Социологические и правовые аспекты аутентификации в социальных сетях через паспортные данные

УДК 316.624 DOI 10.26425/2658-347X-2022-5-2-61-69

Получено 07.04.2022 Доработано после рецензирования 28.04.2022 Принято 12.05.2022

Попов Владимир Владимирович

Канд. юр. наук, доц. каф. частного права, Государственный университет управления, г. Москва, Российская Федерация

ORCID: 0000-0002-6746-6345

E-mail: vv_popov@guu.ru

Ерохина Алла Владимировна

Студент, Государственный университет управления, г. Москва, Российская Федерация

ORCID: 0000-0003-3825-4084

E-mail: erokhina.alvl@mail.ru

Черкасова Светлана Владимировна

Студент, Государственный университет управления, г. Москва, Российская Федерация

ORCID: 0000-0001-7411-1158

E-mail: Cherkasova.s2000@gmail.com

АННОТАЦИЯ

Данная работа посвящена анализу социальных, правовых и психологических аспектов внедрения аутентификации по паспортным данным в интернет–пространстве. В статье наравне с аутентификацией рассмотрено использование биометрических данных, а также особенности российского законодательства в области персональных данных. Показаны положительные и отрицательные стороны введения аутентификации по паспортным данным в социальных сетях, раскрыты психологические и правовые аспекты. Произведен анализ всех особенностей аутентификации, сложности применения и влияние данного нововведения на предупреждение девиантного поведения среди подростковой возрастной группы. Объект исследования – аутентификация по паспортным данным в социальных сетях. Предмет исследования – психологические, правовые аспекты установления аутентификации по паспортным данным. Методологическую и теоретическую основу исследования составили частно- и общенаучные подходы к изучению тематики, применялись формально-логический и сравнительный методы, а также методы структурного анализа. В ходе исследования были сделаны выводы об основных особенностях хранения данных граждан, сложности хранения данных россиян на зарубежных интернет-платформах, выводы о необходимости в фильтрации информации для несовершеннолетних граждан, а также был рассмотрен феномен девиантного поведения среди подростков и влияние информации в социальных сетях на их сознание.

Ключевые слова

Социальная сеть, социологическое исследование, цифровизация, аутентификация, подростки, Интернет, кибербуллинг, паспортные данные, персональные данные, девиантное поведение, анонимность в сети, деструктивная девиация

Для цитирования

Попов В.В., Ерохина А.В., Черкасова С.В. Социологические и правовые аспекты аутентификации в социальных сетях через паспортные данные//Цифровая социология. Т. 5, № 2. С. 61–69.

Благодарности. Исследование выполнено при финансовой поддержке РФФИ и ЭИСИ в рамках научного проекта № 21-011-33051.

Sociological and legal aspects of authentication in social networks through passport data

Received 07.04.2022 Revised 28.04.2022 Accepted 12.05.2022

Vladimir V. Popov

Cand. Sci. (Jur.), Assoc. Prof. at the Private Law Department, State University of Management, Moscow, Russia

ORCID: 0000-0002-6746-6345

E-mail: vv_popov@guu.ru

Alla V. Erokhina

Student, State University of Management, Moscow, Russia

ORCID: 0000-0003-3825-4084

E-mail: erokhina.alvl@mail.ru

Svetlana V. Cherkasova

Student, State University of Management, Moscow, Russia

ORCID: 0000-0001-7411-1158

E-mail: Cherkasova.s2000@gmail.com

ABSTRACT

This work is devoted to the analysis of the sociological and legal aspects of the implementation of authentication in social networks through passport data. In the article, along with authentication, the uses of biometric data, as well as the features of Russian legislation in the sphere of personal data, are considered. The positive and negative aspects of introducing authentication by passport data in social networks are shown and the psychological and legal aspectsare reveled. The authors analyzed all the features of authentication, the complexity of application and the impact of this innovation on the prevention of deviant behavior among the adolescent age group. The object of the research is authentication by passport data in social networks. The subject of the research is psychological and legal aspects of establishing authentication based on passport data. The methodological and theoretical basis of the research is made up of particular and general scientific approaches to the study of this topic, formal logical and comparative methods, as well as methods of structural analysis were used. In the course of the study, conclusions about the main features of storing citizens' data, the complexity of storing data of Russians on foreign Internet platforms, conclusions on the need to filter information for minors were drawn, and also considered the phenomenon of deviant behavior among adolescents and the influence of information in social networks on their consciousness.

