in firms. *ZEW Discussion Papers*. No. 22-047. https://doi.org/10.2139/ssrn.4257740

Chen C., Frey C.B., Presidente G. (2022). Privacy regulation and firm performance: Estimating the GDPR effect globally. *The Oxford Martin Working Paper Series on Technological and Economic Change*. Working Paper No. 2022-1.

De Mauro A., Greco M., Grimaldi M. (2016). A formal definition of Big Data based on its essential features. *Library Review,* no. 65, pp. 122–135. https://doi.org/10.1108/LR-06-2015-0061

Favaretto M., De Clercq E., Schneble C., Elger B. (2020). What is your definition of Big Data? Researchers' understanding of the phenomenon of the decade. *PLoS One*, no. 15, no. 2. https://doi.org/10.1371/journal.pone.0228987

Geradin D., Karanikioti T., Katsifis D. (2021). GDPR Myopia: How a well-intended regulation ended up favouring large online platforms – the case of ad tech. *European Competition Journal*, vol. 17, no. 1, pp. 47–92. https://doi.org/10.1080/17441056.2020.1848059

Godinho de Matos M., Adjerid I. (2019). Consumer consent and firm targeting after GDPR: The case of a large telecom provider. *Management Science*. https://doi.org/10.2139/ssrn.3777417

Goldberg S., Johnson G., Shriver S. (2021). Regulating privacy online: An economic evaluation of the GDPR. *Law & Economics Center at George Mason University Scalia Law School Research Paper Series No. 22-025*. https://doi.org/10.2139/ssrn.3421731

Haucap J. (2019). Data protection and antitrust: New types of abuse cases? An economist's view in light of the German Facebook decision. *CPI Antitrust Chronicle February 2019*.

Hupperich T., Tatang D., Wilkop N., Holz T. (2018). An empirical study on online price differentiation. *Proceedings of the Eighth ACM Conference on Data and Application Security and Privacy (CODASPY '18). Association for Computing Machinery*. NY, USA. Pp. 76–83. https://doi.org/10.1145/3176258.3176338

Jia J., Ginger Zhe J., Wagman L. (2019). The short-run effects of GDPR on technology venture investment. *NBER Working Papers 25248*. National Bureau of Economic Research, Inc. https://doi.org/10.2139/ssrn.3278912

Johnson G., Shriver S., Goldberg S. (2022). Privacy & market concentration: Intended & unintended consequences of the GDPR. *Management Science*. https://doi.org/10.2139/ssrn.3477686

Kemp K. (2020). Concealed data practices and competition law: Why privacy matters. *European Competition Journal*, vol. 16, no. 2-3, pp. 628–672. https://doi.org/10.1080/17441056.2020.1839228

Koski H., Valmari N. (2020). Short-term impacts of the GDPR on firm performance. *ETLA Working Papers 77*. The Research Institute of the Finnish Economy.

Marciano A., Nicita A., Ramello G. (2020). Big data and big techs: Understanding the value of information in platform capitalism. *European Journal of Law and Economics*, no. 50, pp. 1–14. https://doi.org/10.1007/s10657-020-09675-1
Marthews A., Tucker C. (2019, December). Privacy policy and competition. Brookings report. *Brookings Economic Studies*. Pp. 1–27.
Martin N., Matt C., Niebel C., Blind K. (2019). How data protection regulation affects startup innovation. *Information System Frontiers*, vol. 21, pp. 1307–1324. https://doi.org/10.1007/s10796-019-09974-2
Peukert C., Bechtold S., Batikas M., Kretschmer T. (2022). Regulatory spillovers and data governance: Evidence from the GDPR. *Marketing Science*, vol. 41, no. 4, pp. 318–340. https://doi.org/10.1287/mksc.2021.1339
Polinsky A.M., Shavell S. (1989). Legal error, litigation, and the incentive to obey the law. *The Journal of Law, Economics, and Organization,* vol. 5, no. 1, pp. 99–108. https://doi.org/10.1093/oxfordjournals.jleo.a036968
Severo M., Feredj A., Romele A. (2016). Soft data and public policy: Can social media offer alternatives to official statistics in urban policymaking? *Policy & Internet,* vol. 8, no. 3, pp. 354–372. https://doi.org/10.1002/poi3.127
Shavell S. (2004). *Foundations of economic analysis of law*. Cambridge (MA): Harvard University Press.
Zhuo R., Huffaker Br., Claffy C., Greenstein S. (2020). The impact of the general data protection regulation on internet interconnection. *Telecommunications Policy*, vol. 45, no. 2. http://dx.doi.org/10.2139/ssrn.3761288

