ОТВЕТСТВЕННОСТЬ ЦИФРОВОЙ ЛИЧНОСТИ В СЕТИ ИНТЕРНЕТ

Клебанов А.В.,
студент 2 курса юридического факультета
Полоцкого государственного университета
имени Евфросинии Полоцкой

Аннотация. В статье рассматриваются правовые аспекты ответственности пользователей социальных сетей как субъектов цифровых правоотношений. Основное внимание уделено анализу современных подходов к регулированию цифровой идентичности, включая недавние исследования Digital Regulation Cooperation Forum (DRCF) о перспективах развития цифровых идентификаторов. Исследуются механизмы контроля пользовательской активности, борьбы со спамом и применения санкций со стороны платформ, с учетом международного опыта.

Ключевые слова: цифровая личность, социальные сети, ответственность пользователя, цифровая идентичность, DRCF, GDPR, цифровое достоинство.

RESPONSIBILITY OF DIGITAL PERSONALITY IN THE NETWORK INTERNET

Klebanov A.V., 2nd year student of the Law Faculty
Polotsk State University named after Euphrosyne of Polotsk

Abstract. The article examines the legal aspects of responsibility of social network users as subjects of digital legal relations. The main attention is paid to the analysis of modern approaches to the regulation of digital identity, including recent studies of Digital Regulation Cooperation Forum (DRCF) on the prospects of development of digital identifiers. The mechanisms of controlling user activity, fighting spam and applying sanctions on the part of platforms, taking into account international experience, are investigated.

Key words: digital identity, social networks, user responsibility, digital identity, DRCF, GDPR, digital dignity.

Под цифровой личностью понимается совокупность данных, формирующих образ пользователя на основе его онлайн-активности. Как подчеркивается в исследовании DRCF «Exploring the Future of Digital Identity», цифровая идентичность представляет собой «цифровое отражение личности, позволяющее подтверждать свою подлинность при совершении онлайн-взаимодействий и транзакций» [1]. Этот концепт создает новые правовые вызовы для комплексного регулирования защиты персональных данных, свободы самовыражения и ответственности за цифровую активность человека.

Зарубежной практике известны случаи начала правового регулирования ответственности цифровой личности. В частности, в Великобритании разрабатывается «Trust Framework for Digital Identity and Attributes», который устанавливает стандарты для безопасных цифровых идентификаторов, что, в свою очередь, отражает глобальный тренд на усиление регуляторного контроля [2].

На основании данных стандартов, цифровая идентичность пользователя формируется на основе атрибутов – разнообразных данных о личности (имя, дата

рождения, страховой номер и др.). Они могут комбинироваться в рамках централизованных (государственных или корпоративных) или децентрализованных систем, управляемых самими пользователями. Последние, как подчеркивается в исследовании DRCF, вызывают особые дискуссии: хотя они и дают пользователям больше контроля над данными, вопросы ответственности и управления в таких системах остаются трудно поддаваемыми регулированию.

Одним из наиболее значимых нормативных актов, регулирующих поведение пользователей в интернете, является Общий регламент по защите данных (GDPR), принятый в Европейском союзе. Документ устанавливает строгие требования к обработке персональных данных, включая цифровые идентификаторы, которые используются для распознавания личности в интернете. В частности, статья 18 GDPR предоставляет пользователю право на уточнение и ограничение обработки своих данных [3]. Это положение приобретает особую важность в условиях активного использования социальных сетей, где сохраняется риск деанонимизации – раскрытия реальной личности пользователя без его согласия.

В связи с этим, особую роль начинают играть социальные платформы, которые сегодня становятся основной средой цифрового взаимодействия. Именно здесь формируется значительная часть пользовательских цифровых следов, вследствие чего требуется установление юридической ответственности. Важно обеспечить правовое регулирование публикуемого контента, а также внедрение эффективных и прозрачных механизмов контроля за пользовательской активностью. В связи с этим, социальные платформы используют сложную систему модерации контента, направленную на минимизацию возникающих нарушений. Согласно данным DRCF, автоматические фильтры на базе ИИ выявляют до 94% нарушений, однако эффективность данных фильтров зависит от качества алгоритмов и обучения моделей. Санкции к пользователю в случае нарушений могут применяться по трехуровневой системе: предупреждение, теневой бан (ограничение видимости контента) и полная блокировка аккаунта. При этом механизмы обжалования, требуемые ст. 22 GDPR, часто остаются формальностью из-за длительных сроков рассмотрения жалоб [3].

Особую проблему в цифровом пространстве представляет спам-активность, охватывающая не только массовые рекламные рассылки, но и более широкие формы нежелательного взаимодействия – например, автоматическое добавление пользователей в рассылочные списки без их согласия, распространение фальшивых уведомлений или фишинговых сообщений. Все это не только вредит пользовательскому опыту и создает риски мошенничества, но и напрямую затрагивает права личности, включая право на приватность, контроль над своими данными и репутацией в сети. Когда пользователь без ведома или согласия оказывается в списках массовой рассылки, это может привести к утечке его персональных данных, росту цифрового следа и даже включению в черные списки или базы, ассоциирующие его с подозрительной активностью. В результате может пострадать цифровая репутация человека, а также усложниться доступ к определенным онлайн-сервисам, особенно в случаях, когда такие данные используются для оценки его благонадежности (например, при регистрации на платформах или верифика-

ции личности). Это усугубляется наличием такой проблемы как «дата-брокеры» (data-brokers). Данные сайты действуют скрытно от пользователей, собирая, агрегируя, и передавая за определенную цену данные лиц другим платформам [4].