Keywords

Social network, sociological research, digitalization, authentication, teenager, Internet, cyberbullying, passport data, personal data, deviant behavior, online anonymity, destructive deviation

For citation

Popov V.V., Erokhina A.V., Cherkasova S.V. Sociological and legal aspects of authentication in social networks through passport data. *Digital Sociology*, vol. 5, no. 2, pp. 61–69. DOI: 10.26425/2658-347X-2021-5-2-61-69

Acknowledgements. The reported study was funded by Russian Foundation for Basic Research and Expert Institute for Social Research, project number № 21-011-33051.

ВВЕДЕНИЕ / INTRODUCTION

В современном мире тяжело представить жизнь без использования сети «Интернет» (далее – Интернет), а социальные сети стали неотъемлемой частью общения и профессиональной деятельности. Интеграция явлений повседневной жизни в цифровую среду имеет множество преимуществ, однако появляются и новые проблемы.

Дети и подростки – самые активные пользователи социальных сетей, но вследствие того, что критическое мышление у них не сформировано, а жизненной мудрости и опыта еще не хватает, социальные сети, как и цифровая социальная среда в целом, могут принести им больше вреда, нежели пользы. Дети, воспитывающиеся в неблагоприятной социальной обстановке, не получающие должного внимания с родительской стороны, часто пытаются компенсировать желаемое через виртуальную жизнь. Существует большая вероятность кибербуллинга, травли как со стороны сверстников, так и со стороны взрослых людей. Основная причина противоправного поведения в цифровом пространстве состоит в маске анонимности. Мало кто сможет выразить негативное мнение от своего имени, а социальные сети дают возможность скрыть истинную личность. Важно огородить детей и подростков от негативного влияния социальных сетей, пока их психика не до конца сформирована, потому что существует большая вероятность наступления трагических и непоправимых последствий.

Цель исследования состоит в предотвращении негативного влияния социальных сетей на подростков и рассмотрении допустимых способов аутентификации пользователей социальных сетей.

Задачи исследования:

– определить, как цифровая социальная среда влияет на физиологическое и психологическое состояние человека;

– определить, почему подростки являются самой уязвимой перед негативным влиянием социальных сетей группой;

– выяснить, какие негативные последствия могут повлечь за собой социальные сети для подростков;

– определить, почему анонимность способствует росту количества противоправных действий в социальных сетях;

– рассмотреть возможность использования биометрических данных при регистрации в социальных сетях;

– рассмотреть возможность аутентификации по паспортным данным в социальных сетях.

ВЛИЯНИЕ СОЦИАЛЬНЫХ СЕТЕЙ НА ДЕВИАНТНОЕ ПОВЕДЕНИЕ ПОДРОСТКОВ / THE INFLUENCE OF SOCIAL NETWORKS ON THE ADOLESCENTS' DEVIANT BEHAVIOR

Поведение человека, в том числе и социальное, обусловлено разного рода воздействием на его сознание. За это отвечают нейроны в мозге. Как отмечают специалисты по физиологии человека, «и мозг, и нейроны, и поведение существуют в едином информационном системном поле» [Андрианов, 2007]. В современных условиях значительное влияние на мозг оказывают материалы, размещенные в Интернете, в том числе в социальных сетях. Размещение информации в Интернете осуществляется таким образом, чтобы максимально заинтересовывать пользователей, а социальные сети за последние годы значительно изменили устоявшиеся привычки в общении. Эти изменения закрепляются на физиологическом уровне, когда мозг за счет простых стимулов увеличивает выработку дофамина, гормона удовольствия, а затем требует повторения положительных эмоций. Все более популярным становится вывод о том, что цифровая революция, которая происходит на наших глазах, заставляет мозг эволюционировать в невиданном прежде темпе, мы видим новую расу «цифровых аборигенов», которых хай-тек окружал с младенчества [Смолл, Ворган, 2020].

