Министерство науки и высшего образования Российской Федерации
Московский государственный юридический университет имени О.Е. Кутафина (МГЮА)
Кафедра информационного права и цифровых технологий

КУРСОВАЯ РАБОТА

на тему:

« Правовое регулирование защиты персональных данных несовершеннолетних в социальных сетях в РФ»

Выполнил(а): [ФИО студента, курс, группа]

Научный руководитель: [ФИО, должность, звание]

Москва — 2026

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Цифровизация детства стала необратимым социальным фактом: по данным Роскомнадзора, в 2023–2024 годах свыше 80 % российских детей в возрасте от 10 до 17 лет регулярно пользуются социальными сетями, оставляя там массивы сведений о себе: от имени и фотографий до геолокации и поведенческих паттернов. Платформы собирают эти данные в коммерческих целях, алгоритмы профилируют пользователей, а механизмы верификации возраста остаются номинальными. Между тем правовая система, призванная защищать несовершеннолетних в цифровом пространстве, формировалась преимущественно применительно к взрослым субъектам и лишь точечно учитывает специфику детской аудитории.

Актуальность: в 2024 году Роскомнадзор зафиксировал рост числа жалоб на незаконную обработку персональных данных несовершеннолетних на 34 % по сравнению с предыдущим годом, а принятый в декабре 2023 года Федеральный закон № 572-ФЗ о запрете регистрации детей до 14 лет в социальных сетях без верифицированного согласия родителей обнажил системный пробел: механизм реализации этого запрета так и не получил подзаконного закрепления. Одновременно Европейский союз последовательно ужесточает требования GDPR применительно к детским данным, формируя стандарты, которые российские платформы, работающие на международных рынках, вынуждены учитывать де-факто. Совокупность этих обстоятельств делает комплексный правовой анализ защиты персональных данных несовершеннолетних в социальных сетях насущной научной и практической задачей.

Объектом исследования выступают общественные отношения, складывающиеся в сфере обработки и защиты персональных данных несовершеннолетних пользователей социальных сетей в Российской Федерации.

Предметом исследования являются нормы российского законодательства (прежде всего Федерального закона № 152-ФЗ «О

персональных данных»), правоприменительная практика, а также организационно-правовые механизмы, обеспечивающие защиту персональных данных несовершеннолетних в социальных сетях.

Цель работы: комплексно проанализировать правовое регулирование защиты персональных данных несовершеннолетних в социальных сетях в РФ, выявить существующие пробелы и предложить направления их устранения.

Достижение поставленной цели обусловило решение следующих **задач:**

1. Раскрыть понятие и виды персональных данных несовершеннолетних как объекта правовой охраны на основе ст. 3 ФЗ № 152-ФЗ и доктринальных позиций отечественных исследователей.

2. Охарактеризовать социальные сети как особую среду оборота персональных данных, выявив специфические риски, которые они порождают для несовершеннолетних пользователей.

3. Исследовать российскую нормативно-правовую базу защиты персональных данных несовершеннолетних, включая конституционные нормы, ФЗ № 152-ФЗ и смежное законодательство.

4. Проанализировать механизм получения согласия на обработку персональных данных несовершеннолетних, в том числе роль законных представителей и проблемы верификации их волеизъявления.

5. Выявить актуальные угрозы персональным данным несовершеннолетних в социальных сетях и установить причины неэффективности действующих правоприменительных инструментов.

6. Сформулировать предложения по совершенствованию нормативного регулирования и правоприменительной практики в исследуемой сфере.

Методы: формально-юридический метод (анализ текстов нормативных правовых актов), сравнительно-правовой метод (сопоставление российского

регулирования с европейским опытом GDPR), системный метод (рассмотрение норм о персональных данных в их взаимосвязи), метод анализа судебной практики, метод теоретического обобщения доктринальных источников.

Теоретическую основу работы составляют труды Мамай Е.А. (2024), Петрыкиной Н.И. (2021), Аркабаева Н.К. и Базарбаева Э.М. (2023), Теунаева И. (2025), Смородинова Е.В. (2025), Боргоякова Ф. (2021), Корниловой Т. и Лапенкова Е. (2024), Жокова Д. (2023). Нормативную базу образуют Конституция Российской Федерации, Федеральный закон от 27 июля 2006 года № 152-ФЗ «О персональных данных», Федеральный закон от 29 декабря 2010 года № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию», Федеральный закон от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации», а также подзаконные акты Роскомнадзора и решения судов общей юрисдикции.

Структура работы. Курсовая работа состоит из введения, трёх глав, разбитых на параграфы, заключения и списка использованных источников. Первая глава посвящена теоретико-правовым основам защиты персональных данных несовершеннолетних в цифровой среде. Вторая глава раскрывает нормативно-правовое регулирование обработки персональных данных несовершеннолетних в социальных сетях в Российской Федерации. Третья глава содержит анализ проблем правоприменения и авторские предложения по совершенствованию правового регулирования в исследуемой области.

ГЛАВА 1. ТЕОРЕТИКО-ПРАВОВЫЕ ОСНОВЫ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ НЕСОВЕРШЕННОЛЕТНИХ В ЦИФРОВОЙ СРЕДЕ

1.1. Понятие и виды персональных данных несовершеннолетних как объекта правовой охраны

Правовая охрана персональных данных несовершеннолетних начинается с вопроса о том, что именно подлежит защите. Статья 3 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных» определяет персональные данные как любую информацию, относящуюся к прямо или косвенно определённому физическому лицу. Формулировка намеренно широкая, однако именно эта широта порождает устойчивые коллизии: законодательное определение, бытовое понимание гражданами границ «своих» данных и позиция судов при разрешении конкретных споров нередко расходятся. Мамай Е.А. зафиксировала, что абстрактность легального определения влечёт широкую вариативность интерпретации, из-за чего правоприменители в схожих ситуациях приходят к противоположным выводам о том, является ли та или иная информация персональными данными [1].

Применительно к несовершеннолетним эта неопределённость особенно опасна: ребёнок и его родители зачастую не осознают, какие сведения охраняются законом, а суды не выработали единого подхода к оценке информации о детях. Доктрина традиционно делит персональные данные на общие и специальные категории. К общим относятся имя, дата рождения, место учёбы, адрес проживания: сведения, которые идентифицируют личность непосредственно. Специальные категории включают биометрические данные: фотоизображения, голосовые слепки, данные о геометрии лица. Рязанова К. подчёркивает, что биометрические данные обладают принципиально иной природой по сравнению с обычными

[1] Мамай Е.А. Персональные данные как объект правового регулирования: соотношение законодательства, общественного мнения и судебной практики

персональными данными, поскольку позволяют идентифицировать человека без его участия и согласия, а их компрометация необратима: изменить лицо или голос невозможно [2]. Для несовершеннолетних это означает, что фотография ребёнка, размещённая в открытом доступе, не безобидный снимок, а биометрический идентификатор с долгосрочными последствиями для его безопасности.

