

Big Data меняет демократию: манипуляция выбором через микротаргетинг

Аннотация

Современные технологии сбора и анализа данных коренным образом изменили политические кампании, позволив перейти от массовой агитации к персонализированному воздействию на избирателей. В данном эссе исследуется феномен микротаргетинга – технологии, которая использует большие данные (big data) для создания индивидуальных политических сообщений. На примере громких скандалов, таких как деятельность Cambridge Analytica на выборах в США и референдуме по Brexit, анализируются механизмы манипуляции общественным мнением. Особое внимание уделяется последствиям этих технологий для демократических институтов, включая усиление поляризации и снижение доверия к избирательным процессам. В заключении рассматриваются возможные меры противодействия – от законодательного регулирования до повышения цифровой грамотности населения.

Введение

Цифровая революция последних десятилетий кардинально преобразила политический ландшафт. Если раньше предвыборные кампании основывались на широкоэвangelических сообщениях через СМИ и массовые мероприятия, то сегодня ключевым инструментом становится микротаргетинг – технология точечного воздействия на конкретных избирателей через анализ их цифрового следа.

Этот подход, с одной стороны, позволяет более эффективно доносить информацию до граждан, напротив – создает беспрецедентные возможности для манипуляции. Ярким примером стала деятельность компании Cambridge Analytica, которая, как сообщалось, в 2016 году работала с данными пользователей Facebook* и разрабатывала таргетинг для влияния на исход президентских выборов в США (при этом кампания Трампа отрицала использование некоторых наработок [1]) и референдума о выходе Великобритании из ЕС [2].

Цель данного эссе – проанализировать, как технологии больших данных трансформируют демократические процессы, какие риски это создает и какие меры могут помочь сохранить честность и прозрачность выборов в цифровую эпоху.

Механизмы микротаргетинга

Современный микротаргетинг основывается на трех ключевых компонентах: сборе данных, анализе поведения и персонализированном воздействии. Сбор данных осуществляется через множество каналов: активность в социальных сетях (лайки, репосты, время просмотра постов), геолокационные данные смартфонов, история поисковых запросов и онлайн-покупок. Например, Meta Pixel (ранее Facebook Pixel)* – инструмент отслеживания, позволяющий собирать информацию о действиях пользователей не только на самой платформе, но и на тысячах партнерских сайтов [3]. На основе этих данных строится психографический профиль избирателя. Компания Cambridge Analytica использовала модель Big Five OCEAN (Openness, Conscientiousness, Extraversion, Agreeableness, Neuroticism), которая классифицировала людей по пяти личностным чертам,

что позволяло создавать разные сообщения для, например, эмоционально нестабильных и уверенных в себе избирателей [4].

Финальный этап – персонализированная пропаганда. С помощью А/В-тестирования определяются наиболее эффективные формулировки и образы для каждой группы [5]. Так, для одних избирателей делался акцент на иммиграции, для других – на экономике, причем сообщения могут кардинально различаться по тональности и содержанию.

Примеры манипуляций

Практика микротаргетинга уже привела к нескольким громким скандалам. На выборах 2016 года в США Cambridge Analytica использовала данные для подавления явки – сообщалось об использовании категории Deterrence, в которой непропорционально часто оказывались темнокожие избиратели, однако кампания Трампа отрицала использование этих данных.

В Бразилии в 2018 году через WhatsApp* массово распространялись фейковые новости о кандидате Фернанду Аддаде, включая ложные обвинения в коррупции и вирусные слухи, подрывающие его репутацию. Массовые рассылки в некоторых случаях характеризовались различным содержанием, что создавало эффект «индивидуальности» сообщений [6, 7].

В Европе партии активно используют TikTok, где алгоритмы особенно эффективно усиливают контент [8].

Угрозы демократическим процессам

Широкое применение микротаргетинга создает несколько серьезных проблем.

Во-первых, оно усиливает поляризацию общества – разные группы граждан формируют свои «информационные пузыри» с альтернативными фактами. Во-вторых, снижается прозрачность выборов. Если раньше вся агитация была публичной, теперь значительная часть происходит в закрытых чатах и персонализированных лентах. В-третьих, возникает цифровое неравенство – кампании с доступом к большим данным получают преимущество.

Решение и регулирование

Современные вызовы, связанные с использованием больших данных в политике, требуют комплексного подхода к регулированию. Опыт последних лет показывает, что для защиты демократических процессов необходимо действовать одновременно в нескольких направлениях.

Законодательные меры – становятся первым и важнейшим рубежом защиты. Европейский Союз уже продемонстрировал эффективный подход через регламент о защите данных (GDPR), который ограничивает использование персональной информации в политических целях. Особенно важна статья 22, в которой закреплено право человека не подвергаться решению, основанному исключительно на автоматизированной обработке (включая профилирование) и способному повлечь юридические последствия либо иным образом существенно затронуть его, за исключением случаев, когда такое решение необходимо для заключения/исполнения договора, прямо предусмотрено правом ЕС или государства-члена либо основано на явном согласии, при условии наличия гарантий (права на человеческое вмешательство, выражение позиции и оспаривание) [9]. Дополнительным шагом стал Digital Services Act (2022), требующий от платформ раскрывать информацию о политической рекламе [10]. Эти меры создают правовую основу для контроля за микротаргетингом, хотя их реализация требует дальнейшего совершенствования.

