ОТ ТЕОРИИ К ЭКОНОМИЧЕСКОЙ ПОЛИТИКЕ

А.Е. Шаститко
д.э.н., профессор, Московский государственный университет имени М.В. Ломоносова, директор Центра исследований конкуренции и экономического регулирования РАНХиГС при Президенте РФ (Москва)

А.А. Моросанова
к.э.н., н.с., Московский государственный университет имени М.В. Ломоносова, н.с., Институт прикладных экономических исследований РАНХиГС при Президенте РФ (Москва)

ДОРОГАЯ БЕСПЛАТНОСТЬ[1]

Аннотация. Цифровые платформы, как правило, предлагают свои услуги, как минимум, для одной из сторон без денежной платы, но взимая иной ресурс — информационный — в виде персональной информации и «цифровых следов», оставляемых пользователями. Механизмы, позволяющие анализировать собранную информацию, дают компаниям скрытую конкурентную силу, которая, с одной стороны, позволяет повышать эффективность, но с другой — несёт в себе потенциальные угрозы как для множества отдельных пользователей, так и для экономического благосостояния в целом. Главные исследовательские вопросы, поднимаемые в статье, относятся к наличию стимулов по сохранению или усилению приватности в интернете. Последнее касается не только пользователей, но и бизнеса, а также относится к роли государственных регуляторов данного процесса. Некоторые назревшие регуляторные решения по развитию конкурентной среды на цифровых рынках и обеспечению прозрачности процессов внутри экосистем, обсуждаемые в данной статье, могут обеспечить прогресс в плане увеличения пользовательского контроля за своей персональной информацией. Вместе с тем предполагаемые изменения приведут к возникновению дополнительных рисков в части информационной (и других аспектов) безопасности. Вопрос об обеспечении надёжности гаранта, связанный с приватностью в интернете, все равно остаётся открытым.

Ключевые слова: *приватность, цифровая экономика, персональные данные, экосистемы, платформы.*
JEL: L15, L20, L50, L86
УДК: 330.341.1, 330.342.3
DOI: 10.52342/2587-7666VTE_2024_2_56_72

ДЛЯ ЦИТИРОВАНИЯ: *Шаститко А.Е., Моросанова А.А.* Дорогая бесплатность // Вопросы теоретической экономики. 2024. №2. С. 56–72. DOI: 10.52342/2587-7666VTE_2024_2_56_72.
FOR CITATION: *Shastitko A., Morosanova A.* Expensive Free // Voprosy teoreticheskoy ekonomiki. 2024. No. 2. Pp. 56–72. DOI: 10.52342/2587-7666VTE_ 2024_2_56_72.

[1] Статья подготовлена в рамках выполнения научно-исследовательской работы государственного задания РАНХиГС.

Бесплатный сыр бывает только в мышеловке.
Народная мудрость

Введение

Само допущение о преследовании участниками экономической деятельности собственного интереса, который проявляется в том числе в стремлении к прибыли (если не в краткосрочном, то в долгосрочном плане), предполагает, что кажущиеся альтруистические устремления должны пройти проверку через призму устойчивости базовой поведенческой предпосылки экономической науки — следования собственному интересу.

Повсеместное распространение цифровых платформ и связанных с ними экосистем сопряжено со значительным распространением практики предоставления бесплатных сервисов, когда пользователи платформ (домашние хозяйства) оплачивают по нулевой денежной цене предоставляемые им услуги. Казалось бы, куда ещё дешевле? Разве что предположить, что сервисы будут доплачивать пользователям за потребление ими искомых услуг? Неужели перед нами феноменальный результат конкуренции, усиленный технологическим развитием? И возможно ли тогда такое, что сервисы, которые ориентированы на взаимодействие с несколькими группами пользователей, обеспечивают услуги по нулевой цене для всех групп? Да, такое предположение имеет право на существование, но именно как гипотеза, которую необходимо: а) объяснить; б) проверить.

Однако, как нетрудно догадаться, есть и иная картина мира, если согласиться с тем, что пользователи могут расплачиваться не только деньгами или иными конвенциальными активами с возможной их бухгалтерской оценкой. Практика демонстрирует и иные возможности, например, расплачиваться своим вниманием (и связанными с ним действиями), а также собственными данными — не только привычными идентификаторами личности, но и гораздо более широким спектром данных, на основе которых можно, применяя соответствующие алгоритмы их обработки, построить индивидуальный поведенческий профиль, с помощью которого можно как предугадывать желания пользователя (предиктивная аналитика поведения), так и подталкивать его к желаемому для контролёра доступа (gate-keeper) решению. Казалось бы, эта безобидная практика может помочь крупным компаниям лучше понимать потребности пользователя и тем самым улучшить качество его обслуживания и, соответственно, соотношение «цена-качество». Однако не всё так просто. Стоит только вдуматься, как обработка такого рода данных и их последующее использование может повлиять на потребительский выбор пользователя и распределение выигрышей между вовлечёнными в трансакции с применением цифровых алгоритмов действующими лицами (контролёрами доступа, или суперплатформами, разработчиками приложений/платформами, поставщиками услуг, пользователями).

Если раньше образованный, критически мыслящий взрослый человек с высокой вероятностью мог распознать попытки манипулирования его сознанием и поведением, то теперь эта задача многократно усложняется, поскольку эксплуатирующие и исключающие практики могут выглядеть как вполне проконкурентные и дружественные потребителю. Соответственно, для распознавания таких практик могут потребоваться специальные знания и приёмы, в том числе основанные на применении алгоритмов, препятствующих как отслеживанию поведения, сбору данных, так и их использованию. В то же время такая ситуация подталкивает к тому, чтобы вспомнить о феномене превращённых форм, о которых писал Карл Маркс в «Капитале». Только в данном случае она будет выглядеть как *наблюдаемое, осознаваемое* — прямая противоположность *сущему*.

Если мы осознаём, что практика бизнеса подводит пользователей к мысли, что «Солнце вращается вокруг Земли», то, соответственно, встают практические вопросы: 1) кто может объяснить, как выглядит реальное положение вещей; 2) почему, на каком

основании широкая публика должна доверять этим объяснениям; 3) откуда возьмутся стимулы у тех, кто может доказательно объяснить и показать, как кажущееся соотносится с сущим, тратить ресурсы на добывание и распространение знания об этом среди широких масс конечных пользователей услуг платформ и экосистем?

Сначала мы рассмотрим возможные подходы к определению ценности информации и приватности, а также аспекты, влияющие на эту оценку со стороны потребителей. Далее мы покажем, что на подходы цифровых компаний к оценке полезности информации влияют технические (раздел 2: Технические границы приватности) и институциональные (раздел 3) ограничения, которые диктуют их возможности по извлечению дополнительных экономических выгод от сбора и анализа собираемых данных (раздел 4). Однако развитие цифровых технологий не обязательно должно быть сопряжено с расширением возможностей по сбору данных, о чём свидетельствуют возникающие на рынках решения, деятельность некоммерческих организаций и государственные инициативы (раздел 5). В заключении приведены наши выводы.

