

Выгоды и потери от защиты персональных данных: подходы в экономической теории

Пыск Д.А., магистр эконом. наук, аспирант, кафедра экономической теории, Белорусский государственный экономический университет, г. Минск, Республика Беларусь

Аннотация. В статье рассматриваются выгоды и потери от защиты персональных данных и подходы к ним в экономической теории. Также в статье раскрываются понятия, связанные с технологиями усиления конфиденциальности. Определено, что с одной стороны, на данный момент технологии снижают количество доступной информации об индивидах, а с другой информационные технологии могут снижать неопределенность при помощи агрегации информации о трендах и предпочтениях определенных групп потребителей. Также в конце статьи рассмотрены причины, при которых организация может получать выгоды или издержки при работе с данными.

Ключевые слова: неполная информация, нерациональные действия потребителей, микроэкономические взгляды на конфиденциальность, технологии усиления конфиденциальности, субъекты персональных данных, защищенная информация.

Benefits and losses from personal data protection: approaches in economic theory

Pysk D.A., master of Economics, post-graduate student, Department of economic theory, Belarusian state University of Economics, Minsk, Republic of Belarus

Annotation. The article discusses the benefits and losses of personal data protection and approaches to them in economic theory. The article also covers concepts related to technologies for enhancing privacy. It is determined that on the one hand,

technologies currently reduce the amount of available information about individuals, and on the other, information technologies can reduce uncertainty by aggregating information about trends and preferences of certain consumer groups. Also at the end of the article, we discuss the reasons why an organization may receive benefits or costs when working with data.

Keywords: incomplete information, irrational actions of consumers, macroeconomic views on confidentiality, technologies for enhancing confidentiality, personal data subjects, protected information.

В современных экономиках снижение затрат на хранение информации дало возможность удерживать, сохранять и анализировать огромные объемы информации об индивидууме. Например, компании могут сохранять данные обо всех транзакциях клиента или создавать отчеты о действиях на сайте/любых других информационных ресурсах компании. На веб-сайтах также можно сохранять историю поведения клиента на сайте. Агрегаторы данных затем могут связать поступившую информацию с определенным человеком.

Чем чаще организации применяют цифровые технологии, тем дешевле и быстрее становится «выпуск», обработка персональной и потенциально «деликатной» информации. Поэтому можно сделать вывод, что со временем сомнения в том, что потенциально деликатная информация может использоваться без ведома пользователя также растут. Уже сейчас значительное количество ежедневных действий индивидуумов может отслеживаться при помощи информационных технологий. Незначительные объемы персональных данных индивидуумов попадают в базы данных (прим. Информация о cookies для улучшения поиска Google). Затем записанные данные могут позволить создать досье/профайл на определенного человека. Данное событие происходит/может произойти без ведома и согласия человека. Более того, даже в данный момент, сотни миллионов пользователей транслируют свою персональную информацию в сеть (прим. блоги, ютуб-каналы, социальные сети), которая впоследствии может использоваться для создания профайлов [1].

Тем не менее, последствиями общедоступной информации для всех участников рынка (субъекты данных и текущие либо потенциальные держатели данных) может быть как увеличение общественного благосостояния, так и его уменьшение. Балансируя между открытием и сокрытием своих персональных данных, физические лица и организации сталкиваются со сложными и, порой, половинчатыми решениями и компромиссами. Физические лица хотят защитить приватность своей жизни (и, соответственно, персональных данных). Также физлица заинтересованы в том, чтобы предотвратить либо ограничить использования их персональных данных организациями [2]. Тем не менее физические лица могут получать выгоду от передачи информации организациям, либо любым другим третьим лицам: таким образом они могут увеличить степень удовлетворения при взаимодействии друг с другом. Организации заинтересованы в том, чтобы узнать больше о индивидуумах, с которыми они взаимодействуют, например, отслеживая/анализируя их транзакции.

В качестве примера такой ситуации можно привести случай, когда физическое лицо, которое никогда либо редко путешествовало, посещает страны Африки и пользуется там дебетовой картой. Банк в свою очередь, связывается с этим физическим лицом и уточняет, действительно ли он/она сейчас находится в Африке и пользуется картой данного банка. С одной стороны, банк проверяет счет клиента на возможность мошеннических действий с ним и, соответственно, снижает свои потенциальные затраты на будущее расследование, если мошеннические действия имеют место быть. Также банк таким образом повышает лояльность со стороны клиента, показывая обеспокоенность транзакциями в необычных местах. Клиент банка также получает большее удовлетворение от услуг, предоставляемых банком, так как банк показывает, в свою очередь, обеспокоенность именно за этого клиента и, соответственно, клиент, как минимум осознает, что плата за услуги банка является обоснованной [2]. В данном примере потенциально могли использоваться следующие персональные данные: имя, фамилия, номер счета, сумма транзакций, возможное местоположение клиента, контактные данные клиента,

тип и описание транзакции. В данном примере банк использовал достаточно значительное количество как общих персональных данных, так и потенциально деликатных. Однако стоит отметить, что в данном случае действия банка (организации, обрабатывающей персональные данные) улучшили удовлетворенность и благосостояние обеих сторон. Хотелось бы подчеркнуть, что в данном примере персональные данные клиента использовались в конкретном бизнес-процессе банка с определенной целью и имели под собой юридическое и логическое обоснование. Также можно сказать, что количество персональных данных, обработанных клиентом, использовалось пропорционально цели их использования: если убрать какой-либо тип данных из вышеуказанного примера, то эффективность действий банка снизилась бы на порядок [5].

Как отметил лауреат Нобелевской премии по экономике Пол Самуэльсон «Те, кто воспринимают защиту персональных данных как фундаментальную свободу гражданского общества, видят ее как составную часть «автономии личности, достоинства и свободы» в демократическом гражданском обществе» [2].

