

Салишев Даниил Сергеевич

студент

ФГБОУ ВО «Кубанский государственный аграрный

университет им. И.Т. Трубилина»

г. Краснодар, Краснодарский край

ЦИФРОВОЕ ВМЕШАТЕЛЬСТВО В ЧАСТНУЮ ЖИЗНЬ: ЭТИЧЕСКИЕ, ПРАВОВЫЕ И ПСИХОЛОГИЧЕСКИЕ ИЗМЕРЕНИЯ

Аннотация: статья посвящена комплексному анализу проблемы цифрового вмешательства в частную жизнь, рассматриваемой в двух взаимосвязанных измерениях: правовом и психологическом. На основе актуальных данных о масштабах утечек персональной информации, практиках корпоративного надзора и международного регулирования обосновывается тезис о том, что угрозы конфиденциальности давно вышли за рамки технологической проблематики и приобрели характер системного социального вызова. Отдельное внимание уделяется психологическим последствиям цифровой слежки: тревожности, профессиональному выгоранию, феноменам цифровой зависимости и нового одиночества. Делается вывод о необходимости формирования этического консенсуса относительно допустимых границ присутствия государства и корпораций в цифровом пространстве личности.

Ключевые слова: персональные данные, психологическая безопасность, цифровая зависимость, кибербуллинг, цифровое фенотипирование.

К середине 2020-х годов цифровое пространство стало неотъемлемой средой человеческой жизни: более 4,9 млрд человек – свыше 62% населения планеты – регулярно пользуются интернетом. Вместе с беспрецедентными возможностями коммуникации, а «сложнейший процесс коммуникации обеспечивается за счет тесной интеграции в первую очередь информационной техники и интегрированных программ» [1] и доступа к информации эта среда несёт в себе столь

же масштабные риски. Ключевым среди них является систематическое нарушение приватности: государственными структурами, коммерческими компаниями и отдельными злоумышленниками.

Социологические замеры фиксируют тревогу населения: по данным российских исследований, около 60% граждан выражают обеспокоенность процессами цифровизации, а за три года федеральный омбудсмен получил свыше 800 жалоб, связанных с незаконным сбором и обработкой персональных данных. Проблема, таким образом, приобрела отчётливое социальное измерение, далеко выйдя за пределы узкотехнических дискуссий.

Настоящая статья ставит целью систематизировать современное состояние проблемы, выделив два ключевых измерения: нормативно-правовое регулирование и психологические последствия слежки для индивида.

Регулирование искусственного интеллекта в России. В начале 2026 года российский законодатель вновь обратился к вопросу об ограничении систем искусственного интеллекта. Первый заместитель председателя Комитета Совета Федерации по конституционному законодательству Артём Шейкин обозначил перечень «красных линий»: использование ИИ для дискриминации граждан, манипулирования общественным сознанием, неправомерного проникновения в частную жизнь и воздействия на критическую инфраструктуру. Механизмом этического контроля предполагается сделать сочетание нормативного регулирования, экспертных обсуждений и участия научного сообщества – с обязательным учётом отечественных культурных и исторических ценностей. Сам факт возвращения темы в повестку законодателей свидетельствует о признании государством системного характера соответствующих рисков.

Масштабы утечек персональных данных. Статистика Роскомнадзора рисует тревожную картину. В 2024 году было зафиксировано 135 утечек баз данных, в результате которых в открытый доступ попало более 710 млн записей о гражданах России [2]. По оценкам «Сбера», персональные данные порядка 90% взрослого населения страны уже присутствуют в сети – преимущественно через ин-

тернет-магазины и медицинские организации. 2025 год начался с нарастания инцидентной активности: за январь-февраль произошло 19 утечек, обнажив сведения о более чем 24 млн человек. Среди наиболее резонансных случаев – взлом базы данных владельцев автомобилей KIA (500 тыс. записей) и проникновение в реестр ЕГРН, откуда злоумышленники похитили массив данных, содержащий около 82 млн строк с паспортными сведениями, адресами и финансовой информацией граждан. Законодательным ответом стало введение оборотных штрафов: до 15 млн рублей при первом нарушении и до 3% годовой выручки при повторном. По итогам первого полугодия 2025 года было выявлено 601 административное дело о незаконной обработке данных и возбуждено 313 уголовных производств [3].