С целью частичного разрешения проблемы в Европейском союзе была принята Директива об электронной коммерции (2000/31/EC), положения которой обязывают онлайн-платформы бороться с нежелательными электронными сообщениями [5]. Однако ввиду аномально быстрого развития технологий, старые меры не всегда успевают за новыми способами обхода фильтров, что требует разработки более строгого законодательства в сфере регулирования онлайн-сервисов. Так, в Великобритании разрабатывается законопроект Digital Information and Smart Data Bill, который направлен на ужесточение требований к цифровым платформам: документ предусматривает обязательную верификацию рекламодателей и усиливает контроль за источниками спама. Ожидается, что данные меры сделают цифровую среду более прозрачной и безопасной как для пользователей, так и для самих сервисов [6].

Учитывая вышеперечисленные проблемы, обусловленные возрастающей сложностью правовых отношений, вопрос ответственности цифровой личности приобретает особую актуальность. Современное право сталкивается с необходимостью переосмысления традиционных категорий, поскольку цифровая личность все чаще становится самостоятельным участником правовых отношений. Как подчеркивает И.В. Шахновская, для полноценного правового регулирования необходимо признание цифровой личности субъектом, способным нести права и обязанности в цифровой среде [7, с. 98]. Одной из ключевых проблем является сложность установления ответственности в условиях анонимности и технической невозможности точной идентификации нарушителей, что затрудняет применение классических институтов, таких как деликтоспособность, и требует разработки новых правовых механизмов, адекватных в условиях цифровой реальности.

В международной практике прослеживаются разные подходы к решению этой проблемы. В ряде стран усиливается внимание к персональной ответственности пользователей за управление своими данными, в том числе вопросы распоряжения цифровой идентичностью после смерти (например, в Китайской Народной Республике). Это расширяет рамки ответственности пользователя не только при жизни, но и в контексте посмертного управления данными. В Российской Федерации, на уровне законодательства, ответственность за защиту персональных данных возлагается на операторов в соответствии с Федеральным законом «О персональных данных» [8]. Однако на практике эффективность регулирования остается низкой: штрафы за утечки данных несоразмерны причиняемому ущербу, что снижает мотивацию к соблюдению норм и не способствует формированию осознанного подхода к ответственности в цифровом пространстве.

Кроме того, международные экспертные структуры, такие как DRCF, акцентируют свое внимание на то, что обеспечение доверия к цифровой идентичности невозможно без четко выстроенной системы ответственности всех участников: пользователей, платформ и регуляторов. Это включает как механизмы верификации (vouching) и защиту от подмены личности, так и обязательства платформ по обеспечению прозрачности алгоритмов и модерации.

Таким образом, формирование правового института ответственности цифровой личности требует комплексного подхода: в первую очередь, признания ее правосубъектности, создания эффективных механизмов идентификации, установления границ ответственности и внедрения санкций, адекватных цифровым рискам. Без этого невозможно обеспечить ни защиту прав пользователей, ни устойчивость цифровой правовой среды в целом.

Список литературы

1. Digital Regulation Cooperation Forum. Exploring the Future of Digital Identity [Электронный ресурс]. – 2024. – Режим доступа: https://www.gov.uk/government/publications/exploring-the-future-of-digital-identity – Дата доступа: 28.03.2025.
2. UK Government. Digital Identity and Attributes Trust Framework [Электронный ресурс]. – Режим доступа: https://www.gov.uk/government/publications/digital-identity-trust-framework – Дата доступа: 28.03.2025.GDPR (Регламент ЕС 2016/679).
3. General Data Protection Regulation (GDPR) – Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016. – Официальный журнал Европейского Союза. – 2016. – L 119. – С. 1–88.
4. Behind the One-Way Mirror: A Deep Dive Into the Data Broker Industry [Электронный ресурс] // Electronic Frontier Foundation. – URL: https://www.eff.org/wp/behind-the-one-way-mirror – Дата доступа: 28.03.2025.
5. Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce). – Official Journal L 178. – 17.07.2000. – P. 1–16.
6. UK Government. Digital Information and Smart Data Bill [Электронный ресурс]. – Режим доступа: https://bills.parliament.uk/bills/3322 – Дата доступа: 28.03.2025.
7. Шахновская, И.В. Концепция цифровой личности как субъекта конституционно-правовых отношений / И.В. Шахновская // Актуальные проблемы достижения целей устойчивого развития в условиях цифровой трансформации государства и права в Республике Беларусь: материалы Республиканской научно-практической конференции, Минск, 18–19 ноября 2022 г. / Белорусский государственный университет, Юридический факультет, кафедра конституционного права ; редкол.: Г. А. Василевич (отв. ред.) [и др.]. – Минск : БГУ, 2022. – С. 98–104.
8. О персональных данных [Электронный ресурс]: Федеральный закон Российской Федерации от 27 июля 2006 г.: в ред. ФЗ от 08.08.2024 N 233-ФЗ. – М. - КонсультантПлюс, 2024.

ГРЯДУЩИМ ПОКОЛЕНИЯМ ЗАВЕЩАЕМ: ТВОРИТЬ ДОБРО В ЗАЩИТУ ПРАВА

Материалы XI Всероссийской научно-практической конференции (с международным участием) студентов, аспирантов и молодых ученых

г. Оренбург, 26–28 марта 2025 г.

DirectMEDIA