Экономисты писали о конфиденциальности с начала 1970 годов. В рамках неоклассической экономической теории совершенно конкурентных рынков, «исчерпывающая» информация (доступность необходимой информации для всех участников рынка) ведет к экономической эффективности (равновесию). Например, в случае, когда все потребители знают цены, по которым в каждой фирме продается продукт, конкуренция снизит цены до наименьшего уровня, устанавливаемого производственной технологией, и увеличит благосостояние потребителя.

По словам представителя Чикагской школы Ричарда Познера (1978, 1981 годы), защита конфиденциальности ведет к неэффективности рынка, так как она скрывает потенциально необходимую информацию от других экономических агентов [29]. В качестве примера стоит привести ситуацию, когда работник сообщает работодателю неполную информацию о своих навыках и знаниях. В

будущем это может отрицательно повлиять на финансовый результат компании-нанимателя. Таким образом, удаление/сокрытие некоторых типов персональных данных на рынке при помощи законодательства о персональных данных/конфиденциальности перекладывает убытки, которые должен нести недобросовестный работник, на других участников рынка.

Стиглер считает, что государственное вмешательство в рынок персональных данных в любом случае будет неэффективно, так как индивидуумы склонны раскрывать информацию о своих положительных сторонах и скрывать свои отрицательные качества, таким образом те, кто решают защитить свои персональные данные (например заемщик, не желающий раскрывать свою кредитную историю) косвенно показывают, что они обладают негативными чертами (например, неспособность погашать вовремя займы в банках). В таком случае законодательная блокировка потоков персональной информации будет неэффективна: ресурсы или факторы производства будут в конечном итоге использоваться неэффективно или вознаграждение за их использование будет несправедливым [12].

Калзолари и Паван (2006) обнаружили, что неограниченная передача персональных данных между двумя фирмами может снизить провалы рынка и увеличить всеобщее благосостояние. В пользу аргумента о том, что неограниченный обмен информацией может снизить асимметричность информации и, как следствие, привести к росту благосостояния может говорить следующее: Вариян (1996) отметил, что потребители с большей вероятностью могут нести издержки в случае, если слишком мало данных о них передано третьим лицам, чем в случае, если данных передано слишком много [35]. Также Вариян отмечает, что потребитель может хотеть, чтобы определенные типы данных о них были известны третьим сторонам, например, потребитель хотел бы, чтобы его предпочтения об отдыхе были известны маркетологам, чтобы получить от них те предложения, в которых он действительно заинтересован.

Также к аргументам Чикагской Школы, в частности к теореме Коуза, можно причислить мнение Ноама (1997), который утверждал, что защита

персональных данных потребителя не зависит от первоначального распределения прав на защиту персональных данных (например, защищены ли данные потребителя законом). Более того, потребитель может раскрыть или скрыть данные, в зависимости от относительных оценок сторон, которым нужны эти данные. Если потребитель оценивает свое «право на тайну» выше, чем фирма, которой нужны его персональные данные, оценивает получение информации о нем, то эти данные останутся защищенным, потому что даже в отсутствие законов, регулирующих такую защиту, потребитель с большой вероятностью заплатит за право защиты своих персональных данных.

В то же время стоит отметить, что не все экономисты поддерживают позицию, относительно того, что защита персональных данных может привести к провалам/неэффективности рынка.

Например, Мерфи (1996) и Хиршлейфер (1980) критиковали позиции Познера и Стиглера, отмечая, что допущения о рациональном поведении, лежащие в основе моделей о защите персональных данных (приватности) не могут охватить весь спектр механизмов принятия решений потребителя о своих персональных данных.

Первые исследования Чикагской Школы на тему приватности нужно относить к «до-современной-ИТ» эры: развитие новых ИТ-технологий и Интернета, в частности, вынудило исследователей анализировать более детально различные компромиссы, связанные с защитой приватности и передачей данных.

Вариан отмечал, что вторичное использование персональных данных в экономике может привести к тому, что потребитель будет рационально принимать решение о передаче персональных данных фирме, потому что он ожидает получить определенные выгоды от такого типа операций. Таким образом, можно сказать, что потребитель косвенно получает контроль над тем, как фирма будет в дальнейшем использовать его данные. Стоит отметить, что фирма может продавать информацию о потребителях третьим сторонам с целью получения выгоды, но потребитель, в свою очередь, может не получать никаких выгод, а даже, наоборот, нести издержки, например, в случае, если третья

сторона использует его данные для спама или отрицательной ценовой дискриминации (Odlyzko 2003). Такие негативные внешние эффекты, которые несет потребитель, не возлагаются на фирму (Swire and Litan, 1998). Ноам также утверждает, что транзакционные издержки, бедность и другие проблемы могут не позволить потребителю получить защиту своих персональных данных [9].

Хермалин и Катц также критиковали утверждение сторонников чикагской школы о том, что защита персональных данных снижает общее благосостояние. Они также утверждали, что защита персональной информации будет иметь положительное влияние на всеобщее благосостояние. Например, защита приватности позволяет использовать некоторые страховые схемы, которые без нее не существовали бы. Если все потенциальные заинтересованные стороны могли проверять заранее информацию о серьезных заболеваниях, то компании, занимающиеся страхованием жизни, скорректировали бы цены в соответствии с полученной информацией. В то время как фактические итоги будут экономически эффективны (потребители будут покупать страховку по справедливой цене), то в будущем физические лица могут начать спекулировать на рисках, связанных с итогами их медицинского осмотра. Тем не менее, если медосмотр сделать необязательным для получения страховки, то физические лица, склонные к риску, будут покупать полную страховку по средней цене. Поэтому можно сказать, что уровень благосостояния будет выше, чем при обязательном прохождении медосмотра для получения страховки, потому что склонные к риску лица будут спекулировать меньшими рисками. Более того, Хермалин и Катц отмечают, что рынки могут не скорректировать эффективность своего функционирования в соответствии с дополнительной информацией, снижая эффективность итогового равновесия. В их модели два рациональных агента участвуют в транзакции, в которой оба заинтересованы в сборе информации друг о друге. Для них защита их персональных данных может привести к эффективному равновесию и, таким образом, расширенный запрет на передачу информации может быть необходим для эффективного равновесия [10].

