СОЦИАЛЬНАЯ ФИЛОСОФИЯ

DOI: 10.17212/2075-0862-2021-13-2.1-126-142 УДК 316.472.4

ПУБЛИЧНОЕ И ПРИВАТНОЕ В ПРОФИЛЕ СОЦИАЛЬНОЙ СЕТИ (В СВЕТЕ ТЕОРИИ С. ПЕТРОНИО)[1]

Сапон Ирина Валерьевна,
старший преподаватель кафедры социологии, политологии и психологии,
Сибирский государственный университет телекоммуникаций и информатики,
Россия, 630102, г. Новосибирск, ул. Кирова, 86
ORCID: 0000-0002-7970-8460
irina.sapon@bk.ru

Аннотация

Профиль, содержащий персональные данные пользователя, представляет собой как личное, так и публичное пространство социальной сети. В связи с этим возникает проблема разграничения приватного и публичного в рамках данной виртуальной территории. В статье предпринимается попытка ответить на вопросы, где проходят границы приватности в пространстве социальной сети и кто на самом деле является владельцем личной информации, размещенной в профиле. Обозначенная проблема рассматривается сквозь призму теории управления приватностью в коммуникации (*Communication Privacy Management*) Сандры Петронио – одной из популярных в зарубежной литературе в настоящее время теорий, применяемых для изучения приватности в онлайн-среде. При помощи понятийного аппарата данной теории на примере социальной сети «ВКонтакте» рассматриваются особенности управления приватностью на личной странице пользователя (в коммуникации «один-ко-многим»). Отмечается, что для социальных сетей характерно следующее: присутствие администрации сети в качестве совладельца данных (отсутствие у пользователя возможности быть единственным владельцем своей личной информации); сложности с обсуждением правил владения информацией с другими участниками; наличие феноменов «онлайн-друзья» и «воображаемая аудитория», затрудняющих осознание пользователем состава своей реальной аудитории и проведение наиболее верных границ приватности. Также показано, что социальная сеть содержит лишь весьма условные коллективные границы приватности (если вообще можно говорить о какой-либо приватности в сети). Всё, что пользователь размещает в профиле социальной сети, выходит за пределы его личной границы приватности в зону коллективной собственности и мало поддается контролю. В дальнейших теоретических исследованиях процесса управления приватностью личных данных в про-

[1] Автор выражает признательность Д.Е. Леденеву за его неоценимый вклад на этапе подготовки данной статьи.

филе социальной сети следует критически рассмотреть понятие коллективной приватности в цифровом пространстве, а также определить права собственности первоначального владельца в случае, если информация становится общеизвестной.

Ключевые слова: самораскрытие, приватность, социальные сети, «ВКонтакте», границы приватности, теория управления приватностью, Сандра Петронио.

Библиографическое описание для цитирования:
Сапон И.В. Публичное и приватное в профиле социальной сети (в свете теории С. Петронио) // Идеи и идеалы. – 2021. – Т. 13, № 2, ч. 1. – С. 126–142. – DOI: 10.17212/2075-0862-2021-13-2.1-126-142.

Введение

Социальные сети поощряют раскрытие личных данных. Они рекомендуют пользователю указывать в профиле личную информацию (имя, фамилию, телефон, город, ссылки на аккаунты в других социальных сетях), а также делиться своими мыслями и впечатлениями с помощью статусов, записей на стене, фотографий или видео. Обновления страницы и новые публикации появляются в ленте новостей у «друзей» пользователя, привлекая их внимание и вызывая социальное одобрение в виде «лайков». Таким образом, люди добровольно и зачастую с удовольствием раскрывают на страницах социальных сетей информацию о себе [12], и в сети накапливается огромное количество личных данных пользователей. Однако такое необдуманное самораскрытие может быть небезопасно как для пользователя, так и для его близких. Эту информацию могут использовать злоумышленники при совершении различных противоправных действий.

Особенно большое количество персональных данных содержит профиль пользователя[2]. Информация в этой части социальной сети является относительно статичной и меняется реже, чем, например, на стене, где новые сообщения могут появляться достаточно часто.

Профиль представляет собой одновременно как личное, так и публичное пространство сети, что вызывает определенные сложности. Сам пользователь нередко воспринимает данную территорию как *личную*. И не без оснований: наличие возможности контролировать и менять информацию на странице профиля позволяет маркировать это пространство как личное [3, с. 42].

Тем не менее по своей природе профиль является одновременно и *публичным* виртуальным пространством. Однако пользователь может не учитывать факт публичности и продолжать чрезмерно раскрывать лич-

[2] В настоящей работе к профилю социальной сети мы относим фотографии, видео и аудиозаписи, статус, а также все персональные данные, находящиеся в статичном виде в верхней части личной страницы пользователя.

ную информацию на своей странице [13]. Таким образом, возникает проблема теоретического разграничения приватного и публичного в онлайн-среде (в частности, определение границ приватности личной информации в профиле социальной сети).

Одним из возможных подходов, который может пролить свет на эту проблему, на наш взгляд, является теория управления приватностью (ТУП) в коммуникации (Communication Privacy Management)[3] Сандры Петронио. Особенность этой теории заключается в том, что она рассматривает процессы управления приватностью через призму владения информацией, позволяя определять владельцев личной информации, их права и обязанности.

