

ИНФОРМАТИКА

doi: 10.51639/2713-0576_2026_6_3_28

Научная статья

УДК 004.738.5:316.774

ГРНТИ 81.25.17

ВАК 5.3.7

Этические и технические аспекты персонализации и микротаргетинга в интерфейсах

Екатерина Александровна Лопаткина^{1*}, Башер Али Аль-Нами²
ФГБОУ ВО «Санкт-Петербургский государственный университет
телекоммуникаций им. проф. М. А. Бонч-Бруевича»,
г. Санкт-Петербург, Россия

^{1*} lopatkinaekaterina18@gmail.com, ² alnomibasheer@gmail.com

Аннотация

Современные медиапространства не могут существовать без персонализации и микротаргетинга, однако, вместе с удобствами, эти технологии представляют угрозу приватности пользователей. Современные законодательные системы не успевают подстраиваться под цифровизацию и социальные сети. Информирование пользователей о возможных опасностях и рисках, которые могут представлять системы персонализации контента должна стать одной из ключевых целей кибербезопасности.

Ключевые слова: персонализация, микротаргетинг, приватность, персональные данные, большие данные.

Интернет и социальные сети стали неотъемлемой частью современного мира. Во многом эта популярность обеспечена способностью интернет-ресурсов подстраиваться под личность владельца, адаптироваться под его ритм жизни, характер и предпочтения. Персонализация усилила интеграцию цифровых систем в жизнь современного человека и привела к широкому распространению персонализированных и контекстно-зависимых инструментов.

Одновременно с этим персонализация всё чаще трансформируется в микротаргетинг – практику точечного воздействия на узкие сегменты пользователей, вплоть до индивидуального уровня. В отличие от классической персонализации, ориентированной на улучшение пользовательского опыта, микротаргетинг фокусируется на управлении вниманием и поведением, что особенно заметно в сферах цифровой рекламы, электронной коммерции и политической коммуникации [1]. Такая трансформация усиливает риски манипуляции, непрозрачного использования персональных данных и ограничения пользовательской автономии [2].

Однако вместе с пользой, эти инновации принесли и новые проблемы, и морально-этические и технические дилеммы. Интернет до сих пор остается серой зоной для современных законов и мирового права, а достаточно новые технологии и вовсе неизвестны для большинства пользователей Сети. Это создает большое количество юридических прецедентов, связанных с охраной и безопасностью личных данных и цифровой приватности. Зачастую микротаргетинговые стратегии могут напрямую

нарушать эти права, а большие корпорации используют пользовательские соглашения в качестве лазеек в правовых системах, нарушая права своих пользователей.

В условиях усиливающегося правового регулирования цифровых сервисов и роста общественного внимания к вопросам приватности и алгоритмической ответственности возникает необходимость комплексного анализа как технических, так и этических аспектов персонализации интерфейсов.

В современном медиапространстве персонализация представляет собой многоуровневую экосистему адаптации контента под индивидуальные паттерны поведения и предпочтения пользователей: ленты рекомендаций в социальных сетях, микротаргетинг, рекомендательные системы и геоконтекстная адаптация. Эти системы работают за счет сбора информации пользователей, но зачастую являются непрозрачными и могут передавать персональные данные третьим лицам. Вопрос этичности систем микротаргетинга и персонализации и технические способы решения этих проблем являются основными для многих ведущих цифровых компаний.

Одним из наиболее распространенных видов персонализации является микротаргетинг – это персонализированная подгруппа таргетинга, нацеленная на очень узкие сегменты аудитории, вплоть до отдельных пользователей. Микротаргетинг отличается от персонализации влиянием не на вид интерфейса и UX, а более глубинным воздействием на цифровое пространство в соответствии с поведенческими моделями пользователей (как правило, реклама и настройка рекомендаций) [3].

И микротаргетинг, и персонализация получили столь широкое распространение благодаря появлению больших массивов данных, которые позволили обрабатывать как можно больше данных пользователей и выстраивать на этом целые экосистемы, заточенные под личные взгляды и предпочтения.

Обрабатывать такие массивы данных позволяет искусственный интеллект и машинное обучение: эти технологии кластеризируют данные, разделяя их на группы с заданными критериями, затем, на основе созданных кластеров прогнозируют наибольшую отдачу у определенного сегмента пользователей, после чего применяют персонализированные схемы к пользователю и отслеживают его дальнейшее поведение и реакцию на подобранный контент, собирая еще больше персональных данных.

Основной проблемой всех этих процессов является практически полная непрозрачность на протяжении всего процесса – пользователи едва ли могут отследить перемещение персональных данных, что создает серьезные юридический прецедент и значительный пробел в цифровой безопасности. Этичность этих процессов оказывается куда масштабнее с учетом того, что в современном медиапространстве практически невозможно отказаться от персонализации [3].