Аналогичную идею поддерживают модели Хиршлейфера (1971) и Тейлора (2003), которые показывают, что рациональные экономические агенты могут сверх инвестировать средства в процесс сбора персональных данных о других лицах (например, чтобы увеличить выручку на основе знания того, что хочет купить потребитель). Тейлор (2004) также отмечает, что в присутствии трекинговых технологий, которые позволяют фирмам отслеживать предпочтения их потребителей (что позже ведет к ценовой дискриминации), вне зависимости от наличия персональных данных, законодательная защита увеличит активность потребителя и увеличит его благосостояние в зависимости от уровня «сложности» потребителя. Простые потребители не прогнозируют, что продавец имеет возможность использовать прошлую информацию о покупках клиента как основу для ценовой дискриминации, поэтому при достижении равновесия, весь излишек потребителя уйдет к компании-продавцу, кроме случая, когда существует законодательство о защите персональных данных. В то же время стоит отметить, что такой закон не будет нужен, если потребители будут знать, каким образом продавец использует их данные: в таком случае потребитель в долгосрочной перспективе адаптирует свое поведение соответствующим образом.

К похожим выводам пришли Акьюзити и Варян (2005), которые рассматривали модель в двух периодах, где продавец имеет доступ к «трекинговым» технологиям, а потребитель к «анонимизирующим» технологиям. В качестве примера можно привести сферу интернет-торговли: продавец может использовать файлы куки, чтобы определить поведение потребителя (в частности прошлые покупки), а потребители, в свою очередь, имеют доступ к «анонимизирующим технологиям» (удаление файлов куки, использование браузера в режиме инкогнито или анонимных платежных инструментов), которые скрывают их поведение. «Трекинг» потребителей увеличит прибыли продавца только в том случае, если трекинг используется с целью предоставления потребителю более качественных и персонализированных сервисов.

Другие модели, рассматривающие затраты на защиту персональных данных, связанные с ценовой дискриминацией, и последствиями для благосостояния при передаче данных о потребителях третьим лицам, отмечают, что использование персональных данных для «навязчивого» маркетинга может привести к негативным внешним эффектам для потребителя (Hui and Png, 2003). Более того, в то время как большинство теоретических работ по конфиденциальности рассматривают влияние на микроуровне, стоит отметить, что значительные макроэкономические затраты и выгоды могут появиться из-за защиты или торговли персональными данными [12].

Есть причины полагать, что действия потребителей – нерациональны, когда они принимают решения относительно краткосрочных выгод и долгосрочных затрат в плане раскрытия информации и вторжения в частную жизнь. Опыт также показывает, что потребители не способны действовать «рационально» (с точки зрения неоклассической экономической теории), когда сталкиваются с преимуществами и недостатками конфиденциальности информации. В последние годы поток исследований, проводящий анализ так называемого «парадокса конфиденциальности», был сфокусирован на препятствиях, которые мешают людям принимать решения, относящимися к их личным данным. Доказательством могут служить три основных препятствия:

- а) неполная информация
- б) ограниченная способность обрабатывать имеющиеся данные
- в) масса систематических отклонений от теоретически рационального принятия решений, что может быть объяснено когнитивными и поведенческими ошибками, исследуемых поведенческой экономикой и исследований о поведенческом принятии решения (для того чтобы изучить данную область, посмотрите работы Аквисти (2004) и Аквисти и Гроссклагс (2007) [3].

Таким образом можно сделать следующие выводы: современная микроэкономическая теория о конфиденциальности показывает, что потребители не полностью рациональны или, на самом деле, «близоруки», в таком случае, рыночное равновесие будет приводить к тому, что будет

отсутствовать возможность защиты конфиденциальности физических лиц, и таким образом, может потребоваться контроль за конфиденциальностью, чтобы улучшить потребительское и совокупное благосостояние.

В то время как информационные технологии могут быть использованы с целью отслеживания, анализа и объединения огромного количества данных, относящихся к одному лицу, PЕТs или Технологии Усиления Конфиденциальности могут быть использованы для защиты, обезличивания или сбора в одно целое данной информации таким образом, что они одновременно являются эффективными (в том смысле, что повторная идентификация персональных данных становится либо невозможной, либо уже достаточно дорогой, чтобы быть не прибыльной) и целесообразной (в том смысле, что необходимая транзакция может быть регулярно проводиться без дополнительных расходов для сторон, участвующих в процессе).

Существует большое количество исследований в области технологий по усилению конфиденциальности которые говорят о том, что криптографические протоколы могут быть использованы для удовлетворения потребности в передаче и защите персональных данных. Уже возможно осуществлять проверенные и, ещё пока анонимные, или конфиденциальные «транзакции» в разнообразных областях таких, как электронные платежи (Шом, 1983), сетевые коммуникации (Шом, 1985), интернет поиск (Дингледайн и др., 2004), или электронное голосование (Бенало, 1987); но также возможно иметь учётные системы, которые обеспечивают аутентификацию без идентификации (Камениш и Лисянская, 2001), делиться личными предпочтениями с защитой конфиденциальности (Адар и Хуберамн, 2001), использовать возможности рекомендательных систем и совместного фильтрования без раскрытия личных данных (Кэнни, 2002) или даже выполнять вычисления в зашифрованных пространствах (Джентри, 2009), что является открытием дверей для новых сценариев конфиденциальности, сохраняющих сбор данных и их анализ.