Цена информации, цена приватности

Информация давно стала объектом исследования экономистов, а экономика информации — отдельным направлением, в основании которого лежат работы Фридриха фон Хайека [*Hayek*, 1945], Джорджа Стиглера [*Stigler*, 1961], Кеннета Эрроу [*Arrow*, 1962], Джорджа Акерлофа [*Akerlof*, 1970]. В начале XXI в. поднялась волна исследований эффектов от распространения цифровых технологий в современной экономике [*Varian*, 2010; *Chen, Narasimhan, Zhang*, 2001; *Taylor*, 2004]. Со становлением Web 2.0 и в связи с общим снижением уровня анонимности в интернете особо актуальными стали вопросы приватности и конфиденциальности, которые затрагивают не только правовые, но и социальные, этические и экономические аспекты. Экономика информации, как правило, рассматривает предоставление персональной информации пользователями как нахождение баланса между раскрытием информации и её защитой (и зачастую защита отождествляется с приватностью). Однако экономика приватности отталкивается от несколько иной интерпретации приватности, трактуя её не столько как отказ от предоставления данных, сколько как *контроль* над этим процессом разных сторон — пользователей, бизнеса, государства. При этом контроль может иметь различные измерения — и юридические, и технологические, и экономические.

Прежде всего речь идёт о контроле над персональными данными, т. е. «информацией, относящейся прямо или косвенно к определённому или определяемому физическому лицу (субъекту персональных данных)»[2]. Однако даже приведённое юридическое определение не даёт чётких границ между «персональной» и «неперсональной» информацией, о чём свидетельствуют не только различные подходы к проблеме в научной литературе, но и правоприменительная (в том числе судебная) практика [*Петров*, 2021]. Более того, пользователи «делятся» с цифровыми компаниями не только персональной информацией, но и оставляют «цифровые следы» («цифровые отпечатки») — данные, которые не только позволяют напрямую идентифицировать человека, но и многое но говорят о предпочтениях и поведении пользователей в интернете, а это является зачастую более ценным ресурсом для анализа со стороны бизнеса. Такие «цифровые отпечатки» не только скрыты для самих пользователей, но и в большинстве юрисдикций не попадают в сферу контроля со стороны регулятора.

[2] Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных». Статья 3.

Главный вопрос, который стоит перед исследователями в экономике информации — это вопрос о её цене и ценности, в особенности, если речь идёт о характеристиках персональных данных. С одной стороны, для компаний цена информации может быть определена разными способами. Например, информация может рассматриваться как ресурс, который помогает повысить эффективность производства основного товара/услуги через налаживание логистических цепочек, более совершенную прогнозную деятельность, что приведёт к снижению издержек. Компания может подойти к измерению цены персональной информации и схожим с затратным методом способом, включающим издержки на разработку и поддержание информационной системы, на защиту информации, а также потенциальные штрафы в случае «утечек».

Альтернативную цену информации можно искать на «чёрном рынке» — через стоимость «утекших» баз данных. На такую цену влияют множество факторов — полнота и глубина базы, её актуальность и тип информации. Согласно исследованиям цена за одну строчку может колебаться от 5 до 30 руб.[3] Есть примеры как бесплатного распространения актуальных баз данных, так и обратной ситуации — большой стоимости «старых» баз. Однако эти оценки мало что могут сказать о реальной стоимости информации для бизнеса. Во-первых, цена на «чёрном рынке» прежде всего ориентирована на спрос со стороны мошенников или иных лиц, преследующих противозаконные цели, а во-вторых, здесь нельзя найти отражения процессов, которые происходят внутри компании: как эта информация «перерабатывается» (возможно, для многих целей одновременно) и анализируется.

С точки зрения пользователей, попытки оценить собственную информацию являются сложной задачей, которая зависит не только от моральных убеждений, но и от контекста — внешних условий и ситуации, в которой пользователь оказывается. В этой связи часто упоминают парадокс конфиденциальности (privacy paradox [*Marthews, Tucker*, 2019]), который отражает расхождение между декларируемыми ценностями потребителя (заинтересованностью в защите информации или даже полной конфиденциальности) и выявленными действиями (т. е. фактическим поведением в интернете, связанным с предоставлением доступа к данным). Согласно оценкам ВЦИОМ, большинство россиян настороженно относятся к предоставлению информации и частным компаниям, и государственным организациям (в том числе размещению её на портале госуслуг): 52% опрошенных не готовы делиться персональными данными ни с какими сервисами[4]. В то же время число пользователей портала Госуслуг превысило 110 млн пользователей[5], что составляет около 75% от населения РФ[6]. Можно учесть, что в число пользователей портала могут входить и иностранные граждане (но для регистрации требуется российский мобильный телефон и СНИЛС), а также, что доступ к интернету имеет около 81% населения[7]. Даже с учётом этих корректировок видно, что, несмотря все опасения, население оставляет свои очень чувствительные персональные данные на значимых ресурсах вопреки заявленным предпочтениям о конфиденциальности.

Если рассматривать парадокс конфиденциальности с точки зрения экономической теории, он перестаёт быть «парадоксом», а становится отражением ограничено-рационального поведения индивидуумов. Пользователи не только имеют ограниченное представле-

---

[3] Эксперты подсчитали, сколько стоят личные данные россиян на чёрном рынке // ПРАЙМ. URL:https://1prime.ru/telecommunications_and_technologies/20210721/834254826.html (дата обращения: 03.03.2024).

[4] Экономика должна быть персональной // Коммерсантъ. URL:https://www.kommersant.ru/daily?from=burger (дата обращения: 03.03.2024).

[5] Чернышенко заявил, что более 110 млн россиян зарегистрированы на «Госуслугах» // ТАСС. URL:https://tass.ru/obschestvo/19202341 (дата обращения: 03.03.2024).

[6] По данным Росстата, по состоянию на 1 января 2023 года численность постоянного населения Российской Федерации составила 146 447,4 тыс. человек.

[7] Медиаскоп. URL:https://mediascope.net/news/1681112/#:~:text=В%20первом%20полугодии%202023%20года,ниже%2C%20а%20зимой%20—%20выше (дата обращения: 03.03.2024).

ние о реальной ценности своих данных для компаний, но не знают условия их обращения и готовы ими делиться в обмен на удобство пользования сервисами. На принятие решений о предоставлении своей персональной информации влияют нижеприведенные факторы.

Отсутствие или наличие значимых альтернатив и сетевые эффекты. В некоторых сферах экономики не существует явных конкурентов-компаний (как цифровых, так и нецифровых), что не оставляет выбора потребителю не только в части выбора поставщика товара/услуги, но и условий раскрытия информации. Сетевые эффекты [*Шаститко, Маркова*, 2020], свойственные цифровым платформам, могут выступать как барьерами входа для компаний-конкурентов, так и «барьерами выхода» для потребителей.

Проблема коллективных действий и мезоинституты. Этот пункт напрямую связан с наличием компаний-контролёров доступа (gate-keeper) к определённым цифровым услугам. Подобные компании создают собственные правила (мезоинституты [*Шаститко*, *Курдин*, *Филиппова*, 2023]), которые зачастую для пользователя приобретают форму «take it or leave it» («принимай или уходи»). Пользователи не имеют возможности вступать в переговоры с контролёрами доступа по поводу правил оборота их информации. Указанные компании часто используют практику, дающую право вносить изменения в условия защиты данных без согласия потребителя, и налагают на потребителей обязательство периодически проверять наличие таких изменений, пользуясь выгодной переговорной позицией.