Технологическая прозрачность – второй ключевой элемент защиты. Социальные сети должны гарантировать:

- полную публичность политической рекламы (как в библиотеке Meta Ad Library*),
- четкое указание целевой аудитории для каждого сообщения,
- ограничение вирального распространения непроверенного контента в предвыборный период.

Например, X (ранее Twitter) с его системой Community Notes показывает, как краудсорсинг может помочь в проверке фактов. Пользователи самостоятельно отмечают недостоверную информацию, создавая коллективный иммунитет против манипуляций.

Образовательные инициативы составляют третье направление защиты. Опыт Финляндии, где медиаграмотность стала частью школьной программы, доказал свою эффективность [11]. Подобные программы должны учить:

- критическому анализу источников информации,
- распознаванию манипулятивных техник,
- пониманию работы алгоритмов соцсетей.

Международное сотрудничество приобретает особую важность в условиях глобального характера цифровых угроз. Необходимо:

- создание международных стандартов цифровой избирательной прозрачности,
- общие базы данных о дезинформационных кампаниях,
- координация санкций против организаций, занимающихся кибервмешательством.

Реализация этих мер требует времени и политической воли, но альтернативой становится дальнейшая эрозия демократических институтов. Как показывает практика, наиболее эффективен комплексный подход, сочетающий законодательное регулирование, технологические решения и образование граждан. Только так можно сохранить баланс между технологическим прогрессом и защитой основ демократии.

Заключение

Технологии микротаргетинга, основанные на больших данных, создают новые вызовы для демократии. С одной стороны, они делают политическую коммуникацию более эффективной, с другой – открывают возможности для манипуляций в беспрецедентных масштабах.

Для противодействия этим угрозам необходимы комплексные меры: законодательное ограничение использования персональных данных в политике (как это начинает делать ЕС), повышение прозрачности цифровой рекламы и развитие медиаграмотности населения. Как показывает опыт Финляндии, образовательные программы могут значительно повысить устойчивость общества к цифровым манипуляциям.

Будущее демократии в цифровую эпоху будет зависеть от того, удастся ли найти баланс между технологическими возможностями и защитой основополагающих принципов честных выборов. В противном случае сформируется среда, где выигрывают не лучшие программы, а более развитые алгоритмы манипуляции поведением пользователей.

Список использованных источников

1. The Washington Post. Trump's 2016 campaign used Cambridge Analytica to suppress votes, report says / The Washington Post. – 2020. – URL: <https://www.washingtonpost.com/technology/2020/09/28/trump-2016-cambridge-analytica-suppression/> (дата обращения: 14.08.2025)
2. Cadwalladr C., Graham-Harrison E. Revealed: 50 million Facebook* profiles harvested for Cambridge Analytica in major data breach / The Guardian. – 2018. – URL: <https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election> (дата обращения: 14.08.2025)
3. Н. Морозова. Как настроить пиксель в Facebook*, Instagram* и «ВКонтакте» // Статья портала Skillbox Media – Маркетинг. – 2020. – URL: https://skillbox.ru/media/marketing/kak_nastroit_piksel_v_facebook_instagram_i_vkontakte/ (дата обращения 14.08.2025)
4. Alexander Nix (расшифровка презентации). Самый успешный и самый скандальный Data Science проект: Cambridge Analytica // Статья портала Хабр. – 2020. – URL: <https://habr.com/ru/companies/skillfactory/articles/503504/> (дата обращения 14.08.2025)
5. В. Мурашкин. А/В тест – это просто // Статья портала Хабр. – 2014. – URL: <https://habr.com/ru/articles/233911/> (дата обращения 14.08.2025)
6. Fisher M., Taub A. How WhatsApp Is Being Weaponized in Brazil's Election // The New York Times. – 2018. – URL: <https://www.nytimes.com/2018/10/17/opinion/brazil-election-fake-news-whatsapp.html> (дата обращения 14.08.2025)
7. В Бразилии создали комиссию для расследования кампании в WhatsApp* против Амоэду // ТАСС. Международная панорама. – 2018. – URL: <https://tass.ru/mezhdunarodnaya-panorama/5699712> (дата обращения: 28.05.2023).
8. Я. Делькер. TikTok на службе у правопопулистов из АдГ // Deutsche Welle**. – 2024. – URL: <https://www.dw.com/ru/tiktok-na-sluzbe-u-adg-kak-socset-pomogla-uspehu-pravopopulistov-na-vyborah/a-70120389> (дата обращения 14.08.2025)
9. Статья 22 Автоматизированное индивидуальное принятие решений, включая профилирование // Общий регламент по защите данных (GDPR), официальный текст. – URL: <https://gdpr-text.com/ru/read/article-22/> (дата обращения 14.08.2025)
10. Digital Services Act // European Commission. A Europe fit for the digital age. – URL: https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-services-act_en (дата обращения: 14.08.2025)
11. Как Финляндия учит школьников распознавать фейки и манипуляции: Нейромаркетинг в защиту критического мышления // Статья портала Дзен. – 2023. – URL: <https://dzen.ru/a/aB-7TqNY2izAjuJZ> (дата обращения 14.08.2025)

*Организация Meta, а также её продукты Pixel, WhatsApp, Ad Library, Instagram и Facebook, которые упомянуты в настоящем эссе, признаны экстремистскими на территории РФ

**Deutsche Welle – иностранное СМИ, выполняющее функции иностранного агента