Разграничение данных по степени идентифицирующей способности имеет самостоятельное практическое значение. Петрыкина Н.И. обращает внимание на то, что в обороте персональных данных принципиально важно учитывать не только прямые идентификаторы, но и косвенные: те, которые сами по себе не раскрывают личность, однако в совокупности с иными сведениями делают субъекта полностью определимым [3]. Для детей этот механизм агрегации работает особенно наглядно: геолокационная метка из публикации в социальной сети, указание школы в профиле и фотография в школьной форме по отдельности кажутся безвредными, но вместе формируют детальный профиль ребёнка: с маршрутом, расписанием и внешностью. Именно такой профиль создаёт почву для преследования, эксплуатации или иных противоправных действий в отношении несовершеннолетнего.

Отдельную угрозу представляют цифровые следы: массив данных, который несовершеннолетний оставляет в сети не целенаправленно, а в ходе обычной онлайн-активности. История поисковых запросов, реакции на публикации, подписки на сообщества, время и периодичность выхода в сеть: каждый из этих элементов сам по себе не идентифицирует ребёнка, однако их накопление и алгоритмическая обработка позволяют восстановить подробную картину его интересов, социального окружения и поведенческих паттернов. Бисалиев М. и Шакиров К. доказывают, что именно накопление

[2] Рязанова К. Биометрические персональные данные как основание идентификации личности

[3] Петрыкина Н.И. Некоторые вопросы регулирования оборота персональных данных в РФ

цифровых следов представляет ключевой фактор угрозы безопасности персональных данных в киберсреде, поскольку создаёт устойчивые профили пользователей, пригодные для манипулирования и противоправного использования [4]. Для несовершеннолетних эта угроза усугубляется тем, что дети не способны в полной мере осознать долгосрочные последствия своей цифровой активности и не располагают инструментами контроля над тем, как платформы агрегируют и используют собранные сведения.

Персональные данные несовершеннолетних образуют многоуровневую категорию, охватывающую прямые идентификаторы, биометрические характеристики, косвенные сведения и цифровые следы, причём каждый из этих уровней несёт самостоятельные риски, возрастающие при агрегации. Понимание этой структуры необходимо для анализа той среды, в которой данные несовершеннолетних циркулируют наиболее интенсивно, социальных сетей, правовым особенностям которых посвящён следующий параграф.

1.2. Социальные сети как среда оборота персональных данных несовершеннолетних: понятие, особенности и риски

Социальные сети образуют особую технологическую и правовую среду, в которой оборот персональных данных несовершеннолетних приобретает масштаб и специфику, принципиально отличающие её от иных форм обработки информации. Аркабаев Н.К. и Базарбаев Э.М. определяют социальную сеть как интернет-платформу, включающую три взаимосвязанных элемента: создание пользовательского профиля, формирование социальных связей между пользователями и обмен контентом [5]. Именно эта трёхкомпонентная структура обусловливает непрерывный и массовый сбор персональных данных: каждое действие пользователя: регистрация, публикация, отметка геолокации, реакция на чужой контент: генерирует информацию, которая оседает в базах данных платформы.

[4] Бисалиев М., Шакиров К. Цифровые следы как фактор безопасности оборота персональных данных в сети интернет

[5] Аркабаев Н.К., Базарбаев Э.М. Социальные сети: правовое регулирование

Правовой статус самих платформ при этом остаётся дискуссионным. Теунаев И. констатирует, что онлайн-платформы де-факто функционируют как операторы персональных данных миллионов пользователей, однако их конкретные обязательства перед несовершеннолетними в российском законодательстве очерчены недостаточно чётко [6]. Это порождает ситуацию, при которой платформы пользуются широкими возможностями по сбору и монетизации данных детей, не неся при этом соразмерной юридической ответственности. Отсутствие специальных норм, адресованных именно несовершеннолетним пользователям, превращает общие положения Федерального закона № 152-ФЗ «О персональных данных» в инструмент, плохо приспособленный к реалиям детской онлайн-активности, тем более что, как было показано в параграфе 1.1, даже само понятие персональных данных применительно к детям трактуется в правоприменительной практике непоследовательно.

Ситуацию усугубляет разрыв между восприятием рисков детьми и их родителями. Долгополова И.В. на основе сравнительного анализа опросов старшеклассников и их родителей установила, что подростки, как правило, недооценивают опасность публичного раскрытия личной информации, тогда как родители, в свою очередь, не имеют достоверного представления о том, какой объём сведений их дети размещают в открытом доступе [7]. Этот двойной информационный разрыв — между ребёнком и платформой, а также между ребёнком и родителем — создаёт зону правовой уязвимости, в которой персональные данные несовершеннолетних циркулируют фактически бесконтрольно. Подростки открыто публикуют имя, фотографии, место учёбы, распорядок дня, не осознавая, что совокупность этих сведений формирует детальный идентификационный профиль.

[6] Теунаев И. Правовое регулирование социальных сетей и онлайн-платформ: теоретико-правовые аспекты защиты прав пользователей

[7] Долгополова И.В. Социальные сети в жизни старшеклассников: сравнительный анализ оценок учащихся и родителей

Именно здесь на первый план выходит проблема агрегации данных. Ерболатов Е.Е. указывает, что платформы не ограничиваются сбором сведений, которые пользователь вводит самостоятельно: они объединяют данные из множества источников: поведенческую аналитику, метаданные публикаций, информацию от третьих сервисов, формируя профили, несопоставимо более детальные, чем те, что осознанно предоставляет сам пользователь [8]. Применительно к несовершеннолетним это означает, что платформа располагает сведениями об интересах, социальном окружении, психологических особенностях и повседневных маршрутах ребёнка, причём ни он сам, ни его родители не имеют реального представления об объёме и составе этих данных. Такие профили могут использоваться в коммерческих целях: для таргетированной рекламы, направленной на детскую аудиторию, а в руках недобросовестных лиц становятся инструментом противоправного воздействия на несовершеннолетних.

Совокупность перечисленных факторов: технологическая архитектура платформ, ориентированная на максимальный сбор данных, правовая неопределённость статуса платформ как операторов, низкая осведомлённость детей и родителей о реальных рисках, а также возможности агрегации разрозненных сведений в детальные профили: определяет социальные сети как среду повышенного риска для персональных данных несовершеннолетних. Российский законодатель пока не выработал специальных правовых механизмов, адекватных этим рискам. Понять, насколько далеко в их создании продвинулось международное сообщество и какие модели могут служить ориентиром для отечественного права, позволяет обращение к зарубежному опыту и международно-правовым стандартам, которым посвящён следующий параграф.