Сфера деятельности/область предоставления данных. Пользователи гораздо чаще обращают внимание на условия предоставления информации, если соглашение касается этого напрямую (например, при подписании условий использования антивирусной компьютерной программы или переустановки операционной системы на телефоне), но проявляют бо́льшую беспечность в сфере электронной торговли и даже медицины [*Hirschprung*, 2023].

«Глубина» запрашиваемых данных. Пользователь видит «вершину айсберга» — только те данные, которые ему требуется внести при регистрации и пользовании сервисом, но не ощущает значимости своего «цифрового следа», даже если соглашение об использовании cookies доступно в явном виде. Естественно, что при более полном раскрытии информации компаниями пользователи будут более осторожно относиться к предоставлению данных.

Оценка потребителем защищённости информации. Из-за отсутствия профильных специальных знаний уровень технической защищённости пользователи, скорее, оценивают последствия принимаемых решений, исходя из случившихся негативных явлений (утечек персональных данных). То есть всё происходит по факту наступившего — как правило, негативного — события (своего рода «ошибка выжившего» наоборот).

Осведомлённость о целях и способах использования личных данных. Здесь важно подчеркнуть, что само по себе наличие условий пользовательского соглашения не приравнивается автоматически к осведомлённости пользователей. Заинтересованные компании находятся в поиске баланса между полнотой раскрытия информации и её доступностью для прочтения. Но даже в случае достаточно подробного изложения деталей преградой к осведомлённости пользователей выступают следующие факторы:

- сложность предоставления информации, проблематичность преодоления пользователями прагматического фильтра в изучении юридических текстов, что зачастую может запутать пользователя и становится преградой к адекватному анализу раскрытой информации. В некоторых случаях это может быть элементом манипулирования пользовательскими решениями — в случаях, где акценты не расставлены на важных особенностях использования информации, а формулировки позволяют избегать юридических претензий [*Кетр*, 2020];
- размытость определений и понятий, присутствие выражений «иные цели», «иные третьи лица» и пр., которые вносят неопределённость во всё пользовательское соглашение;

- соглашения о конфиденциальности, прежде всего касаются информации, запрашиваемой у индивида в явном виде, но для компаний значимой является информация, собранная с помощью cookies — механизмов, встроенных в сайт, позволяющих отслеживать действия пользователей. При этом, как правило, информация о собираемых данных достаточно размыта. В лучшем случае даются характеристики по типу собираемых cookies (строго необходимые, статистические, технические и пр.), но без раскрытия технических характеристик.

Если рассматривать категорию «персональные данные» как благо, то можно столкнуться с множеством противоречий в интерпретации в зависимости от стороны. Для пользователя эти данные являются неотчуждаемыми, неограниченными, но с точки зрения обеспечения приватности могут быть конкурентными (пользователь может выбирать сервис, который заслуживает доверия). Для компаний-агрегаторов персональные данные неконкурентны, так как они могут собирать данные из любых источников, а сами эти данные могут дублироваться и на других платформах. Однако с точки зрения анализа ценность несут, главным образом, «цифровые следы» («цифровые отпечатки») пользователей, оставленные на сервисе компании, которые, как правило, являются уникальными для каждого ресурса.

Так же как нет единого определения «персональных данных» как блага или как товара, нет и единого рынка персональных данных [*Lane, Stodden, Bender, Nissenbaum*, 2014]. Существует несколько сегментов, на которых данные обращаются, а также имеет значение конфиденциальность: рынки данных между компаниями; рынки между потребителями и компаниями (данные в обмен на «бесплатные услуги» или персонализированный подход); рынки «конфиденциальности», на котором потребители ищут защиту своим данным и пр. Поэтому затруднено создание и применение какого-либо единого и универсального подхода к регулированию в сферах, касающихся персональных данных и/или «цифровых следов».

Технические границы нарушения (сохранения) приватности

С точки зрения стороннего наблюдателя, цифровые компании, как правило, являются «чёрными ящиками», внутри которых происходят процессы сбора, хранения, и главное — анализа персональной информации и «цифровых отпечатков», о которых этот наблюдатель либо не задумывается, либо, если и задумывается, то все равно не имеет предметного представления. Главным объектом анализа обычно выступает реклама, ибо с помощью алгоритмов можно классифицировать пользователя как представителя той или иной группы (по интересам, статусу, доходу), соответствующую определённым запросам, и тем самым обеспечить релевантность и адресность рекламы.

При этом компании держат в тайне глубину процесса сбора данных, а также способы их шифрования и защиты. Пролить свет на возможности цифровых гигантов могут утечки исходных кодов, как случилось, например, с компанией Яндекс в январе 2023 г. В сеть утекли архивы с части сервисов Яндекса, содержащие алгоритмы сбора и хранения «цифровых следов» пользователей. Эксперты в области цифровых технологий [*McCrea*, 2023] сделали следующие выводы:

- все сервисы компании (которых более 90) передают большое количество данных в единую систему Crypta, которая классифицирует пользователя по различным параметрам — не только по половозрастным характеристикам, но и по предпочтениям в музыке и кино, уровню доходов, семейному статусу и количеству детей. Система способна распознавать и объединять в одну группу семьи, находить соседей и коллег;
- данные хешируются (шифруются) — каждому пользователю присваивается определённый код, но код является уникальным и шифрование происходит непоследовательно, данные легко обратимы и сопоставимы друг с другом;

- система не хранит явные персональные данные (номер телефона, ФИО и пр.), однако позволяет при необходимости сопоставлять конкретный «цифровой след» с данными из Яндекс.Паспорт (где эти персональные данные хранятся). Более того, данные из Crypta могут синхронизироваться с данными крупных российских провайдеров (например, государственной компанией Ростелеком) за пределами сервисов Яндекса.

Компании скрывают истинную глубину сбора информации, при этом нет гарантий, что, не соглашаясь с отслеживанием определённой информации (например, геолокации), пользователь не будет найден с помощью иных данных (через сети Wi-Fi, сотовых операторов или соседства с другими устройствами). Компании, как правило, отрицают наличие каких-либо скрытых целей помимо целей таргетированной рекламы, частично же присутствующие персональные данные в «цифровых следах» оправдывают ошибками, связанными с желанием улучшить качество сервиса[8]. Однако наличие межкорпоративных связей говорит о возможности применения данных в иных целях, не прописанных в соглашении пользователя.

Даже если рассматривать улучшение эффективности таргетированной рекламы как главную и единственную цель сбора и анализа «цифровых следов», то можно наблюдать, как она способна воздействовать на выбор пользователя, просачиваясь через фильтр рефлексии и самоконтроля. Не секрет, что устройства умеют отслеживать разговоры находящихся поблизости людей, даже в «спящем» режиме, что приводит к настройке показываемой рекламы, соответствующей распознанным «тегам», ключевым словам [*Kröger, Raschke,* 2019]. Это непосредственно оказывает влияние на принимаемые индивидом решения — как осознанно, так и не осознанно. Также компании могут создавать дополнительные технологические препятствия для пользователя при использовании сервиса в случае отказа делиться какой-то информацией [*Acquisti, Taylor, Wagman,* 2016].

