Экономическая политика. 2025. Т. 20. № 6. С. 96–119 DOI: 10.18288/1994-5124-2025-6-96-119

Цифровая экономика

Персональные данные: экономические проблемы и правовое регулирование

Антонина Давидовна Левашенко
ORCID: 0000-0002-1236-3605
Старший научный сотрудник,
Всероссийская академия внешней торговли Министерства экономического развития Российской Федерации (РФ, 119285, Москва, Воробьевское шоссе, д. 6А)
E-mail: antonina.lev@gmail.com

Сергей Германович Синельников-Мурылев
ORCID: 0000-0001-6667-9958
Доктор экономических наук,
профессор, научный руководитель,
Институт экономической политики им. Е. Т. Гайдара (РФ, 125993, Москва, Газетный пер., 3–5, стр. 1)
E-mail: sinelnikov-sg@iep.ru

Аннотация
Развитие технологий обработки данных и накопление их объема сопровождается появлением новых цифровых бизнес-моделей. Однако новые бизнес-модели могут создавать различные проблемы, требующие совершенствования регулирования сбора и использования персональных данных. Действующие нормы российского законодательства не отвечают на вызовы, связанные с использованием персональных данных для индивидуализации рекламы и сервисов, а также с применением цифровых профилей пользователей в конкуренции платформ за аудиторию. В настоящей работе проведена систематизация проблем и вызовов цифровой экономики для существующего правового режима защиты персональных данных. Цель исследования состоит в том, чтобы наметить пути урегулирования некоторых выявленных проблем. В статье предлагаются возможные решения вопросов, связанных с нарушением интересов пользователей и ограничениями в развитии цифровых рынков. В числе нарушений интересов пользователей рассматривается вторжение в частную жизнь, применение платформами негативных практик при сборе данных, создание и внедрение цифровых профилей пользователей, которые идут вразрез с их интересами, включая ценовую дискриминацию и дискриминацию по социальным признакам. В части регулирования проблемы бесконтрольного сбора и использования персональных данных пользователей авторы рассматривают возможность реформирования института согласия на обработку персональных данных с целью оптимизации ресурсов, затрачиваемых бизнесом и пользователями на формальное соблюдение действующих законодательных требований. В числе проблем, связанных с состоянием цифровых рынков, исследуются ситуации монополизации рынков крупнейшими платформами, использование ценовых алгоритмов как антиконкурентной практики, недостаточно урегулированные условия доступа к данным, включая ограничения для развития научных исследований и регуляторные барьеры для трансграничной передачи данных. Авторами предлагаются решения на уровне как законодательных норм, так и взаимодействия цифрового бизнеса и профильных регуляторов.

Ключевые слова: оборот данных, цифровые бизнес-модели, сетевые рынки, цифровое профилирование
JEL: L86, M15, O14

Ekonomicheskaya Politika, 2025, vol. 20, no. 6, pp. 96–119 DOI: 10.18288/1994-5124-2025-6-96-119

Digital Economy

Personal Data: Economic Problems and Legal Regulation

Antonina D. Levashenko
ORCID: 0000-0002-1236-3605
Senior Researcher, Russian Academy of Foreign Trade of the Ministry of Economic Development of the Russian Federation,[a]
e-mail: antonina.lev@gmail.com

Sergey G. Sinelnikov-Murylev
ORCID: 0000-0001-6667-9958
Dr. Sci. (Econ.), Professor, Scientific Director, Gaidar Institute for Economic Policy,[b]
e-mail: sinelnikov-sg@iep.ru

[a] 6A, Vorob'evskoe shosse, Moscow, 119285, Russian Federation
[b] 3–5, Gazetnyy per., Moscow, 125993, Russian Federation

Abstract
The development of technologies and increasing volume of data worldwide calls for new models of digital business. However, new business models bring new problems in protecting personal data, which cannot be resolved within the existing legal framework. Current Russian legislation does not regulate the use of personal data for the personalization of advertising and services or the use of digital user profiles in the competition for users between different platforms. The paper offers a systematic account of the problems and challenges faced by the digital economy as a result of the existing legal arrangements for personal data protection. The purpose of this study is to develop optimal solutions for two kinds of problems that the authors identify: (1) disregard of user interests; and (2) excessive constraints on competition in digital markets. Disregard of user interests may consist of invasion of privacy and infringement of consumers' economic interests, objectionable practices by platforms in collecting data, and digital profiling of users contrary to their interests, such as price discrimination among users and discrimination on social grounds. Uncontrolled collection and use of consumers' personal data demand reform of the way in which consent to processing personal data is solicited so that the resources businesses and users devote to formal compliance with current legislative requirements are optimized. Digital markets also suffer from the monopolization of markets by the largest platforms, the use of pricing algorithms as an anti-competitive practice, and poor regulation of access to data that restricts scientific research and erects regulatory barriers to cross-border data transfer. The authors propose solutions that require not only amending legal standards but also facilitating interaction between digital businesses and regulators.
Keywords: data circulation, digital business models, network markets, digital profiling
JEL: L86, M15, O14

Введение

После окончания Второй мировой войны во Всеобщей декларации прав человека было зафиксировано базовое право лица на личную и семейную жизнь, и, несмотря на то что персональные данные прямо не упоминаются в этом документе, его положения о защите частной жизни и свободе информации заложили основу современных норм их охраны.

В 70-е — 90-е годы XX века персональные данные использовались в бухгалтерском и управленческом учете, при налогообложении, пенсионном обеспечении, в военном учете, при устройстве на работу и учебу, открытии банковских счетов, оказании медицинских услуг и т. п. Несмотря на то что начиная с середины 1970-х годов начались процессы формирования современной модели интернета (создание электронной почты, передача файлов в рамках проекта ARPANET), данные в основном фиксировались на бумажных носителях. Как следствие, случаи утечки информации были редкими, а риски ее недобросовестного использования для субъекта персональных данных — минимальными.

Начиная с 2000-х годов с развитием цифровизации изменились производственные процессы, возникли новые бизнес-модели. Широкое распространение домашних компьютеров стало ключевым фактором для развития таких онлайн-сервисов, как Wikipedia (2001), Skype (2003), Facebook[1] (2004), YouTube (2005), Twitter (2006), Dropbox (2007), Spotify (2008) [O'Hara, Shadbolt, 2008]. Эти технологии за последние два-три десятилетия привели к качественным изменениям в процессах накопления и использования данных о людях и их поведении в экономике и других сферах общественной жизни.

Накопление данных о поведении, новые методы их обработки привели к созданию цифровых бизнес-моделей, которые прежде всего затрагивают физических лиц как производителей данных цифровой экономики, а значит, правовой режим их персональных данных. Это выражается и в форматах сбора данных (если раньше данные предоставлял сам субъект, то сегодня всё больше данных фиксируется трекинговыми технологиями), и в направлениях использования данных (сегодня данные служат не только ресурсом для оказания услуги, но и ресурсом маркетингового продвижения бизнеса за счет персонализации рекламы на основе формирования цифровых профилей пользователей). В результате субъекты персональных данных оказываются подвержены значительным рискам, затрагивающим всё больше

[1] Запрещен на территории РФ по основаниям осуществления экстремистской деятельности.

сфер жизни человека. Эта проблема сегодня всесторонне обсуждается научным сообществом в России в контексте вопросов цифровизации бизнес-процессов [Иванов, Устинова, 2025], цифрового суверенитета [Остапович, Шахновская, 2024], антимонопольного регулирования рынков [Асадуллина, 2020], правового режима данных в условиях цифровой экономики [Селюк, 2023]. Рост масштабов сбора и использования данных в экономической жизни, изменения в задачах, которые могут эффективно решаться с помощью новых методов обработки данных, возникновение новых бизнес-моделей на основе сбора и анализа данных вызывают целый ряд проблем, касающихся экономических отношений. Для того чтобы сформулировать и систематизировать эти конкретные задачи, а также определить направления для их решения, настоящее исследование опирается на сочетание системного, сравнительно-правового и экономико-правового подходов. Анализ проводится на базе норм действующего российского законодательства, актов ЕС, США, стран БРИКС (Китая и Бразилии), а также материалов профильных органов и международных организаций.