Основные положения ТУП были сформулированы Сандрой Петронио более 40 лет назад (задолго до распространения Интернет-сети) и применялись для изучения процессов раскрытия частной информации в различных сферах (в семье, в медицине, в среде ВИЧ-инфицированных). Однако в настоящий момент теория также приобрела популярность среди зарубежных исследователей приватности в цифровой среде [2]. ТУП была названа «одной из самых ценных и сложных теорий приватности, применяемых для понимания социального онлайн-взаимодействия» [10, p. 12].

В настоящей работе мы рассмотрим вопрос владения личными данными в профиле социальной сети с точки зрения основных положений рассматриваемой теории. В начале статьи приведем краткий обзор исследований приватности в эпоху социальных сетей, далее обозначим ключевые положения ТУП и опишем особенности самораскрытия в профиле с помощью этой теории. Затем представим основные выводы и обозначим направления дальнейших исследований.

Эта статья будет интересна тем, кто занимается эмпирическими и теоретическими исследованиями онлайн-приватности, а также этическими и правовыми вопросами владения личной информации. Надеемся, наша работа будет полезна и внесет свой вклад в изучение проблемы приватности в контексте отечественной науки.

Развитие теорий приватности в эпоху социальных сетей

Хотя приватность исследуется уже более 100 лет в различных сферах социальных наук [12, p. 992], единого и простого ее определения до сих пор не создано [8, p. 76]. В целом можно выделить *физическую* приватность, которая касается доступа к человеку и его личному пространству (например, защита человека и его частной собственности от постороннего вмеша-

[3] В отечественной литературе встречается мало упоминаний о теории Communication Privacy Management (CPM), и на данный момент нет утвердившейся версии ее названия на русском языке. Здесь и далее мы предлагаем использовать название «Теория управления приватностью в коммуникации» (ТУП). На наш взгляд, оно наиболее точно отражает основной смысл английской версии.

тельства, такого как обыск), и *информационную*, касающуюся права на манипуляции с личной информацией индивида (могут ли быть собраны, сохранены, обработаны и распространены его личные данные). Информационный тип приватности наиболее характерен для социальных сетей, он определяется как *возможность контролировать поток личной информации* [12, p. 990]. В рамках настоящей статьи мы будем говорить именно об этом типе приватности.

С момента появления первых интернет-медиа в социологии и психологии сформировалось три основных подхода к изучению информационной онлайн-приватности.

Первый рассматривал приватность как запланированное поведение, которое может зависеть от знаний, прошлого опыта человека и его отношения к приватности [14, p. 118]. Он базировался на теории запланированного поведения (*The Theory of Planned Behavior*, TPB), а также на предположении, что пользователи осознают наличие *рисков* в интернет-коммуникации и способны выявлять причины противоправных действий.

Во втором теоретическом подходе к описанной выше модели онлайн-приватности был добавлен фактор учета пользователем не только рисков, но и *выгод* от раскрытия личной информации, а также фактор *доверия* к социальной сети [6, p. 63]. С этой точки зрения люди часто жертвуют своей онлайн-приватностью для удовлетворения определенных потребностей и получения преимуществ.

Однако оба подхода имели серьезные ограничения при изучении приватности в социальных сетях, так как в этой среде риски потери приватности оказались неочевидны (противоправные действия выявляются далеко не всегда, а негативные последствия могут быть значительно оттянуты во времени, что часто затрудняет понимание причин и следствий) [9, p. 298].

Но существовал также и третий подход, который значительно отличался от двух предыдущих. Он был представлен теорией управления приватностью в коммуникации Сандры Петронио. Эта теория рассматривает информационную приватность как социальный и коммуникативный процесс, включающий установление личных и коллективных границ приватности и собственности на частную информацию, создание договоренностей о правилах владения этой информацией, наложение санкций за неправомерное разглашение тайн. Также в ТУП описаны универсальные критерии, влияющие на управление приватностью: культурные ценности, гендерные и возрастные различия между людьми, контекст, мотивы и цели общения, результат субъективной оценки выгод и рисков от раскрытия данных [11, p. 37].

Истоки этой теории зародились в русле психологии второй половины XX в. Многие идеи, ставшие основой ТУП, были в том или ином виде сформулированы Ирвингом Альтманом [4]. Он ввел метафору границ

приватности, которая впоследствии стала важным понятием ТУП (см. теорию границ приватности, *The Privacy Regulation Theory*). Также он описал модель взаимного самораскрытия как процесс развития взаимоотношений в диаде, целью которого является близость: партнеры рассказывают что-то откровенное о себе в ответ на подобные действия другого, взвешивают затраты и выгоды от раскрытия и решают, продолжать ли общение (см. теорию социального проникновения, *The Social Penetration Theory*).

Однако в отличие от идей Ирвинга Альтмана, ТУП постулировала, что далеко не всякое раскрытие приводит к сближению людей и далеко не всегда близость является целью самораскрытия. Так, на принятие решения о раскрытии информации могут влиять самые различные мотивы, к примеру: попытка снизить переживания, поделившись воспоминаниями о травмирующем событии (о насилии, болезни, утрате), стремление получить контроль над ситуацией или человеком.

