УДК 316.472.4

Управление приватностью в профиле социальной сети: анализ теории Сандры Петронио

Сапон Ирина Валерьевна[1], Леденев Дмитрий Евгеньевич[2]

[1] *Кафедра социологии, политологии и психологии, Сибирский государственный университет телекоммуникаций и информатики, Новосибирск, Российская Федерация.*

[2] *Кафедра вычислительных систем, Сибирский государственный университет телекоммуникаций и информатики, Новосибирск, Российская Федерация.*

Аннотация. В статье обсуждается возможность применения теории управления приватностью в коммуникации (Communication privacy management) Сандры Петронио для исследования самораскрытия пользователей в профиле социальной сети. В связи с возросшей популярностью социальных сетей и приложений, использующих открытые данные пользователей, конфиденциальность личных данных стала одной из важных областей исследований. Однако принятие решения относительно раскрытия личных данных и степени их приватности в онлайн-пространстве представляет собой более сложный процесс по сравнению с традиционными видами коммуникации. Он не может быть объяснён с точки зрения классических моделей самораскрытия, созданных в эпоху до Интернета. Цель данной статьи — рассмотреть процесс управления приватностью в профиле социальной сети (в коммуникации «один-ко-многим») и проверить, возможно ли объяснить данный процесс с помощью теории Сандры Петронио. Проведённый в статье анализ литературы позволил выделить характерные особенности управления приватностью в профиле: пользователь не может видеть реакцию других на раскрытие своих данных, при этом он сталкивается с такими явлениями как воображаемая аудитория и коллапс кон*текстов.* Всё это затрудняет осознание состава реальной аудитории и проведение наиболее верных границ приватности. Критический анализ основных положений теории Сандры Петронио показал, что теория позволяет описать социальные отношения, возникающие при управлении приватностью в профиле, и определить права и обязанности участников процесса коммуникации. В то же время авторами отмечается, что теория не учитывает некоторые особенности онлайн-контекста. Например, администрация социальной сети всегда является совладельцем информации, которую раскрыл пользователь. При этом у него нет возможности договориться с другими пользователями о правилах приватности, поэтому ответственность за приватность личных данных лежит на самом пользователе. В дополнение к уже описанным в данной теории факторам, оказывающим влияние на процесс принятия решения о приватности информации, авторы приводят факторы, имеющие значение в онлайн-среде.

Ключевые слова: самораскрытие, личные данные, социальные сети, профиль, теория управления приватностью.

Privacy Management on SNS Profile: Analysis of Sandra Petronio's Theory

Irina V. Sapon[1], Dmitrii E. Ledenev[2]

[1]*Department of Sociology, Political Science and Psychology, Siberian State University of Telecommunications and Informatics, Novosibirsk, Russian Federation*

[2]*Department of Computing Systems, Siberian State University of Telecommunications and Informatics, Novosibirsk, Russian Federation*

Abstract. The article discusses the possibility of Communication Privacy Management theory applying to research the self-disclosure in a social network site (SNS) profile. In response to increased popularity of SNS and applications that use open user data, the privacy of personal information has become an important area of research. However, making the decision about self-disclosure and privacy in the online space is a more complex process compared to traditional forms of communication. It cannot be explained in terms of the self-disclosure classical models created in the pre-Internet era. The purpose of this article is to test the possibility of explaining the privacy management process in the SNS profile (in one-to-many communication) using Sandra Petronio's theory. Analyzing the results of research, we highlighted the features of privacy management in the profile: the user cannot see the others reaction to his self-disclosure and he also face such phenomena as an imaginary audience and the context collapse. It makes difficult to understand the real audience composition and draw the most correct privacy boundaries. A critical analysis of the main suppositions of the Sandra Petronio's theory has been conducted. The results showed that the theory allows to describe social relations and determine the rights and participants obligations in the privacy management process in SNS profile. At the same time, the theory does not take into account certain features of the online context. For example, SNS administration is always the co-owner of the user's disclosed information. Meanwhile, only user is fully responsible for privacy his personal data because he does not have the ability to discuss privacy rules with other users. The authors present their own factors that influence the decision-making process on the information privacy online in addition to the factors already described in the theory.
Keywords: self-disclosure, personal data, social network sites, profile, communication privacy management.

Тюменский индустриальный университет

Известия высших учебных заведений. Социология. Экономика. Политика.