Детям цифровой эпохи сложнее различать эмоции, сопереживать окружающим. Мозг теряет базовые коммуникационные механизмы, становится труднее считывать мимику человека, появляются сложности с контактами. Часто акцент смещается с ценности дружбы на количество друзей. Меняется структура мышления и памяти: зона, отвечающая за абстрактное мышление, используется реже, становится менее актуальной долгосрочная память, нужнее – оперативная. В цифровой эпохе, безусловно, есть множество плюсов, но минусы тоже существуют, и они крайне значительны. С появлением Интернета общество столкнулось с целым рядом проблем, многие из которых имеют глобальный характер.

В современном мире проблема деструктивной социальной девиации стоит достаточно остро. В феномен отрицательной девиации включают преступную деятельность, алкоголизм, наркоманию, экстремистское поведение и т.д. Большой процент деструктивной девиации приходится на подростковый возраст. Сопряжено это, главным образом, с пубертатным кризисом, который традиционно описывается как самый яркий,

эмоциональный, но одновременно тяжелый и противоречивый период в жизни каждого человека.

Главная особенность подросткового периода состоит в личностной нестабильности. Подросток всеми силами стремится к обретению статуса взрослого, однако, как показывает практика, по причине современного информационного общества он обретает не чувство взрослости, а скорее чувство возрастной неполноценности [Позднякова, 2018]. В окружении близких людей подросток проявляет черты негативизма (психологи относят его к первичной форме механизма отчуждения), стремится противостоять любым предложениям и советам членов семьи, все действия идут как бы от обратного. Одновременно с такой линией поведения образовывается и полярная линия, называемая конформизмом (эффект повального увлечения), свойственная подростку в кругу сверстников. Конформизм представляет собой приспособленчество и пассивное принятие господствующего порядка. Многим подросткам свойственны эгоцентрические увлечения, например изучение редких иностранных языков, принадлежность к популярной субкультуре, участие в художественной самодеятельности. На этом жизненном этапе любое дело представляет собой средство демонстрации успехов. В эмоциональном плане подростки с признаками деструктивной девиации характеризуются крайне низкой ответственностью за свои поступки, наблюдаются вспышки неконтролируемой агрессии и истерики.

Подростковый возраст – очень важный жизненный период, в котором ребенок отвечает себе на три экзистенциальных вопроса: «кто я?», «зачем я здесь?» и «чего я хочу?». Родителям необходимо как можно раньше устанавливать доверительные отношения со своими детьми, однако часто родители переоценивают собственную осведомленность о поведении ребенка в социальных сетях. Постоянная целенаправленная коммуникация родителей и детей позволит проговорить и обсудить важные темы для ребенка, даст возможность ему лучше чувствовать и понимать себя, а обеспечение его максимально самостоятельного социального развития, может направить его интересы в Интернет с приобретением вследствие этого заинтересованности в сомнительных, зачастую пропагандирующих депрессивное состояние сообществах, при этом последствия такого вовлечения предугадать невозможно.

Американский психолог Р. Чалдини разработал интересную психологическую концепцию, согласно положениям которой число несчастных случаев со смертельным исходом существенно увеличивается только в тех регионах, где о случаях самоубийства рассказывали общественности. Чем шире огласка, которую получает определенный случай, тем больше впоследствии происходит несчастных случаев. Отдельные индивиды, склонные к самоубийству, могут реагировать на неблагоприятные социальные факторы, решая, как бы покончить со всем этим и, в первую очередь, с самим собой [Чалдини, 2020].