[8] Ерболатов Е.Е. Особенности правового регулирования оборота персональных данных в сети интернет

1.3. Международно-правовые стандарты и зарубежный опыт защиты персональных данных детей в онлайн-среде

Международно-правовое измерение защиты персональных данных детей в онлайн-среде задаётся прежде всего двумя ключевыми инструментами: Конвенцией ООН о правах ребёнка 1989 года и Общим регламентом о защите данных Европейского союза (GDPR, Регламент 2016/679). Статья 16 Конвенции ООН прямо гарантирует ребёнку право на неприкосновенность частной жизни, и в условиях цифровизации это право неизбежно распространяется на персональные данные, которые несовершеннолетние генерируют в онлайн-среде. Россия ратифицировала Конвенцию ещё в 1990 году, однако специального закона, транслирующего статью 16 в конкретные механизмы защиты данных детей в социальных сетях, до сих пор не принято. Это порождает устойчивый разрыв между принятыми международными обязательствами и реальным состоянием внутреннего права.

Европейский регламент GDPR предлагает наиболее детально проработанную модель: статья 8 устанавливает возраст цифрового согласия на уровне 16 лет с правом государств-членов снижать его, но не ниже 13 лет, и одновременно требует верифицированного согласия родителей или законных представителей для лиц, не достигших установленного порога. Овчинникова Е.А. и Троеглазова А.В. в своём анализе показывают, что российское законодательство восприняло ряд принципов европейской модели: в частности, концепцию согласия субъекта как основания обработки данных, однако принципиальные конструктивные элементы GDPR, касающиеся именно несовершеннолетних, в российском праве последовательного отражения не нашли [9]. Это расхождение носит не технический, а концептуальный характер: европейский регулятор рассматривает ребёнка как субъекта, нуждающегося в особом, автономном

[9] Овчинникова Е.А., Троеглазова А.В. Анализ общих особенностей применения европейских норм при регулировании правового института персональных данных в РФ

правовом режиме, тогда как российский законодатель ограничивается общими нормами о согласии законных представителей.

Американский закон COPPA (Children's Online Privacy Protection Act, 1998) формирует альтернативную модель: он адресован непосредственно операторам онлайн-сервисов и обязывает их получать поддающееся проверке родительское согласие перед сбором данных детей до 13 лет, а также предоставлять родителям право на удаление уже собранной информации. Дубовицкая О.Б. в сравнительно-правовом исследовании фиксирует, что ни GDPR, ни COPPA не имеют функционального аналога в российском ФЗ № 152-ФЗ «О персональных данных»: закон не содержит специальной нормы о возрасте цифрового согласия для несовершеннолетних и не предусматривает механизма верификации родительского разрешения применительно к онлайн-платформам, что квалифицируется как существенный пробел нормативного регулирования [10]. Следствием этого пробела становится правовая неопределённость: платформы самостоятельно устанавливают возрастные ограничения в пользовательских соглашениях, не неся реальной ответственности за их обход.

Помимо нормативных конструкций, значимым фактором реализации прав субъектов данных выступает правовая культура пользователей. Соловьёв А., Шеяфетдинова Н., Завадская Л. и соавторы обращают внимание на то, что в странах с высоким уровнем правовой культуры в интернете несовершеннолетние и их родители значительно активнее прибегают к механизмам защиты, предусмотренным национальным законодательством, подают жалобы регуляторам, требуют удаления данных, используют право на доступ к собранной информации [11]. В России же низкая осведомлённость о правах субъектов персональных данных дополнительно обесценивает и без того ограниченный нормативный инструментарий: даже существующие правовые средства остаются практически невостребованными.

[10] Дубовицкая О.Б. Защита персональных данных: сравнительно-правовой анализ

[11] Соловьёв А., Шеяфетдинова Н., Завадская Л. и др. Интернет и персональные данные как факторы влияния на правовую культуру

Совокупность рассмотренных международных стандартов обнажает системную проблему: Россия, будучи участником Конвенции ООН о правах ребёнка и принимая во внимание опыт GDPR при реформировании законодательства о персональных данных, сохраняет принципиальную лакуну: отсутствие специального регулирования цифрового согласия несовершеннолетних и обязательств операторов социальных сетей перед детской аудиторией. Это обстоятельство служит отправной точкой для анализа конкретных норм российского права, которому посвящена следующая глава настоящей работы: именно там будет детально рассмотрено, как существующая нормативная база: при всей её фрагментарности: пытается заполнить пространство, которое международные стандарты очерчивают значительно чётче.

ГЛАВА 2. НОРМАТИВНО-ПРАВОВОЕ РЕГУЛИРОВАНИЕ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ НЕСОВЕРШЕННОЛЕТНИХ В СОЦИАЛЬНЫХ СЕТЯХ В РОССИЙСКОЙ ФЕДЕРАЦИИ

2.1. Система российского законодательства о персональных данных: общая характеристика применительно к несовершеннолетним

Конституционный фундамент защиты персональных данных в России заложен статьями 23 и 24 Конституции РФ, гарантирующими каждому право на неприкосновенность частной жизни, личную и семейную тайну, а также запрещающими сбор, хранение, использование и распространение информации о частной жизни лица без его согласия. Применительно к несовершеннолетним эти конституционные гарантии дополняются статьёй 38, устанавливающей обязанность государства защищать детство. Тем самым Конституция формирует двухуровневую охрану — общий режим неприкосновенности частной жизни и специальный режим для лиц, не достигших совершеннолетия, чья уязвимость в информационных отношениях предопределяет необходимость повышенного правового внимания.

Центральным актом отраслевого регулирования выступает Федеральный закон от 27 июля 2006 года № 152-ФЗ «О персональных данных». Закон закрепляет принципы обработки персональных данных: законность и справедливость, ограничение цели, минимизация объёма собираемых сведений, обеспечение точности и сохранности данных. Мамай Е.А. обращает внимание на то, что абстрактность формулировки понятия «персональные данные» в статье 3 указанного закона порождает широкую вариативность интерпретаций в законодательстве, общественном мнении и судебной практике, что существенно осложняет правоприменение [12]. Это наблюдение особенно значимо для детской аудитории социальных сетей: неопределённость базовых дефиниций транслируется в неопределённость

[12] Мамай Е.А. Указ. соч.

обязательств операторов. Дурина А. и Осадченко Э. фиксируют, что организационно-правовые механизмы исполнения принципов обработки данных операторами на практике не обеспечивают реальной защиты персональных сведений субъектов, а разрыв между буквой закона и поведением платформ остаётся значительным [13]. Применительно к социальным сетям, чья аудитория включает миллионы несовершеннолетних пользователей, этот разрыв приобретает особую остроту.