1. Новая роль данных в экономике: изменение традиционных бизнес-моделей

Рост объема услуг, оказываемых с применением технологий анализа данных, и развитие интернета радикально изменили двусторонние рынки [Паркер и др., 2017; Armstrong, 2006]. Они приняли вид многосторонних цифровых платформ, распространившихся на различные сферы экономики для организации взаимодействия продавцов и покупателей товаров и услуг, работников и нанимателей рабочей силы, пользователей сервисов социальных сетей, финансовых технологий и рекламодателей.

Двусторонние и многосторонние (сетевые) рынки соединили различные группы пользователей, которые в ряде случаев могут совпадать (например, рынок видеоигр объединил пользователей программного обеспечения и пользователей оборудования для игр). В этом случае покупки различных видов продуктов становятся скоординированными [Rochet, Tirole, 2003]. При функционировании многосторонних платформ процессы координации рынка обеспечиваются компаниями — владельцами платформ: они выступают в роли “matchmakers”, то есть агентов-посредников для пользователей и поставщиков услуг [Evans, Schmalensee, 2016]. Агенты собирают большие объемы данных, генерируемые взаимодействием участников платформы. При этом возникает так называемый эффект агрегации,

когда комплекс данных имеет бóльшую ценность, чем сумма фрагментов данных [Solve, 2004].

Возможности получения различной информации о потребителях, включающей не только персональные данные, прямо определяющие лицо (например, личные данные из различных документов), но и самую разнообразную информацию, косвенно характеризующую потребителя, включая данные об образе жизни, привычках, характере работы, состоянии здоровья, членах семьи и т. п., коренным образом изменили подход к рекламе. Значительную роль в сборе такой информации играют социальные сети. Они, оказывая влияние на формирование образа жизни человека в личном и профессиональном плане, накапливают о нем различную поведенческую информацию, которая может быть использована для создания индивидуальных маркетинговых предложений.

Персонализация рекламы на основе больших массивов информации о пользователях цифровых сервисов резко повысила ее эффективность. Реклама стала с большей интенсивностью демонстрироваться не потенциально заинтересованным в рекламируемом товаре различным группам лиц, выделяемых по доходам, возрасту, образованию, месту проживания и т. п., а отдельным конкретным людям, которые с большой вероятностью ее посмотрят (кликнут) и в дальнейшем приобретут соответствующий товар или услугу. Повышение эффективности рекламы за счет ее таргетирования во многих случаях может рассматриваться как улучшение качества услуги, заключающейся в предоставлении покупателям информации о новых товарах и их особенностях.

Важнейшим изменением в маркетинге, связанным со сбором и обработкой персональных данных, помимо отмеченного повышения эффективности рекламы является появившаяся возможность прогнозирования не только наличия у потребителя потенциальной потребности в рекламируемом товаре или услуге, но и оценка интенсивности этой потребности. «Аналитика, производящая таргетированную рекламу, создает основу для новых рынков поведенческих фьючерсов, которые торгуют предсказаниями поведения потребителя» [Зубофф, 2024. С. 285].

Следом за распространением таргетированной рекламы цифровые компании стали прибегать к негативным практикам, таким как размещение фейкового контента, который увеличивает время, проводимое пользователями на соответствующем ресурсе, а значит, и предоставляет больше возможностей для демонстрации рекламы. Сбор поведенческих данных пользователей позволяет компаниям не просто манипулировать их мнением в тот или

иной момент времени (например, стимулирование однократной покупки товара), но и формировать привычки его поведения в интернете, что существенно повышает «пожизненную ценность пользователя» [Hooked, 2014. P. 13]. «Привычка делает пользователя “привязанным” к продукту (например, к подписке на аудиовизуальный сервис), а значит, менее чувствительным к росту цен на продукт» [Hooked, 2014. P. 14].

Накопление беспрецедентно больших объемов информации в совокупности с массовым ее использованием в управленческих и маркетинговых целях и удаленной работой (через облачные сервисы, инструменты видео-конференц-связи и платформы управления проектами) создает высокие риски утечки данных, включая персональные данные клиентов. Чем больше накопленные базы данных, тем выше риски пользователей при атаках на эти базы: так, по данным Роскомнадзора, в 2023 году в результате 168 атак несанкционированному доступу подверглось 300 млн записей персональных данных, тогда как в 2024 году при меньшем количестве атакованных баз данных — 135 — пострадало 600 млн записей[2]. При этом преступления в цифровой сфере в меньшей степени, чем в реальном мире, могут контролироваться государственными органами охраны правопорядка. Поэтому управление рисками информационной безопасности в значительной степени остается в зоне ответственности частных лиц — пользователей и компаний [Wall, 2024].

Ряд отмеченных проблем не может быть успешно урегулирован в рамках существующего нормативно-правового поля. Требуется разработка новых подходов к регулированию процессов сбора, накопления, обмена и использования персональных данных.

2. Ключевые проблемы и решения в интересах индивида

Регулирование сбора и использования персональных данных. Согласие на сбор и обработку персональных данных на практике в настоящее время представляет собой имитационный инструмент. Компании осуществляют массовый сбор данных как без согласия, так и с формальным согласием потребителей, что никак не влияет на последствия использования и обработки этих данных. Пользователи не знают, в каких целях их данные используются.

Вторжение в частную жизнь и ущемление экономических интересов потребителей. Можно выделить несколько направлений, связанных с использованием персональных данных потребителей в целях, которые могут противоречить их экономическим инте-

[2] Роскомнадзор раскрыл число утечек: за год их стало вдвое меньше // Cnews. 2025. 7 февраля. https://www.cnews.ru/news/top/2025-02-07_roskomnadzor_zafiksiroval.

ресам: (1) для манипуляций с поведением потребителей; (2) для ценовой дискриминации потребителей; (3) для дискриминации лица по социальным признакам (вере, национальности, полу, возрасту, месту проживания и др.) на рынке труда, в сферах образования, здравоохранения, госуслуг и др., в том числе с использованием моделей искусственного интеллекта; (4) для различного рода мошеннических действий.

Законодательство в России устанавливает двенадцать причин для сбора и обработки персональных данных[3], которые включают такие основания, как «согласие» и «исполнение договора в интересах лица». Во втором случае закон дает право не оформлять согласие. Но на практике использование такого аргумента, как «необходимость исполнения договора», почти не применяется.

Согласие является самым распространенным, но недостаточно проработанным основанием для сбора и обработки данных[4].

Во-первых, законодательное требование о том, что персональные данные должны быть обработаны только для достижения конкретных целей, является неясным и имеет множество толкований при его исполнении как со стороны компаний, так и со стороны ведомств[5]. Возникают следующие вопросы: должна ли быть одна форма согласия с одной целью или может быть одна форма согласия для нескольких целей и в каком месте необходимо ставить подпись? Часто компании стараются указать общую цель в одном согласии, что приводит к формализации исполнения принципа «одно согласие — одна цель». Этот же подход отражен в разъяснениях отдельных ведомств.

Во-вторых, институт согласия уже получил свое развитие в других отраслевых законах. Например, в ситуации, когда заключается договор об оказании услуги мобильной связи, допускается использовать оба основания для обработки данных: и согласие на обработку данных, и «необходимость исполнения договора»[6]. Однако закон «О связи» включает оговорки о согласии абонента на обработку его персональных данных: передача данных абонента третьим лицам допускается только с его письменного согласия[7]. В финансовой сфере, например, банк не может включать согласие

---

[3] Федеральный закон от 27.07.2006 № 152 «О персональных данных» (далее – ФЗ № 152), ч. 1 ст. 6.