Таким образом, описываемая теория вышла за рамки исследования самораскрытия в диаде: она смогла объяснить процессы передачи личной информации в самых различных ситуациях и формах (слухи, прилюдные разговоры, утечка информации) при взаимодействии любого количества людей.

Также этот подход существенно расширил возможности объяснения процесса управления приватностью в социальных сетях, в связи с чем получил широкое распространение среди исследователей онлайн-среды. Далее мы кратко рассмотрим основные понятия и положения ТУП.

Основные понятия и положения теории управления приватностью Сандры Петронио

В психологической традиции для обозначения раскрытия секретной, непубличной или интимной информации о себе использовался термин *самораскрытие* [11, с. 5]. Однако Сандра Петронио отходит от этого традиционного термина и расширяет предметную область до любой секретной информации. Она говорит о *раскрытии частной информации*, понимая под содержанием такого раскрытия информацию не только о себе, но и о других.

Итак, базовым термином ТУП является понятие *частная информация* (*private information*[4]). *Это любая информация, которая есть у человека (о себе или других) и в отношении которой он решает, как и когда она будет раскрыта.*

Фундаментальным положением ТУП является утверждение, что человек обладает *правом собственности на частную информацию*, то есть считает, что

[4] На русский язык термин *private information* можно перевести двояко: 1) как *частная информация*, то есть с акцентом на принадлежность к какому-либо лицу; 2) как *приватная информация*, где акцент смещается на секретность или конфиденциальность. Мы предлагаем для перевода данного термина использовать понятие *частная информация*, так как в рамках ТУП наибольшее значение все-таки имеет не секретность информации, а ее принадлежность кому-то и его право владения ею.

владеет ею и может решать, предоставлять другим доступ или отказывать им в праве владения. Соответственно, попытки со стороны посторонних людей завладеть данной информацией без согласия владельца расцениваются им как нарушение его права на неприкосновенность частной жизни.

Существует два уровня владения частной информацией и контроля над ней: *индивидуальный и коллективный* (рис. 1).

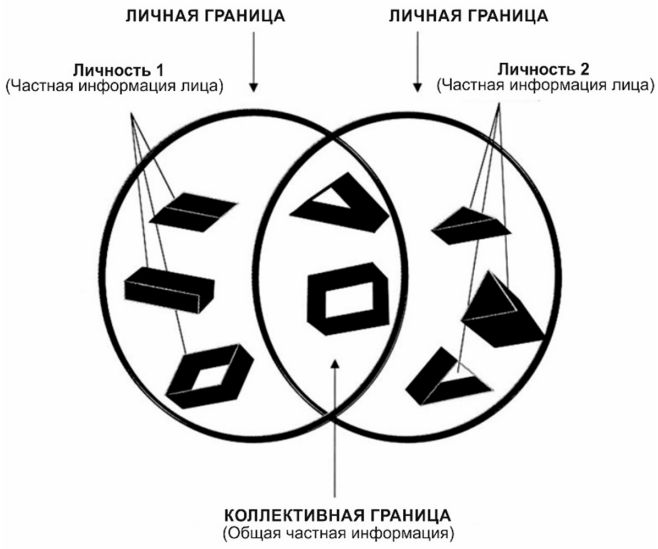

Рис. 1. Личные и коллективные границы приватности в теории управления приватностью в коммуникации

Находясь на первом (*индивидуальном*) уровне владения, субъект самораскрытия – *первоначальный владелец частной информации (original owner)* – сам решает, кому, когда и при каких обстоятельствах будет раскрыта его информация. И пока он не доверил своей информации никому, он остается ее полноправным владельцем.

Но так как люди – существа социальные и часто делятся своей информацией с другими, то нередко к первому уровню владения добавляется второй – *коллективный (second level of ownership and boundaries)*. Как только человек раскрыл кому-либо свой секрет, эта частная информация становится общей, и вокруг нее формируется *коллективная граница приватности* (выражаясь в терминах ТУП, происходит процесс *формирования совместной собственности*). Те, кому была раскрыта информация, становятся ее *уполномоченными совладельцами (authorized co-owner)* и могут распоряжаться ею в соответствии с оговоренными правилами. Правила приватности определяют, сколько информации будет раскрыто и кому, а также вправе ли совладельцы передавать информацию.

Правила устанавливаются несколькими способами. Иногда правила задаются первоначальным владельцем или передаются в ходе социализации (когда новым совладельцам сообщают об уже существующих правилах). Например, когда взрослые члены семьи учат детей не разглашать семейные тайны, или когда новых сотрудников обучают соблюдать правила конфиденциальности, принятые в организации.

Правила также могут рождаться во время совместного обсуждения. Люди договариваются о таком наборе правил, который будет удовлетворять все стороны. Так они «согласуют набор правил, согласно которым будет происходить управление границами приватности для конкретной информации» [11, p. 52]. При этом оговаривается характер границ приватности (какая ответственность ожидается от совладельцев, и насколько владельцы свободны в определении того, кто еще может узнать информацию).

После оглашения или обсуждения правил каждый совладелец должен их соблюдать, в противном случае он нарушает ожидания первоначального владельца или других членов группы и может подвергнуться наказанию. Если же правила не оговариваются и не обсуждаются, то они остаются неясными для участников коммуникации.