Цифровой контроль в трудовых отношениях. Особую зону напряжения представляет производственная среда. Согласно данным платформы «Работа.ру», 72% российских компаний осуществляют мониторинг продуктивности сотрудников – с помощью видеокамер, трекинга веб-активности и хронометража рабочего времени. При этом о факте наблюдения осведомлены 95% работников [4]. Как известно, «информационно-коммуникационная компетенция имеет высокую значимость для конкурентоспособности специалиста» [5].

Психологические последствия цифровой слежки. Психологические исследования фиксируют измеримые последствия цифровой слежки для индивида. Постоянное ощущение наблюдения ухудшает мнемические функции, снижает концентрацию внимания и усиливает симптоматику тревожных и депрессивных состояний. В сфере социальных медиа аналогичные эффекты провоцируют поведенческие практики слежения за другими пользователями – отслеживание статусов «прочитано», мониторинг онлайн-присутствия. Одним из наиболее устойчивых факторов риска выступает FOMO (fear of missing out) – страх упущенных возможностей, усиливающий социальную тревогу и чувство собственной несостоятельности.

Феномен цифровой интимности. Российские психологи фиксируют формирование нового поведенческого паттерна – цифровой интимности: глубокой эмоциональной привязанности к виртуальным собеседникам, чат-ботам и ИИ-партнёрам, так как «с появлением сети появилась возможность круглосуточно присутствовать в виртуальной жизни» [6]. Психолог М.А. Макаренко выделяет четыре ключевых фактора уязвимости в рамках подобных отношений:

- круглосуточная доступность формирует привычку к мгновенному удовлетворению эмоциональных потребностей;
- безусловное одобрение искажает представления о нормах здоровых межличностных отношений;
- образ «идеального собеседника» снижает толерантность к несовершенству реальных людей;
- атрофия навыков саморегуляции повышает тревожность и снижает качество живого общения [7].

Хроническое одиночество и кибербуллинг. Клинический психолог М.В. Логинова охарактеризовала хроническое одиночество как одно из наиболее характерных расстройств цифровой эпохи: человек присутствует среди людей, однако ощущает себя чужим. Социальные сети не только не устраняют это ощущение, но нередко его усиливают – посредством постоянного сравнения себя с тщательно отредактированными «идеальными жизнями» других пользователей. Отдельную угрозу представляет кибербуллинг, который во многих случаях оказывается деструктивнее офлайн-травли. Опосредованность цифровой среды устраняет эмоциональную обратную связь: агрессор не видит реакции жертвы, что снижает внутренние барьеры для продолжения преследования и делает последствия для пострадавшего труднопредсказуемыми [8].

Позиция ВОЗ: цифровая среда как детерминанта психического здоровья.

В мае 2025 года Всемирная организация здравоохранения опубликовала аналитическую записку «Работа с цифровыми детерминантами психического здоровья молодёжи». Ключевой тезис документа: цифровое пространство формирует психическое здоровье молодых людей с той же интенсивностью, что семья и

школа, однако при значительно меньшем уровне защиты. К основным рискам ВОЗ относят: киберзапугивание, пропаганду нереалистичных стандартов внешности, контент, нормализующий самоповреждение, непрозрачные алгоритмы, усиливающие деструктивный контент, а также ненадлежащее управление пользовательскими данными без осознанного согласия. Региональный директор ВОЗ в Европе доктор Ханс Клюге призвал к немедленным координированным действиям – от повышения цифровой грамотности до усиления регуляторного контроля над платформами [9].