[4] Компании отдельно оформляют его даже в случаях заключения с лицом договора, требующего для его исполнения сбора и обработки персональных данных (покупка авиабилета).

[5] ФЗ № 152, ч. 2 ст. 5.

[6] Причем договор об оказании услуг мобильной связи заключается в письменной форме. Так, согласно п. 6 ст. 44 ФЗ № 126 «О связи» оператор связи «обязан внести в такой договор достоверные сведения об абоненте, перечень которых установлен правилами оказания услуг связи».

[7] Абзац 3 ст. 10 ФЗ № 99 от 07.05.2013 «О внесении изменений в отдельные законодательные акты Российской Федерации в связи с принятием Федерального закона “О ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных” и Федерального закона “О персональных данных”».

на обработку данных в кредитный договор, это должны быть два разных документа[8].

В-третьих, отдельные ведомства формируют на подзаконном уровне свое ви́дение того, как должно оформляться согласие. Например, при поступлении в вуз абитуриент дает согласие на обработку данных для тех целей, которые указаны в политике конфиденциальности вуза. Поэтому в форме согласия часто используется широкая формулировка. Это позволяет вузу менять конкретные цели в своей политике конфиденциальности без дополнительного сбора согласия. Но такой подход может быть признан регулирующим органом неправомерным.

Предприятиям и организациям часто выгодно получать формально отдельное согласие. Дело в том, что при заключении договора обработка данных на основании необходимости исполнения договора должна осуществляться с единственной целью — исполнение договора, где лицо является выгодоприобретателем. В то же время при получении отдельного формального согласия у бизнеса есть возможность получить данные не только для исполнения договора, но также для их использования в иных целях и на постоянной основе (например, для их включения в программу лояльности продавца, для рассылки рекламных предложений и др.). Иначе говоря, даже когда формальное согласие не требуется, бизнес может делать выбор в пользу его получения с целью сбора данных пользователей.

В США сам факт предоставления пользователем своих персональных данных, необходимых для заключения и исполнения договора, который он добровольно подписывает (или принимает условия онлайн), рассматривается как подразумеваемое согласие. На уровне штатов США могут устанавливаться различные перечни исключений из правила о подразумеваемом согласии (для цифрового профилирования, персонализированной рекламы, продажи данных)[9]. Также явное согласие нужно, если обрабатываются чувствительные данные (включая биометрические данные)[10] или если данные собираются от несовершеннолетних пользователей[11].

---

[8] «Если согласие заемщика на обработку его персональных данных включено в иные документы (например, заявление о предоставлении потребительского кредита (займа), согласие субъекта кредитной истории на получение кредитного отчета), то рекомендуем кредиторам обеспечить возможность выражения заемщиком согласия на обработку его персональных данных путем проставления заемщиком отдельной подписи о согласии в таком документе». Информационное письмо Банка России № ИН-06-59/57, Роскомнадзора № 08ЛА-48666 от 29.07.2021 «О согласии заемщиков на обработку их персональных данных».

[9] Oregon Senate Bill 619. https://legiscan.com/OR/text/SB619/id/2830293/Oregon-2023-SB619-Enrolled.pdf; https://archive.legmt.gov/bills/2023/billpdf/SB0384.pdf.

[10] Washington Biometric Privacy Law (H.B. 1493). https://app.leg.wa.gov/RCW/default.aspx?cite=19.375&full=true.

[11] The United States of America. Children's Online Privacy Protection Act of 1998 (15 U.S.C. 6501). https://www.ecfr.gov/current/title-16/chapter-I/subchapter-C/part-312.

В ЕС Регламент 2016 года по защите персональных данных закрепляет подход, основанный на необходимости получения явного согласия[12]. Однако ввиду высокой административной нагрузки на бизнес в ЕС неоднократно выдвигались инициативы по упрощению этой нормы.

Следует напомнить, что еще в 1980 году на этапе формирования международного стандарта обработки персональных данных на площадке ОЭСР речь шла о важности обеспечения лица знанием или получения от него согласия на то, как его данные будут использоваться[13]. Однако ключевым условием эффективного порядка сбора согласия является осознание лицом последствий обработки его данных, а не оформление согласия.

С точки зрения поставщика товаров или услуг можно выделить две ключевые цели обработки персональных данных на основе изъявления гражданами согласия на такое предоставление данных.

Первая цель — это предоставление определенной услуги (или товара), которая не может быть оказана гражданину без передачи определенных данных. Здесь сам факт оказания услуги (продажи товара) должен по умолчанию обеспечивать признание законного характера сбора и обработки персональных данных клиента, ведь цель и объем данных, необходимых для этой цели, в сущности, будет задавать сам субъект персональных данных, обращающийся за услугой или покупкой товара. Сам факт желания осуществить сделку (или действие) выражает в конклюдентной форме согласие на передачу персональных данных поставщику услуги или товара[14].

Вторая цель — обработка и анализ персональных данных для прочих, более широких целей бизнеса, таких как маркетинговые цели, задачи прогнозирования поведения потребителя. И эту цель субъект персональных данных чаще всего не осознаёт.

Регламентация использования данных в целях, непосредственно не связанных с оказанием требуемой потребителю услуги или продажей продукта, может быть установлена за счет перехода от концепции «исключительного отнесения персональных данных к нематериальному благу» (что происходит сегодня при отнесении

---

[12] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC. Article 6(1, a), 7. https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng.

[13] OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. 1980: "Collection Limitation Principle. There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject."

[14] В России признание конклюдентных действий законным основанием установления или изменения договорных отношений подтверждается судебной практикой толкования положений Гражданского кодекса РФ (п. 3 ст. 438 «Акцепт»). См., например, п. 5 информационного письма Президиума ВАС РФ от 05.05.1997 № 14.

данных к объектам гражданского права) к концепции «определения персональных данных в качестве информации для включения в предмет договора». Целесообразно внести изменения в федеральный закон о персональных данных, уточнив право лица на заключение договора об оказании услуг по предоставлению информации — персональных данных[15]. Однако для реализации этого права субъект персональных данных должен быть заинтересован в том, чтобы разрешить использование или передачу третьим лицам своих данных в целях более широких, чем непосредственная продажа товара или оказание ему услуги. Эта заинтересованность может обретать форму дополнительных преимуществ, скидок, участия в программах лояльности, продления подписок, в некоторых случаях — оплаты передаваемых данных. Указанное изменение даст субъекту персональных данных инструмент для законного предоставления собственных данных и получения за них компенсации, а участники рынка, в свою очередь, обретут возможность законно получать информацию и ставить ее на баланс в качестве нематериального актива [Posner, Weyl, 2018].

«Согласие по умолчанию» работает с единственной целью оказания услуги или покупки товара, а согласие, предоставляемое на прочие цели, становится более осознанным со стороны субъекта персональных данных. Одновременно с этим эти изменения создают более прозрачные правила работы с персональными данными для компаний. Большое количество запрошенных согласий не обеспечивает надежную защиту субъекта персональных данных, однако увеличивает административную нагрузку на компании и повышает риск того, что контролирующий орган определит, что компания нарушила эти сложные и часто противоречащие друг другу правила[16].

Негативные (темные) практики при сборе персональных данных. Задача цифровых компаний — получить как можно больше данных, поэтому при работе с персональными данными они применяют набор негативных практик (dark patterns)[17]. Речь идет о целом комплексе методов манипулирования пользователями, заставляющих их принимать решения, касающиеся передачи персональных данных, которые они при честном и прозрачном подходе со стороны компаний принимать бы не стали [Зубофф, 2024; 2025]. Клиенты цифровых компаний могут быть поставлены в положение, когда не могут отказаться от принятия пользовательского соглашения, если хотят продолжать использовать сервис. Интерфейс сервиса может быть организован таким образом, что

[15] В соответствии со ст. 783.1 ГК РФ.
[16] См., например, Постановление Верховного суда РФ от 12.07.2024 № 5-АД24-74-К2.
[17] Dark commercial patterns. OECD Digital Economy Papers. No 336. October 2022.