Главная проблема, связанная с техническими характеристиками систем отслеживания персональных данных и «цифровых следов», кроется в закрытости этих технологий не только для пользователей или регулятора, но даже для самой компании, особенно если эта компания характеризуется разветвлённой системой сервисов (таким свойством обладают в первую очередь цифровые экосистемы). Большинство данных собирается автоматически, без участия человека, так что становится трудно оценить реальное положение дел с обеспечением приватности в сфере сбора, обработки и использования данных о пользователях сервисов.

Институциональные границы нарушения (сохранения) приватности

Озабоченность нарушением приватности приводит к тому, что регуляторы ищут возможности её восстановления для пользователей и/или введения ограничений на применение технологий отслеживания.

С точки зрения теории есть три структурные альтернативы отношений регулятора, цифровых компаний и пользователей, которые соответствуют различным предпосылкам о цене информации [*Kemp*, 2020]:

- с точки зрения полной рациональности поведения конфиденциальность является осознанным выбором каждого индивида, основанным на субъективных предпочтениях. Согласно этой позиции, только небольшая группа потребителей предпочтёт приватность удобству пользования из-за рисков раскрытия информации и ненадлежащего её использования, в том числе с причинением вреда

[8] «Яндекс» раскрыл первые итоги расследования утечки кода. РБК. URL:https://www.rbc.ru/technology_and_media/30/01/2023/63d7ee2e9a794727f84e437c?from=copy (дата обращения: 03.03.2024).

пользователю. Однако, несмотря на отсутствие необходимости вводить дополнительные ограничения по использованию средств сбора и анализа данных, перед регулятором стоит вопрос о принуждении компаний раскрывать информацию об использовании данных;

- если признать существование асимметрии информации (как о ценности собираемых данных, так и о способах их защиты) и отсутствие переговорной силы у потребителей, то перед регулятором стоят вызовы не только в информационной политике, но и в разработке «компенсаторного» механизма, позволяющего возместить примерную недоплачиваемую цену потребителям за использование их данных. При этом «компенсация» не обязательно будет иметь денежную характеристику, а выражаться в предоставлении более широкого спектра персонализированных услуг, в улучшении качества услуг и товаров, а также их институциональных характеристик («бьюкененовские товары» [*Тамбовцев*, 2005; *Shastitko, Markova, Morozov*, 2022]);
- предпосылка о возможности ценового измерения персональной информации и «цифрового следа», с одной стороны, упрощает возможности по созданию механизма компенсации, так как становится возможным «доплачивать» потребителям за сбор и обработку их информации. С другой стороны, для регулятора необходимо не только добиться полного раскрытия информации компаниями о механизмах использования данных, но и обладать сопоставимыми технологическими мощностями и навыками, позволяющими контролировать выполнение компаниями установленных регуляторных требований.

Тем не менее политика по раскрытию информации для потребителя лежит в основе любой из предложенных альтернатив. Требования по снижению асимметрии информации могут также иметь различные степени.

1. Уведомление пользователя об использовании данных. В этом случае пользователю, по сути, либо предлагают контракт «take it or leave it», либо возлагают на пользователя ответственность по поиску возможностей отказаться от предоставления данных (например, на собственном сайте).

2. Предоставление информации об использовании данных в явном виде, но без расширенных подробностей о целях/качестве/количестве данных.

3. Необходимость разрешения о сборе определённой информации от пользователя. Например, в европейском Общем регламенте по защите данных (General Data Protection Regulation, GDPR) есть требование о полном предоставлении информации о типах собираемых cookies, с их описанием и характеристиками, с возможностью выбрать приемлемый вариант из «меню контрактов» (а также с возможностью так же легко отписаться от всех соглашений, как и подписаться на них).

Поскольку внимание пользователя является ограниченным ресурсом, а также из-за того, что существуют различные когнитивные искажения (например, предпочтение «status quo»), то вышеперечисленные альтернативы будут неравнозначны с точки зрения последствий для пользователей и платформ. Более того, если регулирование будет основано только на необходимости получения согласия пользователя, это может привести к ухудшению конкурентной среды на рынке. Ведь пользователи «с большей вероятностью дадут свое согласие крупным сетям с широким охватом, а не менее авторитетным фирмам» [*Campbell, Goldfarb, Tucker*, 2015. P. 64], что создаёт барьеры для входа на рынок.

Один из фундаментальных вопросов развития алгоритмической экономики — кто заинтересован в ограничении отслеживания информации и как эти заинтересованные лица или организации соотносятся с множеством тех, кто имеет возможность: а) установить подобные ограничения; б) обеспечить их соблюдение. На наш взгляд, простого и очевидного ответа тут нет, хотя известны практические случаи, когда участники рынка, идя

против течения, помогают пользователям обеспечить необходимый уровень приватности (см. раздел 5). Актив, который может получить компания и тем самым обеспечить избирательность стимулов, — доверие со стороны пользователей на фоне непонятных для них практик других компаний.

Уровень нарушения (сохранения) приватности, соответствующий максимизации прибыли платформами

Несмотря на то, что цифровые компании конкурируют на разных рынках, большинство технологических гигантов применяют, по крайней мере, одну бизнес-модель: *негласное наблюдение* [*Cyphers, Doctorow,* 2021]. Цифровые экосистемы собирают информацию о пользователях из каждого своего сервиса, объединяют эти данные в профили и используют эти профили для таргетирования рекламы. Они также собирают информацию о своих конкурентах через магазины приложений и сторонние трекеры, что может также приводить к поглощениям или вытеснениям с рынка.

Компании, обладающие большой персональной информацией клиентов, могут их классифицировать по различным признакам и проводить дискриминацию третьей или даже первой степени. Персонализированное ценообразование помогает компании улавливать излишек потребителя, и чем совершеннее алгоритмы, тем точнее будут прогнозные значения цены спроса конкретного индивида. В литературе встречается большое количество работ, посвящённых динамическому или персонализированному ценообразованию [*Chen*, 1997; *Шаститко, Маркова, Мелешкина, Морозов*, 2020], но лишь некоторые из них касаются вопросов конфиденциальности.

В некоторых исследованиях подчёркиваются положительные стороны для потребителей от раскрытия персональной информации. Так, фирмы могут устанавливать цены ниже для «переманивания» клиентов с конкурирующих сервисов [*Asplund, Eriksson, Strand,* 2008], снижать цену для новых клиентов [*Jeong, Maruyama,* 2009] или для любых клиентов «в обмен» на больший объём информации [*Chen, Narasimhan, Zhang,* 2001], в том числе и для обмена информацией с другими компаниями [*Calzolari, Pavan,* 2006].

Исследования политики конфиденциальности в целом подтверждают тот факт, что степень необходимости регуляторного вмешательства из-за опасений злоупотреблений со стороны доминирующих компаний зависит от уровня просвещённости потребителей в вопросах о целях и методах использования их данных [*Taylor*, 2004]. Верно и обратное, если пользователи обладают технологией «анонимизации» (например, способны удалять файлы cookie), то сбор и анализ персональных данных станет положительно сказываться на прибыли компании только в случае предоставления потребителям широкого спектра персонализированных услуг [*Acquisti, Varian,* 2005]. Компании могут даже инициировать собственную разработку механизма конфиденциальности и без вмешательства регулятора, но в этом случае пользователи будут платить некоторый «эквивалент» ценности персональной информации [*Conitzer, Taylor, Wagman,* 2012]. Тем не менее такое позитивное влияние на экономическое благосостояние возможно только в случае, если пользователи не только могут управлять степенью своей конфиденциальности, но и уверены, что эти механизмы работают прозрачно и никаких действий компании от них не скрывают. Но на данный момент времени это практически недостижимо.