Помимо ФЗ № 152-ФЗ, присутствие детей в цифровом пространстве регулируется смежными актами. Федеральный закон от 29 декабря 2010 года № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию» устанавливает возрастную классификацию контента и ограничения его распространения. Федеральный закон от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации» регулирует общие отношения в информационной сфере, включая требования к операторам информационных систем. Однако ни один из этих законов не содержит специальных норм, непосредственно регламентирующих обработку персональных данных несовершеннолетних именно в социальных сетях. Петрыкина Н.И. указывает на то, что регулирование оборота персональных данных в России складывалось без учёта специфики отдельных категорий субъектов, в том числе детей, что обусловливает фрагментарность нормативной базы [14]. В итоге смежный нормативный массив лишь косвенно затрагивает интересующую нас сферу, не восполняя пробелов профильного законодательства.

Вместе с тем доктрина предлагает универсальные организационно-правовые модели, пригодные для адаптации к условиям социальных платформ. Сороколетова М. и Лесовский Ю., исследуя защиту персональных данных работников, выделяют трёхзвенную структуру организационно-правовой охраны: назначение ответственного лица за обработку данных, разработка и введение в действие локальных актов оператора, а также

[13] Дурина А., Осадченко Э. Организационно-правовая защита персональных данных

[14] Петрыкина Н.И. Указ. соч.

реализация технических мер защиты информации [15]. Эта модель, сложившаяся в трудовых отношениях, в адаптированном виде вполне применима к социальным сетям как операторам данных несовершеннолетних: тем более что ФЗ № 152-ФЗ адресует соответствующие требования любому оператору вне зависимости от сферы его деятельности.

Российское законодательство о персональных данных формирует общий режим охраны, опирающийся на конституционные гарантии и принципы ФЗ № 152-ФЗ, однако специальные нормы, учитывающие особый правовой статус несовершеннолетних как субъектов данных в социальных сетях, рассредоточены по смежным актам и не образуют целостного механизма. Этот вывод задаёт рамку для последующего анализа конкретных институтов: прежде всего механизма согласия на обработку персональных данных детей, которому посвящён следующий параграф.

2.2. Механизм согласия на обработку персональных данных несовершеннолетних: правовые требования и практика социальных сетей

Согласие субъекта персональных данных на их обработку занимает центральное место среди правовых оснований, предусмотренных российским законодательством. Смородинов Е.В. убедительно показывает, что именно согласие превратилось в универсальный инструмент легализации обработки данных в цифровой среде, причём широкое распространение этого основания среди интернет-сервисов объясняется не столько его удобством для пользователей, сколько отсутствием чётко закреплённых законом требований к форме и содержанию такого согласия [16]. Применительно к несовершеннолетним эта неопределённость приобретает особую остроту: дети, не достигшие четырнадцати лет, не обладают полной дееспособностью, а значит, их согласие на обработку данных лишено самостоятельной юридической силы.

[15] Сороколетова М., Лесовский Ю. Защита персональных данных работника

[16] Смородинов Е.В. Письменное согласие на обработку персональных данных в цифровой среде

Статья 9 Федерального закона № 152-ФЗ «О персональных данных» прямо устанавливает, что согласие за несовершеннолетнего, не достигшего четырнадцати лет, даёт его законный представитель: родитель, усыновитель или опекун. Норма выглядит достаточно определённой, однако её практическое исполнение вызывает серьёзные сомнения. Боргояков Ф. констатирует, что у значительной части граждан давно сложилась привычка механически подписывать согласие на обработку персональных данных: как собственных, так и своих детей, не вникая в правовые последствия подобных действий и не проверяя, какие именно условия закреплены в пользовательском соглашении конкретного сервиса [17]. Родитель, формально выступающий законным представителем, фактически не осознаёт, от чего именно он отказывается в пользу платформы, и это полностью обесценивает гарантию информированного согласия, которую призван обеспечить закон.

Ситуацию усугубляет повсеместно распространённая практика сбора согласия через принятие публичной оферты. Егорова О., исследуя механизмы сбора персональных данных клиентов, фиксирует, что пользовательские соглашения платформ, как правило, включают согласие на обработку данных в качестве условия по умолчанию: нажатие кнопки «Зарегистрироваться» или «Принять» автоматически означает акцепт всего пакета условий, в том числе разрешения на сбор, хранение и использование персональных данных [18]. Такая схема фактически подменяет требование явного и информированного согласия формальной процедурой, при которой пользователь лишён реального выбора: отказ от акцепта равнозначен отказу от доступа к сервису. Применительно к несовершеннолетним аудитории социальных сетей это означает, что дети либо регистрируются самостоятельно, обходя возрастные ограничения путём указания заведомо недостоверной даты рождения, либо их данные обрабатываются на основании согласия, полученного в обход требований о законном представительстве.

[17] Боргояков Ф. Судебная защита прав ребенка при незаконном использовании его персональных данных

[18] Егорова О. Как собирать персональные данные клиентов

Правовая неопределённость дополнительно нарастает в силу особенностей конструкции электронной сделки. Кусаинова А. и Кусаинов Д., анализируя регулирование заключения электронных сделок посредством сети Интернет, указывают, что акцепт публичной оферты несовершеннолетним без ведома и согласия родителей порождает неустранимую правовую неопределённость относительно действительности такого согласия на обработку данных [19]. С одной стороны, сделка может быть оспорена законным представителем как совершённая лицом, не обладающим необходимым объёмом дееспособности. С другой: платформа формально ссылается на факт акцепта оферты как на достаточное основание для обработки данных. Российское законодательство не содержит специального механизма, который разрешал бы это противоречие применительно к цифровым сервисам с детской аудиторией.

Совокупность описанных проблем обнажает системный разрыв между буквой закона и реальной практикой социальных сетей. Норма о согласии законного представителя существует, однако ни требования к его форме в цифровой среде, ни санкции за её несоблюдение операторами не конкретизированы настолько, чтобы обеспечить реальную защиту данных ребёнка. Именно этот пробел предопределяет необходимость рассмотреть, какие обязанности российское законодательство возлагает на операторов — социальные сети — и насколько эффективно Роскомнадзор контролирует их исполнение в части защиты персональных данных несовершеннолетних пользователей.