пользователь в большинстве случаев принимает условия соглашения о сборе данных по ошибке — такая схема эффективно работает примерно для четверти пользователей [Luguri, Strahilevitz, 2021].

Представляется, что Роскомнадзору совместно с ФАС целесообразно отслеживать подобные негативные практики, вести их перечень и регулярно выпускать рекомендации по противодействию им для поставщиков и потребителей цифровых услуг.

Ценовая дискриминация потребителя. Необходимо изменение подходов к антимонопольному регулированию в целях ограничения практики ценовой дискриминации, которая проводится путем использования индивидуализированного динамического ценообразования на основе цифровых профилей потребителей товаров и услуг. Собирая персональные данные о потребителях, алгоритмы порождают ценовую дискриминацию, основанную на предполагаемой готовности человека платить [Gal, Rubinfeld, 2019; Porat, 2025].

Например, история покупок пользователя служит сигналом о готовности платить, на основе чего ему предлагаются скидки лояльности, купоны и пр. [Acquisti, Varian, 2005]. При анализе поведения покупателя по просмотрам веб-страниц, по кликам могут определяться его предпочтения, семейный статус, примерный возраст и пр. С учетом этого с некоторых потребителей может взиматься более высокая плата, чем с других, за тот же продукт [Shiller, 2014]. Например, авиакомпании анализируют данные о покупательском поведении клиентов, их предпочтениях и времени бронирования, чтобы устанавливать цены, максимально соответствующие готовности клиента платить [Krämer et al., 2018]. Ценовая дискриминация пользователей не только позволяет предприятиям, обладающим рыночной силой, изымать потребительский излишек, но и, предлагая специальные цены для новых клиентов, переманивать их у предприятий-конкурентов [Fudenberg, Villas-Boas, 2006].

Несмотря на то что ценовая дискриминация выгодна части потребителей (по некоторым оценкам, около 60% потребителей получают выгоду от снижения персонализированных цен), цены на товары и услуги, продаваемые на рынках, где производители обладают рыночной силой, не должны изменяться по решению производителя [Dubé, Misra, 2023]. Даже если предприятие за счет использования прогнозов поведения потребителя может практиковать совершенную ценовую дискриминацию (при этом, как известно, не возникает безвозвратных потерь общественного благосостояния), перераспределение потребительского излишка в пользу производителя носит несправедливый характер. Напри-

мер, в США 78% респондентов не хотели бы получать индивидуальные скидки, если эти скидки основываются на том, что продавец следит за их активностью на сайтах [Turow, 2009].

Динамическая балансировка спроса и предложения при наличии монопольной власти у производителя или цифровой платформы нарушает принципы справедливости, если общество считает, что у соответствующих товаров и услуг есть свойства мериторности.

Дискриминация лица по социальным признакам. Развитие технологии искусственного интеллекта повышает риски использования персональных данных для дискриминации определенных групп граждан. Предвзятость, заложенная в алгоритмы и применяемая в различных отраслях, может угрожать целым группам населения, вызывая за счет нарушения их прав совершенно непредсказуемые последствия [O'Neil, 2016].

Такое положение может быть обусловлено, например, отсутствием социального и человеческого контекста в некоторых видах решений, принимаемых в отношении человека алгоритмами или с использованием алгоритмов. Например, в поисковых системах алгоритмом могут приниматься решения о необъективной приоритетной выдаче тех или иных результатов в отношении конкретного пользователя [Noble, 2018].

Алгоритмы, обученные на исторических данных, могут непреднамеренно унаследовать и усилить существующие социальные предубеждения. Так, автоматизированные системы оценки кредитоспособности снижают субъективность процесса принятия решений, но при этом существует риск усиления предубеждений, если алгоритмы обучены на исторических данных, содержащих дискриминационные элементы [Garcia et al., 2024].

Уязвимые группы населения особенно подвержены негативным эффектам применения искусственного интеллекта. Предиктивные модели и алгоритмы могут маркировать бедных пользователей как объект рискованных инвестиций или как проблемных родителей, что может влиять на возможность получения такими лицами услуг страхования, кредитов или социальной помощи [Eubanks, 2018].

Развитие моделей искусственного интеллекта усиливает риски скрытой и труднообнаружимой дискриминации, поскольку алгоритмы могут использовать персональные данные для принятия решений, неочевидно ущемляющих права отдельных лиц и групп, например решений об отказе в приеме на работу [Wachter et al., 2021]. Близким понятием является так называемая прокси-дискриминация, при которой дискриминирующие признаки учитываются не напрямую, а опосредованно через предпочтения пользователей,

когда алгоритм адаптируется к поведению пользователей, а это поведение носит дискриминационный характер.

Таким образом, развитие моделей искусственного интеллекта и алгоритмов машинного обучения увеличивает риски дискриминации в случае, когда персональные данные используются для принятия решений моделями, обученными на неполных, предвзятых или исторически искаженных выборках [Mehrabi et al., 2021]. Поэтому недопустимо бесконтрольное использование моделей распознавания людей при обвинении их в совершении преступления в силу существенной вероятности ошибки [Angwin et al., 2016].

3. Ключевые проблемы и решения для развития рынков

Недостаточная защита прав на базы данных. Формирование баз данных, включающих персональные данные, регламентируется государством с помощью законодательства о защите персональных данных. Кроме того, порядок доступа к базам данным регламентируется гражданским законодательством. К таким активам применимы нормы и принципы защиты интеллектуальной собственности. Однако их использование сдерживается тем, что, во-первых, определение понятия «база данных»[18] толкуется чрезмерно ограничительно и, как следствие, права интеллектуальной собственности владельца базы данных ограничены тем, что́ будет считаться частью этой базы данных. Сегодня это понятие не включает в себя «данные», «сведения», а лишь «совокупность самостоятельных материалов». Во-вторых, те данные, которые собрала компания и которые она считает своей собственностью, по закону не всегда фактически могут принадлежать только ей. Если часть данных являются персональными, то субъект данных может воспользоваться своим правом на их перенос, исправление или удаление. Часть этих данных может принадлежать другим хозяйствующим субъектам, которые их создали (как, например, данные продавцов на цифровой платформе — маркетплейсе) [Lanier, 2013; Posner, Weyl, 2018].

На практике права компаний на базы данных (их содержание) защищаются, если их создание потребовало существенных затрат. В таких случаях должно быть предусмотрено соглашение о распределении прибыли от использования этих данных [Раджан, 2025]. Российская судебная практика показывает, что компании не всегда могут доказать факт инвестиций в создание баз данных,

[18] Ст. 1260 ГК РФ: «Базой данных является представленная в объективной форме совокупность самостоятельных материалов (статей, расчетов, нормативных актов, судебных решений и иных подобных материалов), систематизированных таким образом, чтобы эти материалы могли быть найдены и обработаны с помощью электронной вычислительной машины (ЭВМ)».

а значит, защитить свои исключительные права[19]. Кроме того, проблемы могут возникнуть при охране исключительных прав на большие данные, так как в соответствии с российским законодательством одной из характеристик базы данных является ее систематизированность, а большие данные по своей природе таковыми не являются [Войниканис, 2020].

По аналогии с патентами может быть установлен ограниченный срок исключительных прав на использование определенных агрегированных наборов данных, собранных компанией (то есть неперсональных). Возможно также, по аналогии с существующим институтом принудительного лицензирования, что в случаях, когда база данных представляет общественный интерес и нужна для решения социально-экономических задач, право на ее использование может быть предоставлено лицу по решению суда.