Цифровое фенотипирование: новые риски психиатрического паноптикума. Одной из наиболее острых этических проблем становится цифровое фенотипирование – систематический сбор поведенческих и физиологических данных со смартфонов, носимых устройств и интернет-активности с целью прогнозирования психического состояния пользователя. Ряд разработчиков позиционирует подобные системы как инструмент ранней диагностики психических расстройств, однако практика их применения вызывает серьёзные возражения. Исследователи предупреждают: приложения для психического здоровья способны превращать уязвимых пользователей в невольных производителей коммерчески ценных данных – в момент, когда люди наиболее открыты и незащищены. В научном сообществе активно обсуждается вопрос о допустимости присвоения человеку статуса «группы риска» психических заболеваний на основании цифровых следов, а также о последствиях подобной классификации в случае её ошибочности. Цифровое вмешательство в частную жизнь представляет собой устойчивую и нарастающую реальность, охватывающую как минимум два взаимосвязанных измерения. В правовом измерении государства и международные институты вырабатывают механизмы регулирования цифровой среды, однако их эффективность остаётся ограниченной: крупнейшие корпорации воспринимают штрафы как приемлемую стоимость ведения бизнеса. В психологическом измерении цифровая среда генерирует новые формы тревожности, зависимости, одиночества и уязвимости. Адекватный ответ на обозначенные вызовы предполагает системный подход, включающий: развитие цифровой грамотности населения, последовательное

ужесточение ответственности за незаконный оборот персональных данных, совершенствование законодательства о защите информации и – что, возможно, важнее всего – формирование нового этического консенсуса относительно допустимых границ присутствия государства и бизнеса в приватном пространстве личности. Технологический прогресс необратим. Однако, как справедливо замечено, технологии могут стать не угрозой, а ресурсом – при условии, что человек сохранит способность критически осмыслять свои взаимодействия с цифровой средой. Следует также подчеркнуть, что «эпоха цифровых технологий кардинально меняет образовательный ландшафт» [10]. Именно от того, успеет ли общество выстроить этот навык, зависит, сохранятся ли в обозримом будущем сами понятия приватности и психологической автономии личности.

Список литературы

1. Донскова Л.А. Международные ONLINE-конференции как способ оптимизации обучения иностранным языкам / Л.А. Донскова // Язык как зеркало культуры : материалы Всероссийской научно-практической конференции / Министерство сельского хозяйства Российской Федерации; ФГОУ ВО Кубанский государственный аграрный университет имени И.Т. Трубилина. – Краснодар, 2021. – С. 71–75. EDN VWNVRH
2. Роскомнадзор. Ежегодный доклад о состоянии защиты персональных данных. – М. : РКН, 2025.
3. Сбербанк России. Исследование утечек данных в России. – М.: Сбер, 2025.
4. Работа.ру. Мониторинг сотрудников в российских компаниях: результаты опроса. – М., 2025.
5. Ваганова О.И. Проектно-исследовательская деятельность как интегративное дидактическое средство формирования межкультурного диалога / О.И. Ваганова, М.Р. Желтухина, Л.А. Донскова // Современные проблемы науки и образования. – 2022. – №3. – С. 27. DOI 10.17513/spno.31730. EDN VJMCHE

6. Донскова Л.А. Использование социальных сетей в молодежной среде / Л.А. Донскова // Современные векторы развития науки: сборник статей по материалам ежегодной научно-практической конференции преподавателей по итогам НИР за 2023 год. – Краснодар, 2024. – С. 414–416. EDN FBDVAZ
7. Макаренко М.А. Цифровая интимность как форма поведенческой зависимости / М.А. Макаренко // Психологический журнал. – 2025. – Т. 46, №2. – С. 88–97.
8. Логинова М.В. Цифровизация и психическое здоровье: новые риски : доклад на форуме «Территория будущего. Москва 2030». – 2025.
9. World Health Organization. Working with digital determinants of young people's mental health. – Geneva: WHO, 2025.
10. Донскова Л.А. Образование как фактор формирования исследовательской инициативы и научного мышления у молодых специалистов / Л.А. Донскова, Е.П. Донсков // Казанская наука. – 2026. – №1. – С. 168–171. EDN JTJWFJ