Граница приватности – это линия, отделяющая частную информацию от публичной; это граница собственности, показывающая, что информация находится в частном владении (см. рис. 1). Личные границы приватности регулируются одним человеком, в то время как коллективные зависят от каждого члена группы: диады, семьи, организации или общества в целом.

Каждый человек обычно является совладельцем одновременно нескольких видов частной информации и может участвовать в управлении достаточно большого количества различных границ приватности. Например, можно иметь личный или семейный секрет, знать коммерческую тайну компании, а также военную или государственную тайну своей страны.

Сандра Петронио выделяет три основных типа проницаемости границ (рис. 2), предполагающих и разные виды контроля (*высокий, умеренный и низкий*). Когда *границы закрыты, непроницаемы*, информация в пределах границ будет максимально секретной. И наоборот: *проницаемые границы* означают открытый доступ и ничем не ограниченное раскрытие информации.

Также существует риск сбоя в управлении границами приватности и нарушения правил (то есть незапланированное владельцем распространение частной информации). Это обозначается как *турбулентность границ приватности* [11, p. 33].

Причины турбулентности можно разделить на три группы: 1) нечеткие или несовпадающие границы, 2) намеренные нарушения границ и 3) ошибки.

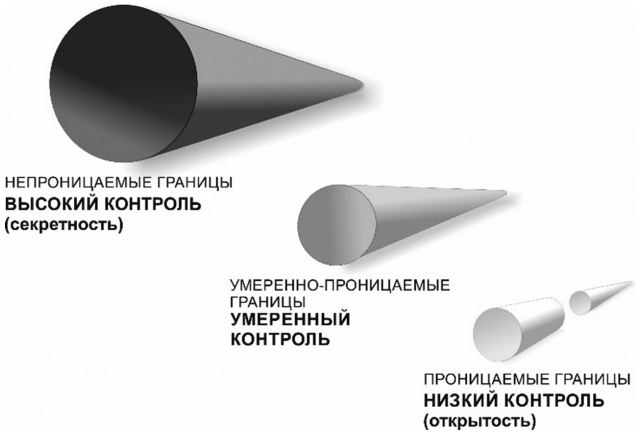

Рис. 2. Уровни контроля и проницаемость границ приватности

К примеру, *несовпадающие границы* возникают, когда пациент и врач не обсудили, что можно и чего нельзя рассказывать близким больного. В том случае, когда пациент приходит в кабинет не один, врач не обязан заботиться о конфиденциальности медицинских данных. Но пациент может расстроиться, когда доктор сошлется на предыдущее состояние здоровья больного, о котором присутствующий человек ничего не знал.

Классический случай *намеренных нарушений границ приватности* – когда отвергнутый партнер после разрыва отношений начинает раскрывать интимные детали личной жизни другого.

А примером *ошибок* являются ситуации, когда тайные сведения обсуждаются в общественных местах. Например, два врача в переполненном больничном лифте рассуждают о преимуществах удаления части легких мужчины. В этом лифте может ехать жена пациента, которая услышит их разговор. Мы совершаем подобную ошибку, когда публикуем в социальных сетях личную информацию, думая, что только друзья получат доступ к ней [7, p. 178].

Далее рассмотрим, какие особенности существуют в процессе управления приватностью в профиле социальной сети, и опишем этот процесс в терминах ТУП.

Самораскрытие пользователей в профиле социальной сети с точки зрения ТУП

На наш взгляд, для социальных сетей характерно следующее.

1. *У пользователя отсутствует возможность быть единственным владельцем своей личной информации.*

В социальных сетях управление приватностью размещаемых данных осуществляется пользователем в момент публикации или удаления личных

данных, а также с помощью применения настроек приватности профиля и добавления «друзей».

При этом об индивидуальном уровне владения частной информацией (зоне личных решений) в социальной сети говорить бессмысленно. Как только человек опубликует какие-либо сведения в сети (даже если он скроет их настройкой «Только я»), данные автоматически переходят на уровень коллективного владения, так как становятся доступны, как минимум, администрации социальной сети.

Администрация соцсети становится своеобразным молчаливым совладельцем любой информации, загружаемой пользователем. По сути, она выступает в роли арендодателя некой виртуальной территории и может видеть все данные пользователя, включая личную переписку и информацию, скрытую настройками приватности, а в некоторых случаях она имеет право использовать и передавать личную информацию пользователя другим.

Такое право на просмотр (а часто и передачу) личных данных прописано и закреплено в документе «Политика конфиденциальности», с которым каждый новый пользователь должен ознакомиться при регистрации (но его в действительности мало кто читает). Подписывая его, человек соглашается с тем, как именно в данном виртуальном пространстве будут распоряжаться его личной информацией. Закономерно, что пользователя может возмущать любая передача его данных или же их утечка в результате технического сбоя, ведь он доверил администрации сети свои личные данные, ожидая от нее неразглашения. И его ожидания не оправдались.

Но часто проблема именно в том, что пользователь не прочитал соглашение о конфиденциальности и не знает, какие права на его личные данные имеет администрация социальной сети. Таким образом, у участников онлайн-коммуникации часто не согласованы правила и не совпадают границы приватности (то есть присутствует турбулентность границ).