То есть технологии усиления конфиденциальности могут позволить достичь равновесия, при котором держатели данных могут ещё анализировать

агрегированные и анонимизированные данные. Стоит отметить, что персональные данные индивидуумов будут под защитой, так как их невозможно будет сопоставить с конкретным человеком. Вероятно, что переход к такому новому равновесию может быть улучшением условий жизни для потребителей и общества в целом. Тем не менее возможность того, что Технологии Усиления Конфиденциальности могут привести к рыночным результатам с ненулевыми суммами, только недавно стала предметом явного обсуждения. (Аквисти, 2008) [3].

Далее будет рассмотрена экономическая ценность персональных данных и неприкосновенности частной жизни с помощью анализа индивидуальных и общественных затрат, связанных с раскрытием и защитой информации.

Сфокусируемся на конфиденциальности информации. В контексте нашего анализа, субъекты персональных данных – потребители, а держатели данных – фирмы. Мы рассмотрим анализ, представив рынок личной информации и рынок конфиденциальной информации, как две стороны одной медали, когда защищённые данные могут иметь преимущества и недостатки, являющимися двойными или симметричными к затратам и преимуществам, связанными с раскрытой информацией для субъектов и держателей информации одновременно. Тем не менее мы не будем пытаться предоставить полный список и подробную классификацию всех возможных типов затрат и выгод, связанных с защищённой и раскрытой информацией [16].

Под раскрытой информацией мы понимаем в некоторой степени состояния, где субъект информации может намеренно или ненамеренно делиться общими данными с другими сторонами (держателями информации), или состояния, где другие стороны могут вступить во владение объектами информации независимо от её знания или даже согласия. Под защищённой информацией мы понимаем ситуации, при которых такое раскрытие не имеет место в прошлом, вне зависимости от того, может ли это быть связанным с объектами информации целенаправленной защиты личной информации или защитой держателя информации, который не способен или не заинтересован в

получении доступа к последней. Во-первых, мы заинтересованы в компромиссах между затратами и выгодами, которые появляются следствием такой раскрытой или защищённой информации. Во-вторых, мы также рассматриваем компромиссы, связанные с фактическими действиями раскрытия (или сбора) информации или защиты (или не раскрытия) информации [18].

Наш анализ начинается с экономических выгод от раскрытой информации. Мы сосредоточимся на:

- а) потенциальных выгодах от раскрытой информации для держателя информации и субъектов информации; тем не менее мы также упоминаем
- б) об альтернативных издержках, которые могут быть, когда ценная информация не раскрыта, а также
- в) о затратах на необходимое инвестирование с целью сбора и обработки личной информации.

В статье, опубликованной до появления коммерческого интернета, Блаттберг и Дейтон (1991) отмечают: это «мечта маркетолога» – возможность наладить интерактивное общение с отдельными потребителями. Технические средства в форме базы данных превращают данную мечту в реальность. Сегодня компании могут отслеживать предпочтения клиентов и настраивать индивидуальную рекламу под их нужды. К примеру, система продуктовых магазинов могла бы отметить, что как только вы купили обычный флакон с жидкостью для мытья посуды, то она тут же может предложить вам купон на покупку большого флакона [15].

То, что Блаттберг и Дейтон (1991) более двадцати пяти лет назад описали как будущее интерактивной торговли в период адресной рекламы, сегодня стало реальностью. Онлайн, сочетание IP адресов, куки файлы, информация о посещаемости и углублённая проверка пакетов делает возможным создание точного представления потребительских «демографических характеристик и поведения». В автономном режиме работы, бюро кредитной информации и агрегаторы данных покупательской способности от личных и публичных

организаций, удаление секретной информации и объединение, личные предпочтения, образцы покупок – дальше продажа (в совокупных и индивидуальных формах) в публичные и частные сектора. Сочетание онлайн и офлайн личной информации также стало возможным и таким образом мониторинг онлайн поведения на различных вебсайтах или рекламных сетях, и сочетание онлайн просмотра и информация о поведении вместе с самостоятельно предоставленной личной информацией, полученной из социальных сетей, используемых покупателями. Мы живем в эпоху революции в рыночной сфере управления данными потребителя, где личность является в то же время потребителем и производителем самого ценного актива – личной информации.

Фирмы могут получать значительное количество выгод от знания предпочтений и привычек о своих текущих или потенциальных клиентах. Наборы данных с полной информацией о потребителях могут улучшить и снизить их затраты на рекламу (Блаттберг и Дейтон, 1991). Таким образом компании могут увеличивать свою выручку посредством предложения потребителям именно тех товаров, в которых они заинтересованы (Аквизити, Вариян, 2005)[3], более персонализированных скидки и более высокое качество общения с клиентом (более совершенные CRM системы могут дать четкое понимание как потребностей клиента, так и предпочтительных способов коммуникации). Также можно отметить, что все вышесказанное может увеличить уровень лояльности клиента (затраты потребителя увеличатся, если он захочет «уйти» от фирмы, предоставляющей персонализированный сервис) [23].

При помощи анализа больших объемов данных о потребителях, компании могут предсказывать общие тренды (например колебания спроса), а также предпочтения индивидуумов. Таким образом компании могут минимизировать риски, связанные с запасами и увеличить отдачу от вложений в маркетинг. Также фирмы могут улучшить способность делать полезные рекомендации для клиентов и проводить ценовую дискриминацию с целью увеличения прибыли.

Более того, наблюдая за поведением физического лица, фирмы могут получать информацию о том, как они могут улучшить свои услуги или изменить их с целью получения больших прибылей.