Техническая архитектура персонализации состоит из нескольких уровней.

Сбор данных – ключевой аспект персонализации, без которого технология не может существовать. Персонализация предполагает различные виды сбора данных, на некоторые из них пользователь дает свое согласие, другие же осуществляются без его ведома.

Cookies (небольшие текстовые файлы, который веб-сайт сохраняет на устройстве пользователя через браузер, содержащие данные, которые помогают сайту «запомнить» информацию о пользователе или его действиях), web-beacons (невидимые элементы на веб-странице или в email, используемые для скрытого отслеживания пользовательской активности) и device fingerprinting (технология сбора и анализа множества параметров устройства и браузера пользователя для создания его уникального «цифрового слепок»,

который может использоваться для идентификации и отслеживания даже при отключенных cookies и в режиме инкогнито).

Логи взаимодействия и телеметрия UX: инструменты, предназначенные для детального отслеживания механических действий пользователя в реальном времени, которые так же нужны для полного формирования статистики больших данных о пользователях.

Запросы разрешений (геолокация, контакты, доступ к приложениям). Еще один из способов данных, на которые пользователи дают свое согласие, что делает эти функции более прозрачными, однако основные процессы работы и результаты все еще скрыты от глаз. Именно запросы разрешений собирают наиболее персональную информацию, их главная опасность заключается в рисках кражи этих данных и передачи их третьим лицам.

Персонализация не может существовать без этих технологий, но при этом все они грубо нарушают приватность пользователей, GDPR/ССРА и приводят к утечке данных.

Хранилища и профили пользователей. Для грамотной работы персонализации собранные данные должны быть отсортированы и структурированы, чтобы юзеры получали персонализированный контент в соответствии с и предпочтениями и личностью [4].

DMP (Data Management Platform), CDP (Customer Data Platform), CRM: DMP работают в основном с анонимными cookie-данными для рекламного таргетинга. CDP – более современное решение, создающее единый, идентифицируемый профиль клиента на основе данных со всех каналов (онлайн/офлайн). CRM – исторически ядро для известных контактов, теперь часто интегрируется с CDP.

Статические и динамические профили: статические (пол, возраст, город) дополняются динамическими (текущая локация, настроение, жизненный этап), которые обновляются в реальном времени.

Сегментация и кластеризация: на основе профилей пользователи группируются в сегменты (по правилам) или кластеры (алгоритмами ML – machine learning) для точечных коммуникаций.

Основная проблема этих технологий заключается в потенциальной краже персональных данных, поэтому компаниям стоит усилить цифровую безопасность хранилищ данных.

Алгоритмы и модели нужны для превращения всех собранных и отсортированных данных в персонализированный контент.

Рекомендательные системы: collaborative filtering («смотрите то, что смотрели похожие на вас») и content-based filtering («смотрите то, что похоже на просмотренное вами»). Современные гибридные модели комбинируют эти подходы.

ML-модели предсказания поведения: предсказывают вероятность конверсии, оттока, стоимости жизненного цикла (LTV). На основе этих предсказаний распределяются маркетинговые усилия.

A/B/N-тестирование и decision engines: не все решения отдаются на откуп AI. Decision engines (движки принятия решений) управляют тем, какая версия интерфейса, контента или оффера показывается какому сегменту на основе результатов постоянного A/B-тестирования.

Все предыдущие этапы реализуются в интерфейсных компонентах персонализации:

UI-адаптация: динамические баннеры, порядок элементов, персонализированные сценарии onboarding, карточки товаров.

Контекстная персонализация: изменение интерфейса в зависимости от времени суток, типа устройства или местоположения.

Поскольку персонализация не может существовать без персональных пользователей, ее функционирование поднимает ряд важных этических вопросов от утечек данных до нарушения прав потребителей.

Нарушение приватности: персонализация и микротаргетинг собирают данные пользователей, зачастую без их согласия, а пользовательские соглашения фиктивны, поскольку намеренно используют тактики, направленные на введение потребителей в заблуждение. Пользователь редко понимает, на что он соглашается, и какие личные данные могут утечь в сеть [6].

Манипуляция поведением пользователя: персонализация и микротаргетинговые стратегии, которые направлены не на интересы пользователя, а на интересы компании могут манипулировать не только мировосприятием одного человека, но и целых групп, вплоть до политических. Крупные компании и социальные сети проводят неэтичные эксперименты над своими пользователями (в частности Meta^{*1}, которая намеренно влияла на ментальное состояние своих пользователей, манипулируя их лентой рекомендаций) [1, 5].

Социальный разрыв и дискриминация: алгоритмы обучаются на цифровых данных реальных пользователей, что, при недостаточной фильтрации персонализированного контента, может привести к увеличению негативного и провоцирующего конфликта в лентах рекомендаций пользователя, обостряя неустойчивые и конфликтные ситуации в мире и медиа.