2.3. Обязанности операторов — социальных сетей и надзор Роскомнадзора за соблюдением законодательства о персональных данных несовершеннолетних

Социальные сети, аккумулируя персональные данные миллионов пользователей, в правовом смысле выступают операторами в соответствии с

[19] Кусаинова А., Кусаинов Д. Правовое регулирование заключения электронных сделок посредством сети интернет

ФЗ № 152-ФЗ и несут весь объём предусмотренных им обязанностей. Теунаев И. систематизирует их следующим образом: уведомление Роскомнадзора о начале обработки данных, назначение лица, ответственного за организацию этой обработки, обеспечение конфиденциальности и технической безопасности информационных систем [20]. Принципиально важно при этом, что российское законодательство не выделяет платформы, аудитория которых включает несовершеннолетних, в отдельную категорию операторов с повышенными требованиями. Иными словами, ВКонтакте, обрабатывающая данные школьников, и корпоративный HR-портал формально находятся в одном правовом режиме: общем, не учитывающем уязвимость детской аудитории.

Отсутствие специальных императивных норм для платформ с детской аудиторией прямо сказывается на качестве технических мер защиты. Лукошкин А.А. выявил, что шифрование пользовательских данных, гибкие настройки приватности и механизмы ограничения видимости профилей реализуются социальными сетями преимущественно в добровольном порядке, а не в силу обязательных правовых предписаний [21]. Следствием этого становится существенная вариативность: одни платформы предоставляют развитые инструменты управления данными, другие ограничиваются минимальным набором настроек. Применительно к несовершеннолетним данная вариативность особенно опасна: ребёнок лишён возможности осознанно оценить уровень защиты конкретного сервиса и самостоятельно минимизировать риски.

Надзор за соблюдением законодательства о персональных данных возложен на Роскомнадзор, который наделён широкими полномочиями: проведение плановых и внеплановых проверок операторов, вынесение предписаний об устранении нарушений, обращение в суд с исками о прекращении незаконной обработки данных, а также привлечение виновных

[20] Теунаев И. Указ. соч.

[21] Лукошкин А.А. Personal data protection in social networks: mechanisms of user data protection, privacy issues and citizens' rights

лиц к административной ответственности по ст. 13.11 КоАП РФ. После поправок 2022 года максимальный штраф за повторное нарушение составляет 500 тысяч рублей. Для малого бизнеса эта сумма ощутима, однако для крупной социальной сети с многомиллиардной аудиторией она несопоставима с выгодами от монетизации пользовательских данных. Сравнительный анализ показывает разительный контраст с европейской практикой: GDPR предусматривает штрафы до 20 млн евро или до 4% годового мирового оборота компании: именно такой масштаб санкций способен формировать реальные поведенческие стимулы для платформ. Российские же размеры взысканий не создают превентивного эффекта, который побуждал бы операторов инвестировать в защиту данных несовершеннолетних сверх законодательного минимума. Сопоставимую картину демонстрирует и международный контекст: Аркабаев Н.К. и Базарбаев Э.М. фиксируют, что в ряде государств ответственность платформ за нарушения в сфере данных пользователей строится на принципиально иных, более жёстких механизмах, тогда как постсоветское пространство в целом отстаёт в части санкционного давления на операторов [22].

Результирующая картина правоприменения оказывается предсказуемой. Дурина А. и Осадченко Э. констатируют, что на практике организационно-правовая защита персональных данных нередко сводится к формированию пакета документов: политик конфиденциальности, регламентов обработки данных, приказов о назначении ответственных лиц, тогда как содержательный контроль за фактическим соблюдением прав субъектов данных остаётся недостаточным [23]. Применительно к несовершеннолетним этот разрыв между документальным и реальным особенно значим: ребёнок не располагает инструментами самостоятельной защиты своих прав, а родители зачастую не осведомлены о том, какие данные собирает платформа и на каких основаниях. Ограниченные кадровые и финансовые ресурсы Роскомнадзора не позволяют обеспечить

[22] Аркабаев Н.К. и др. Указ. соч.
[23] Дурина А. и др. Указ. соч.

систематический мониторинг десятков крупных платформ, а реактивная модель надзора: когда проверка инициируется преимущественно по жалобам: заведомо запаздывает по отношению к уже совершённым нарушениям.

Подводя итог второй главе, необходимо зафиксировать системный характер выявленных пробелов. Российская нормативная база защиты персональных данных несовершеннолетних в социальных сетях складывается из общего режима ФЗ № 152-ФЗ, конституционных гарантий частной жизни и разрозненных норм смежного законодательства, однако специальное регулирование, учитывающее особый статус детской аудитории цифровых платформ, фактически отсутствует. Механизм согласия не адаптирован к реалиям социальных сетей, обязанности операторов не дифференцированы по возрастному составу аудитории, а санкционный инструментарий надзорного органа не сопоставим с масштабом деятельности крупнейших платформ. Совокупность этих обстоятельств определяет необходимость комплексного реформирования, анализу направлений которого посвящена следующая глава работы.

ГЛАВА 3. ПРОБЛЕМЫ ПРАВОПРИМЕНЕНИЯ И НАПРАВЛЕНИЯ СОВЕРШЕНСТВОВАНИЯ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ НЕСОВЕРШЕННОЛЕТНИХ В СОЦИАЛЬНЫХ СЕТЯХ

3.1. Актуальные угрозы персональным данным несовершеннолетних в социальных сетях и проблемы их уголовно-правовой защиты

Цифровая среда открыла перед злоумышленниками принципиально новые возможности для доступа к сведениям о детях, и социальные сети оказались наиболее уязвимым каналом утечки таких сведений. Корнилова Т. и Лапенков Е. систематизируют угрозы персональным данным несовершеннолетних в интернете, выделяя четыре основных вектора: несанкционированный сбор данных платформами и третьими лицами, их продажа рекламным агрегаторам, использование в целях таргетированного воздействия на детей и: наиболее опасный сценарий: применение собранных сведений для установления контакта с ребёнком с целью сексуальной эксплуатации или вовлечения в противоправную деятельность [24]. Показательно, что первые три угрозы нередко воспринимаются как коммерческая практика, тогда как последняя влечёт прямые уголовно-правовые последствия для жертвы.

Механизм превращения «безобидных» данных профиля в инструмент преступления подробно раскрывает Жоков Д.: геолокационные метки, фотографии с подписями о распорядке дня, сведения о школе и кружках: всё это позволяет злоумышленнику выстраивать психологический контакт с ребёнком задолго до физической встречи, имитируя осведомлённость и близость [25]. Иными словами, открытые страницы несовершеннолетних в социальных сетях функционируют как непреднамеренно составленное досье, которое преступник может использовать в качестве готовой легенды для

[24] Корнилова Т., Лапенков Е. Problems of criminal law protection of personal data on the Internet

[25] Жоков Д. Ответственность за вовлечение несовершеннолетних в совершение преступлений с использованием информационно-телекоммуникационных технологий и сети интернет

манипуляций. Особую тревогу вызывает то, что сами дети, как правило, не осознают связи между публикацией геометки под фотографией и последующим появлением незнакомца, «случайно» оказавшегося рядом с их домом.