В качестве примера, как информация о потребителях может увеличить прибыль, можно привести онлайн-рекламу. Рынок электронной коммерции и онлайн рекламы сейчас составляет более 300 миллиардов долларов в США, обеспечивая занятость более чем 3.1 миллиона жителей США. По сравнению с офлайн-аналогами рекламы, онлайн-реклама может быть нацелена на каждого индивидуума, основываясь на его поведении в Интернете (например, история поиска, посещенные вебсайты, информация о кликах и др). Такая точность ведет к тому, что фирмы снижают затраты на рекламу: вероятность того, что рекламный бюджет будет потрачен на потребителя, которому неинтересны предлагаемые фирмой товары будет ниже. Более того, так как онлайн поведение во время и после клика по рекламе можно измерить, маркетологи могут отслеживать и улучшать эффективность онлайн-рекламы в большей степени, чем по другим каналам. Именно данный факт позволяет увеличивать выручку как компаниям, занимающимся маркетингом, так и продавцам товаров и услуг. Также потребитель может получать определенные выгоды, например, полезную информацию о товарах, так как рекламы «подогнаны» к интересам потребителей. Также такой тип рекламы может снизить затраты производителей на коммуникацию с клиентами и затраты клиентов на получение полезной информации (Ленард и Рубин, 2009, Голдфарб и Тукер, 2010). В свою очередь выручка от таргетированной и нетаргетированной рекламы может давать средства для развития и открытия новых линий товаров и услуг или улучшению операционной бизнес модели компании. Потребители, исходя из более эффективной бизнес-модели компании и оптимизированных затрат на маркетинг могут получить товары и услуги по более низкой цене [30].

Исходя из аргументов Ленард и Рубин, 2001, сфера, где продают отчеты о кредитоспособности покупателей может являться еще одним пример, как сбор и анализ потоков данных о клиентах могут привести к увеличению

общественного благосостояния. Ленард и Рубин считают, что собранная и проанализированная информация, и затем перепроданная агентствам, занимающимся генерацией отчетов о платежеспособности, может использоваться для установления эффективной процентной ставки среди потенциальных заемщиков. Таким образом, рынок получает более равновесную процентную ставку.

Организации также могут получать косвенные выгоды от информации о клиентах, продавая ее другим компаниям. Примером может служить ситуация, когда фирма, чьим основным продуктом являются не данные о потребителях, нашла информацию, которая будет важной для другой фирмы, не являющейся ее прямым конкурентом. Примером могут служить социальные сети: для таких компаний информация о потребителях не является основным активом, и, поэтому, их пользователи становятся «продуктом». Прямым клиентом для социальных сетей являются интернет-маркетологи и дигитал-агентства, агрегаторы информации, которым интересна поведенческая информация из данной соцсети о ее пользователях.

Агрегация информации о клиентах может приносить выгодные не только тогда, когда данные являются «привязаны» к каждому пользователю продукта/услуги. Фирмы могут извлекать прибыль из знания о трендах среди потребителей. Некоторые компании, анализирующие интернет-тренды, при помощи комбинирования поведенческой информации и данных, собранных из опросов потребителей, затем могут продавать данные о трендах своим клиентам. Конечный потребитель на основе полученных данных может составить обновленную сегментацию клиентов, проверить гипотезы о выводе нового продукта на рынок и др.

Также стоит отметить, что нераскрытие некоторых данных (потенциально ведущих к общественному благосостоянию) может привести к оппортунистическим издержкам и неэффективности определенного рынка. Например, фирмы без доступа к информации о клиентах могут столкнуться со значительными входными барьерами на рынок и более низкой

конкурентноспособностью по сравнению с фирмами, владеющими большими объемами данных о клиентах. Такая ситуация может привести как к снижению конкуренции на рынке, так и к образованию монополии в долгосрочном периоде. Или обязательные Политики конфиденциальности для определенных типов данных могут быть перга стоящими для фирм, что может привести к потерям ценных данных (Статен, Кат 2003). Более того, Недостаток данных о потребителях может сделать более сложным для фирмы заниматься инновациями и предлагать новые услуги. По той же причине, неопределенность о возможных юридических ответных мерах, следующими за обработкой или сбором данных о потребителях, могут замедлить инновации продукта [18].

Аналогично затраты из-за нераскрытия данных могут быть понесены обществом в больших размерах. Например, в 2010 году канадское министерство промышленности объявило, что долгосрочный опросник Ценсус больше не будет обязательным.

Данные инициатива была обоснована позицией государства, что “Канадцев не нужно принуждать под угрозой штрафов, тюремного заключения или и того и другого одновременно, разглашать личную и частную информацию. (Даже не смотря на то что данные цензуса никогда не выпускались лицам, находящимся вне канадской статистике). Переход от обязательного к добровольному, тем не менее может привести к значительному снижению общего количества ответов в данном опроснике, Соответствующий рост риска неполучения информации свою очередь, может привести к негативному влиянию на работу политиков, исследователей и поставщиков услуг здравоохранения [25].

Выгоды от раскрытия данных должны сравниваться против инвестиционных затрат, необходимых на сбор и обработку таких данных. Данные затраты экономически обоснованы, когда фирмы ожидают получить больше выгод от анализа данных потребителей. Стоит отметить, что выгоды должны перевешивать потенциальный ущерб от нецелевого использования таких данных. Затраты на хранение, сбор данных постоянно снижаются

благодаря развитию информационных технологий. Тем не менее, внедрение систем, которые делают использование таких данных эффективным, не является простой задачей. В то же время стоит отметить, что влияние CRM систем на результативность компаний остается темой для споров. Например, Krasnikov (2009) определил, что внедрение CRM систем связано с ростом прибыльности компаний, но снижение эффективности по издержкам [29].

Субъекты данных могут получать прямые выгоды от распространения информации среди фирм. Например, клиент может получать немедленную денежную компенсацию от раскрытия ее/его персональных данных (например, скидки), или она/он может получать нематериальные выгоды (например, персонализация и кастомизация контента). В некоторых случаях, физическое лицо может также получать выгоды от его своих данных, переданных третьим сторонам. Такие выгоды могут иметь форму: улучшенных сервисов, специальных предложений, или меньшего количества спама.