Выпуск: №01/2020

Том: 1

УПРАВЛЕНИЕ ПРИВАТНОСТЬЮ В ПРОФИЛЕ СОЦИАЛЬНОЙ СЕТИ: АНАЛИЗ ТЕОРИИ САНДРЫ ПЕТРОНИО

Сапон Ирина Валерьевна

-, Старший преподаватель, Кафедра социологии, политологии и психологии гуманитарного факультета, Сибирский государственный университет телекоммуникаций и информатики

Леденев Дмитрий Евгеньвич

-, студент, Кафедра вычислительных систем, Сибирский государственный университет телекоммуникаций и информатики

Аннотация

В статье обсуждается возможность применения теории управления приватностью в коммуникации (Communication privacy management) Сандры Петронио для исследования самораскрытия пользователей в профиле социальной сети. В связи с возросшей популярностью социальных сетей и приложений, использующих открытые данные пользователей, конфиденциальность личных данных стала одной из важных областей исследований. Однако принятие решения относительно раскрытия личных данных и степени их приватности в онлайн-пространстве представляет собой более сложный процесс по сравнению с традиционными видами коммуникации. Он не может быть объяснён с точки зрения классических моделей самораскрытия, созданных в эпоху до Интернета. Цель данной статьи — рассмотреть процесс управления приватностью в профиле социальной сети (в коммуникации «один-ко-многим») и проверить, возможно ли объяснить данный процесс с помощью теории Сандры Петронио. Проведённый в статье анализ литературы позволил выделить характерные особенности управления приватностью в профиле: пользователь не может видеть реакцию других на раскрытие своих данных, при этом он сталкивается с такими явлениями как воображаемая аудитория и коллапс контекстов. Всё это затрудняет осознание состава реальной аудитории и проведение наиболее верных границ приватности. Критический анализ основных положений теории Сандры Петронио показал, что теория позволяет описать социальные отношения, возникающие при управлении приватностью в профиле, и определить права и обязанности участников процесса коммуникации. В то же время авторами отмечается, что теория не учитывает некоторые особенности онлайн-контекста. Например, администрация социальной сети всегда является совладельцем информации, которую раскрыл пользователь. При этом у него нет возможности договориться с другими пользователями о правилах приватности, поэтому ответственность за приватность личных данных лежит на самом пользователе. В дополнение к уже описанным в данной теории факторам, оказывающим влияние на процесс принятия решения о приватности информации, авторы приводят факторы, имеющие значение в онлайн-среде.

Ключевые слова:

самораскрытие, личные данные, социальные сети, профиль, теория управления приватностью

Industrial University of Tyumen

Proccedings of Higher Educational Institutions. Sociology. Economy. Politics.

Issue: №01/2020

Volume: 1

Privacy Management on SNS Profile: Analysis of Sandra Petronio's Theory

Sapon Irina Valeryevna

-, The Senior Lecturer, Department of Sociology, Political Science and Psychology of The Faculty of Humanities, Siberian State University of Telecommunications and Informatics

Ledenev Dmitrii Evgenievich

-, студент, Department of Computing Systems, Siberian State University of Telecommunications and Informatics

Abstract

The article discusses the possibility of Communication Privacy Management theory applying to research the self-disclosure in a social network site (SNS) profile. In response to increased popularity of SNS and applications that use open user data, the privacy of personal information has become an important area of research. However, making the decision about self-disclosure and privacy in the online space is a more complex process compared to traditional forms of communication. It cannot be explained in terms of the self-disclosure classical models created in the pre-Internet era. The purpose of this article is to test the possibility of explaining the privacy management process in the SNS profile (in one-to-many communication) using Sandra Petronio's theory. Analyzing the results of research, we highlighted the features of privacy management in the profile: the user cannot see the others reaction to his self-disclosure and he also face such phenomena as an imaginary audience and the context collapse. It makes difficult to understand the real audience composition and draw the most correct privacy boundaries. A critical analysis of the main suppositions of the Sandra Petronio's theory has been conducted. The results showed that the theory allows to describe social relations and determine the rights and participants obligations in the privacy management process in SNS profile. At the same time, the theory does not take into account certain features of the online context. For example, SNS administration is always the co-owner of the user's disclosed information. Meanwhile, only user is fully responsible for privacy his personal data because he does not have the ability to discuss privacy rules with other users. The authors present their own factors that influence the decision-making process on the information privacy online in addition to the factors already described in the theory.

Keywords:

self-disclosure, personal data, social network sites, profile, communication privacy management

УДК 316.472.4

Управление приватностью в профиле социальной сети: анализ теории Сандры Петронио

Сапон Ирина Валерьевна[1], Леденев Дмитрий Евгеньевич[2]

[1] *Кафедра социологии, политологии и психологии, Сибирский государственный университет телекоммуникаций и информатики, Новосибирск, Российская Федерация.*

[2] *Кафедра вычислительных систем, Сибирский государственный университет телекоммуникаций и информатики, Новосибирск, Российская Федерация.*