Итак, в социальной сети невозможна ситуация единоличного владения частной информацией и всегда есть вероятность использования личных данных пользователя не так, как он бы этого хотел.

2. *У пользователя нет возможности устанавливать для совладельцев (других пользователей) правила владения раскрытой в профиле информацией.*

Помимо администрации соцсети, другими совладельцами данных являются сетевые друзья пользователя. После того как он раскроет сведения о себе в профиле, он может с помощью настроек приватности выбрать, какой аудитории будет доступна эта информация. Можно сказать, так пользователь очерчивает границы приватности и определяет, кто имеет право видеть ту или иную информацию в профиле. Личные дан-

ные пользователя становятся частью коллективной собственности выбранной аудитории, и их распространение начинает зависеть от решений новых совладельцев.

Однако если с администрацией социальной сети у пользователя формально согласованы правила приватности, то договориться с каждым сетевым «другом» о правилах использования открытых данных профиля невозможно. В социальных сетях не предусмотрен механизм, с помощью которого пользователь мог бы сообщать «друзьям», как им распоряжаться его информацией.

Вероятно, когда нет четко оговоренных правил, тогда правилами можно считать принятые по умолчанию социальные нормы, существующие в данной культуре или в конкретном сообществе (границы дозволенного). Подозреваем, что в таком публичном онлайн-пространстве, как социальная сеть, существует основное негласное правило: всё, что загружается в сеть, может быть скопировано и распространено. Следуя этой логике, информация в профиле, раскрытая некоторому кругу сетевых «друзей», может быть передана другим лицам. Предполагается, что пользователь осознает эти риски. Однако, как показывают исследования, далеко не все пользователи задумываются об этом [13, p. 14].

Но если сетевые друзья пользователя получают информацию без четких инструкций от первоначального владельца о том, как распоряжаться этими данными, можем ли мы считать их совладельцами информации? То есть должна ли быть у доверенного лица какая-либо степень ответственности за распространение раскрытой информации, чтобы человек считался совладельцем? На наш взгляд, ответ отрицательный. Аудитория не может являться полноценным совладельцем частной информации, так как не несет никакой ответственности за приватность информации. Поэтому, раскрывая свои данные в публичном онлайн-пространстве, человек фактически лишает их приватности, но при этом нередко остается в иллюзии приватности.

Итак, раскрытие информации в профиле – процесс однонаправленный и публичный, контролировать дальнейшее распространение раскрытой информации невозможно. У первоначального владельца данных нет возможности договориться с другими о правилах совместного владения опубликованной информацией.

3. *Социальные сети изменили привычное понятие «друг» и заменили пользователю знание «реальной аудитории» представлением о «воображаемой аудитории», что создает сложности при проведении границ приватности.*

Управление границами приватности и потоком личных данных онлайн может затрудняться тем, что в социальных сетях термин «друг» обозначает любого человека, добавленного в список «друзей». Так как пользовате-

ли обычно стараются увеличить свой социальный капитал, обрастая новыми полезными связями, или пытаются достичь популярности, увеличивая число «друзей» и подписчиков, то в эту категорию попадают не только фактические друзья, но и самая разнообразная аудитория: родственники, коллеги, учителя, ученики, соседи и незнакомцы [8, p. 78].

При увеличении количества «друзей» пользователю становится сложно помнить состав этого списка. Не зная своей реальной аудитории, он заменяет ее ментальной картиной той аудитории, с которой чаще всего общается. Так его «воображаемая аудитория» начинает расходиться с реальной [5, p. 640]. В связи с этим пользователь может чрезмерно доверять своим сетевым друзьям и раскрывать для них намного больше личной информации, ошибочно проводя границы приватности не там, где мог бы их провести, если бы осознавал реальный состав этой аудитории.

4. *Внешние и внутренние коллективные границы приватности социальной сети являются открытыми или умеренно проницаемыми.*

Согласно ТУП, в каждой социальной группе могут быть как минимум две коллективные границы приватности: *внешняя* и *внутренняя*. Рассмотрим это на примере малой социальной группы – семьи.

Внешняя коллективная граница приватности семьи показывает, насколько открыто члены группы ведут себя с представителями внешнего мира, что могут и чего не могут раскрывать посторонним. Если в семье принято «не выносить сор из избы», то никто не рассказывает о семейных тайнах посторонним, то есть информация внутри семьи защищена непроницаемой внешней границей приватности. И наоборот: если члены семьи не условились хранить общие секреты, то внешняя граница приватности будет открытой или умеренно проницаемой.

Внутренняя коллективная граница приватности определяет, насколько беспрепятственно циркулирует информация внутри группы – в данном случае между членами семьи. Например, у сестры есть личный секрет. Если она раскроет его брату, то этот секрет станет их общим, и они начнут хранить его вместе (совместно удерживать коллективную границу приватности вокруг него). И если они сохранят секрет в тайне, то эта внутренняя граница приватности будет плотной, непроницаемой.

По аналогии с семьей, в социальной сети также можно увидеть внешнюю и внутренние коллективные границы приватности. Но где проходят эти границы?