Более качественная маркетинговая информация в руках компаний может также косвенно принести выгоды клиентам и обществу в виде позитивных внешних эффектов. Например, более качественные данные о потребителях могут помочь фирмам принести на рынок нишевые продукты, которые без точных данных о потенциально заинтересованных потребителях, могут посчитать слишком рискованными, чтобы их развивать (Блаттберг, Дейтон, 1991). Цены могут *иногда* снижаться как результат более таргетированной (и менее бесполезной) рекламы и маркетинга. Общественные потери усилий, потраченных на неполную и ошибочную информацию могут быть снижены в присутствии хорошо работающего рынка персональных данных. (Лаудон 1996). Правильная комбинация распространения и сокрытия различных частей информации может поэтому помочь как фирмам, так и потребителям снизить количество бесполезных мейлов и рекламы, с одной стороны и увеличить надежность собираемых данных с другой стороны [20].

Более того, потребители, ищущие скидок и выгодных предложений, могут получить выгоды от ценовой дискриминации на основе точной информации, так

как они будут иметь возможность получать товары по сниженным ценам. В соответствии с определенными микроэкономическими условиями, такие потребители могут получить выгоды от ценовой дискриминации, если им предлагают товары, которые могли никогда не быть произведены (или им предложены) в отсутствие премии, выплачиваемой такими клиентами [23].

Онлайн-реклама и в особенности таргетированная реклама, могут как информировать потребителей (обеспечивая их лучшей информацией с более низкими затратами времени на поиск), а также позволять другим сервисам, например новостным, быть бесплатными для потребителей. Такая реклама может быть визуально менее надоедлива в сравнении с нетаргетированной рекламой (Голдфарб и Тукер, 2010).

Существование вторичного рынка данных клиентов может быть также источником позитивных внешних эффектов для потребителей. Такие внешние эффекты могут иметь место, когда, например, данные, переданные вебсайту делают данные сервис более удобным или эффективным.

Агрегирование данных потребителей может дать еще одну форму позитивных внешних эффектов для потребителей. Например, потребители могут получать выгоды от транзакций, содержащих их персональные данные. Выгоды могут выражаться в форме более простого доступа к страхованию и кредиту [28].

Более того, макроэкономические выгоды могут быть следующими: анализ и агрегация онлайн-поведения, данные сенсоров и индивидуальные решения каждого отдельного экономического агента могут позволить определить заранее тренды и паттерны, которые по-другому было бы сложно или невозможно заметить, или, как минимум невозможно обнаружить в течение ограниченного периода времени. Это может принести выгоды обществу в целом: мониторинг и агрегация веб-поиска может позволить быстро определить распространение инфекционных заболеваний (Вилсон и Браунштейн, 2009), совокупность данных из мобильных устройств может быть использована для контроля за движением и пробками, данные из удаленных и распределенных сенсоров из устройств

потребителей могут быть использованы для мониторинга за окружающей средой (Дережинский и Дейттерих 2007).

Как уже указывалось выше, можно поспорить, что такие выгоды могут быть использованы потребителями без раскрытия их данных (позволяющих их определить). В то же время стоит отметить, что использование технологий, усиливающие конфиденциальность может удовлетворить как и потребность в конфиденциальности, так и необходимость в распространении данных при помощи выборочной защиты и раскрытия только части личной информации [29].

Держатели данных могут нести как материальные, так и нематериальные затраты от раскрытых данных. Некоторые из этих затрат можно связать только со сбором данных (например, когда потребители считают определенную стратегию сбора информации слишком назойливой). Другие затраты могут быть связаны с текущим использованием (и нецелевым использованием) собранных данных [33].

Онлайн и оффлайн компаний наказывались рынком за сбор данных, которое не было незаконным, но воспринималось как вторжение в личную жизнь потребителя. Самый яркий кейс был связан с клиентом amazon.com, когда клиент купил DVD за 24,49 доллара США, а после того, как клиент очистил куки, цена стала 22.74 доллара США (Стрейтфилд, 2000). Итогом данного кейса было значительное падение репутации компании. Ей пришлось выплатить компенсации клиентам, которые купили DVD по завышенным ценам, а также пообещать прекратить практику динамического ценообразования или ценовой дискриминации [35].

Не только amazon.com оказался в длинном списке компаний, которые привлекли негативное внимание клиентов из-за действий по сбору или обработке данных. Из-за тяжелых ошибок, связанных с конфиденциальностью, на многие фирмы был наложен штраф из-за нарушения их собственных политик в области конфиденциальности.

Таким образом можно сделать вывод, что целом выгоды и издержки от защиты или раскрытия персональных данных достаточно сильно зависят от:

- Бизнес-среды, в которой работает компания.

- В некоторых регионах существуют достаточно жесткие законодательные барьеры и ограничения по работе с персональными данными клиентов и сотрудников. В таких случаях работа с персональными данными становится достаточно дорогой из-за необходимых процессных и инфраструктурных изменений. Если все же работа с данными ведется, то затраты на построение инфраструктуры и изменение процессов попадают в себестоимость выпускаемого компанией продукта, что влияет на конечную цену для потребителя.

- В случае с отсутствием/нестрогими законодательными барьерами по работе с персональными данными может наблюдаться их переиспользование или сбор «лишних» данных т.е. данных, которые в текущем контексте не смогут принести пользу для организации, но затраты на их сбор, хранение, организацию, анализ уже понесены. С другой стороны из-за отсутствия стандартов и регламентов организация может использовать самые простые и недорогие решения для хранения данных, что в свою очередь может положительно сказаться на стоимости конечного продукта для потребителя.

- Внутренней культуры компании:

- Недостаточное внимание к данным и менеджмент «по ощущениям» при наличии процессов по сборе и обработке данных не приносит пользы и не дает возможность организации расти устойчиво.