Аннотация. В статье обсуждается возможность применения теории управления приватностью в коммуникации (Communication privacy management) Сандры Петронио для исследования самораскрытия пользователей в профиле социальной сети. В связи с возросшей популярностью социальных сетей и приложений, использующих открытые данные пользователей, конфиденциальность личных данных стала одной из важных областей исследований. Однако принятие решения относительно раскрытия личных данных и степени их приватности в онлайн-пространстве представляет собой более сложный процесс по сравнению с традиционными видами коммуникации. Он не может быть объяснён с точки зрения классических моделей самораскрытия, созданных в эпоху до Интернета. Цель данной статьи — рассмотреть процесс управления приватностью в профиле социальной сети (в коммуникации «один-ко-многим») и проверить, возможно ли объяснить данный процесс с помощью теории Сандры Петронио. Проведённый в статье анализ литературы позволил выделить характерные особенности управления приватностью в профиле: пользователь не может видеть реакцию других на раскрытие своих данных, при этом он сталкивается с такими явлениями как воображаемая аудитория и коллапс кон*текстов.* Всё это затрудняет осознание состава реальной аудитории и проведение наиболее верных границ приватности. Критический анализ основных положений теории Сандры Петронио показал, что теория позволяет описать социальные отношения, возникающие при управлении приватностью в профиле, и определить права и обязанности участников процесса коммуникации. В то же время авторами отмечается, что теория не учитывает некоторые особенности онлайн-контекста. Например, администрация социальной сети всегда является совладельцем информации, которую раскрыл пользователь. При этом у него нет возможности договориться с другими пользователями о правилах приватности, поэтому ответственность за приватность личных данных лежит на самом пользователе. В дополнение к уже описанным в данной теории факторам, оказывающим влияние на процесс принятия решения о приватности информации, авторы приводят факторы, имеющие значение в онлайн-среде.

Ключевые слова: самораскрытие, личные данные, социальные сети, профиль, теория управления приватностью.

Privacy Management on SNS Profile: Analysis of Sandra Petronio's Theory

Irina V. Sapon[1], Dmitrii E. Ledenev[2]

[1]*Department of Sociology, Political Science and Psychology, Siberian State University of Telecommunications and Informatics, Novosibirsk, Russian Federation*

[2]*Department of Computing Systems, Siberian State University of Telecommunications and Informatics, Novosibirsk, Russian Federation*

Abstract. The article discusses the possibility of Communication Privacy Management theory applying to research the self-disclosure in a social network site (SNS) profile. In response to increased popularity of SNS and applications that use open user data, the privacy of personal information has become an important area of research. However, making the decision about self-disclosure and privacy in the online space is a more complex process compared to traditional forms of communication. It cannot be explained in terms of the self-disclosure classical models created in the pre-Internet era. The purpose of this article is to test the possibility of explaining the privacy management process in the SNS profile (in one-to-many communication) using Sandra Petronio's theory. Analyzing the results of research, we highlighted the features of privacy management in the profile: the user cannot see the others reaction to his self-disclosure and he also face such phenomena as an imaginary audience and the context collapse. It makes difficult to understand the real audience composition and draw the most correct privacy boundaries. A critical analysis of the main suppositions of the Sandra Petronio's theory has been conducted. The results showed that the theory allows to describe social relations and determine the rights and participants obligations in the privacy management process in SNS profile. At the same time, the theory does not take into account certain features of the online context. For example, SNS administration is always the co-owner of the user's disclosed information. Meanwhile, only user is fully responsible for privacy his personal data because he does not have the ability to discuss privacy rules with other users. The authors present their own factors that influence the decision-making process on the information privacy online in addition to the factors already described in the theory.
Keywords: self-disclosure, personal data, social network sites, profile, communication privacy management.

Введение

Одной из причин невероятной популярности социальных сетей является то, что они просты в использовании и позволяют «буквально в один клик» обмениваться информацией (новостями, мыслями, опытом) с близкими и знакомыми независимо от расстояния [1]. Как отмечают исследователи, публикуя информацию на своей личной странице, пользователь получает определённые социальные выгоды: упрощение процесса построения отношений с другими, увеличение доверия с ними [2], возможность добиться определённой популярности и создать положительное впечатление о себе [3].

Одним из способов рассказать о себе в социальной сети является заполнение профиля. Он представляет собой личное пространство пользователя, в котором тот может указать, например, свои интересы, мировоззрение, образование, место работы, номер телефона, а также ссылки на аккаунты в других социальных сетях. Данное пространство является не только личным, но и публичным: вся информация, размещенная в нём, доступна и другим пользователям, которым был предоставлен доступ.

Заполнение профиля можно считать некой социальной нормой: пользователь рассказывает о себе какую-либо информацию, другие, в свою очередь, также раскрывают личные данные. Обычно участникам социальной сети интересно, что публикуют другие пользователи, и они часто наблюдают друг за другом: просматривают фотографии, списки друзей, записи и комментарии на стене [4]. Заполненный профиль создает ощущение открытости и готовности к коммуникации, позволяет пользователю создать положительный образ себя [5]. Раскрытие интересов в профиле может облегчить знакомство и узнавание других людей, помочь в поиске единомышленников. Схожие интересы создают предпосылки к успешной коммуникации и развитию отношений [6].