Монополизация рынков. Важной проблемой организации отраслевых рынков, порожденной развитием цифровизации, стало нарушение конкуренции. Компании, первыми вышедшие на соответствующий рынок или представляющие собой крупные экосистемы с большим количеством сервисов, позволяющих аккумулировать большие массивы данных, имеют существенные преимущества перед новыми предприятиями, что создает барьеры для конкуренции и свободного входа новых компаний на рынок.

Органы антимонопольного регулирования должны учитывать объем и уникальность данных при оценке сделок слияний и поглощений, рассматривать обязательства по предоставлению доступа к данным для доминирующих игроков, бороться с практиками «огороженных садов», ограничивающими передачу данных. Например, в Законе о конкуренции Германии накопленные данные являются одним из признаков определения доминирующего положения платформы[20]. Также оценивается возможность объединять данные из различных источников (разных сервисов или дочерних сервисов). В Китае антимонопольный орган при оценке товарных рынков, на которых работает платформа, также оценивает доступ к данным, возможности их передачи[21].

С целью регулирования деятельности цифровых платформ за последние пять лет европейским законодательством был принят ряд актов, направленных на ограничение возможности неконтролируемого сбора и оборота данных пользователей: Регламент ЕС

[19] См., например: дело «ВКонтакте» против «Дабл Дата», дело № А40-18827/2017. https://www.sudact.ru›arbitral/doc/8aoBRhz9tqY4/.

[20] Gesetz gegen Wettbewerbsbeschränkungen – GWB. Item 3a(4) Section 18, Item 3a(4). https://www.gesetze-im-internet.de/englisch_gwb/englisch_gwb.html#p0027.

[21] The Anti-Monopoly Committee of the State Council on the Platform Economy. Anti-Monopoly Guidelines. 2021. https://www.gov.cn/xinwen/2021-02/07/content_5585758.htm.

2022/1925[22], Регламент ЕС 2022/868[23], Регламент ЕС 2023/2854[24]. Например, ЕС считает злоупотреблением доминирующим положением, если крупные платформы для конкуренции со своими бизнес-пользователями (например, продавцами на маркетплейсах) используют какие-либо закрытые данные, которые были сгенерированы этими бизнес-пользователями (например, переходы по ссылкам, поиск, данные просмотра, голосовые данные и пр.). Платформы не могут использовать такие данные для продвижения, например, собственных товаров или услуг в ущерб пользователям.

Высказанные соображения требуют со стороны ФАС РФ оценки отмеченных преимуществ в виде накопленных персональных данных при определении доминирующего положения на рынке и рассмотрении вопросов о разрешении осуществления различного рода сделок слияний и поглощений в тех сегментах экономики, где оперируют крупные цифровые компании.

Низкий уровень обмена данными между компаниями и компаниями и государством. Компании и организации не только сами собирают и обрабатывают данные для повышения эффективности своей работы, но и заинтересованы в получении данных, в том числе персональных, собираемых как государством, так и другими компаниями. Стимулирование обмена данными на уровне компаний и их клиентов или между отдельными компаниями предполагает формирование практик, которые могут развиться в масштабные проекты национального и регионального уровней, такие как организация партнерств для международного обмена данными или создание дата-хабов в приоритетных направлениях развития. Например, в ЕС организуются общеевропейские пространства данных по четырнадцати направлениям, среди которых здравоохранение, энергетика и др.[25] В ЕС также создаются хабы для поддержки цифровых инноваций, включая проекты по управлению данными[26]. Так, существует дата-хаб, который собирает данные для построения прогноза урожая в регионе[27].

---

[22] Устанавливает специальные требования и ограничения в деятельности компаний в статусе гейткипера (статус, определяемый по критериям количества пользователей, торговому обороту). Под регулирование попали такие крупные компании, как *Alphabet* (все сервисы Google, YouTube), *Amazon, Apple, Meta* (запрещена на территории РФ по основаниям осуществления экстремистской деятельности), *Microsoft, Tiktok* и пр.

[23] Устанавливает механизмы обмена данными между различными субъектами. Например, институт «дата-альтруизма» (см. далее) повышает доступность персональных данных для таких общественно значимых целей, как медицинские исследования.

[24] Устанавливает обязательство поставщиков продуктов на основе интернета вещей (IoT) предоставлять данные, собранные с помощью IoT, их пользователям.

[25] Common European Data Spaces. https://digital-strategy.ec.europa.eu/en/policies/data-spaces.

[26] European Digital Innovation Hubs (EDIH). European Commission. https://digital-strategy.ec.europa.eu/en/policies/edihs.

[27] European Digital Innovation Hubs (EDIH) Catalogue. European Commission. https://european-digital-innovation-hubs.ec.europa.eu/edih-catalogue.

Не только компании, но и государство заинтересовано в данных, собираемых компаниями. Цели государства могут быть самыми разными: совершенствование государственного управления, предоставление переданных компаниями данных в общественный доступ, обеспечение безопасности государства, предоставление данных научным организациям, предоставление данных зарубежным правительствам в рамках автоматизированного налогового обмена или в рамках оказания помощи в расследовании противоправных действий.

Доступ государства и его ведомств к персональным данным, собираемым компаниями, должен иметь четкие законодательные основания для каждого типа передаваемых данных. Государство должно стимулировать раскрытие данных предприятиями. Одним из возможных механизмов является заключение соглашений между компаниями и государством об обмене данными. Соглашения должны определять цели раскрытия данных (например, научные исследования), степень раскрытия, порядок доступа третьих лиц к данным. Для стимулирования участия предприятий в этом процессе государство может осуществлять необходимые инвестиции в инфраструктуру хранения, обмена и обработки данных. Кроме того, данные, которые связаны с рисками раскрытия персональных данных и коммерческой тайны, могут предоставляться государству через безопасные среды, которые предотвращают их копирование. Механизмы передачи данных государству должны включать платформы защищенного обмена, API с контролем доступа, системы анонимизации или агрегации перед передачей. В ряде случаев целесообразна компенсация компаниям затрат за выполнение государственных запросов.

Данные для научных исследований. Для секторов исследований и инноваций улучшение доступа к данным непосредственно влияет на скорость и качество развития научной работы. Так, в России развитие технологий на основе искусственного интеллекта в области медицины получило значительную поддержку в рамках экспериментального правового режима, для которого на уровне федерального законодательства предусматривался специальный доступ к персональным данным[28]. Однако научным организациям нужен более широкий доступ к данным.

Необходимо соблюдение баланса между обеспечением доступа к данным в научных целях и защитой прав субъектов и коммерческих интересов компаний. При этом необходимо применение стандартов высокого уровня для анонимизации, использование

[28] См. п. 9.1 ч. 1 ст. 6 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»; Федеральный закон от 31.07.2020 № 258-ФЗ «Об экспериментальных правовых режимах в сфере цифровых инноваций в Российской Федерации».

безопасной среды обработки, обеспечение доступа к данным без возможности их выгрузки. Следует использовать специальную форму широкого согласия (то есть согласия на все цели, для которых разумно ожидать использование собранных данных) субъектов на использование их данных в будущих исследовательских проектах определенной сферы. Важно обеспечить обязательный этический надзор и предусматривать обязательства по публикации научных результатов и методологии исследований [Colavizza et al., 2024; Huang et al., 2024].

Информация, необходимая для научных исследований, разрознена (для проведения исследований иногда необходимо использовать множество различных источников данных, не сопоставимых между собой); отсутствует удобный инструментарий для поиска как внутри каждого конкретного источника, так и между ними; нет архивов данных (как статистических, так и административных); не зафиксированы ряды сопоставимых показателей после изменения методики их расчета. В качестве важной меры, направленной на улучшение описанной ситуации, большинство развитых стран (например, Австралия, Великобритания[29], Германия, Канада[30], Нидерланды, Франция, Швеция[31]) создали агрегаторы социально-экономической информации, а некоторые (например, Германия) — любой статистической информации независимо от области научного знания. Все такие проекты создаются и развиваются либо на базе консорциумов, включающих университеты, научные центры, органы официальной статистики, министерства (например, в Германии[32], Франции[33]), либо на базе центров, которые сами по себе являются такими консорциумами (например, в Австралии[34]).