Во многих интернет-сообществах, чтобы иметь доступ к личной информации пользователей, необходима регистрация. В таком случае степень проницаемости внешней границы приватности сообщества определяется сложностью процедуры регистрации. В социальной сети «ВКонтакте» процедура регистрации не составляет большого труда. Кроме того,

пользователи могут вовсе не применять настройки приватности, тогда их информация становится публичной и автоматически доступной всем членам данной социальной сети (а зачастую и всем интернет-пользователям). Таким образом, внешняя граница приватности данной социальной сети является достаточно проницаемой (открытой).

Внутренние границы социальной сети устанавливаются с помощью настроек приватности. В социальной сети «ВКонтакте» таких настроек несколько: «*Только я», «Некоторые друзья», «Некоторые списки друзей», «Только друзья», «Друзья и друзья друзей», «Все, кроме…», «Все пользователи»* (подробнее о применении настроек приватности в данной социальной сети можно прочитать в нашей предыдущей статье [1]).

На наш взгляд, наиболее плотную границу с высокой степенью контроля, при которой информация остается недоступной другим пользователям, может обеспечить настройка «Только я» (например, человек может добавлять аудиозаписи, скрывая их от других). Но даже при такой настройке личная информация всегда остается доступной как минимум администрации сети, поэтому нельзя считать эту границу полностью непроницаемой. Таким образом, любые настройки приватности социальной сети создают умеренно проницаемые или полностью проницаемые (открытые) границы.

Выводы

Теория управления приватностью в коммуникации Сандры Петронио, созданная до появления социальных сетей, удивительным образом оказалась созвучной настоящему времени. Понимание приватности в этой теории совпало с актуальным в эпоху социальных медиа понятием информационной приватности, определяемой как *возможность человека контролировать, какая информация и при каких условиях станет известна другим или останется в тайне*.

Понятийный аппарат этой теории позволяет описать процессы владения и управления личными данными в профиле социальной сети, что является важным для разграничения приватного и публичного в онлайн-пространстве.

Первоначальным владельцем данных, обладающим правом владения личной информацией в профиле, является пользователь. Однако его фактическое владение опубликованными личными данными и контроль над их распространением в социальной сети весьма условны. Всё, что пользователь размещает в профиле, выходит за пределы личной границы приватности в зону коллективной приватности и мало поддается контролю. В цифровой среде всегда велика вероятность турбулентности, а информация может быть скопирована бесконечное число раз и распространяться независимо от желания владельца. Конечно, турбулентность случается и

в реальной жизни, но в онлайн-среде компрометирующие данные могут стать доступны большому количеству людей практически моментально. В случае такой утечки оценить масштабы распространения информации очень сложно, а удалить данные практически невозможно.

Кроме того, в социальной сети невозможно быть единственным владельцем информации: всегда есть как минимум второй совладелец, с которым пользователь при регистрации заключает договор, – это администрация сети. При этом участник не всегда действует открыто и не всегда четко прописывает, как именно будут использованы личные данные пользователя. Даже если в «Политике конфиденциальности» честно сказано, что администрация социальной сети может передавать личные данные пользователя сторонним лицам, мало кто из участников сети читает этот документ. К тому же правила могут периодически изменяться без согласия пользователя. Таким образом, границы приватности участников коммуникации и их ожидания об ответственности могут не совпадать, и пользователи могут ошибочно считать, что их данные находятся под защитой.

Сандра Петронио утверждает, что для успешной коммуникации люди должны чаще договариваться о правилах приватности, сверяя с другими свои ожидания по поводу совместно контролируемой информации (чтобы добиться совпадения границ приватности). Проблема в том, что из-за специфики односторонней коммуникации «один-ко-многим», которая свойственна профилю, договориться о правилах владения и распространения личной информации невозможно. Обсуждение правил может происходить в личных сообщениях, в чатах и закрытых группах социальной сети, то есть в процессе диалога, где пользователь имеет возможность сообщить собеседникам, как они могут распоряжаться раскрытой им личной информацией. Профиль же не предполагает таких функций, что существенно усложняет управление приватностью.

Помимо этого, первоначальный владелец данных из-за специфики социальных сетей не всегда до конца осознаёт состав своей аудитории, поэтому зачастую доверяет ей больше данных, чем следовало бы, неверно проводя границы приватности.

У пользователя есть несколько способов управления границами приватности в профиле социальной сети: раскрытие или удаление информации, добавление других в «друзья» и применение настроек приватности (настройки «Только я» и «Только друзья» – умеренный контроль, «Друзья и друзья друзей» и «Все пользователи» – низкий контроль). Но эффективны ли такие средства для обеспечения приватности? На наш взгляд, есть лишь один эффективный способ сохранить конфиденциальность данных – вовсе не раскрывать их в сети. Всё, что раскрыто, останется на серверах и имеет шанс когда-либо стать доступным кому-либо еще.

В целом социальная сеть представляется нам пространством с весьма условными коллективными границами приватности (если вообще можно говорить о какой-либо приватности в сети). На данный момент никто не может гарантировать полную защиту информации, публикуемой пользователем в социальной сети: ни администрация сети, ни государство. То есть вся ответственность за приватность личных данных лежит скорее на самом пользователе.