Однако самораскрытие в социальных сетях связано с определёнными рисками: персональные данные в профиле могут использоваться злоумышленниками в преступных целях. Также маркетинговые компании без ведома и согласия самих пользователей собирают и анализируют их личную информацию для предложения микротаргетинговой рекламы. Нередко пользователи знают о возможных рисках, но продолжают публиковать личную информацию в социальной сети. Из-за кажущейся нелогичности такого поведения, данное явление получило название «парадокс приватности» [7].

В связи с этим становится необходимым более подробно рассмотреть, как пользователь принимает решение о самораскрытии в профиле социальной сети и управляет приватностью личных данных в этом онлайн-пространстве.

Однако социальная сеть, и, в частности, профиль, является относительно новым и малоизученным пространством коммуникации со своими характерными особенностями. В связи с этим возникает вопрос, применимы ли существующие теоретические концепции для описания процессов самораскрытия и управления приватностью в профиле социальной сети.

В 2018 году нами был проведён теоретический обзор, который включил 76 зарубежных эмпирических исследований, опубликованных с 1999 по 2017 годы [8]. Он показал, что при изучении процессов самораскрытия и приватности в социальных сетях применяются следующие теории:

Теория управления приватностью в коммуникации Сандры Петронио (ТУП) была оценена нами как наиболее разработанная и перспективная теория, с помощью которой можно описать поведение пользователей, связанное с самораскрытием и приватностью в профиле социальной сети (в коммуникации по типу «один-ко-многим»). К тому же, в отличие от других, она даёт наиболее широкое представление о факторах, влияющих на решение пользователя о приватности.
В данной работе мы рассмотрим управление приватностью в профиле социальной сети и оценим, применимы ли основные принципы ТУП для описания данного процесса. Сформулируем исследовательские вопросы статьи:

В ходе нашего исследования мы выделим сильные стороны данной теории, которые в

дальнейшем могут быть использованы при создании теоретической концепции, способной наиболее полно охватить все аспекты приватности в таком уникальном пространстве, как профиль социальной сети. Данная работа может быть интересна исследователям, занимающимся вопросами самораскрытия и приватности, а также администрациям социальных сетей, которые задумываются об удобстве и безопасности пользователей.

Материалы и методы

В данной работе под управлением приватностью мы понимаем управление потоком личной информации [9, с 990]. Соответственно, неотъемлемой частью данного процесса является решение человека о раскрытии. Самораскрытие определяется современными исследователями как намеренная передача информации о себе другому [10].

Профиль рассматривается нами как часть лично-публичного пространства социальной сети, в котором пользователь раскрывает информацию о себе. Это могут быть фото и видеозаписи, сведения о месте работы и образовании, а также интересы и взгляды пользователя. В рамках нашей работы мы не относим записи на стене к самораскрытию в профиле, так как рассматриваем последнее как однонаправленную коммуникацию между адресатом и его аудиторией по типу «один-ко-многим».

Материалами для исследования стали зарубежные эмпирические работы, в которых изучались вопросы приватности личных данных пользователей социальных сетей и проверялись положения ТУП. Анализируя положения теории, мы также опирались на монографию и статьи автора теории — Сандры Петронио: «Boundaries of Privacy: Dialectics of Disclosure» [11], «Brief status report on communication privacy management theory» [12], «Communication privacy management theory» [13].

Для выявления характерных особенностей процесса управления приватностью в профиле социальной сети авторами использовался метод синтеза, который позволил соединить результаты анализа зарубежной литературы с выводами, основанными на личном опыте пребывания в социальных сетях.

Особенности управления приватностью в профиле социальной сети

Исследователи утверждают, что решение о раскрытии личных данных зависит от среды, в которой происходит общение [14]. В зависимости от ситуации и контекста человек выбирает подходящую стратегию управления приватностью [11], которая обеспечивала бы желаемый уровень приватности в конкретный момент времени [15]. Профиль социальной сети — это уникальная среда, являющаяся одновременно и личной, и публичной. Соединение приватного и публичного пространств усложняет процесс управления приватностью в данной среде.

Для профиля также характерны и другие особенности, которые, так или иначе, оказывают влияние на решение пользователя о приватности. Приведём их ниже.

1. В профиле социальной сети коммуникация строится по типу «один-ко-многим»: информация раскрывается для определённой аудитории и не предполагает

интерактивного взаимодействия. Преимуществом социальной сети является возможность продвижения личного профиля как бренда. Чтобы добиться популярности, пользователи нередко увеличивают количество друзей и подписчиков, добавляя незнакомцев. Однако у данного поведения есть и минусы: пользователь перестаёт осознавать реальный состав своей аудитории. Это объясняется тем, что её размер начинает превышать «число Данбара» - максимальное количество людей (150-200), с которыми в силу когнитивных и временных причин возможно поддерживать связь и считать их близкими [16]. В этом случае пользователь начинает распространять свойства знакомого ему круга лиц на всех потенциальных получателей информации. Данный феномен получил название «воображаемая аудитория» [17]. Он объясняет, почему пользователь начинает чрезмерно доверять своим сетевым «друзьям» и раскрывать в профиле намного больше личной информации, чем если бы он точно знал реальный состав аудитории.