Существует так называемый феномен «Колумбайна» – по названию школы, в которой произошло массовое убийство, совершенное двумя ее учащимися. Эта трагедия в США в 1999 г. стала ключевой для истории скулшутинга (от англ. school – «школа» и shoot – «стрельба»). В 2009 г. социолог Р. Ларкин написал, что убийцы заложили сценарий для последующих случаев стрельбы в школах. У них появилось множество подражателей, которые даже основали свое сообщество в социальных сетях и стали называть себя «колумбайнерами». По сценарию убийств в школе «Колумбайн» развивались и многие другие трагедии в США[1]. В России феномен «Колумбайна» наиболее известен массовыми убийствами в образовательных организациях Керчи (в 2018 г.,) Перми и Казани (в 2021 г.), вследствие чего Верховный Суд Российской Федерации по иску Генеральной прокуратуры Российской Федерации признал «Колумбайн» террористической организацией. Исследователи выделяют черты, позволяющие отнести идеологию «Колумбайна» к терроризму: привлечение внимания; активное вовлечение молодежи посредством Интернета; повышенная общественная опасность, связанная с непосредственной угрозой жизни людей; безразличие к жертвам; направленность действий на неопределенный круг лиц; тенденция перехода от конкретных целей к беспорядочным убийствам; заранее спланированное нападение [Пучнин, Пучнина, 2021]. Особая опасность данного рода девиантного поведения требует обратить внимание на профилактические меры в учебных заведениях. Специалисты отмечают положительный опыт Германии в данной области [Суходольская, 2020]. Не только Россия, но и другие страны – участники СНГ реализуют комплекс профилактических мероприятий и принимают меры по противодействию вовлечению подростков в группы деструктивной направленности [Долгова, 2021].

Дети и подростки характеризуются крайне неустойчивой психикой, отсутствием критического

[1] *Джанашия В.* (2018). Смертельный урок // Эксперт. № 5 (1061). Режим доступа: https://expert.ru/expert/2018/05/smertelnyij-urok/ (дата обращения: 05.04.2022).

мышления, четко сформированных жизненных взглядов, моральных принципов. Еще одним примером деструктивного влияния может послужить сообщество «Синий кит», участники которого кончали жизнь самоубийством. Агрессивную среду, оказывающую разрушительное влияние на несформировавшуюся детскую психику, составляют не одни лишь дети и подростки. Многие взрослые зачастую участвуют в кибербуллинге, именно взрослые являются создателями деструктивных сообществ, поэтому вопрос безопасности детей, в том числе в интернет-пространстве, должен быть первостепенным.

Далеко не каждый родитель устанавливает близкие и доверительные отношения со своим ребенком, поэтому про интернет-безопасность ребенок может знать исключительно в общих чертах. В социальных сетях используются разного рода инструменты, демонстрирующие выражения внимания (просмотры) и одобрения (лайки), которые имеют значительное влияние на пользователей, особенно на несовершеннолетних. Многие из них сконцентрированы на популярности, на мнении общественности касательно собственной личности, при этом часто за потребностью иметь так называемую известность в кругах сверстников кроется желание сдружиться с определенным человеком или компенсировать отсутствие родительского внимания. Возвращаясь к вопросу об агрессивном интернет-пространстве и людях, создающих его, стоит отметить, что взрослые люди бывают не только зрелыми и незрелыми личностями – у многих наблюдаются серьезные психологические и/или психиатрические отклонения. Интернет дает анонимность, и поэтому человек может действовать девиантно, не раскрывая свою личность и не опасаясь встретиться с критикой общественности в свой адрес. Также снижается риск быть привлеченным к ответственности за совершение противоправных действий. К сожалению, известно много случаев, когда взрослые люди с объективно нездоровой психикой, а именно с перверсией, вступали в доверительные отношения с детьми или подростками, выпрашивали у них фотографии различного характера, затем шантажировали или сразу распространяли в кругу знакомых полученный материал. Распространение интимных фотографий для жертвы по ощущениям сравнимо с состоянием после изнасилования, ребенок переживает, ему наносится глубокая психологическая травма. Общество в социальных сетях должно оберегать детей от самих себя.