References

Morosanova A.A. (2022). Social media and digital platforms in new conditions: quo vadis? *Vestnik Moskovskogo universiteta. Seriya 6, Ekonomika / Moscow University Economics Bulletin,* no. 4, pp. 39–63. https://doi.org/10.38050/01300105202243. (in Russ.)
Polterovich V.M. (2001). Transplantation of economic institutions. *Ekonomicheskaya nauka sovremennoy Rossii / Economics of Contemporary Russia,* no. 3, pp. 24–50. (in Russ.)
Polterovich V.M. (2006). Strategies for institutional reforms. Promising trajectories. *Ekonomika i matematicheskie metody / Economics and Mathematical Methods,* vol. 42, no. 1, pp. 1–19. (in Russ.)
Popov E.V. (2019). Business institutions of economic activity digitalization. *Upravlenets / The Manager,* vol. 10, no. 2, pp. 2–10. https://doi.org/10.29141/2218-5003-2019-10-2-1. (in Russ.)
Savelyev A.I. (2015). Problems of applying legislation on personal data in the era of Big Data. *Pravo. Zhurnal Vysshey shkoly ekonomiki / Law. Journal of the Higher School of Economics,* no. 1, pp. 43–66. (in Russ.)
Shastitko A.E. (2011). Type I and II errors in economic exchanges involving a third party guarantor. *Zhurnal Novoy ekonomicheskoy assotsiatsii / The Journal of the New Economic Association,* no. 10, pp. 125–148. (in Russ.)
Shastitko A.E. (2019). Meso-institutions: Proliferating essences or evolving economic research programme? *Voprosy Ekonomiki,* no. 5, pp. 5–25. https://doi.org/10.32609/0042-8736-2019-5-5-25. (in Russ.)
Shastitko A.E., Kurdin A.A., Filippova I.N. (2023). Meso-institutions for digital ecosystems. *Voprosy Ekonomiki,* no. 2, pp. 61–82. https://doi.org/10.32609/0042-8736-2023-2-61-82. (in Russ.)
Shastitko A.E., Markova O.A., Meleshkina A.I., Morozov A.N. (2020). Big Data-based pricing: The problem field. *Vestnik Moskovskogo universiteta. Seriya 6, Ekonomika / Moscow University Economics Bulletin,* no. 6, pp. 3–22. https://doi.org/10.38050/01300105202061. (in Russ.)
Yuchinson K.S. (2017). Big Data and legislation on competition. *Pravo. Zhurnal Vysshey shkoly ekonomiki / Law. Journal of the Higher School of Economics,* no. 1, pp. 216–245. https://doi.org/10.17323/2072-8166.2017.1.216.245. (in Russ.)
Acquisti A., Taylor C., Wagman L. (2016). The economics of privacy. *Journal of Economic Literature*, vol. 54, no. 2, pp. 442–492. https://doi.org/10.1257/jel.54.2.442
Adjerid I., Acquisti A., Telang R., Padman R., Adler-Milstein J. (2016). The impact of privacy regulation and technology incentives: The case of health information exchanges. *Management Science*, vol. 62, no. 4, pp. 1042–1063. https://doi.org/10.1287/mnsc.2015.2194
Arcuri M.C. (2020). General Data Protection Regulation (GDPR) implementation: What was the impact on the market value of European financial institutions? *Eurasian Journal of Business and Economics,* vol. 13, no. 25, pp. 1–20. https://doi.org/10.17015/ejbe.2020.025.01
Athey S., Catalini C., Tucker C. (2017). The digital privacy paradox: Small money, small costs, small talk. *NBER Working Papers 23488*. National Bureau of Economic Research, Inc.
Becker G.S. (1968). Crime and punishment: An economic approach. *Journal of Political Economy*, no. 76, pp. 169–217.
Blind K., Niebel C., Rammer C. (2022). The impact of the EU General Data Protection Regulation on innovation in firms. *ZEW Discussion Papers*. No. 22-047. https://doi.org/10.2139/ssrn.4257740
Chen C., Frey C.B., Presidente G. (2022). Privacy regulation and firm performance: Estimating the GDPR effect globally. *The Oxford Martin Working Paper Series on Technological and Economic Change*. Working Paper No. 2022-1.
De Mauro A., Greco M., Grimaldi M. (2016). A formal definition of Big Data based on its essential features. *Library Review,* no. 65, pp. 122–135. https://doi.org/10.1108/LR-06-2015-0061
Favaretto M., De Clercq E., Schneble C., Elger B. (2020). What is your definition of Big Data? Researchers' understanding of the phenomenon of the decade. *PLoS One*, no. 15, no. 2. https://doi.org/10.1371/journal.pone.0228987
Geradin D., Karanikioti T., Katsifis D. (2021). GDPR Myopia: How a well-intended regulation ended up favouring large online platforms – the case of ad tech. *European Competition Journal*, vol. 17, no. 1, pp. 47–92. https://doi.org/10.1080/17441056.2020.1848059