2. Если для пользователя личная информация является способом рассказать о себе, то для социальной сети она является неким «товаром», который можно использовать для предложения персонализированной рекламы. Поэтому социальные сети заинтересованы в том, чтобы пользователи раскрывали личную информацию в профиле. Они обычно устроены таким образом, чтобы подталкивать пользователя к самораскрытию. Например, на странице пользователя обычно располагается баннер «Что у вас нового?» или упоминание о том, какая информация в профиле осталась не указана.

3. Раскрываемая в профиле информация (как и любые цифровые данные), обладает свойством масштабируемости: она может распространяться дальше, чем это изначально задумывалось пользователем, раскрывшим её [7]. Данные становятся доступными для поиска и копирования, что усложняет или даже делает невозможным их полное удаление из социальной сети. Поэтому в контексте профиля социальной сети пользователь должен быть особенно осторожным, когда решает опубликовать ту или иную информацию о себе.

4. В социальной сети размывается понятие «друг» - его можно применить к различным категориям людей: родственникам, одногруппникам, коллегам по работе или просто знакомым. В связи с этим пользователю становится сложнее определить, какую информацию он может раскрывать, не нарушая при этом ожиданий каждого. Данное явление получило название «коллапс контекста» - ситуации, в которой пользователь вынужден соответствовать одновременно ожиданиям различных аудиторий, которые ранее разделялись временными, пространственными и социальными границами [7]. Таким образом, если в традиционной коммуникации человек с разными людьми может вести себя по-разному, то в публичном пространстве социальной сети у него такой возможности нет.

5. Процесс управления приватностью в профиле социальной сети осложняется тем, что в отличие от традиционной коммуникации, он представляет собой двухэтапный процесс. Решение о том, что раскрывать и кому — оторваны друг от друга и реализуются с помощью разных функций [3]. Так, чтобы раскрыть информацию в профиле необходимо заполнить определенные поля. Однако если информация предназначена только для определённой аудитории, необходимо также выбрать

соответствующее положение настроек приватности.

Таким образом, профиль социальной сети - уникальное пространство, для которого характерны не только простота использования, но и ряд трудностей, возникающих в процессе управления приватностью. Нормы, сложившиеся в контексте данного онлайн-пространства, а также администрация социальной сети подталкивают пользователя заполнять информацию в профиле. Также пользователь сталкивается с явлениями «воображаемой аудитории» и «коллапса контекстов», масштабируемости и неудаляемости данных.

Учитывая перечисленные выше особенности рассмотрим, можно ли применить ТУП для описания процесса управления приватностью в профиле социальной сети.

Применение положений ТУП к изучению самораскрытия в профиле социальной сети

Теория управления приватностью в коммуникации разрабатывалась Сандрой Петронио для объяснения того, как люди управляют приватностью на индивидуальном и коллективном уровнях. Согласно ТУП, на индивидуальном уровне люди принимают решение о раскрытии и сокрытии личной информации, а также выбирают степень её секретности и аудиторию, для которой она будет доступна [11;12]. Они считают, что владеют своей личной информацией и имеют право контролировать доступ к ней [18]. На коллективном уровне происходит раскрытие информации другим людям, с которыми оговариваются правила её хранения и передачи третьим лицам. В случае, если информация, вопреки желанию людей, теряет свою секретность, они предпринимают меры по защите её от дальнейшего распространения.

Рассмотрим основные принципы ТУП подробнее.

Принцип 1. Люди считают, что они владеют своей частной информацией и управляют степенью её приватности.

Фундаментальным положением ТУП является утверждение о том, что люди могут считать определённые данные своей собственностью. В терминах теории такая информация называется *частной* (private information) и подразумевает любую информацию о себе или о других, в отношении которой человек может решать, что будет происходить с ней в дальнейшем. Так, например, он вправе определять степень её публичности, то есть выбирать аудиторию, для которой она будет доступна.

Применяя это положение к интернет-среде, следует учесть следующее. При регистрации в социальной сети пользователь вынужден принять «Политику конфиденциальности» и согласиться с тем, что в любой момент времени администрация платформы имеет доступ к его личным данным. То есть любая информация, которую пользователь размещает в своём профиле, также является собственностью администрации социальной сети. Таким образом, можно говорить о том, что человек в этом онлайн-пространстве теряет право единоличного владения частной информацией, даже если сам так не считает.

Согласно ТУП, информация, которая принадлежит человеку, находится в пределах его *личной границы приватности*. Она представляют собой условную черту, выходя за

которую частная информация становится известна другим [11, с. 6]. Границы могут быть *проницаемыми* (открытыми) и *непроницаемыми* (закрытыми). Если человек не раскрыл личную информацию, она остаётся в пределах его личной границы, которую в данном случае можно считать закрытой и непроницаемой. В случае же если он сообщает кому-либо данные, он делает границу приватности вокруг них проницаемой.