Чуняева В.А. прослеживает эту цепочку до её криминального завершения: утечка персональных данных из социальных сетей выступает одним из ключевых факторов, облегчающих совершение преступлений против половой неприкосновенности несовершеннолетних, поскольку снижает временны́е и психологические барьеры для установления первичного контакта с потенциальной жертвой [26]. При этом исследователь констатирует серьёзный законодательный пробел: российское уголовное право не содержит самостоятельного состава, криминализирующего незаконный сбор персональных данных детей в онлайн-среде именно как подготовительное действие к преступлению. Сам по себе сбор данных квалифицируется лишь тогда, когда правоохранительным органам удаётся доказать прямую связь с последующим деянием, а это удаётся редко [27].

Теоретически уголовный закон располагает инструментами реагирования. Статья 137 УК РФ, предусматривающая ответственность за нарушение неприкосновенности частной жизни, распространяется на незаконный сбор и распространение сведений о частной жизни лица без его согласия. Статья 272 УК РФ о неправомерном доступе к компьютерной информации охватывает случаи взлома аккаунтов и перехвата данных. Однако практическое применение обеих норм к ситуациям с детскими данными наталкивается на системные препятствия: доказать умысел на нарушение именно неприкосновенности частной жизни несовершеннолетнего крайне сложно, если данные были получены из открытого профиля; идентификация нарушителя в условиях анонимизирующих сервисов и VPN требует значительных процессуальных ресурсов; наконец, сам факт «открытости» детского аккаунта нередко

[26] Чуняева В.А. Protection of sexual integrity of minors on the Internet

[27] Там же.

трактуется как молчаливое согласие на ознакомление с опубликованными сведениями. Корнилова Т. и Лапенков Е. прямо указывают, что действующий уголовно-правовой инструментарий не адаптирован к специфике цифровой среды и требует существенного пересмотра с учётом реальных схем использования персональных данных [28].

Совокупность описанных угроз формирует картину, при которой наиболее уязвимая категория субъектов: дети: оказывается наименее защищённой именно в той среде, где они проводят значительную часть времени. Пробел в уголовном законодательстве, на который указывают как Чуняева В.А. [29], так и Жоков Д. [30], носит не технический, а концептуальный характер: законодатель до сих пор не признал незаконный сбор данных несовершеннолетних самостоятельным общественно опасным деянием, предшествующим более тяжким преступлениям. Насколько эффективно с этим пробелом справляются гражданско-правовые и судебные механизмы защиты: вопрос, требующий отдельного рассмотрения.

3.2. Судебная защита прав несовершеннолетних при незаконной обработке их персональных данных в социальных сетях

Установленные в предыдущем параграфе угрозы: несанкционированный сбор данных несовершеннолетних, их использование злоумышленниками для выхода на контакт с детьми: закономерно ставят вопрос о том, насколько эффективно действующее право позволяет пострадавшим восстановить нарушенные интересы. Картина, которую рисует анализ судебной и административной практики, оказывается весьма далёкой от идеальной.

Отправной точкой служит парадокс, зафиксированный Боргояковым Ф.: большинство родителей попросту не обращаются за судебной защитой, поскольку не осознают самого факта нарушения. Подписанное при регистрации ребёнка на платформе согласие на обработку данных

[28] Корнилова Т. и др. Указ. соч.
[29] Чуняева В.А. Указ. соч.
[30] Жоков Д. Указ. соч.

воспринимается законными представителями как универсальное разрешение, охватывающее любые последующие операции с информацией о несовершеннолетнем, тогда как по смыслу ФЗ № 152-ФЗ каждая новая цель обработки требует отдельного согласия [31]. Это когнитивное заблуждение фактически блокирует запуск любого защитного механизма ещё до того, как родитель успевает оценить правовые возможности.

Между тем гражданско-правовые инструменты формально существуют. Статья 24 ФЗ № 152-ФЗ наделяет субъекта персональных данных: а применительно к несовершеннолетним его законных представителей: правом требовать компенсации морального вреда, причинённого незаконной обработкой. Помимо этого, законный представитель вправе предъявить требование об уничтожении неправомерно собранных сведений. Однако судебная практика по делам о нарушении прав детей в социальных сетях насчитывает единичные случаи: платформы, как правило, ссылаются на факт получения согласия при регистрации, а суды нередко принимают этот аргумент, не вникая в соответствие конкретных операций заявленным целям обработки. Дурина А. и Осадченко Э. фиксируют, что организационно-правовые механизмы защиты персональных данных в России в целом функционируют со значительными сбоями именно на стадии правоприменения: декларируемые принципы защиты не подкреплены эффективной процедурой их судебного отстаивания [32].

Дополнительную сложность создаёт проблема квалификации самого объекта защиты. Мамай Е.А. указывает на устойчивое расхождение между законодательным определением персональных данных и их трактовкой в судебной практике: суды систематически отказывают в защите, квалифицируя сведения из публичных профилей: имя ребёнка, его фотографии, геолокационные отметки, как общедоступную информацию, не подпадающую под режим ФЗ № 152-ФЗ [33]. Абстрактность формулировки ст.

[31] Боргояков Ф. Указ. соч.
[32] Дурина А. и др. Указ. соч.
[33] Мамай Е.А. Указ. соч.

3 закона, определяющей персональные данные через признак «относимости к физическому лицу», порождает широкий судейский дискреционный люфт, который на практике оборачивается против интересов субъектов данных. Применительно к несовершеннолетним это особенно болезненно: именно публичная часть детского профиля — фотографии, сведения о школе, маршруты — чаще всего становится объектом незаконного использования, однако именно она с наибольшей вероятностью будет выведена судом за пределы охраняемой сферы.

На этом фоне административный порядок защиты через подачу жалобы в Роскомнадзор выглядит для родителей несовершеннолетних более доступным маршрутом: порог входа ниже, специальных правовых знаний не требуется, а сам факт обращения к регулятору способен стимулировать платформу к добровольному устранению нарушения. Вместе с тем этот механизм имеет очевидные ограничения. Сроки рассмотрения жалоб растягиваются, санкции, которые регулятор вправе применить к оператору-нарушителю, несоразмерны масштабу деятельности крупных платформ, а сам Роскомнадзор лишён полномочий присудить компенсацию пострадавшему ребёнку. В результате административный путь, даже завершившись формальным успехом, не восстанавливает нарушенное право в полном объёме.