В российских условиях для обеспечения данными научных исследований так же, как и в других развитых странах, целесообразно создание национального центра данных. Центр должен объединить усилия держателей данных в публичном и частном секторах по работе с данными, необходимыми для различных отраслей знания, общественных и естественно-научных исследований, обеспечить исследователей большими данными. Для эффективной работы с данными в исследовательских целях следует на законодательном уровне установить возможность предоставления персональных данных для общественно значимых

[29] The UK Data Service. https://ukdataservice.ac.uk/.

[30] Odesi. Canadian social science data repository. https://odesi.ca/en.

[31] Swedish National Data Service. https://snd.se/en.

[32] KonsortSWD. Data in the social, behavioral, educational, and economic sciences. https://www.konsortswd.de/en/.

[33] DB. Nomics. The World's Economic Database. https://db.nomics.world/.

[34] Australian Research Data Commons. https://ardc.edu.au/.

целей (научных исследований) на основе специальной формы согласия.

Трансграничный оборот данных для международной торговли. Трансграничный оборот данных происходит как между государствами, так и между хозяйствующими субъектами разных стран. И в первом, и во втором случае персональные данные составляют существенную часть обмениваемых данных. Однако различия регуляторных режимов вызывают конфликты юрисдикций. Например, правовой режим данных, основанный на европейском подходе, накладывает на контролеров данных обязательства по обеспечению целого ряда прав субъектов персональных данных, от права на отзыв согласия до права на получение уведомления о нарушении безопасности данных. В США на уровне штатов установлен противоположный подход: однажды предоставленные персональные данные поступают в полное распоряжение компании, поэтому права субъекта персональных данных практически ограничены правом распорядиться судьбой данных на этапе их сбора, например запретить их продажу третьим лицам. Примечательно, что в странах БРИКС, включая Россию, законодатели отдают предпочтение европейской модели, что выражается в установлении как можно большего круга прав субъекта персональных данных [Sharma, 2024].

Разнообразие подходов к регулированию создает проблемы для международной торговли не только цифровыми товарами и услугами, но и обычными товарами и услугами, поскольку современная мировая торговля также требует передачи данных между участниками внешнеэкономической деятельности, в значительной степени опирается на интернет вещей и цифровую логистику, обеспечивающую оптимизацию цепочек поставок с помощью трекинга и анализа данных. Соответственно, встает вопрос о согласованном единообразном регулировании трансграничного оборота данных, в первую очередь персональных, не возлагающем на участников внешнеэкономической деятельности излишнего бремени расходов. Например, для преодоления противоречий, накладывающих ограничения на возможность трансграничной передачи данных между юрисдикциями, ЕС и США неоднократно согласовывали условия трансграничных потоков данных.

Могут быть предложены два направления совершенствования порядка защиты данных при их трансграничной передаче. Первое заключается в обеспечении гармонизации законодательств о персональных данных. Следует стремиться к гармонизации стандартов, сближению подходов по защите персональных данных и потребительских прав, кибербезопасности, использованию надежных механизмов трансграничной передачи, таких как стан-

дартные договорные клаузулы (например, предусмотрено статьей 46(2)(c) Регламента 2016/679), обязательные корпоративные положения (например, статья 47 Регламента 2016/679), сертификация (статья 42 Регламента 2016/679). Необходима разработка и заключение международных соглашений для взаимного признания адекватности защиты (статья 45 Регламента 2016/679), заключение соглашений о свободном потоке данных с надежными правовыми гарантиями. Таким является, например, Соглашение ЕС и Японии об экономическом партнерстве, включившее поправки о трансграничных потоках данных в 2023 году[35].

Второе направление заключается в развитии международного сотрудничества компетентных органов для осуществления взаимных консультаций, обмена информацией, рассмотрения жалоб, оказания помощи в проведении расследований, применении санкций и возмещении ущерба.

Что касается российского законодательства о трансграничной передаче данных, то ограничительные меры в отношении трансграничных потоков должны быть пропорциональны угрозам и рискам, возникающим при их осуществлении. В настоящее время российские компании обязаны уведомлять Роскомнадзор о намерении передачи данных в другую страну до ее осуществления[36]. Фактически возможность передавать данные зависит от позиции Роскомнадзора: принять уведомление или запретить передачу. Оператор данных может приступить к трансграничной передаче данных только спустя десять рабочих дней после передачи уведомления в Роскомнадзор, если за этот срок не было принято решения о запрете такой передачи. Риск этой нормы для бизнеса заключается в неопределенности, вызываемой возможным отрицательным решением исполнительного органа. Представляется целесообразным определить перечень стран, для которых уведомление о передаче персональных данных может осуществляться уже после их передачи.

4. Основные предложения по развитию регулирования данных

Предлагаемый подход к совершенствованию порядка использования данных в России предполагает решение двух ключевых задач: повышение личного контроля гражданина над его персональными данными и обеспечение конкурентных условий в циф-

---

[35] Protocol Amending the Agreement Between the European Union and Japan for an Economic Partnership — Data Flows and Personal Data Protection. 8 December 2023. https://circabc.europa.eu/ui/group/09242a36-a438-40fd-a7af-fe32e36cbd0e/library/f9c7b4f0-ea0f-467a-bb9e-208013b07312/details?download=true.

[36] Ч. 3 ст. 12 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных».

ровой экономике. Решение этих задач должно основываться на реализации права гражданина на конфиденциальность личной жизни, развитии рынка данных для компаний, расширении использования данных государства и бизнеса для принятия управленческих решений, проведении научных исследований. В соответствии с предлагаемыми подходами целесообразно внесение важных изменений, как минимум, в следующие нормативно-правовые акты:

— в Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» — в части обновления подхода к институту согласия субъекта персональных данных: (1) в случаях, когда персональные данные необходимы для оказания услуги или продажи товара, которые регламентируются государством (то есть необходимы для заключения и (или) исполнения договора), необходимо перейти от требования явного получения согласия от субъекта персональных данных согласно пункту 1 части 1 статьи 6 и части 1 статьи 9 ФЗ № 152 к его выражению в конклюдентной форме согласно пункту 5 части 1 статьи 6 ФЗ № 152; (2) расширение прав субъекта персональных данных, в том числе права на перенос данных; (3) введение упрощенной процедуры уведомления Роскомнадзора о намерении осуществлять трансграничную передачу данных для государств широко сотрудничающих с Россией;
— в Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» — в части введения права субъекта персональных данных на заключение договора об оказании услуг по предоставлению информации о своих персональных данных (в соответствии со статьей 783.1 ГК РФ);
— в Закон РФ от 07.02.1992 № 2300-1 (ред. от 08.08.2024) «О защите прав потребителей» — в части ограничения недобросовестных практик сбора и обращения с персональными данными пользователей;
— в Федеральный закон от 26.07.2006 № 135-ФЗ «О защите конкуренции» — в части введения оценки порядка использования персональных данных при антиконкурентных расследованиях и ограничения практики использования больших данных для построения и обучения ценовых алгоритмов;
— в нормативные акты Правительства РФ, регламентирующие практику разработки и регулярного обновления стандартов безопасности процессов сбора, обработки и обмена данными, критерии оценки соответствия мер безопасности информационным рискам бизнеса, модельные соглашения о взаимодействии по обмену данными.