- И наоборот, усиленная работа с данными и постоянный их анализ с целью получения инсайтов ведет к ускорению цикла выпуска новых продуктов, оптимизации бизнес-процессов, принятию решений на основе данных. Также постоянная и последовательная работа с данными может ускорить процесс цифровизации организации, что также несет свои выгоды в виде повышения доверия инвесторов в компании и собственников компании к действиям менеджмента.

Стоит отметить, что в зависимости от размера, выгоды и недостатки от работы с данными могут изменяться, и для выработки оптимальных

рекомендаций по внедрению политики работы с данными нужно обязательно руководствоваться лучшими практиками, совмещенными с пониманием особенностей деятельности конкретной организации.

Библиографический список:

1. https://obamawhitehouse.archives.gov/sites/default/files/docs/20150204_Big_Data_Seizing_Opportunities_Preserving_Values_Memo.pdf
2. <https://ico.org.uk> – «Big data, artificial intelligence, machine learning and data protection»
3. Acquisti, A. and J. Grossklags (2007). What can behavioral economics teach us about privacy? In S. G. C. L. Alessandro Acquisti, Sabrina De Capitani di Vimercati (Ed.), *Digital Privacy: Theory, Technologies and Practices*, pp. 363–377. Auerbach Publications (Taylor and Francis Group).
4. Joint WPISP-WPIE Roundtable – «Background paper № 3: The economics of personal data and the economics of privacy»/ Authors: Alessandro Acquisti
5. Master's thesis international business law: «Data protection in Dutch corporations». Author: Helena Uršič, Academic supervisor: Vladimir Mirkov, LL.M.
6. *The journal of legal studies* / volume 42 (2) / june 2013 – «What Is Privacy Worth?»/ Authors: Alessandro Acquisti, Leslie K. John, and George Loewenstein
7. London School of Economics – «Research and analysis to quantify the benefits arising from personal data rights under the GDPR»
8. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2580411 – «The Economics of Privacy»/ Authors: Alessandro Acquisti, Curtis Taylor, Liad Wagman
9. Lenard, T. M. and P. H. Rubin (2009). *In defense of data: Information and the costs of privacy*. Technology Policy Institute.
10. Blattberg, R. C. and J. Deighton (1991). *Interactive marketing: Exploiting the age of addressability*. *Sloan Management Review* 33(1), 5–14.
11. Chaum, D. (1983). *Blind signatures for untraceable payments*. In *Advances in Cryptology*, pp. 199–203. Plenum Press.

12. Blattberg, R. C. and J. Deighton (1991). Interactive marketing: Exploiting the age of addressability. *Sloan Management Review* 33(1), 5–14
13. https://obamawhitehouse.archives.gov/sites/default/files/docs/20150204_Big_Data_Seizing_Opportunities_Preserving_Values_Memo.pdf
14. <https://ico.org.uk> – “Big data, artificial intelligence, machine learning and data protection”
15. Acquisti, A. and J. Grossklags (2007). What can behavioral economics teach us about privacy? In S. G. C. L. Alessandro Acquisti, Sabrina De Capitani di Vimercati (Ed.), *Digital Privacy: Theory, Technologies and Practices*, pp. 363–377. Auerbach Publications (Taylor and Francis Group).
16. Joint WPISP-WPIE Roundtable - “Background paper #3: The economics of personal data and the economics of privacy”/ Authors: Alessandro Acquisti
17. Master’s thesis international business law: “Data protection in Dutch corporations”. Author: Helena Uršič, Academic supervisor: Vladimir Mirkov, LL.M.
18. *The journal of legal studies* / volume 42 (2) / june 2013 – “What Is Privacy Worth?”/ Authors: Alessandro Acquisti, Leslie K. John, and George Loewenstein
19. London School of Economics – “Research and analysis to quantify the benefits arising from personal data rights under the GDPR”
20. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2580411 – «The Economics of Privacy»/ Authors: Alessandro Acquisti, Curtis Taylor, Liad Wagman
21. Lenard, T. M. and P. H. Rubin (2009). In defense of data: Information and the costs of privacy. Technology Policy Institute.
22. Chaum, D. (1983). Blind signatures for untraceable payments. In *Advances in Cryptology*, pp. 199–203. Plenum Press.
23. Blattberg, R. C. and J. Deighton (1991). Interactive marketing: Exploiting the age of addressability. *Sloan Management Review* 33(1), 5–14
24. Akerlof, G. (1970). The Market for «Lemon»: Quality Uncertainty and the Market Mechanism. *The Quarterly Journal Of Economics*, 84(3), 488. doi: 10.2307/1879431

25. Spence, M. (1973). Job Market Signaling. *The Quarterly Journal Of Economics*, 87(3), 355. doi: 10.2307/1882010
26. Stiglitz, J. (2000). The contributions of the economics of information to twentieth century economics. *The Quarterly Journal of Economics*, 115(4), 1441–1478.
27. Spence, M. (2002). Signaling in retrospect and the informational structure of markets. *Am Econ Rev*, 92(3), 434–459.
28. Kirzner, I. (1997). Entrepreneurial discovery and the competitive market process: an Austrian approach. *J Econ Perspect*, 35(1), 60–85
29. Posner, R. A. (1978). The right of privacy. *Georgia Law Review* 12(3), 393–422.
30. Posner, R. A. (1981, May). The economics of privacy. *The American Economic Review* 71(2), 405–409.
31. Calzolari, G. and A. Pavan (2006). On the optimality of privacy in sequential contracting. *Journal of Economic Theory* 130(1), 168–204.
32. Varian, H. R. (1996). *Economic Aspects of Personal Privacy*. Technical report, University of California, Berkeley.
33. Noam, E. M. (1997). Privacy and self-regulation: Markets for electronic privacy. In U.S. Department of Commerce, *Privacy and Self-Regulation in the Information Age*.
34. Murphy, R. (1996). Property rights in personal information: An economic defense of privacy. *Geo. LJ* 84, 2381–2573.
35. Hirshleifer, J. (1980, December). Privacy: Its origins, function and future. *Journal of Legal Studies* 9(4), 649–664.
36. Odlyzko, A. (2003). Privacy, economics, and price discrimination on the internet. In *Proceedings of the 5th International Conference on Electronic Commerce (ICEC 2003)*.