Совокупность описанных факторов: правовая неосведомлённость родителей, рестриктивная судебная трактовка понятия персональных данных, номинальность санкций в административном порядке: свидетельствует о том, что существующие механизмы защиты не образуют реально работающей системы. Устранение этих пробелов предполагает изменения не только на уровне правоприменения, но и в самом нормативном регулировании, о конкретных направлениях которого речь пойдёт в следующем параграфе.

3.3. Направления совершенствования правового регулирования защиты персональных данных несовершеннолетних в социальных сетях

Анализ угроз и недостатков судебной защиты, проведённый в предыдущих параграфах, закономерно ставит вопрос о том, каким должно быть реформированное законодательство. Ответ на него складывается из нескольких взаимосвязанных направлений: нормативного, процедурного, технологического и образовательного.

Первое и наиболее неотложное направление: введение обязательной верификации возраста пользователей социальных сетей и специального режима «детского аккаунта» с ограниченным набором собираемых данных. Лукошкин А.А. обосновывает, что существующие механизмы защиты персональных данных в социальных сетях не учитывают возрастную специфику пользователей, а ключевой уязвимостью остаётся отсутствие в российском праве возрастного порога цифрового согласия [34]. Европейский регламент GDPR решает эту проблему через ст. 8, устанавливающую такой порог на уровне 16 лет с правом государств-членов снижать его до 13. Перенос аналогичной конструкции в российское право позволил бы устранить ситуацию, при которой платформы формально соблюдают закон, получая согласие родителей, но фактически никак не ограничены в объёме сбора данных о детях.

Конкретную законодательную модель предлагают Овчинникова Е.А. и Троеглазова А.В.: по их мнению, в ФЗ № 152-ФЗ необходимо имплементировать специальную главу о защите данных несовершеннолетних, установив возраст цифрового согласия в 14 лет: цифру, согласующуюся с возрастом частичной дееспособности по ст. 26 ГК РФ, а также закрепить упрощённый порядок отзыва согласия и обязательный принцип «privacy by design» для всех функций платформ, ориентированных на детскую аудиторию [35]. Такой подход имеет очевидное системное

[34] Лукошкин А.А. Указ. соч.

[35] Овчинникова Е.А. и др. Указ. соч.

преимущество: он не создаёт изолированный специальный закон, а встраивает детскую защиту в действующую архитектуру законодательства о персональных данных, обеспечивая единство правоприменения.

Третье направление касается качества самого механизма согласия. Смородинов Е.В. фиксирует, что в российском праве отсутствуют формально определённые требования к форме и содержанию согласия на обработку персональных данных в цифровой среде, что открывает операторам широкие возможности для составления непрозрачных, объёмных пользовательских соглашений [36]. Применительно к несовершеннолетним этот пробел особенно критичен: согласие законного представителя должно содержать исчерпывающий перечень категорий обрабатываемых данных, конкретные цели обработки и чётко определённый срок хранения, причём изложенные в форме, понятной как родителю, так и самому ребёнку. Без такой формализации даже добросовестно подписанное согласие не выполняет своей защитной функции: именно это подтверждает вывод параграфа 3.2 о том, что родители воспринимают подписанный документ как универсальное разрешение на любую обработку.

Четвёртое направление — повышение правовой культуры несовершеннолетних и их родителей — нередко воспринимается как факультативная мера, однако без него любые нормативные изменения рискуют остаться декоративными. Соловьёв А. и соавторы указывают, что уровень правовой культуры в интернет-среде напрямую определяет способность граждан защищать собственные персональные данные, а её формирование требует целенаправленных государственных усилий [37]. Включение основ законодательства о персональных данных в школьные программы: например, в рамках курса обществознания или информатики: и введение обязательного краткого инструктажа при регистрации несовершеннолетнего в социальной сети способны создать первичный барьер против наиболее распространённых нарушений. Такой инструктаж мог бы

[36] Смородинов Е.В. Указ. соч.

[37] Соловьёв А. и др. Указ. соч.

содержать информацию о праве на удаление данных, о рисках геолокационных сервисов и о порядке обращения к оператору с требованием прекратить обработку.

Совокупность предложенных мер: возрастной порог цифрового согласия, специальная глава в ФЗ № 152-ФЗ, формализованные требования к содержанию согласия и системное правовое просвещение: образует комплексный ответ на те пробелы, которые были выявлены в предшествующих параграфах настоящей главы. Угрозы персональным данным несовершеннолетних в социальных сетях не исчезнут сами по себе по мере развития платформ; их нейтрализация требует последовательной законодательной воли, подкреплённой работающими механизмами правоприменения и реальной осведомлённостью граждан о своих правах.

ЗАКЛЮЧЕНИЕ

Проведённое исследование обнажило принципиальное противоречие, которое пронизывает всю систему охраны персональных данных несовершеннолетних в российских социальных сетях: декларативная защита, закреплённая в Конституции РФ и ФЗ № 152-ФЗ, существует в значительной мере отдельно от реальных правовых механизмов, способных эту защиту обеспечить. Российское законодательство не знает понятия «возраст цифрового согласия», не предусматривает обязательной верификации возраста пользователей социальных сетей и не устанавливает повышенных требований к операторам, чья аудитория включает детей. В результате несовершеннолетний, зарегистрировавшийся во ВКонтакте или TikTok, формально подпадает под действие тех же норм, что и взрослый, при том что его уязвимость перед манипулятивными алгоритмами, профилированием и несанкционированным сбором данных несопоставимо выше. Этот системный разрыв не является случайным упущением законодателя: он отражает общую логику ФЗ № 152-ФЗ, создававшегося в эпоху, когда социальные сети ещё не стали повседневной средой обитания детей.

Фрагментарность нормативной базы предопределяет и практическую неэффективность механизмов защиты. Судебная практика по делам о нарушении режима персональных данных несовершеннолетних в социальных сетях остаётся крайне скудной: не потому, что нарушений нет, а потому что их крайне сложно доказать, а санкции, даже в случае успешного разбирательства, несоразмерны масштабу деятельности платформ. Административные штрафы, предусмотренные КоАП РФ, не создают для крупных операторов реального стимула к соблюдению законодательства: для компании с многомиллиардной выручкой штраф в несколько сотен тысяч рублей представляет собой операционные издержки, а не угрозу. Роскомнадзор, располагая полномочиями по надзору в сфере персональных данных, использует их в отношении детской аудитории социальных сетей непоследовательно. Правовая неосведомлённость родителей замыкает этот

круг: большинство из них не осознают ни объём данных, которые платформы собирают об их детях, ни инструменты, которые теоретически позволяют эту обработку ограничить. Совокупность этих факторов превращает существующую систему защиты в конструкцию, которая выглядит убедительно на бумаге, но практически не работает в точке реального нарушения прав ребёнка.