Проблемный ребенок обычно является симптомом дисфункциональности семьи. Именно в семье проходит первичная социализация ребенка. При отсутствии полного взаимопонимания и поддержки в этот непростой жизненный период происходит компенсация извне. Дети, не охваченные в должной мере вниманием родителей, предоставлены сами себе. В результате зачастую у них развивается интернет-зависимость или подверженность влиянию сверстников.

В каждой отдельно взятой трагедии нельзя определить одну единственную проблему, послужившую причиной катастрофы, это всегда совокупность факторов. Однако влияние цифровой среды нельзя недооценивать. Сегодня социальные сети стали частью жизни человека, их отсутствие практически означает выпадение из социума. Тем не менее, для детей они не являются острой необходимостью. Для старших школьников и взрослых социальные сети – неотъемлемый элемент профессиональной жизни, средство общения, платформа для работы и прочей деятельности. У детей младшего школьного возраста ведущей деятельностью является учебная. Ввиду отсутствия критического мышления, повышенной любознательности ребенка социальные сети принесут ему больше вреда, чем пользы. Во многом это обусловлено и агрессивной средой в целом. Для детей, не получающих должного внимания и заботы от родителей, риск вовлечения в деструктивные контакты возрастает.

ПРОТИВОДЕЙСТВИЕ НЕГАТИВНОМУ ВЛИЯНИЮ СОЦИАЛЬНЫХ СЕТЕЙ ПОСРЕДСТВОМ АУТЕНТИФИКАЦИИ ПОЛЬЗОВАТЕЛЕЙ / COUNTERING THE NEGATIVE IMPACT OF SOCIAL NETWORKS THROUGH USER AUTHENTICATION

Поскольку, как отмечалось выше, основная причина столь агрессивной интернет-среды заключается в анонимности пользователей, следует изменить подходы к регистрации в социальных сетях. В настоящее время процесс регистрации в социальных сетях в большинстве случаев устроен так, что пользователь идентифицируется посредством электронной почты и/или телефонного номера. Электронная почта может быть создана за несколько минут и никак не привязана к прочим идентификаторам личности пользователя, телефонный номер может также быть зарегистрирован на другое лицо. Таким образом, пользователь может избрать любой псевдоним, возраст, пол, внешность и прочие характеристики. Скрываясь за такой маской, он может выражать девиантные суждения, совершать противоправные деяния, не опасаясь ответственности

за свои действия. Именно анонимность «развязывает руки» многим людям, впоследствии эта свобода может привести, в том числе, к трагедиям. В связи с этим целесообразно было бы предусмотреть аутентификацию по паспортным данным для регистрации в социальных сетях или же использование биометрических данных граждан.

Развитие информационных технологий открыло современному человеку возможность использовать свои данные без предоставления бумажного (паспорт, иные документы) или пластикового носителя (банковская карта). Такая возможность появилась благодаря использованию биометрических данных россиян и созданию нового носителя для переноса информации (телефон, «умные» часы). Биометрия – наука, основанная на описании и измерении характеристик организмов живых существ [Барсуков, 2021]. Самыми известными типами биометрии являются радужная оболочка глаза, изображение лица, отпечаток пальца, ладони и голос. Что касается нормативной базы, то статья 14.1 федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»[2] определяет порядок получения биометрической информации, идентификацию лица с помощью биометрии и само ее размещение в единой биометрической системе.

Одним из ярких примеров использования биометрии можно назвать недавнее нововведение оплаты проезда в московском метрополитене лишь по сканированию лица пассажира. Биометрические данные используются государственными органами при получении виз, заграничных паспортов и банками при оформлении карт.