Впрочем, с течением времени защитные механизмы социальных сетей совершенствуются. К примеру, в 2018 г. в сети «ВКонтакте» была проведена важная реформа приватности, благодаря которой у пользователей появилась возможность сделать свой профиль максимально закрытым от тех, кто не добавлен в «друзья» (раньше данная социальная сеть не позволяла скрывать даже такие важные типы информации, как список «друзей»). Но, несмотря на меры, принимаемые для защиты безопасности пользователей, до сих пор велико количество взломов аккаунтов, поэтому пользователям нужно тщательно обдумывать всю информацию, которую они выкладывают в сеть даже для близких друзей.

Ответственность за неправомерное использование данных пользователя сейчас ложится на любого оператора персональных данных (в рамках Федерального закона РФ от 27 июля 2006 года № 152-ФЗ «О персональных данных»), в том числе и на администрацию социальной сети. Тем не менее отследить факты ненадлежащей обработки данных (без согласия пользователей сети) очень сложно. Поэтому стоит быть более аккуратным с размещением личной информации в онлайн-пространстве.

Таким образом, ТУП позволила четко разграничить владельцев и совладельцев личных данных в социальных сетях и показала наличие проблем в договоренностях между совладельцами, а также существование несовпадения границ приватности между всеми участниками данной коммуникации.

Однако, на наш взгляд, остаются некоторые нерешенные теоретические вопросы. Возможна ли приватность в онлайн-пространстве? Существует ли коллективный уровень приватности в социальной сети? Где грань между коллективной приватностью и публичной информацией? И какова роль первоначального владельца в случае добровольного раскрытия своих личных данных широкой общественности? Остается ли он владельцем данных и какими обладает правами?

Возможно, этот вопрос тянет за собой и вопрос о верхней границе социальной группы. Но можем ли мы вообще говорить о социальной сети как о социальной группе, общности и сообществе, или лучше рассматривать ее как сеть, СМИ и аудиторию? Эти вопросы всё еще требуют ответа.

Литература

1. *Сапон И.В., Леденев Д.Е.* Границы приватности пользователей социальной сети «ВКонтакте» // Научное обозрение. Серия 2, Гуманитарные науки. – 2018. – № 6. – С. 93–105. – DOI: 10.26653/2076-4685-2018-6-08.

2. *Сапон И.В., Леденев Д.Е.* Самораскрытие пользователей в социальных сетях: теоретический обзор // Вестник НГУЭУ. – 2018. – № 3. – С. 267–288.

3. *Сильченкова И.А.* Конструирование личного пространства посредством онлайн-коммуникации: выпускная квалификационная работа (040100) / Санкт-Петербургский государственный университет. – СПб., 2016. – 95 с.

4. *Altman I., Taylor D.A.* Social penetration: The development of interpersonal relationships. – New York: Holt, Rinehart & Winston, 1973.

5. *Bazarova N.N., Choi Y.H.* Self-disclosure in social media: Extending the functional approach to disclosure motivations and characteristics on social network sites // Journal of Communication. – 2014. – Vol. 64, N 4. – P. 635–657. – DOI: 10.1111/jcom.12106.

6. *Dinev T., Hart P.* An extended privacy calculus model for e-commerce transactions // Information Systems Research. – 2006. – Vol. 17, N 1. – P. 61–80. – DOI: 10.1287/isre.1060.0080.

7. *Griffin E.A.* A first look at communication theory. – New York: McGraw-Hill, 2012. – 460 p.

8. *Houghton D.J., Joinson A.N.* Privacy, social network sites, and social relations // Journal of Technology in Human Services. – 2010. – Vol. 28, N 1–2. – P. 74–94. – DOI: 10.1080/15228831003770775.

9. Predicting users' privacy boundary management strategies on Facebook / Q. Liu, M.Z. Yao, M. Yang, C. Tu // Chinese Journal of Communication. – 2017. – Vol. 10, N 3. – P. 295–311. – DOI: 10.1080/17544750.2017.1279675.

10. *Margulis S.T.* Three theories of privacy: An overview // Privacy online: Perspectives on Privacy and Self-Disclosure in the Social Web. – Heidelberg; New York: Springer-Verlag, 2011. – P. 9–17.

11. *Petronio S.* Boundaries of Privacy: Dialectics of Disclosure. – Albany: State University of New York Press, 2002. – 288 p.

12. *Smith H.J., Dinev T., Xu H.* Information privacy research: an interdisciplinary review // MIS Quarterly. – 2011. – Vol. 35, N 4. – P. 989–1016.

13. *Tuunainen V.K., Pitkänen O., Hovi M.* Users' awareness of privacy on online social networking sites-case Facebook // Proceeding of the the 22nd Bled eConference. – Slovenia, 2009. – P. 42.

14. Privacy online: Perspectives on privacy and self-disclosure in the social web / ed. by S. Trepte, L. Reinecke. – Hamburg: Springer Science & Business Media, 2011. – 267 p.

Статья поступила в редакцию 14.09.2020.
Статья прошла рецензирование 11.11.2020.