Международный опыт указывает на возможный выход из этого положения. GDPR и британский Кодекс надлежащей практики в отношении детей (Age Appropriate Design Code) демонстрируют, что специальное регулирование, ориентированное именно на детскую аудиторию цифровых платформ, технически реализуемо и правоприменительно эффективно. Принципы «privacy by design» и «privacy by default», возраст цифрового согласия в диапазоне 13–16 лет, обязательная верификация возраста, запрет на профилирование несовершеннолетних в маркетинговых целях: всё это уже апробированные инструменты, а не теоретические конструкции. Для российского законодателя наиболее перспективным представляется путь принятия специального федерального закона о защите персональных данных несовершеннолетних в онлайн-среде либо введения в ФЗ № 152-ФЗ самостоятельной главы с аналогичным предметом регулирования. Такой акт должен установить возраст самостоятельного цифрового согласия, ввести обязанность платформ по верификации возраста пользователей с использованием технологически нейтральных методов, закрепить повышенные санкции за нарушения в отношении детской аудитории и возложить на операторов бремя доказывания правомерности обработки данных несовершеннолетних. Параллельно необходимо системное повышение цифровой правовой грамотности: включение соответствующих модулей в школьные программы и информационные кампании для родителей, поскольку даже совершенное законодательство остаётся малоэффективным без субъектов, способных им воспользоваться.

Настоящая работа достигла поставленной цели: комплексный анализ правового регулирования защиты персональных данных несовершеннолетних в социальных сетях позволил установить конкретные нормативные лакуны, объяснить причины практической неэффективности действующих механизмов и сформулировать обоснованные направления реформирования. Значимость полученных выводов определяется не только академическим измерением: они могут служить ориентиром для законопроектной работы в условиях, когда российский законодатель всё отчётливее осознаёт необходимость специального регулирования цифровой среды применительно к детям. Каждый год промедления с принятием такого регулирования означает, что миллионы несовершеннолетних пользователей российских и зарубежных платформ продолжают оставаться в правовом вакууме: защищёнными лишь номинально.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Аркабаев Н.К., Базарбаев Э.М. Социальные сети: правовое регулирование // Bulletin of Osh State University. — 2023. — DOI: 10.52754/16948610_2023_2_19.

2. Смородинов Е.В. Письменное согласие на обработку персональных данных в цифровой среде // Труды по интеллектуальной собственности. — 2025. — DOI: 10.17323/tis.2025.27960.

3. Ерболатов Е.Е. Особенности правового регулирования оборота персональных данных в сети интернет // Bulletin of Toraigyrov University. Law series. — 2023. — DOI: 10.48081/emgr5259.

4. Петрыкина Н.И. Некоторые вопросы регулирования оборота персональных данных в РФ // Moscow Journal of International Law. — 2021. — DOI: 10.24833/0869-0049-2007-2-68-80.

5. Овчинникова Е.А., Троеглазова А.В. Анализ общих особенностей применения европейских норм при регулировании правового института персональных данных в РФ // Interexpo GEO-Siberia. — 2023. — DOI: 10.33764/2618-981x-2023-8-1-156-161.

6. Корнилова Т., Лапенков Е. Problems of criminal law protection of personal data on the Internet // Ius Publicum et Privatum. — 2024. — DOI: 10.46741/2713-2811.2024.25.1.012.

7. Бисалиев М., Шакиров К. Цифровые следы как фактор безопасности оборота персональных данных в сети интернет // Bulletin of L.N. Gumilyov Eurasian National University Law Series. — 2023. — DOI: 10.32523/2616-6844-2023-142-1-81-98.

8. Жоков Д. Ответственность за вовлечение несовершеннолетних в совершение преступлений с использованием информационно-телекоммуникационных технологий и сети интернет // Вопросы

устойчивого развития общества. — 2023. — DOI: 10.34755/irok.2022.60.21.006.

9. Чуняева В.А. Protection of sexual integrity of minors on the Internet // Current Issues of the State and Law. — 2022. — DOI: 10.20310/2587-9340-2022-6-4-611-618.

10. Соловьёв А., Шеяфетдинова Н., Завадская Л. и др. Интернет и персональные данные как факторы влияния на правовую культуру // Современное право. — 2020. — DOI: 10.25799/ni.2020.66.60.018.

11. Рязанова К. Биометрические персональные данные как основание идентификации личности // Financial and Economic Journal. — 2023. — DOI: 10.34755/irok.2023.65.72.046.

12. Мамай Е.А. Персональные данные как объект правового регулирования: соотношение законодательства, общественного мнения и судебной практики // Информационное общество: образование, наука, культура и технологии будущего. — 2024. — DOI: 10.17586/2587-8557-2024-7-273-292.

13. Теунаев И. Правовое регулирование социальных сетей и онлайн-платформ: теоретико-правовые аспекты защиты прав пользователей // Вестник Чеченского государственного университета. — 2025. — DOI: 10.36684/chesu-2025-1-57-196-202.

14. Лукошкин А.А. Personal data protection in social networks: mechanisms of user data protection, privacy issues and citizens' rights // Ekonomika i upravlenie: problemy, resheniya. — 2025. — DOI: 10.36871/ek.up.p.r.2025.02.06.017.

15. Сороколетова М., Лесовский Ю. Защита персональных данных работника // Тенденции развития науки и образования. — 2022. — DOI: 10.18411/trnio-06-2022-340.

16. Дурина А., Осадченко Э. Организационно-правовая защита персональных данных // Тенденции развития науки и образования. — 2023. — DOI: 10.18411/trnio-06-2023-149.

17. Дубовицкая О.Б. Защита персональных данных: сравнительно-правовой анализ // Bulletin of Toraigyrov University. Law series. — 2022. — DOI: 10.48081/mrfo1440.

18. Боргояков Ф. Судебная защита прав ребенка при незаконном использовании его персональных данных // Тенденции развития науки и образования. — 2021. — DOI: 10.18411/lj-05-2021-166.

19. Егорова О. Как собирать персональные данные клиентов // Интернет-маркетинг. — 2023. — DOI: 10.36627/2619-1369-2023-3-3-182-193.

20. Кусаинова А., Кусаинов Д. Правовое регулирование заключения электронных сделок посредством сети интернет // Наука и жизнь Казахстана. — 2021. — DOI: 10.52334/nzhk.2021.62.69.011.

21. Тхабисимова Л., Камилов М. Constitutional and legal regulation of public events on the Internet // Социально-гуманитарные знания. — 2022. — DOI: 10.34823/sgz.2021.6.51717.

22. Долгополова И.В. Социальные сети в жизни старшеклассников: сравнительный анализ оценок учащихся и родителей // Психология и психотехника. — 2016. — DOI: 10.7256/2070-8955.2016.10.21800.