Godinho de Matos M., Adjerid I. (2019). Consumer consent and firm targeting after GDPR: The case of a large telecom provider. *Management Science*. https://doi.org/10.2139/ssrn.3777417

Goldberg S., Johnson G., Shriver S. (2021). Regulating privacy online: An economic evaluation of the GDPR. *Law & Economics Center at George Mason University Scalia Law School Research Paper Series No. 22-025*. https://doi.org/10.2139/ssrn.3421731

Haucap J. (2019). Data protection and antitrust: New types of abuse cases? An economist's view in light of the German Facebook decision. *CPI Antitrust Chronicle February 2019*.

Hupperich T., Tatang D., Wilkop N., Holz T. (2018). An empirical study on online price differentiation. *Proceedings of the Eighth ACM Conference on Data and Application Security and Privacy (CODASPY '18). Association for Computing Machinery*. NY, USA. Pp. 76–83. https://doi.org/10.1145/3176258.3176338

Jia J., Ginger Zhe J., Wagman L. (2019). The short-run effects of GDPR on technology venture investment. *NBER Working Papers 25248*. National Bureau of Economic Research, Inc. https://doi.org/10.2139/ssrn.3278912

Johnson G., Shriver S., Goldberg S. (2022). Privacy & market concentration: Intended & unintended consequences of the GDPR. *Management Science*. https://doi.org/10.2139/ssrn.3477686

Kemp K. (2020). Concealed data practices and competition law: Why privacy matters. *European Competition Journal*, vol. 16, no. 2-3, pp. 628–672. https://doi.org/10.1080/17441056.2020.1839228

Koski H., Valmari N. (2020). Short-term impacts of the GDPR on firm performance. *ETLA Working Papers 77*. The Research Institute of the Finnish Economy.

Marciano A., Nicita A., Ramello G. (2020). Big data and big techs: Understanding the value of information in platform capitalism. *European Journal of Law and Economics*, no. 50, pp. 1–14. https://doi.org/10.1007/s10657-020-09675-1

Marthews A., Tucker C. (2019, December). Privacy policy and competition. Brookings report. *Brookings Economic Studies*. Pp. 1–27.

Martin N., Matt C., Niebel C., Blind K. (2019). How data protection regulation affects startup innovation. *Information System Frontiers*, vol. 21, pp. 1307–1324. https://doi.org/10.1007/s10796-019-09974-2

Peukert C., Bechtold S., Batikas M., Kretschmer T. (2022). Regulatory spillovers and data governance: Evidence from the GDPR. *Marketing Science*, vol. 41, no. 4, pp. 318–340. https://doi.org/10.1287/mksc.2021.1339

Polinsky A.M., Shavell S. (1989). Legal error, litigation, and the incentive to obey the law. *The Journal of Law, Economics, and Organization,* vol. 5, no. 1, pp. 99–108. https://doi.org/10.1093/oxfordjournals.jleo.a036968

Severo M., Feredj A., Romele A. (2016). Soft data and public policy: Can social media offer alternatives to official statistics in urban policymaking? *Policy & Internet,* vol. 8, no. 3, pp. 354–372. https://doi.org/10.1002/poi3.127

Shavell S. (2004). *Foundations of economic analysis of law*. Cambridge (MA): Harvard University Press.

Zhuo R., Huffaker Br., Claffy C., Greenstein S. (2020). The impact of the general data protection regulation on internet interconnection. *Telecommunications Policy*, vol. 45, no. 2. http://dx.doi.org/10.2139/ssrn.3761288

Информация об авторе

Моросанова Анастасия Андреевна

Кандидат экономических наук, научный сотрудник Центра исследований конкуренции и экономического регулирования. **Российская академия народного хозяйства и государственной службы при Президенте РФ**, г. Москва, РФ. E-mail: aamorosanova@gmail.com

Information about the author

Anastasia A. Morosanova

Cand. Sc. (Econ.), Researcher of the Center for Studies of Competition and Economic Regulation. **Russian Presidential Academy of National Economy and Public Administration (RANEPA)**, Moscow, Russia. E-mail: aamorosanova@gmail.com