DOI: 10.17212/2075-0862-2021-13-2.1-126-142

PUBLIC AND PRIVATE ON A SOCIAL MEDIA PROFILE THROUGH THE LENS OF SANDRA PETRONIO'S THEORY

Sapon Irina,
Senior Lecturer,
Department of Sociology, Political Science, Psychology,
Siberian State University of Telecommunications and Informatics,
86 Kirova Street, Novosibirsk, 630102, Russian Federation
ORCID: 0000-0002-7970-8460
irina.sapon@bk.ru

Abstract

A profile on a social network site (SNS) containing the user's personal information qualifies as both a personal and public space, which raises the problem of delineating, what is private and what is public in this virtual domain. The paper attempts to identify privacy boundaries in the social media environment and the actual ownership of personal information disclosed on users' profiles. The stated problem is considered through the lens of Communication Privacy Management theory, an influential approach to the study of privacy in the online environment proposed by Sandra Petronio. The terms and concepts of the theory are applied to analyze the peculiarities of privacy management of the user's personal information on the pages of the social network VKontakte (i.e. in the context of 'one-to-many' communication). The peculiarities noted are as follows: the presence of social media administration as a co-owner of the data (i.e. the user is not granted exclusive ownership of their personal information); difficulties with discussing information ownership rules with other social media participants; the presence of such phenomena as 'online friends' and 'the imagined audience' making it difficult for the user to recognize the composition of their actual audience and set proper privacy boundaries. It is also shown that the social network provides what can only be described as rather vague collective privacy boundaries (if the term privacy is even applicable to the social media environment). All the information shared by the user on the social media profile crosses the personal privacy boundaries and is moved almost uncontrollably to the collective ownership domain. The further theoretical research of privacy management of personal information on social media profiles should aim to critically examine the concept of collective privacy in the digital space and determine the ownership rights of original owners of personal information gone public.

Keywords: self-disclosure, privacy, social network sites, VKontakte, privacy boundaries, Communication Privacy Management, Sandra Petronio.

Bibliographic description for citation:
Sapon I. Public and Private on a Social Media Profile through the Lens of Sandra Petronio's Theory. *Idei i idealy = Ideas and Ideals*, 2021, vol. 13, iss. 2, pt. 1, pp. 126–142. DOI: 10.17212/2075-0862-2021-13-2.1-126-142.

References

1. Sapon I.V., Ledenev D.E. Granitsy privatnosti pol'zovatelei sotsial'noi seti "VKontakte" [The privacy boundaries of users of social network site VKontakte]. *Nauchnoe obozrenie. Seriya 2, Gumanitarnye nauki = Scientific Review. Series 2. Human Sciences*, 2018, no. 6, pp. 93–105. DOI: 10.26653/2076-4685-2018-6-08.

2. Sapon I.V., Ledenev D.E. Samoraskrytie pol'zovatelei v sotsial'nykh setyakh: teoreticheskii obzor [Self-disclosure on social network sites: A theoretical review]. *Vestnik NGUEU = Vestnik NSUEM*, 2018, no. 3, pp. 267–288.

3. Sil'chenkova I.A. *Konstruirovanie lichnogo prostranstva posredstvom onlain-kommunikatsii*: vypusknaya kvalifikatsionnaya rabota [Designing personal space through online communication. Bachelor's thesis]. St. Petersburg, 2016. 95 p.

4. Altman I., Taylor D.A. *Social penetration: The development of interpersonal relationships*. New York, Holt, Rinehart & Winston, 1973.

5. Bazarova N.N., Choi Y.H. Self-disclosure in social media: Extending the functional approach to disclosure motivations and characteristics on social network sites. *Journal of Communication*, 2014, vol. 64, no. 4, pp. 635–657. DOI: 10.1111/jcom.12106.

6. Dinev T., Hart P. An extended privacy calculus model for e-commerce transactions. *Information Systems Research*, 2006, vol. 17, no. 1, pp. 61–80. DOI: 10.1287/isre.1060.0080.

7. Griffin E.A. *A first look at communication theory*. New York, McGraw-Hill, 2012. 460 p.

8. Houghton D.J., Joinson A.N. Privacy, social network sites, and social relations. *Journal of Technology in Human Services*, 2010, vol. 28, no. 1–2, pp. 74–94. DOI: 10.1080/15228831003770775.

9. Liu Q., Yao M.Z., Yang M., Tu C. Predicting users' privacy boundary management strategies on Facebook. *Chinese Journal of Communication*, 2017, vol. 10, no. 3, pp. 295–311. DOI: 10.1080/17544750.2017.1279675.

10. Margulis S.T. Three theories of privacy: An overview. *Privacy online: Perspectives on Privacy and Self-Disclosure in the Social Web*. Heidelberg, New York, Springer-Verlag, 2011, pp. 9–17.

11. Petronio S. *Boundaries of Privacy: Dialectics of Disclosure*. Albany, State University of New York Press, 2002. 288 p.

12. Smith H.J., Dinev T., Xu H. Information privacy research: an interdisciplinary review. *MIS Quarterly*, 2011, vol. 35, no. 4. pp. 989–1016.

13. Tuunainen V.K., Pitkänen O., Hovi M. Users' awareness of privacy on online social networking sites-case Facebook. *Proceeding of the the 22nd Bled eConference*, Slovenia, 2009, p. 42.

14. Trepte S., Reinecke L., eds. *Privacy online: Perspectives on privacy and self-disclosure in the social web*. Hamburg, Springer Science & Business Media, 2011. 267 p.

The article was received on 14.09.2020.
The article was reviewed on 11.11.2020.