Доверие и прозрачность: персонализация строится на схемах, использующих принцип «черного ящика», что может отталкивать и пугать пользователей [1].

Компании должны стремиться к интерфейсам, которые могут кратко и понятно объяснить принцип работы и техническим решениям, защищающим данные пользователей.

Существование такой экосистемы как персонализация и микротаргетинг неизбежно привело к правовым рамкам, ограничивающим полномочия компаний и регулирующим их деятельность по отношению к пользователям. GDPR (ЕС) и CCPA (Калифорния) установили новые стандарты: принцип минимизации используемых данных, явное согласие, право на удаление, прозрачность логики автоматизированных решений. Регуляторы начинают ограничивать особенно манипулятивный таргетинг (например, на детей или в политике). Этические кодексы для UX-дизайнеров и дата-сайентистов становятся необходимостью.

Помочь с разрешением этих этических вопросов может ряд технических и дизайнерских решений.

Объяснимые интерфейсы: пользователи должны понимать, как работают цифровые системы, с которыми они взаимодействуют каждый день – от cookies до пользовательских соглашений, которые должны быть просты и понятны, а опции персонализации иметь краткие пояснения о принципах своей работы.

Контроль персонализации: пользователь должен иметь возможность минимизировать персонализацию и, соответственно, передачу своих данных сервисам без угрозы неполноценной работы сервиса.

Безопасность хранения: личные данные пользователей должны быть защищены и не передаваться третьим лицам.

¹ Организация, действия которой запрещены на территории Российской Федерации.

Отказ от техник, которые собирают информацию даже без согласия пользователей.

Персонализация и микротаргетинг это не только технологии, которые делают жизнь современного человека проще и легче, но огромный риск самому существованию приватности и согласия.

Необходимо найти баланс между работой систем персонализации и правовыми нормами, потому что этические аспекты персонализации и микротаргетинга – это не второстепенный элемент цифрового дизайна, а необходимое условие устойчивого и справедливого развития цифровых технологий.

Только сочетание технологической инновации с гуманистическими принципами способно обеспечить доверие, безопасность и подлинную свободу пользователя в цифровую эпоху.

Конфликт интересов

Авторы статьи заявляют, что на момент передачи статьи в редакционную коллегию у них нет возможного конфликта интересов с третьими лицами.

Список источников:

1. О'Нил К. Убийственные алгоритмы: как Big Data увеличивает неравенство и угрожает демократии. – М.: АСТ, 2018. – 352 с. – ISBN 978-5-17-112595-5. (O'Neil C. Weapons of Math Destruction) // (дата обращения 19.12.2025). – Текст: электронный.
2. Иванов А. В., Петрова С. К. Этические дилеммы алгоритмической персонализации в социальных медиа // Вестник Московского университета. Серия 10: Журналистика. – 2022. – № 3. – С. 45–67. – DOI: 10.30547/vestnik.journ.3.2022.4567. // (дата обращения 19.12.2025). – Текст: электронный.
3. Кузнецов Д. А. Микротаргетинг в политических кампаниях: технологические возможности и угрозы демократии // Политическая наука. – 2021. – № 4. – С. 78–99. – DOI: 10.31249/poln/2021.04.05. // (дата обращения 18.12.2025). – Текст: электронный.
4. Смирнова О. М. Приватность в эпоху Big Data: правовые и этические аспекты сбора пользовательских данных // Информационное право. – 2020. – № 2. – С. 23–30. // (дата обращения 18.12.2025). – Текст: электронный.
5. Федоров Р. Ю. Алгоритмическая дискриминация: природа, формы проявления и пути минимизации // Социологические исследования. – 2023. – № 1. – С. 120–130. – DOI: 10.31857/S013216250022456-2. // (дата обращения 18.12.2025). – Текст: электронный.
6. Яковлева Е. Н. Dark Patterns как манипулятивный инструмент в цифровых интерфейсах // Человек и компьютер: взаимодействие. – 2022. – № 5. – С. 89–102. // (дата обращения 18.12.2025). – Текст: электронный.

Ethical and technical aspects of personalization and microtargeting in interfaces

Ekaterina Alexandrovna Lopatkina ^{1*}, Al-Nami Basher Ali ²

*Federal State Budget-Financed Educational Institution of Higher Education The Bonch-Bruевич Saint Petersburg State University of Telecommunications,
St Petersburg, Russia*

^{1*} lopatkinaekaterina18@gmail.com, ² alnomibasheer@gmail.com

Abstract

Modern media spaces cannot exist without personalization and microtargeting, however, along with convenience, these technologies pose a threat to user privacy. This article is devoted to the study of the ethical and technical aspects of personalization and microtargeting, the principles of personalization and the solution of ethical and legal problems that they create.

Keywords: personalization, microtargeting, privacy, personal data, big data.