Литература

1. *Асадуллина А. В.* Конкуренция между владельцами цифровых платформ в мировой экономике // Российский внешнеэкономический вестник. 2020. № 1. С. 51–59. DOI: 10.24411/2072-8042-2020-00005.
2. *Войниканис Е. А.* Регулирование больших данных и право интеллектуальной собственности: общие подходы, проблемы и перспективы развития // Закон. 2020. № 7. С. 135–156.
3. *Зубофф Ш.* Надзорный капитализм или демократия / пер. с англ. А. Смирнова. М.: Издательство Института Гайдара, 2025.
4. *Зубофф Ш.* Эпоха надзорного капитализма / пер. с англ. А. Васильева. М.: Издательство Института Гайдара, 2024.
5. *Иванов С. Л., Устинова К. А.* Зарубежный опыт цифровизации предпринимательского сектора и возможности его применения в России // Экономика, предпринимательство и право. 2025. Т. 15. № 3. С. 1453–1474. DOI: 10.18334/epp.15.3.122488.
6. *Остапович И. Ю., Шахновская И. В.* Право на забвение в контексте развития концепции цифрового суверенитета личности // Вестник Полоцкого государственного университета. Серия D: Экономические и юридические науки. 2024. № 4. С. 100–103.
7. *Паркер Г. Г., Ван Алстайн М. У., Чоудхари С. П.* Революция платформ: как сетевые рынки меняют экономику – и как заставить их работать на вас / пер. с англ. Е. Пономаревой. М.: Альпина Паблишер, 2017.
8. *Раджан Р.* Третья опора: как рынки и государства пренебрегают сообществом / пер. с англ. С. Моисеева. М.: Издательство Института Гайдара, 2025.
9. *Селюк А. С.* Защита персональных данных в цифровом пространстве // Вестник Университета им. О. Е. Кутафина. 2023. № 2(102). С. 110–119. DOI: 10.17803/2311-5998.2023.102.2.110-119.
10. *Acquisti A., Varian H. R.* Conditioning Prices on Purchase History // Marketing Science. 2005. Vol. 24. No 3. P. 367–381. DOI: 10.1287/mksc.1040.0103.
11. *Angwin J., Larson J., Mattu S., Kirchner L.* Machine Bias: There's Software Used Across the Country to Predict Future Criminals. And It's Biased Against Blacks // ProPublica. 2016. https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing.
12. *Armstrong M.* Competition in Two-Sided Markets // The RAND Journal of Economics. 2006. Vol. 37. No 3. P. 668–691. DOI: j.1756-2171.2006.tb00037.x.
13. *Colavizza G., Cadwallader L., LaFlamme M., Dozot G., Lecorney S., Rappo D., Hrynaszkiewicz I.* An Analysis of the Effects of Sharing Research Data, Code, and Preprints on Citations // Computer Science. 2024. https://arxiv.org/abs/2404.16171.
14. *Dubé J.-P., Misra S.* Personalized Pricing and Consumer Welfare // Journal of Political Economy. 2023. Vol. 131. No 1. P. 131–189. DOI: 10.1086/720793.
15. *Evans D. S., Schmalensee R.* Matchmakers: The New Economics of Multisided Platforms. Brighton: Harvard Business Review Press, 2016.
16. *Eyal N.* Hooked: How to Build Habit-Forming Products. New York: Portfolio, 2014.
17. *Fudenberg D., Villas-Boas J. M.* Behavior-Based Price Discrimination and Customer Recognition // Handbook of Economics and Information Systems. Vol. 1. Leeds: Emerald Publishing Ltd., 2006. P. 377–436.
18. *Gal M. S., Rubinfeld D. L.* The Hidden Costs of Free Goods: Implications for Antitrust Enforcement // Antitrust Law Journal. 2019. Vol. 80. No 2. P. 521–562. DOI: 10.2139/ssrn.2529425.
19. *Garcia A. C. B., Garcia M. G. P., Rigobon R.* Algorithmic Discrimination in the Credit Domain: What Do We Know About It? // AI & Society. 2024. Vol. 39. P. 2059–2098. DOI: 10.1007/s00146-023-01676-3.
20. *Huang C. K., Neylon C., Montgomery L., Hosking R., Diprose J., Handcock R., Wilson K., Kamak R.* Open Access Research Outputs Receive More Diverse Citations // Scientometrics. 2024. No 129. P. 825–845. DOI: 10.1007/s11192-023-04894-0.

21. *Krämer A., Friesen M., Shelton T.* Are Airline Passengers Ready for Personalized Dynamic Pricing? A Study of German Consumers // Journal of Revenue and Pricing Management. 2018. Vol. 17. No 2. P. 115–120. DOI: 10.1057/s41272-017-0122-0.
22. *Lanier J.* Who Owns the Future? New York: Simon and Schuster, 2013.
23. *Luguri J., Strahilevitz L. J.* Shining a Light on Dark Patterns // Journal of Legal Analysis. 2021. Vol. 13. No 1. P. 43–109. DOI: 10.2139/ssrn.3431205.
24. *Mehrabi N., Morstatter F., Saxena N., Lerman K., Galstyan A.* A Survey on Bias and Fairness in Machine Learning // ACM Computing Surveys. 2021. Vol. 54. No 6. P. 1–35. DOI: 10.1145/3457607.
25. *Noble S. U.* Algorithms of Oppression: How Search Engines Reinforce Racism. New York: New York University Press, 2018.
26. *O'Hara K., Shadbolt N.* The Spy in the Coffee Machine: The End of Privacy as We Know It. Oxford: Oxford University Press, 2008.
27. *O'Neil C.* Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy. New York: Crown Publishing Group, 2016.
28. *Porat H.* Algorithmic Personalized Pricing in the United States: A Legal Void // The Cambridge Handbook of Algorithmic Price Personalization and the Law / ed. by F. Esposito, M. Grochowski. Cambridge: Cambridge University Press, 2025.
29. *Posner E. A., Weyl E. G.* Radical Markets: Uprooting Capitalism and Democracy for a Just Society. New Jersey: Princeton University Press, 2018.
30. *Rochet J.-C., Tirole J.* Platform Competition in Two-Sided Markets // Journal of the European Economic Association. 2003. Vol. 1. No 4. P. 990–1029. DOI: 10.1162/154247603322493212.
31. *Sharma A., Sharma R.* Comparative Analysis of Data Protection Laws and AI Privacy Risks in BRICS Nations: A Comprehensive Examination // Global Journal of Comparative Law. 2024. Vol. 13. No 1. P. 56–85. DOI: 10.1163/2211906X-13010003.
32. *Shiller B. R.* First-Degree Price Discrimination Using Big Data. Brandeis University. Working Paper No 109. 2014.
33. *Solve D. J.* The Digital Person: Technology and Privacy in the Information Age. New York: New York University Press, 2004.
34. *Turow J., King J., Hoofnagle C. J., Bleakley A., Hennessy M. H.* Americans Reject Tailored Advertising and Three Activities That Enable It // Information Privacy Law eJournal. 2009. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1478214.
35. *Wachter S., Mittelstadt B., Russell C.* Why Fairness Cannot Be Automated: Bridging the Gap Between EU Non-Discrimination Law and AI // Computer Law & Security Review. 2021. No 41. Article 105567. DOI: 10.1016/j.clsr.2021.105567.
36. *Wall D. S.* Cybercrime: The Transformation of Crime in the Information Age. 2nd ed. Cambridge: Wiley; Polity Press, 2024.