Использование биометрических данных дает множество преимуществ, основными из которых являются простота использования и практическая невозможность их потери, сложность в подделке данных [Грушо и др., 2019]. Использование биометрии было бы логичным при регистрации в социальных сетях и на других интернет-площадках, но при этом биометрия гражданина несет за собой большой пласт информации о человеке, а внедрение и создание специальных хранилищ с целью сохранности и использования данных нецелесообразно по некоторому ряду причин.

Во-первых, биометрические данные, ставшие известными другим лицам, невозможно обновить, а следовательно, злоумышленник сможет использовать их в течение всей жизни хозяина данных. Согласно п. 1 ст. 17 федерального закона «Об информации, информационных технологиях и о защите информации», лица, виновные в нарушении требований ст. 14.1 данного закона в части обработки, включая сбор и хранение биометрических персональных данных, несут административную, гражданскую и уголовную ответственность в соответствии с законодательством России.

Во-вторых, с использованием биометрии любая социальная сеть или интернет-платформа (иностранная или российская) будут иметь доступ к практически всем данным граждан. Страницы пользователей социальных сетей нередко подвергаются взлому, а со взломом страницы злоумышленникам попадут не только личные переписки, фотографии, но и биометрия.

В-третьих, необходимо пересмотреть политику использования и сохранности данных на сторонних ресурсах, что невозможно. Сами по себе биометрические данные охраняются властными структурами, а передача их, например, иностранной социальной сети может нанести вред не только гражданину, но и государству.

В-четвертых, появится необходимость в налаживании отношений между властными структурами и непосредственно руководителями социальных сетей. Как известно, далеко не во всех случаях администрация интернет-ресурсов готова сотрудничать с властями и предоставлять информацию о пользователях находящихся в ее ведении социальных сетей.

Одним из наиболее удобных вариантов для предотвращения противоправных действий и фильтрации информационных ресурсов в Интернете можно назвать использование аутентификации по паспортным данным. Данный пункт позволит узнать возраст пользователя и использовать правильные алгоритмы для подбора материалов. Использование паспортных данных в социальных сетях применяется на некоторых сайтах уже давно, например, для восстановления доступа к аккаунту (от англ. account – учетная запись) пользователя (социальная сеть «ВКонтакте») или же для подтверждения учетной записи (Госуслуги). Предполагаемого пользователя просят сфотографироваться с паспортом в руках, где будут видны сам документ в раскрытом виде на странице с информацией о гражданине и его лицо около документа. В некоторых случаях можно закрыть серию и номер документа и оставить только фамилию, имя и отчество. У каждого сайта свои критерии.

Гражданин Российской Федерации в 14 лет получает паспорт и становится частично дееспособным. Данный возраст относится к подростковой

[2] Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации». Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_61798/ (дата обращения: 05.04.2022).

категории, а как уже было сказано выше, подростки – особая категория, восприимчивая к любому роду информации. Социальные сети – основной способ общения и получения информации, а использование аутентификации по паспорту позволит создать благоприятную среду для каждой возрастной группы. Если же гражданину нет 14 лет и у него, соответственно, отсутствует паспорт, можно использовать и свидетельство о рождении. Минусом использования свидетельства о рождении является то, что там содержится информация о родителях ребенка, а, например, при украденной базе паспортных данных не составит труда найти ребенка данных лиц. Поэтому необходимо обеспечить достаточную защиту персональных данных. Основным нормативным правовым актом в данной области является федеральный закон от 27 июля 2006 г. № 152-ФЗ «Операсональных данных»[3], где указаны как основные принципы и положения, так и лица, ответственные за обработку персональных данных, уполномоченных орган по защите прав субъектов в данной области и другие. Согласно ст. 3 указанного федерального закона под персональными данными стоит понимать любую информацию, относящуюся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных). Персональные данные граждан – ценный ресурс для злоумышленников. Ошибочно предполагать, что данные несовершеннолетних не будут представлять ценность. Паспорт получают в 14 лет, и действует он до его замены, происходящей при достижении гражданином 20-летнего возраста. При возможной краже данных злоумышленники могут сначала хранить эти данные, а потом уже при достижении 18-летнего возраста владельца, использовать их. Зачастую и сайты, которые уже используют паспортные данные для получения определенного рода услуг, подвергаются атакам и утечке данных. В данном случае ответственные за сайт лица должны пересмотреть политику защиты своих пользователей и создать наиболее безопасные места для хранения данных.