Учитывая вышеописанные свойства социальной сети, нетрудно догадаться, что единственной возможностью пользователя сохранить приватность данных в онлайн-пространстве является отказ от их раскрытия. Лишь в этом случае информация остаётся в пределах его личной границы приватности и доступна только ему.

Таким образом, применяя принцип №1 теории, можно отметить, что в социальной сети у пользователя нет возможности единоличного владения частной информацией. Администрация социальной сети является совладельцем всех данных пользователя. Следовательно, единственным способом сохранить приватность является отказ от самораскрытия, что в терминах ТУП означает проведение непроницаемой личной границы приватности.

Принцип 2. Люди управляют конфиденциальностью своей частной информации с помощью личных правил приватности.

Второй принцип теории гласит, что границы приватности зависят от *правил приватности*, которые отражают личные установки, убеждения и ожидания людей относительно того, кто, когда и при каких обстоятельствах может узнать данную информацию [13]. На правила приватности оказывают влияние культурные, гендерные, мотивационные и контекстуальные критерии, а также соотношение воспринимаемых рисков и выгод от раскрытия [11, с. 24-25]. К примеру, на решение пользователя о публикации фотографии в купальнике на странице социальной сети могут повлиять мотивы, а также уместность такого раскрытия в культуре пользователя.

Однако, как показал анализ литературы, в онлайн-пространстве, существует ряд дополнительных факторов, влияющих на формирование правил приватности пользователей. Было замечено, что ценность информации влияет на то, будет ли она раскрыта: пользователи чаще публикуют те данные, которые представляют для них наименьшую ценность [19]. При этом одна и та же информация для разных людей может иметь неодинаковую ценность [20]. К тому же, чем больше пользователь заботится о приватности своей информации, тем меньше объём его самораскрытия в социальных сетях [21].

На процесс управления приватностью также оказывает влияние уровень цифровой грамотности: наиболее «подкованные» пользователи, как правило, знают о существовании настроек приватности и чаще их применяют [22]. Использование настроек создаёт у пользователя ощущение контроля и позволяет ему чувствовать себя в безопасности [20]. И чем более подробные настройки приватности доступны в социальной сети, тем сильнее это чувство [4].

Таким образом, при раскрытии информации в профиле социальной сети, пользователь руководствуется личными правилами приватности. На них, как мы показали, влияют

не только факторы, обозначенные Сандрой Петронио (культура, гендер, мотивы, контекст, соотношение рисков и выгод), но и критерии, обусловленные особенностями данной среды. Например, ценность информации, беспокойство о приватности, уровень цифровой грамотности. Так, если информация не обладает большой ценностью для пользователя и он не обеспокоен её приватностью, вероятнее всего, он раскроет её для других. С большей вероятностью пользователь заполнит профиль, если социальная сеть позволяет установить подробные настройки приватности. Однако если уровень цифровой грамотности пользователя высок, он скорее откажется от раскрытия.

Принцип 3. При предоставлении доступа к частной информации другому человеку, тот становится совладельцем этой информации.

Как только человек решает поделиться частной информацией, она покидает личную границу приватности и становится коллективной собственностью. Тот, кто раскрывает свою информацию, согласно теории, является *первоначальным владельцем,* а те, кому информация раскрывается, становятся *уполномоченными совладельцами.* Они вместе начинают нести ответственность за то, как используется и распространяется общая информация [11;12], которая теперь находится в *коллективной границе приватности.*

Как было рассмотрено в первом принципе, в случае, если пользователь заполнил профиль социальной сети, первым совладельцем данной информации становится администрация платформы. Чтобы включить в коллективную границу не только администрацию социальной сети, но и других пользователей, первоначальный владелец использует настройки приватности. С помощью них он выбирает, какая информация будет доступна той или иной группе пользователей. Как правило, пользователи из списка «друзей» наделяются правом доступа к большему количеству информации, чем остальные. Между пользователем и данными людьми создается наиболее проницаемая граница приватности [23].

Однако, как мы отмечали ранее, в категорию «друзья» в социальной сети могут попадать различные группы пользователей. В том числе и незнакомые. Следовательно, в коллективной границе приватности не всегда оказываются люди, которые готовы нести ответственность за совместное хранение личной информации.

Таким образом, с момента регистрации пользователя в социальной сети вся размещённая им информация в профиле становится доступна и для администрации сети, то есть последняя наделяется правами владения этих данных. Чтобы сформировать коллективную границу приватности с другими пользователями, необходимо предоставить им доступ с помощью настроек приватности. Однако размытие понятия «друг» и наличие явления «воображаемой аудитории» затрудняет пользователю проведение наиболее верных границ приватности в социальной сети.

Принцип 4. Совладельцы частной информации должны договориться о взаимоприемлемых правилах приватности.