References:

1. https://obamawhitehouse.archives.gov/sites/default/files/docs/20150204_Big_Data_Seizing_Opportunities_Preserving_Values_Memo.pdf
2. <https://ico.org.uk> – «big data, artificial intelligence, machine learning and data protection»
3. Acquisti, A. and J. Grossklags (2007). What can behavioral Economics tell us about privacy? In S.G.C.L. Alessandro Acquisti, Sabrina De Capitani di Vimercati (Ed.), *Digital Privacy: Theory, Technologies and Practices*, pp. 363-377. Auerbach publications (Taylor and Francis group).
4. joint WPISP-WPIE round table – «reference document № 3: the Economics of personal data and the Economics of privacy» / authors: Alessandro Acquisti
5. master's thesis on international business law: «data protection in Dutch corporations». Author: Elena Urshich, research supervisor: Vladimir mirkov, LL.M.
6. *The journal of legal studies* / volume 42 (2) / June 2013 – «What Is Privacy Worth?»/ authors: Alessandro Acquisti, Leslie K. John and George Lowenstein
7. London school of Economics – “research and analysis to quantify the benefits of personal data rights under the GDPR”
8. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2580411 – «the Economics of private life» / Authors: Alessandro Axisti, Curtis Taylor, Liad Wagman
9. Lenard, T.M. and P. H. Rubin (2009). In defense of data: information and the costs of confidentiality. Institute Of Technology Policy.
10. Blattberg, R.C. and J. Deighton (1991). Interactive marketing: using the targeting age. *Sloan Management Review* 33(1), 5-14.
11. Chaum, D. (1983). Blind signatures for untraceable payments. In *Advances in Cryptology*, pp. Plenum Press.
12. Blattberg, R.C. and J. Deighton (1991). Interactive marketing: using the targeting age. *Sloan Management Review* 33(1), 5-14
13. https://obamawhitehouse.archives.gov/sites/default/files/docs/20150204_Big_Data_Seizing_Opportunities_Preserving_Values_Memo.pdf

14. <https://ico.org.uk> – «big data, artificial intelligence, machine learning and data protection»
15. Acquisti, A. and J. Grossklags (2007). What can behavioral Economics tell us about privacy? In S.G.C.L. Alessandro Acquisti, Sabrina De Capitani di Vimercati (Ed.), *Digital Privacy: Theory, Technologies and Practices*, pp. 363-377. Auerbach publications (Taylor and Francis group).
16. joint WPISP-WPIE round table – «reference document № 3: the Economics of personal data and the Economics of privacy» / authors: Alessandro Acquisti
17. master's thesis on international business law: «data protection in Dutch corporations». Author: Elena Urshich, research supervisor: Vladimir mirkov, LL.M.
18. *The journal of legal studies* / volume 42 (2) / June 2013 – «What Is Privacy Worth?»/ authors: Alessandro Acquisti, Leslie K. John and George Lowenstein
19. London school of Economics – “research and analysis to quantify the benefits of personal data rights under the GDPR”
20. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2580411 – «the Economics of private life» / Authors: Alessandro Axisti, Curtis Taylor, Liad Wagman
21. Lenard, T.M. and P.H. Rubin (2009). In defense of data: information and the costs of confidentiality. Institute Of Technology Policy.
22. Chaum, D. (1983). Blind signatures for untraceable payments. In *Advances in Cryptology*, pp. Plenum Press.
23. Blattberg, R. C. and J. Deighton (1991). Interactive marketing: using the targeting age. *Sloan Management Review* 33(1), 5-14
24. Akerlof, G. (1970). The market for "lemons": quality uncertainty and the market mechanism. *The Quarterly Journal Of Economics*, 84(3), 488. doi: 10.2307/1879431
25. Spence, M. (1973). Signalling In The Labour Market. *The Quarterly Journal Of Economics*, 87(3), 355. doi: 10.2307/1882010
26. Stiglitz, J. (2000). Contribution of the information economy to the economy of the XX century. *The Quarterly Journal of Economics*, 115(4), 1441-1478.

27. Spence, M. (2002). Signaling in retrospect and the informational structure of markets. *Am Econ Rev*, 92(3), 434-459.
28. Kirzner I. (1997). Entrepreneurial Discovery and the competitive market process: an Austrian approach. *J Econ Perspect*, 35(1), 60-85
29. Posner R. A. (1978). Right to privacy. *Georgia Law Review* 12(3), 393-422.
30. Posner R. A. (1981, May). Economics of private life. *The American Economic Review* 71(2), 405-409.
31. Calzolari, G. and A. Pavan (2006). On the optimality of confidentiality in the sequential conclusion of contracts. *Journal of economic theory* 130(1), 168-204.
32. Varian, H. R. (1996). Economic aspects of personal life. Technical report, University of California, Berkeley.
33. Noam, E.M. (1997). Privacy and self-regulation: electronic privacy markets. At the U.S. Department of Commerce, privacy and self-regulation in the information age.
34. Murphy, R. (1996). Property rights in personal information: an economic defense of privacy. *Geo. LJ* 84, 2381-2573.
35. Hirshleifer, J. (1980, December). Privacy: its origins, functions, and future. *Journal of legal research* 9(4), 649-664.
36. Odlyzko A. (2003). Privacy, Economics, and price discrimination on the Internet. In proceedings of the 5th International conference on electronic Commerce (ICEC 2003).