Практику, когда компании имеют слабые стимулы для защиты конфиденциальности пользователей, в то время как объём и глубина данных, методы работы с ними и последствия этих методов скрыты от потребителей, называют «практикой сокрытия данных» («concealed data practices» [*Kemp*, 2020]). Это приводит к чрезмерному сбору, хранению и анализу персональной и иной информации сверх ожиданий пользователя.

Из-за возможностей по сокрытию информации и истинной её ценности компания (неявно или даже явно) увеличивает цену для потребителя за пользование ресурсом. Более того, если компания может удерживать пользователей и при снижении уровня защиты и/или конфиденциальности персональных данных, то это является одним из показателей её рыночной власти [*Shelanski*, 2013]. Обратное также верно: доминирующая на рынке фирма (или «gate-keeper», если речь идёт о компании, которая контролирует несколько связанных между собой сервисов/платформ) способна в одностороннем порядке и без уведомлений изменять уровень и качество собираемой информации, применяя для этого корректировки институтов мезоуровня (мезоинституты). В частности, в Германии антимонопольная служба (Bundeskartellamt) вводила ограничение на действия Facebook*[9] из-за признания злоупотребления доминирующим положения в виде навязывания своим пользователям «эксплуататорских деловых условий» [*Bundeskartellamt*, 2019]. Более того, цифровые гиганты аккумулируют данные не только со своих сервисов, но и информацию, собираемую их «друзьями-соперниками» [*Эзрахи, Стаки*, 2022], — компаниями, которые размещаются или связаны с этими «суперплатформами» (например, Google имеет доступ к информации разработчиков приложений в Google Play). Это приводит к искажённым стимулам (с точки зрения пользователей) для разработчиков — тайный сбор и обмен информацией поощряется, но ровно до тех пор, пока сама «суперплатформа» не решит вытеснить или поглотить своего «друга-конкурента» из своей ниши.

При участии третьей стороны — рекламодателей, которые заинтересованы в улучшении эффективности показа таргетированной рекламы, возникают дополнительные эффекты. С одной стороны, персонализированная реклама может усиливать ценовую конкуренцию: из-за ограниченного внимания потребителя, увеличения эффективности «мэтчинга» в контекстной рекламе компании будут вынуждены применять специальные ценовые стратегии [*de Cornière*, 2016]. Но если платформа, размещающая рекламу, будет злоупотреблять своим доминирующим положением, взымая слишком высокую плату за размещение рекламы, то это может нивелировать любые преимущества персонализированного подхода. Опасность завышения цены для рекламодателей со стороны платформы кроется и в самой специфике работы с данными. Она связана и с улучшением механизмов таргетинга, и с увеличением количества персональных данных и повышением их качества, и даже с дополнительным раскрытием информации о сегменте пользователей.

При этом, у крупной платформы есть стимулы к корректировке эластичности спроса через дискриминирующее поведение: рекламодатель, предложивший наибольшую цену (или иные привлекательные условия для платформы), может получить большее число показов [*Hagiu, Jullien,* 2011]. Можно учесть, что экосистемы в таком случае могут быть заинтересованы в продвижении собственных, а не сторонних сервисов. Но даже в случае наличия нескольких конкурентов-платформ, если все они способны отслеживать и фиксировать действия потребителей в интернете, может возникнуть равновесие, при котором каждая из таких фирм будет вести себя как монополист — манипулировать потребителями, заставляя их покупать наиболее маржинальные продукты, а не те, которые наиболее соответствуют их потребностям [*Board, Lu,* 2018].

В целом механизмов для извлечения выгод со стороны компаний, собирающих и анализирующих персональные данные, множество, и они, при всей их закрытости для других сторон, приносят огромную прибыль и дают не только возможности конкурентного преимущества, но и рыночной власти. Логично, что крупные платформы и экосистемы не заинтересованы в установлении более жёстких норм в обеспечении приватности в интернете, но всё же решения, направленные на обеспечение большей сохранности данных, возникают на цифровых рынках.

---

[9] Социальная сеть *Facebook (принадлежит Meta) запрещена в РФ. Решением суда от 21.03.2022 компания Meta признана экстремистской организацией на территории Российской Федерации.

Приватность в интернете: кто за?

Если есть основания для постановки вопроса о необходимости поддержания определённого уровня приватности, то как эта необходимость может быть связана со способностью (в данном случае — использованием стимулов) отдельных действующих лиц или групп, обладающих возможностями если и не обеспечить, то, по крайней мере, содействовать поддержанию приватности.

Частные цифровые компании

Частные компании — владельцы уже популярных операционных систем и/или программного обеспечения могут быть заинтересованы в продвижении своих продуктов, как обеспечивающих бо́льшую приватность. Это может как служить дополнительным аргументом в их пользу в конкурентной борьбе, так и положительно сказаться на мнении регуляторов, следящих за соблюдением прав и свобод в интернете. Однако ситуация с HTTP-заголовком «Do Not Track» (DNT), который был призван сигнализировать сайтам о том, что пользователь не хочет, чтобы его данные отслеживались, демонстрирует, что без законодательной поддержки подобные технические инициативы не найдут широкого применения даже при активной деятельности некоторых крупных цифровых коммерческих компаний. Функция DNT могла быть включена пользователем в большинстве браузеров (в некоторых даже была установлена по умолчанию, например, в Internet Explorer 10). Однако уже спустя несколько лет её функционирования стало понятно, что многие сайты (особенно активно использующие персональные данные для продвижения рекламы, такие как Google и *Facebook) игнорируют ограничение, продолжая аккумулировать «цифровые следы». Компания Apple и вовсе убрала эту функцию из браузера Safari с 2019 г., полагая, что эта HTTP-метка не мешает, а, наоборот, помогает следить за пользователями [*Simon*, 2019], заменив её, по их словам, более совершенной технологией — интеллектуальным предотвращением отслеживания.

На замену DNT в 2020 г. пришёл протокол Global Privacy Control (GPC), который имеет «законодательное подкрепление» — California Consumer Protection Act (CCPA) — действующий на территории Калифорнии (США) закон, который предписывает цифровым компаниям соблюдать ограничения, выставленные пользователем. Разработчиками новой версии протокола являются компании New York Times, DuckDuckGo и Brave, а также Уэслианский университет. Со временем эту практику могут перенять иные юрисдикции. Самым очевидным потенциальным участником видится Евросоюз со своим строгим законодательством (пока насчёт применимости GPC в имеющихся формулировках GDPR есть большие сомнения [*Pandit*, 2021]).