Особенно необходимо при использовании аутентификации по паспорту поставить вопрос о защите и использовании персональных данных несовершеннолетних. Согласно ст. 3 и ст. 9 федерального закона «О персональных данных» предусмотрена обработка вышеуказанных данных с согласия гражданина или его представителя. Дети – несовершеннолетние граждане и в зависимости от возраста они ограничены в своих действиях, хотя несовершеннолетние в возрасте от 14 до 18 лет имеют право самостоятельно совершать некоторые сделки. Распоряжение данными не относится к понятию «сделки», но этот пример демонстрирует ограничения несовершеннолетних в некоторых областях. Права и законные интересы ребенка защищаются его родителями – законными представителями. Согласие на использование персональных данных, соответственно, дают они же. Если использовать аутентификацию как новый способ ограничения детей от нежелательной информации и информации, относящейся не к их возрастной группе, то необходимо каждый раз при регистрации на новом ресурсе просить законных представителей дать разрешение. В большинстве случаев подростки скрывают личную информацию и интересы от своих родителей, а использование их согласия для регистрации позволит родителям знать, где просматривает материалы их ребенок. В первую очередь данное нововведение навредит отношениям между детьми и родителями. Подростки – группа нестабильная в психоэмоциональном плане и любой контроль или малейшее вмешательство со стороны родителей может расцениваться как посягательство на их личное пространство. В будущем травмированный ребенок может вырасти в нестабильную личность, которая сможет нанести вред не только себе, но и окружающим. Законодателю необходимо предусмотреть пункт об использовании персональных данных несовершеннолетних в федеральном законе «О персональных данных» в случае добавления аутентификации по паспорту.

ЗАКЛЮЧЕНИЕ / CONCLUSION

Главной проблемой использования социальных сетей остается анонимность их пользователей. Для предотвращения негативного влияния социальных сетей на подростков предлагается сочетание разнородных методов влияния, одним из которых выступает аутентификация пользователей в социальных сетях по паспортным данным.

При введении системы аутентификации пользователей в социальных сетях по паспортным данным необходимо учитывать все риски нарушения прав и законных интересов указанной категории граждан и обеспечить их всестороннюю защиту. Ошибочно было бы предполагать, что использование биометрии более опасно, чем аутентификация по паспорту, а последняя не влечет никаких рисков для пользователей. Если какие-либо

[3] Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных». Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_61801/ (дата обращения: 05.04.2022).

персональные данные попадут в распоряжение злоумышленников, вред может быть причинен различными способами, и российское общество должно быть готово к подобным вызовам.

Например, есть социальные сети, подчиняющиеся российским законам (либо по причине того, что они управляются российскими организациями или действуют в интересах российских бенефициаров), а есть социальные сети, администрации которых находятся в состоянии конфронтации с российскими властями и не подчиняются их предписаниям. Ярким примером являются социальные сети Facebook и Instagram, принадлежащие Meta Platforms Inc. (признана в Российской Федерации экстремистской и запрещена). И до запрета их деятельности взаимоотношения российских властей с оператором данных платформ были весьма напряженными, что связано в том числе и с несоблюдением требований о защите персональных данных российских пользователей. При этом часть российских граждан до сих пор продолжает использовать эти запрещенные платформы, и очевидно, что властями Российской Федерации придется обеспечить применение комплекса мер юридического и технического характера для их полной блокировки на своей территории.

Также возникают и иные вопросы, которые нуждаются в правовом регулировании, учитывающем особенности прав и законные интересы подростков: какие санкции применять для операторов социальных сетей в случаях утраты данных или их передачи злоумышленникам; как обеспечить доступ в социальные сети лицам, у которых нет паспорта, и др.