Когда люди раскрывают личную информацию, они теряют часть контроля над её дальнейшим распространением, что может вызвать чувство уязвимости. Чтобы сохранить ощущение контроля над информацией, совладельцы участвуют в процессе

согласования правил приватности, то есть договариваются о том, как совместно владеть и распоряжаться частной информацией. Эти правила регламентируют, каким количеством прав обладает каждый из совладельцев, а также кому и в каком количестве разрешено раскрывать совместную информацию. CPM определяет три типа таких правил [20]:

Рассмотрим их подробнее.

1) Правила совместного владения определяют, какие права и обязанности есть у совладельцев относительно общей информации.

В социальных сетях предметом договора является личная информация пользователя. А совладельцем данной информации является администрация платформы. Их права и обязанности оговорены в «Политике конфиденциальности» социальной сети. При этом участник соцсети не имеет возможность обсудить с ней правила совместного владения. В любой момент администрация сети может внести изменения в этот документ и, соответственно, пользователь либо соглашается с ними и продолжает использование социальной сети, либо отказывается и прекращает участие в ней.

2) Правила объединения границ приватности определяют, для кого разрешается раскрывать совместно хранимую информацию. То есть кто ещё может быть включён в круг совладельцев. Например: «Не говорите маме об этом».

В социальной сети с помощью настроек приватности мы сообщаем администрации платформы свои ожидания по поводу того, каких пользователей мы бы хотели видеть в качестве совладельцев. Впрочем, возможен выбор варианта настройки «только мне», при котором совладельцем остаётся только администрация сети.

3) *Правила проницаемости границ* определяют, какое количество совместной информации можно раскрывать третьим лицам — людям, не входящим в круг совладельцев. Например, может быть установлено следующее правило: «Вы можете сказать маме, но не говорите ей слишком много деталей».

В социальной сети с помощью настроек приватности пользователь определяет, какую информацию в профиле он бы хотел сделать доступной для различных категорий пользователей. К примеру, он может сделать открытыми для всех пользователей данные о городе проживания, так как не считает их секретными. В то же время он может ограничить круг лиц, для которого будет доступен номер его телефона, так как не хочет, чтобы эту информацию знали многие.

Таким образом, согласно ТУП, раскрывая информацию другим и включая их в коллективную границу приватности, люди должны договориться о правилах приватности. Однако в профиле социальной сети, в отличие от оффлайн-коммуникации, невозможно договориться о правилах приватности ни с кем, кроме администрации сети. При этом договор является односторонним: пользователь может лишь соглашаться с установленными правилами, но не может вносить в них изменения. В то же время пользователь имеет право сообщать администрации свои ожидания по поводу третьих лиц с помощью предоставляемых социальной сетью инструментов (например,

добавляя пользователя в «друзья» и применяя настройки приватности). Так он показывает, в каком объёме и кому он бы хотел сделать доступной свою частную информацию.

Принцип 5. Когда совладельцы частной информации не договариваются о совместных правилах приватности и не придерживаются их, может возникнуть турбулентность границ.

В большинстве случаев согласование правил приватности является достаточно эффективным методом управления приватностью коллективной информации. Но бывают случаи, когда частная информация выходит за установленные границы и становится доступной лицам, которые не были выбраны в качестве уполномоченных совладельцев. Такие случаи незапланированного распространения частной информации называются *турбулентностью границ приватности* [11, с. 33].

Частой причиной турбулентности в социальной сети является игнорирование пользователями «Политики конфиденциальности». Как правило, они редко читают данный документ, а ведь именно в нём содержатся правила приватности, определяющие, как и кем будет использована раскрываемая в профиле информация. Таким образом, участники социальной сети могут даже не догадываться, что дали согласие на использование своих данных в коммерческих и иных целях. В таком случае, с точки зрения пользователя, возникает ситуация турбулентности границ приватности: его информация используется не так, как он ожидал. Хотя на самом деле, формально он согласился со всеми условиями пребывания в социальной сети. Поэтому нельзя говорить о намеренном нарушении правил и границ приватности администрацией платформы, скорее речь идёт о том, что не все участники процесса полностью понимают условия договора, их границы приватности проходят по-разному, а правила приватности не согласованы.

Другой пример турбулентности в социальных сетях — это утечка данных. Доверив свою информацию социальной сети, пользователь надеется, что администрация несёт определённую ответственность за приватность раскрываемых данных. Особенно если речь идет об информации, скрытой от других настройкой приватности «только мне». В случае утечки можно говорить о том, что администрация сети не предприняла необходимые меры по защите приватности данных, которые гарантировала предпринять в рамках «Политики конфиденциальности». В результате чего информация стала доступна для аудитории, которой не предназначалась.

Согласно ТУП, турбулентность границ обычно является стимулом к изменению правил приватности — так владелец пытается вернуть контроль над информацией. Турбулентность может помочь людям увидеть, где им нужно скорректировать правила управления приватностью: часто они не могут определить, что нужно изменить, пока их приватность каким-либо образом не будет нарушена. Исследования подтвердили, что пользователи после столкновения с турбулентностью выбирали более эффективные меры по защите приватности своих данных [25]. Например, изменяли настройки приватности [26], уменьшали количество чувствительной информации в профиле [3] или полностью удаляли её (что считается наиболее радикальным способом вернуть контроль над личной информацией) [4].