Независимые разработчики приватного ПО/поисковых систем

Несмотря на парадокс конфиденциальности, определённая доля потребителей обеспокоена контролем своих персональных данных в интернете. Поэтому неудивительно, что на рынке присутствуют частные компании, сделавшие «приватность» главной особенностью своего продукта (поисковой системы и/или браузера). Компании могут пойти различными путями для обеспечения прибыли такой компании:

- платное ПО. Самый очевидный способ — взимать плату с потребителей за покупку/подписку на производимый «приватный» продукт. Однако этот путь непопулярен среди производителей по следующим причинам: 1) разрабатываемое независимое ПО, как правило, основывается на открытом исходном коде; 2) конкурентное давление со стороны иных распространённых «бесплатных» браузеров, сопряжённое со сложностью оценки со стороны потребителя ценности приватности; 3) идеология, согласно которой поль-

зование интернетом должно быть бесплатно и безопасно для потребителей. Плата может взыматься за предоставление каких-либо дополнительных функций, например, функции VPN (как в браузере от Avast) и возможностей тонкой настройки на нескольких устройствах (как в программе Disconnect);

- размещение рекламы. Как ни парадоксально, но привлечение «третьей стороны» в виде рекламодателей не противоречит условию обеспечения приватности. Однако компании делают упор на безопасных, с точки зрения пользователей, методах размещения рекламы — например, контекстной. Это позволяет не собирать дополнительную информацию, но вполне может отражать интересы пользователя (так как она соответствует его поисковому запросу). Примером может служить экосистема компании Brave, которые предоставляют бесплатный браузер с интегрированной поисковой системой, но также и со своей платформой для рекламодателей, а также довольно известный сервис DuckDuckGo;
- краудфандинг/пожертвования. Некоторое ПО разработано некоммерческими организациями (см. далее), осуществляющими широкую деятельность по продвижению приватности и безопасности в интернете, оно также может быть создано в рамках краудфандинга, под определённые запросы потребителей.

Стоит отметить, что в последнее время подобные компании выстраивают собственные «экосистемы», состоящие из браузера, поисковой системы, платформы для рекламодателей, сервиса VPN и даже антивируса. Это продиктовано не только коммерческим интересом, но и тем, что только использование всех сервисов в совокупности может служить гарантией приватности (например, пользование «приватной» поисковой системой отдельно таких гарантий дать не может из-за агрессивных действий со стороны цифровых гигантов, использующих уязвимости внутри рекламных баннеров). Но здесь так или иначе возникает вопрос о действенности этих гарантий — как проверить заявления компании о том, что она не собирает персональные данные? Действительно ли она этого не делает? И как быть, если какой-то пользователь, обладающий специфическими навыками, обнаружит обратное? Это приводит к необходимости не столько введения регуляторного контроля, сколько наличия правовых механизмов, на которые могут опереться пользователи или содействующие им некоммерческие организации.

Некоммерческие организации

Как было сказано ранее, пользователи по одиночке не могут противостоять нормам мезоуровня, диктуемым цифровыми гигантами. Но помощь в этом могут оказать некоммерческие объединения, заинтересованные в продвижении гражданских свобод и защиты приватности в интернете. Самой крупной подобной организацией является Фонд электронных рубежей (Electronic Frontier Foundation, EFF) — американская некоммерческая компания, действующая с 1990 г. Компания существует на пожертвования, в основном индивидуальные, но и корпорации вносят свою лепту [*EFF*, 2023].

Под эгидой EFF был разработан ряд приложений, помогающих сохранить приватность в интернете, например, Privacy Badger — расширение для браузера, которое не позволяет рекламодателям или иным трекерам тайно отслеживать действия пользователя в интернете. Приложение не блокирует рекламу, если она «не следит» за пользователем, что, по мнению компании, стимулирует рекламодателей к внедрению лучших практик конфиденциальности, т. е. помогает выполнять функцию фильтрации. Согласно данным в Google Chrome это расширение установило более 1 млн пользователей, в Firefox — более 1,2 млн, в Opera — более 800 тыс. Помимо прочего Фонд оказывает поддержку в судебных разбирательствах, которые касаются соблюдения прав и свобод человека в интернете: обеспечения приватности, но вместе с тем и гласности, прозрачности в части обеспечения защиты заявленных ценностей, а также осуществляет лоббирование соответствующих нормативных документов.

Некоммерческие организации могут выступать и в роли надзорного органа, как минимум, осуществляя технический мониторинг компаний на предмет соблюдения условий распространения персональных данных/обеспечения приватности. Обеспечение прозрачности и гласность в этой сфере сами по себе могут служить заметным рычагом давления на коммерческие компании, но из-за ряда причин, перечисленных в начале статьи, это может не сказаться на деятельности цифровых гигантов, что ещё раз говорит о необходимости государственных механизмов, способствующих защите пользователей.

Государство (регулятор)

Ответы на вопрос о том, насколько регулятор должен и может принимать активное участие в защите приватности пользователей, в литературе различны — многие эксперты полагают, что саморегулирование в отрасли является самым эффективным вариантом. Такая позиция основывается на том, что затраты фирм и пользователей на соблюдение приватности выше, чем затраты, которые связаны с её нарушением [*Rubin, Lenard,* 2002]. Можно сказать, что подобный подход был характерен для политики США, где предпочитали не внедрять жёсткое регулирование цифровой экономики. Но ситуация изменилась с введением уже упомянутого California Consumer Protection Act (CCPA), который в какой-то мере сопоставим с европейским GDPR. Принятие CCPA, конечно, не означает изменения политики США. Однако не будем забывать, что Калифорния является «флагманским» штатом, в котором находятся и Кремниевая долина, и Голливуд, а это сопряжено с большим числом результатов интеллектуальной деятельности и развитием креативной экономики.

В целом из представленных выше примеров видно, что даже при наличии сильных частных игроков, заинтересованных в усилении приватности и контроля за данными в интернете, другая сторона — цифровые «компании-привратники» — обладают мощными технологическими и институциональными механизмами, которые препятствуют этому. «Механизмы прозрачности», призванные дать больший контроль в руки потребителей, не работают: нередко те, кто отстаивают политику конфиденциальности, не информируют пользователей о своих истинных целях, манипулируют мнением и даже вносят путаницу в понимание сути проблемы конфиденциальности в интернете [*McDonald, Cranor,* 2008].

Может ли государство выступать здесь надёжным регулятором и, главное, гарантом? Не будет ли вступать в противоречие концепция «государства как защитник» с концепцией «государство как интересант»? Государство не меньше, если не больше, чем цифровые гиганты, заинтересовано в сборе персональной информации, которую можно получать или напрямую от граждан (через собственные цифровые сервисы), или же опосредованно — от цифровых компаний. Это может происходить как открыто, так и неявно — например, в целях безопасности. И сами задачи скрытого наблюдения и мониторинга могут быть достаточно широкими [*Königs*, 2022]. Следовательно, появляется задача не только создания условий открытости процессов для цифровых компаний, но и выработки механизмов по регулированию этих процессов, что, как правило, означает возможность участия в этих процессах, хотя бы на уровне законотворческой деятельности, некоммерческих и саморегулируемых отраслевых организаций.