Полученные результаты могут быть направлены на создание комфортной среды в социальных сетях и организацию должного контроля за публикуемой в Интернете информацией в целях безопасности несовершеннолетних.

СПИСОК ЛИТЕРАТУРЫ

Андрианов В.В. (2007). Нейроны, мозг и поведение // Вестник Международной академии наук. Русская секция. № 2. С. 25–29.

Барсуков С.С. (2021). Криминалистическая идентификация по радужной оболочке и сетчатке глаза: современные возможности и проблемы применения // Юристъ-Правоведъ. № 1. С. 170–175.

Грушо А.А., Забежайло М.И., Смирнов Д.В., Тимонина Е.Е. (2019). Имитационное моделирование постбиометрического метода аутентификации на основе данных о пользователе // International Journal of Open Information Technologies. Т. 7, № 4. С. 43–50.

Долгова С.И. (2021). Отдельные аспекты организации деятельности органов внутренних дел государств – участников СНГ по противодействию вовлечению несовершеннолетних в деструктивные группы в сети Интернет // Административное право и процесс. № 6. С. 68–73. https://doi.org/10.18572/2071-1166-2021-6-68-73

Позднякова О.В. (2018). К вопросу развития образа взрослого в подростковом возрасте // Проблемы науки. № 6. С. 108–112.

Пучнин А.В., Пучнина М.Ю. (2021). Идеология «Колумбайн» как экстремистская и террористическая угроза национальной безопасности Российской Федерации // Общество и право. № 2. С. 38–43.

Смолл Г., Ворган Г. (2020). Мозг онлайн. Человек в эпоху Интернета / Пер. с англ. Б.М. Козловский: М.: КоЛибри. 352 с.

Суходольская Ю.В. (2020). Субкультуризация массового убийства в образовательных организациях как новый российский криминологический феномен // Законность. № 10. С. 37–40.

Чалдини Р. (2020). Психология влияния. Убеждай, воздействуй, защищайся / Пер. с англ. Е. Бугаева, Е. Волков, О. Пузырева. СПб.: Питер. 464 с.

REFERENCES

Andrianov V.V. (2007), “Neurons, brain and behavior”, *Herald of the International Academy of Science. Russian Section*, no. 2, pp. 25–29.

Barsukov S.S. (2021), “Forensic identification by the iris and retina: Current opportunities and problems of application”, *Urist-Pravoved*, no. 1, pp. 170–175.

Cialdini R. (2020), *Influence*, Trans. from Eng. Bugayeva E., Volkov E., Puzyreva O., Piter, St. Petersburg, Russia (in Russian).

Dolgova S.I. (2021), “Some aspects of organization of operations of internal affairs agencies of the CIS member states aimed at prevention of the involvement of minors in destructive groups on the Internet”, *Administrativnoe pravo i process*, no. 6, pp. 68–73, https://doi.org/10.18572/2071-1166-2021-6-68-73

Grusho A.A., Zabezhailo M.I., Smirnov D.V., E. Timonina E.E. (2019), “Simulation modeling of post-biometric authentication on the basis of user’s data”, *International Journal of Open Information Technologies*, vol. 7, no. 4, pp. 43–50.

Pozdnyakova O.V. (2018), “To the question of the development of the image of an adult in adolescence”, *Problemy nauki*, no. 6, pp. 108–112.

Puchnin A.V., Puchnina M.Yu. (2021), “The ideology of Columbine as an extremist and terrorist threat to the national security of the Russian Federation”, *Obshchestvo i pravo*, no. 2, pp. 38–43.

Small G., Vorgan G. (2020), *iBrain: Surviving the Technological Alteration of the Modern Mind*, Trans. from Eng. Kozlovsky B., KoLibri, Moscow, Russia (in Russian).

Sukhodolskaya Yu.V. (2020), “Subculturization of massacre in educational institutions as a new Russian criminological phenomenon”, *Zakonnost’*, no. 10, pp. 37–40.