Таким образом, в контексте профиля социальной сети существуют две основные причины возникновения турбулентности. К первой относится то, что пользователь часто не читает «Политику конфиденциальности» при регистрации и в результате не осознает, как может быть использована раскрываемая им информация. Вторым случаем можно считать утечку данных в результате недостаточных действий администрации соцсети по защите приватности пользователя. Как и предсказывает теория, опыт столкновения с турбулентностью нередко вынуждает пользователи применять дополнительные меры по защите приватности своих данных, вплоть до их удаления.

Выводы

В рамках данной статьи было рассмотрено, как пользователи управляют приватностью частной информации в таком относительно новом пространстве, как профиль социальной сети. Было показано, что, принимая решение о раскрытии или сокрытии личных данных, человек сталкивается с рядом сложностей, которые обусловлены как спецификой профиля, так и особенностями интернет-среды.

Часть трудностей связана со свойствами коммуникации один-ко-многим: пользователь не может увидеть реакцию на самораскрытие и не всегда понимает реальный состав своей аудитории, что может привести к тому, что он раскрывает информации больше, чем планировал. К этому подталкивают и принятые в социальной сети нормы открытости, а также уведомления от администрации («Укажите Ваши контакты»). При этом никто не информирует пользователя о минусах чрезмерного раскрытия: цифровые данные невозможно полностью удалить (даже по требованию владельца), так как они легко копируются и распространяются. Дополнительной сложностью является и то, что управление приватностью в профиле представляет собой двухэтапный процесс, который реализован с помощью разных технических функций. Сначала пользователь принимает решение о том, какую информацию раскрывать, а затем с помощью настроек приватности выбирает аудиторию, для которой она будет доступна. Таким образом, управление приватностью в профиле социальной сети, по сравнению с традиционными видами коммуникации, представляет собой более сложный процесс.

В данной статье мы также попытались проверить, возможно ли объяснить процесс управления приватностью в профиле социальной сети используя теорию Сандры Петронио. В целом, применяя положения и термины ТУП, мы пришли к выводу, что управление приватностью в данном пространстве включает себя решение пользователя о приватности, а также некое соглашение между ним и администрацией.

В соответствии с теорией, пользователь, принимая решение о самораскрытии, руководствуется личными правилами приватности, на которые оказывают влияние 5 критериев (культура, гендер, мотивы, контекст, соотношение рисков и выгод). Мы показали, что помимо этих факторов в социальной сети имеют значение и другие. Например: ценность информации, беспокойство о приватности, уровень цифровой грамотности и количество настроек, предлагаемых социальной сетью. Таким образом, можно увидеть, что ТУП хорошо описывает процесс управления приватностью в профиле на индивидуальном уровне.

Однако при описании коллективного уровня приватности следует учитывать следующее. В профиле не существует возможности договориться с другими пользователями о правилах приватности: договор происходит с администрацией социальной сети. Пользователь принимает «Политику конфиденциальности» при регистрации и соглашается с тем, что администрация становится «совладельцем» (наделяется правами собственности на его информацию). Администрация платформы в свою очередь предоставляет пользователю инструменты для контроля за приватностью личных данных: настройки приватности и список «друзей». Они позволяют выбирать, какие участники социальной сети могут стать совладельцами публикуемой частной информации.

Однако стоит учитывать, что из-за специфики социальной сети изменяется понятие «дружбы», и в коллективной границе не всегда оказываются люди, которые готовы нести ответственность за совместное хранение частной информации. Поэтому ответственность за приватность данных лежит, в основном, на самом пользователе. В случае турбулентности границ приватности он обычно предпринимает меры по защите информации от дальнейшего распространения: изменяет настройки приватности или уменьшает количество чувствительной информации в профиле. Самым эффективным же способом сохранения приватности является абсолютное нераскрытие данных.

Таким образом, теория хорошо описывает управление приватностью в профиле социальной сети на индивидуальном уровне, однако при объяснении коллективного уровня возникает множество сложностей, связанных с отсутствием возможности обсуждения правил приватности с другими пользователями. При этом, вся ответственность за приватность частной информации лежит на самом пользователе: поэтому весь процесс управления приватностью в профиле можно описать как решение пользователя о раскрытии с дальнейшим принятием мер по защите приватности в случае возникновения турбулентности. Роль администрации и других пользователей при этом сводится к минимуму.

Благодарности

Исследование выполнено при финансовой поддержке РФФИ и Правительства Новосибирской области в рамках научного проекта № 19-411-543002 “Исследование самораскрытия в профиле на примере социальной сети «ВКонтакте»”.

Библиографический список

References

Библиографический список

References