Вопрос о государственном регулировании уже не рассматривается с точки зрения необходимости — очевидно, что там, где имеются «цифровые гиганты», оно необходимо, но применяемые механизмы могут быть разными и, вероятно, унифицированных решений нет. Вопросы приватности сопряжены с необходимостью поддержания конкуренции, которая даёт пользователям возможность выбирать, с кем делиться информацией, а с кем — нет, и «голосовать ногами». К механизмам, которые призваны усилить или сохранить конкуренцию, можно причислить:

- унификацию стандартов сбора и обращения больших и персональных данных — повышение уровня «конкурентной совместимости» (competitive compatibility, ComCom) [*Doctorow,* 2020]. Единые технологические стандарты могут помочь в перенесении данных с одной платформы на другую, а также снизить барьеры входа для новых фирм, но могут и негативно сказаться на приватности пользователей — так как станут легко сопоставимы друг с другом. Получается некоторый парадокс — путь к конкуренции создаёт дополнительные риски для конфиденциальности, которые тоже необходимо учитывать. Текущее международное законодательство, например, Закон об авторском праве в цифровую эпоху (DMCA), используется корпорациями для защиты от возможных регуляторных вмешательств;
- «внутреннюю совместимость» [*Cyphers, Doctorow,* 2021] платформ — требование, по которому пользователи схожих или смежных сетей могут взаимодействовать кроссплатформенно (т. е. не заводя дополнительного аккаунта). Эта норма сопряжена с большими затратами со стороны компаний и нуждается в дополнительном строгом инфорсменте и мониторинге. Однако в целом она эффективна и способна снизить рыночную власть цифровых гигантов;
- принятие права «переноса данных» пользователями с платформы на платформу, которая гарантирует, что данные с переносимой платформы будут удалены. Данная мера внедрена в Евросоюзе (GDPR) и в Калифорнии (CCPA);
- сосредоточение внимания на процессах, происходящих внутри экосистем при обработке и анализе данных, а не только на возможностях их обмена или продажи;
- анализ эффектов от сделок экономической концентрации, включающий в себя возможные синергетические эффекты от слияния данных и/или технологий их обработки;
- повышение информированности пользователей о рисках и последствиях предоставления персональной информации, просветительская деятельность, направленная на повышение цифровых навыков.

Главная задача регулятора — перестройка стимулов больших платформ и экосистем в соответствии со стимулами их пользователей. Сильное вмешательство в деятельность компаний, действительно, может привнести больший ущерб для экономических процессов, чем даже сохранение status quo, так как ни у кого нет более эффективных технических решений, связанных с безопасностью данных платформ, чем у самих платформ.

Заключение

Размножение цифровых платформ и появление цифровых экосистем, функционирующих на основе сбора, обработки и использования больших данных, включая «цифровые следы» отдельных пользователей, поднимает вопрос о том, в какой мере кажущаяся рядовым пользователям бесплатность сервисов угрожает их благосостоянию, с одной стороны, и может стать ограничителем поддержания и развития конкуренции — с другой. Осознание цены бесплатности сервисов выводит на широкий пласт вопросов о приватности пользователей в интернете и инструментов обеспечения контроля чувствительных данных. Перспективные направления исследований и поиска вариантов сбалансированного решения вопроса обеспечения приватности тесно связаны с существованием отдельных групп интересов, одним из приоритетов в деятельности которых является поддержание искомого уровня приватности.

Рынок сам по себе не гарантирует воспроизводство частных стимулов по удержанию/усилению приватности в интернете. При безусловной экономической привле-

кательности этой ниши само отсутствие корректно спроектированных регуляторных механизмов в отношении крупнейших цифровых платформ (главных охотников за персональными данными) создаёт дополнительные проблемы, что в результате не приводит к желаемым эффектам. Однако важно понимать сложность проблемы. Хотя для регуляторов, защищающих конкуренцию, критерием достижения целей является степень защищённости прав потребителей и их выигрыши, они также не могут не учитывать и то, что находится на другой чаше весов. А это — и вопросы экономической эффективности, благосостояния всего общества (что включает в себя и доходы цифровых платформ, лидеров цифровых экосистем и их участников), и в то же время заинтересованность органов власти в получении доступа к большему объему информации не только для решения чисто экономических задач, но и задач, связанных с безопасностью как всего общества, так и государства.

ЛИТЕРАТУРА/REFERENCES

Петров А. (2021). Являются ли e-mail и IP-адрес персональными данными? [*Petrov A.* (2021). Are email and IP address personal data?] // *ФГБУ «Редакция «Российской газеты».* https://pravo.rg.ru/rubrics/question/38477 (дата обращения: 03.03.2024).

Тамбовцев В.Л. (2005). *Экономическая теория институциональных изменений* [*Tambovcev V.L.* (2005). Economic theory of institutional changes]. — М.: ТЕИС.

Шаститко А.Е., Курдин А.А., Филиппова И.Н. (2023). Мезоинституты для цифровых экосистем [*Shastitko A.E., Kurdin A.A., Filippova I.N.* (2023).Mesoinstitutions for digital ecosystems] // *Вопросы экономики.* № 2. С. 61–82. DOI: 10.32609/0042-8736-2023-2-61-82.

Шаститко А.Е., Маркова О.А. (2020). Старый друг лучше новых двух? Подходы к исследованию рынков в условиях цифровой трансформации для применения антимонопольного законодательства [*Shastitko A.E., Markova O.A.* (2020). An old friend is better than two new ones? Approaches to market research in the context of digital transformation for the antitrust laws enforcement] // *Вопросы экономики*. № 6. С. 37–55. DOI: 10.32609/0042-8736-2020-6-37-55.

Шаститко А.Е., Маркова О.А., Мелешкина А.И., Морозов А.Н. (2020). Ценообразование на основе больших данных: предметное поле проблемы [*Shastitko A.E., Markova O.A., Meleshkina A.I., Morozov A.N.* (2020). Pricing based on big data: subject field of the problem] // *Вестник Московского университета. Серия 6. Экономика.* № 6. С. 3–22. DOI: 10.38050/01300105202061.

Эзрахи А., Стаки М. (2022). *Виртуальная конкуренция: посулы и опасности алгоритмической экономики:* Учебник [*Ezrahi A., Staki M.* (2022).Virtual competition: promises and dangers of algorithmic economics: textbook]. — М.: Дело РАНХиГС.

Acquisti A., Taylor C., Wagman L. (2016). The Economics of Privacy // *Journal of Economic Literature.* No. 442. Pp. 447–448.

Acquisti A., Varian H. (2005). Conditioning Prices on Purchase History // *Marketing Science*. No. 24(3). Pp. 367–381. DOI:10.1287/mksc.1040.0103

Akerlof G.A. (1970). The Market for 'Lemons': Quality Uncertainty and the Market Mechanism // *Quarterly Journal of Economics.* No. 84(3). Pp. 488–500.

Arrow K.J. (1962). The Economic Implications of Learning By Doing // *Review of Economic Studies.* No. 29(3). Pp. 155–73.

Asplund M., Eriksson R., Strand N. (2008). Price Discrimination in Oligopoly: Evidence from Regional Newspapers // *Journal of Industrial Economics*. No. 56(2). Pp. 333–46. DOI: 10.1111/j.1467-6451.2008.00343.x.

Board S., Lu J. (2018). Competitive Information Disclosure in Search Markets // *Journal of Political Economy*. No. 126(5). Pp. 1965–2010. DOI: 10.1086/699211.

Bundeskartellamt. (2019). *Bundeskartellamt prohibits Facebook* from combining user data from different sources: Background information on the Bundeskartellamt's Facebook* proceeding.* https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2019/07_02_2019_Facebook.html (access date: 03.03.2024).