References

1. Asadullina A. V. Konkurentsiya mezhdu vladel'tsami tsifrovykh platform v mirovoy ekonomike [Competition Between Digital Platform Owners in the Global Economy]. *Rossiyskiy vneshneekonomicheskiy vestnik [Russian Foreign Economic Bulletin]*, 2020, no. 1, pp. 51-59. DOI: 10.24411/2072-8042-2020-00005. (In Russ.)
2. Voynikanis E. A. Regulirovanie bol'shikh dannykh i pravo intellektual'noy sobstvennosti: obshchie podkhody, problemy i perspektivy razvitiya [Big Data Regulation and Intellectual Property Law: General Approaches, Problems, and Development Prospects]. *Zakon [Law]*, 2020, no. 7, pp. 135-156. (In Russ.)
3. Zuboff Sh. Surveillance Capitalism or Democracy? The Death Match of Institutional Orders and the Politics of Knowledge in Our Information Civilization. *Organization Theory*, 2022, vol. 3, no. 3. DOI: 10.1177/26317877221129290.
4. Zuboff Sh. *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power.* New York, Public Affairs, 2019.

5. Ivanov S. L., Ustinova K. A. Zarubezhnyy opyt tsifrovizatsii predprinimatel'skogo sektora i vozmozhnosti ego primeneniya v Rossii [International Experience in Digitalization of the Business Sector and the Possibilities of Its Application in Russia]. *Ekonomika, predprinimatel'stvo i pravo [Economics and Business Law]*, 2025, vol. 15, no. 3, pp. 1453-1474. DOI: 10.18334/epp.15.3.122488. (In Russ.)
6. Ostapovich I. Yu., Shakhnovskaya I. V. Pravo na zabvenie v kontekste razvitiya kontseptsii tsifrovogo suvereniteta lichnosti [The Right to Be Forgotten in the Context of the Development of the Concept of Digital Sovereignty of the Individual]. *Vestnik Polotskogo gosudarstvennogo universiteta. Seriya D: Ekonomicheskie i yuridicheskie nauki [Bulletin of Polotsk State University. Series D: Economic and Legal Sciences]*, 2024, no. 4, pp. 100-103. (In Russ.)
7. Parker G. G., *The Platform Revolution: How Network Markets Are Changing the Economy - And How to Make Them Work for You.* New York, W. W. Norton & Company, 2016.
8. Rajan R. *The Third Pillar: How Markets and States Neglect Community.* New York, Penguin Press, 2019.
9. Selyuk A. S. Zashchita personal'nykh dannykh v tsifrovom prostranstve [Protection of Personal Data in the Digital Space]. *Vestnik Universiteta im. O. E. Kutafina [Bulletin of the O. E. Kutafin University*], 2023, vol. 2, no. 102, pp. 110-119. DOI: 10.17803/2311-5998.2023.102.2.110-119. (In Russ.)
10. Acquisti A., Varian H. R. Conditioning Prices on Purchase History. *Marketing Science*, 2005, vol. 24, no. 3, pp. 367-381. DOI: 10.1287/mksc.1040.0103.
11. Angwin J., Larson J., Mattu S., Kirchner L. Machine Bias: There's Software Used Across the Country to Predict Future Criminals. And It's Biased Against Blacks. *ProPublica,* 2016. https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing.
12. Armstrong M. Competition in Two-Sided Markets. *The RAND Journal of Economics*, 2006, vol. 37, no. 3, pp. 668-691. DOI: j.1756-2171.2006.tb00037.x.
13. Colavizza G., Cadwallader L., LaFlamme M., Dozot G., Lecorney S., Rappo D., Hrynaszkiewicz I. An Analysis of the Effects of Sharing Research Data, Code, and Preprints on Citations. *Computer Science*, 2024. https://arxiv.org/abs/2404.16171.
14. Dubé J.-P., Misra S. Personalized Pricing and Consumer Welfare. *Journal of Political Economy*, 2023, vol. 131, no. 1, pp. 131-189. DOI: 10.1086/720793.
15. Evans D. S., Schmalensee R. *Matchmakers: The New Economics of Multisided Platforms*. Brighton, Harvard Business Review Press, 2016.
16. Eyal N. *Hooked: How to Build Habit-Forming Products.* New York, Portfolio, 2014.
17. Fudenberg D., Villas-Boas J. M. Behavior-Based Price Discrimination and Customer Recognition. In: *Handbook of Economics and Information Systems*. 2006, vol. 1, pp. 377-436.
18. Gal M. S., Rubinfeld D. L. The Hidden Costs of Free Goods: Implications for Antitrust Enforcement. *Antitrust Law Journal*, 2019, vol. 80, no. 2, pp. 521-562. DOI: 10.2139/ssrn.2529425.
19. Garcia A. C. B., Garcia M. G. P., Rigobon R. Algorithmic Discrimination in the Credit Domain: What Do We Know About It? *AI* & *Society*, 2024, vol. 39, pp. 2059-2098. DOI: 10.1007/s00146-023-01676-3.
20. Huang C. K., Neylon C., Montgomery L., Hosking R., Diprose J., Handcock R., Wilson K., Kamak R. Open Access Research Outputs Receive More Diverse Citations. *Scientometrics*, 2024, no. 129, pp. 825-845. DOI: 10.1007/s11192-023-04894-0.
21. Krämer A., Friesen M., Shelton T. Are Airline Passengers Ready for Personalized Dynamic Pricing? A Study of German Consumers. *Journal of Revenue and Pricing Management*, 2018, vol. 17, no. 2, pp. 115-120. DOI: 10.1057/s41272-017-0122-0.
22. Lanier J. *Who Owns the Future?* New York, Simon and Schuster, 2013.
23. Luguri J., Strahilevitz L. J. Shining a Light on Dark Patterns. *Journal of Legal Analysis*, 2021, 13(1), pp. 43-109. DOI: 10.2139/ssrn.3431205.
24. Mehrabi N., Morstatter F., Saxena N., Lerman K., Galstyan A. A Survey on Bias and Fairness in Machine Learning. *ACM Computing Surveys*, 2021, vol. 54, no. 6, pp. 1-35. DOI: 10.1145/3457607.

25. Noble S. U. *Algorithms of Oppression: How Search Engines Reinforce Racism*. New York, New York University Press, 2018.
26. O'Hara K., Shadbolt N. *The Spy in the Coffee Machine: The End of Privacy as We Know It.* Oxford, Oxford University Press, 2008.
27. O'Neil C. *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy*. New York, Crown Publishing Group, 2016.
28. Porat H. Algorithmic Personalized Pricing in the United States: A Legal Void. In: Esposito F., Grochowski M. (eds.). *The Cambridge Handbook of Algorithmic Price Personalization and the Law.* Cambridge, Cambridge University Press, 2025.
29. Posner E. A., Weyl E. G. *Radical Markets: Uprooting Capitalism and Democracy for a Just Society.* New Jersey, Princeton University Press, 2018.
30. Rochet J.-C., Tirole J. Platform Competition in Two-Sided Markets. *Journal of the European Economic Association*, 2003, vol. 1, no. 4, pp. 990-1029. DOI: 10.1162/154247603322493212.
31. Sharma A., Sharma R. Comparative Analysis of Data Protection Laws and AI Privacy Risks in BRICS Nations: A Comprehensive Examination. *Global Journal of Comparative Law*, 2024, vol. 13, no. 1, pp. 56-85. DOI: 10.1163/2211906X-13010003.
32. Shiller B. R. First-Degree Price Discrimination Using Big Data. *Brandeis University,* Working Paper no. 109, 2014.
33. Solve D. J. *The Digital Person: Technology and Privacy in the Information Age*. New York, New York University Press, 2004.
34. Turow J., King J., Hoofnagle C. J., Bleakley A., Hennessy M. H. Americans Reject Tailored Advertising and Three Activities That Enable It. *Information Privacy Law eJournal*, 2009. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1478214.
35. Wachter S., Mittelstadt B., Russell C. Why Fairness Cannot Be Automated: Bridging the Gap Between EU Non-Discrimination Law and AI. *Computer Law & Security Review*, 2021, no. 41, article 105567. DOI: 10.1016/j.clsr.2021.105567.
36. Wall D. S. *Cybercrime: The Transformation of Crime in the Information Age,* 2nd ed. Cambridge, Wiley, Polity Press, 2024.