Calzolari G., Pavan A. (2006). On the Optimality of Privacy in Sequential Contracting // *Journal of Economic Theory*. Vol. 130. No. 1. Pp. 168–204. DOI: 10.1016/j.jet.2005.04.007.

Campbell J., Goldfarb A., Tucker C. (2015). Privacy Regulation and Market Structure // *Journal of Economics and Management Strategy.* Vol. 24. No. 1. Pp. 47–73. DOI: 10.1111/jems.12079.

Chen Y. (1997). Paying Customers to Switch // *Journal of Economics and Management Strategy*. Vol. 6. No. 4. Pp. 877–897. DOI: 10.1111/j.1430-9134.1997.00877.x.

Chen Y., Narasimhan C., Zhang Z. J. (2001). Individual Marketing with Imperfect Targetability // *Marketing Science*. Vol. 20. No. 1. Pp. 23–41. DOI: 10.1287/mksc.20.1.23.1020.

Conitzer V., Taylor C., Wagman L. (2012). Hide and Seek: Costly Consumer Privacy in a Market with Repeat Purchases // *Marketing Science*. Vol. 31. No. 2. Pp. 277–92. DOI: 10.1287/mksc.1110.0691.

Cornière A. de (2016). Search Advertising // *American Economic Journal: Microeconomics*. No. 8(3). Pp. 156–88. DOI: 10.1257/mic.20130138.

Cyphers B., Doctorow C. (2021). Privacy Without Monopoly: Data Protection and Interoperability // *Electronic Frontier Foundation*. https://www.eff.org/wp/interoperability-and-privacy (access date: 03.03.2024).

Doctorow C. (2020). Competitive Compatibility: Year in Review 2020 // *Electronic Frontier Foundation*. www.eff.org/deeplinks/2020/12/competitive-compatibility-year-review (access date: 03.03.2024).

EFF. (2023). 2022 Annual report // *Electronic Frontier Foundation*. https://annualreport.eff.org (access date: 03.03.2024).

Hagiu A., Jullien B. (2011). Why Do Intermediaries Divert Search? // *RAND Journal of Economics*. Vol. 42. No. 2. Pp. 337–362. DOI: 10.1111/j.1756-2171.2011.00136.x.

Hayek F.A. (1945). The Use of Knowledge in Society // *American Economic Review*. Vol. 35. No. 4. Pp. 519–530.

Hirschprung R.S. (2023). Is the Privacy Paradox a Domain-Specific Phenomenon // *Computers*. No. 12. P. 156. DOI: 10.3390/computers12080156.

Jeong Y., Maruyama M. (2009). Commitment to a strategy of uniform pricing in a two-period duopoly with switching costs // *Journal of Economics*. No. 98. Pp. 45–66. DOI: 10.1007/s00712-009-0083-x.

Kemp K. (2020). Concealed data practices and competition law: why privacy matters // *European Competition Journal. UNSW Law Research Paper*. No. 19–53. DOI: 10.1080/17441056.2020.1839228.

Königs P. (2022). Government Surveillance, Privacy, and Legitimacy // *Philosophy and Technology*. Vol. 35. No. 8. Pp. 1–22. DOI: 10.1007/s13347-022-00503-9.

Kröger J., Raschke P. (2019). Is My Phone Listening in? On the Feasibility and Detectability of Mobile Eavesdropping // *Data and Applications Security and Privacy XXXIII*. Vol. 11559. DOI: 1007/978-3-030-22479-0_6.

Lane J., Stodden V., Bender S., Nissenbaum H. (2014). *Privacy, Big Data, and the Public Good: Frameworks for Engagement*. — Cambridge and New York: Cambridge University Press.

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

McCrea K. (2023). The Yandex Leak: How a Russian Search Giant Uses Consumer Data. *Confiant*. https://www.confiant.com/news/the-yandex-leak-how-a-russian-search-giant-uses-consumer-data (дата обращения: 03.03.2024).

McDonald A., Cranor L. F. (2008). The Cost of Reading Privacy Policies // *A Journal of Law and Policy for the Information Society*. Vol. 4. No. 3. Pp. 540–565.

Pandit H.J. (2021). Global Privacy Control (GPC) + GDPR: Will It Work? // *Sustainable Computing Lab*. https://www.sustainablecomputing.eu/blog/5993/gpc-gdpr-will-it-work/ (дата обращения: 03.03.2024).

Rubin P., Lenard T. (2002). *Privacy and the Commercial Use of Personal Information*. — New York: Springer, Kluwer Academic. DOI: 10.1007/978-1-4615-1719-1.

Shastitko A.E., Markova O.A., Morozov A.N. (2022). Deceptive evidence: The experience of product market definition for the purpose of competition law enforcement // *Russian Journal of Economics. ARPHA Platform*. Vol. 8. No. 3. Pp. 255–275. DOI: 10.32609/j.ruje.8.82144.

Shelanski H. (2013). Information, Innovation, and Competition Policy for the Internet // *University of Pennsylvania Law Review*. Vol. 161. No. 6. Pp. 1663–1705.

Simon M. (2019). Apple is removing the Do Not Track toggle from Safari, but for a good reason. *Macword*. https://www.macworld.com/article/232426/apple-safari-removing-do-not-track.html (access date: 03.03.2024).

Stigler G.J. (1961). The Economics of Information // *Journal of Political Economy*. Vol. 69. No. 3. Pp. 213–225.

Taylor C.R. (2004). Consumer Privacy and the Market for Customer Information // *RAND Journal of Economics*. Vol. 35. No. 4. Pp. 631–50.

Varian H.R. (2010). Computer Mediated Transactions // *American Economic Review*. Vol. 100. No. 2. Pp. 1–10.

Шаститко Андрей Евгеньевич
aes99@yandex.ru

Andrey Shastitko
Doctor of Economics, Professor, Head of the Department of Competitive and Industrial Policy, Faculty of Economics, Moscow State University; Director of the Center for Research on Competition and Economic Regulation of the Russian Presidential Academy of National Economy and Public Administration under the President of the Russian Federation (Moscow)
aes99@yandex.ru

Моросанова Анастасия Андреевна
aamorosanova@gmail.com

Anastasia Morosanova
Candidate of Economics, Researcher of Lomonosov Moscow State University; Researcher of Russian Academy of National Economy and Public Administration under the President of the Russian Federation (Moscow)
aamorosanova@gmail.com

EXPENSIVE FREE[10]

Abstract. Digital platforms, as a rule, offer their services to at least one of the parties without a monetary fee, but by charging another resource — information — in the form of personal information and digital footprints. Analysis mechanisms of collected information provide companies with hidden competitive power, which, on the one hand, allows them to increase efficiency, but on the other hand, carries potential threats for many individual users and for economic welfare. The main research question concerns the presence of incentives to maintain or enhance privacy on the Internet, which arise not only from users, but also from business, as well as the role of government regulators in this process. Some of the urgent regulatory decisions to develop a competitive environment in digital markets and ensure transparency of processes within ecosystems, discussed in this article, can provide progress in user control over their personal information. At the same time, the proposed changes will lead to additional information security risks (and other aspects). The question of ensuring the guarantor reliability related to privacy on the Internet remains open.

Keywords: *privacy, digital economy, personal data, ecosystems, platforms.*
JEL: L15, L20, L50, L86.

[10] The article was written on the basis of the RANEPA state assignment research programme.