НОВЫЕ ТЕХНОЛОГИИ

Обзор будущих тенденций в гражданском пространстве

ПУНАМ ДЖОШИ

Информационный обзор для Инициативы
«Гражданское пространство 2040»
Международного центра некоммерческого права
Опубликовано: март 2020

ICNL
INTERNATIONAL CENTER
FOR NOT-FOR-PROFIT LAW
WWW.ICNL.ORG

ТЕНДЕНЦИИ БУДУЩЕГО: НОВЫЕ ТЕХНОЛОГИИ

В течение следующих двух десятилетий экологические, технологические и демографические тенденции кардинально изменят наш образ жизни. Динамичное гражданское пространство необходимо для обеспечения того, чтобы каждый мог в полной мере участвовать в формировании этого будущего. МЦНП учредил проект "Гражданское пространство 2040" — футуристическую инициативу по разработке концепции позитивного развития гражданского пространства и разработке стратегий реализации этого видения. Данная инициатива исследует тенденции, которые радикально изменят будущее, и рассматривает то, как эти тенденции повлияют на гражданское пространство. Эта публикация является составляющей серии исследований как новых возможностей, так и новых вызовов, проводимых по заказу МЦНП с целью оказания информационной поддержки защитникам гражданского пространства.

Потенциальное воздействие новых цифровых технологий[1] на гражданское общество сейчас широко обсуждается, но для подготовки гражданского общества к цифровому миру можно сделать гораздо больше. Окажут ли цифровые технологии положительное или отрицательное влияние на гражданское пространство и благотворительность, будет зависеть от целого ряда факторов:

- Целесообразность реформирования практики и бизнес-моделей технологических компаний;
- Управление Интернетом и степень, в которой государства используют технологии для достижения своих собственных геополитических и внутренних целей;
- Набирают ли обороты усилия разработчиков технологий по переосмыслению и децентрализации инфраструктуры Интернета, и
- Способность гражданского общества — помимо небольшой группы экспертов по цифровым правам — уделять особое внимание цифровым технологиям во всех аспектах своей работы.

В этом обзоре рассматриваются тенденции в области новых цифровых технологий, которые, скорее всего, окажут влияние на формирование гражданского пространства, а также возможности для защитников ГО смягчить последствия и извлечь выгоду из грядущих перемен.

1 Для целей данной статьи под новыми цифровыми технологиями понимается аппаратное и программное обеспечение, созданное с использованием информационно-коммуникационных технологий и/или Интернета, таких как программы искусственного интеллекта, инструменты распознавания лиц, социальные онлайн-сети, и т.д.

НОРМОТВОРЧЕСТВО И УПРАВЛЕНИЕ ЦИФРОВЫМИ ТЕХНОЛОГИЯМИ И ИНТЕРНЕТОМ

Цифровые технологии привнесли широкий спектр как преимуществ, так и проблем для бизнеса, частных лиц и общества в целом. Интернет коренным образом изменил доступность и получение информации для всех. Это позволило акторам гражданского общества преуспевать и конкурировать на так называемом «рынке идей», но также создало условия и для вмешательства злонамеренных субъектов в выборы, углубления поляризации и разжигания ненависти.

БИЗНЕС-МОДЕЛИ

Угрозы, которые цифровые технологии представляют для гражданского пространства и демократии, коренятся в бизнес-модели наиболее успешных технологических компаний и в управлении экосистемой Интернета на сегодняшний день.

Цифровая экономика основана на накоплении, анализе и продаже огромных объемов данных несколькими платформами, базирующимися в основном в США: Facebook, Amazon, Alphabet (материнская компания Google) и Apple. Эти данные, основанные на привычках просмотров в Интернете, профилях в социальных сетях, онлайн—покупках и результатах поиска пользователей в Google, могут использоваться для отправки целевых сообщений, чтобы влиять на поведение все более конкретизированных групп пользователей социальных сетей в личных целях, для общественного блага или в злонамеренных целях.

Следующее поколение цифровых технологий позволит компаниям извлекать данные не только из онлайн-пространств, но и из искусственно созданной среды. Интернет вещей[2] позволит компаниям собирать персональные данные с камер, умных часов, фитнес-трекеров, игрушек и автоматизированных путешествий. Технологии распознавания лиц и датчики в умных городах[3] также позволят собирать данные от пользователей в общественных местах.

Хотя эти данные могут быть использованы для улучшения физической формы, здравоохранения, транспорта или энергоэффективности, без должного регули-

2 В самом широком смысле термин Интернет вещей (IoT) охватывает все, что подключено к Интернету, но он также все чаще используется для определения устройств, которые «разговаривают» друг с другом, от простых датчиков до смартфонов и носимых устройств. Объединяя эти подключенные устройства, можно собирать информацию, анализировать ее и предпринимать действия, которые призваны оптимизировать жизнь пользователя.

3 Умный город - это городская территория, которая использует различные типы электронных датчиков Интернета вещей для сбора данных, а затем использует информацию, полученную на основе этих данных, для эффективного управления объектами, ресурсами и услугами. Это включает данные, собранные от граждан, устройств и различных объектов, которые обрабатываются и анализируются для мониторинга и управления дорожным движением и транспортными системами, электростанциями, коммунальными службами, сетями водоснабжения, вывозом отходов, выявлением преступлений, информационными системами, школами, библиотеками, больницами и другими общественными службами.

рования или надзора они в равной степени могут способствовать беспрецедентному манипулированию или слежке со стороны злонамеренных государств, компаний или иных негосударственных субъектов.

РЕГУЛИРОВАНИЕ ИНТЕРНЕТА

Будут ли современные или новые технологии использоваться для общественного блага или таким образом, чтобы угрожать гражданскому пространству, будет определяться тем, кто управляет Интернетом. Созданное и управляемое частным сектором, техническое управление Интернетом с самого начала было глобальным и основанным на консенсусе, а не государственным или регулируемым законодательством.

В отсутствие всеобъемлющей правовой или нормативной базы, управление Интернетом в значительной степени оставалось в руках американских технологических платформ. Сопротивляющиеся регуляторным механизмам, эти платформы в значительной степени оказались неспособными взять на себя ответственность за социальные и политические последствия своих систем и операций или предложить что-либо помимо мер, направленных на частичное исправление ситуации.[4]

Стремясь доминировать в секторе искусственного интеллекта[5] (ИИ), эволюция технологий, которые, вероятно, изменят гражданское пространство, будет отдана на откуп технологическим гигантам, если только правительства не предпримут шаги по регулированию данного сектора или реформированию базовой бизнес-модели в партнерстве с гражданским обществом.

Однако эффективное регулирование интернета, ИИ и будущих цифровых технологий будет возможно только

> **Послужат ли новые технологии общественному благу или поставят под угрозу общественное пространство, будет определяться тем, кто установит контроль над Интернетом.**

4 Действия по улучшению, предпринятые технологическими платформами, задокументированы в Governance Innovation for a Connected World («Инновациях в области управления для взаимосвязанного мира») под редакцией Эйлин Донохо и Фен Ослер Хэмпсон, Центр инноваций в области международного управления, 2018 год.

5 Искусственный интеллект (ИИ) относится к совокупности технологий, которые включают машинное обучение, восприятие, мышление и обработку естественного языка. См.: The Social and Economic Implications of Artificial Intelligence: Technologies in the Near-Term, AI Now, July 7, 2016.

при сотрудничестве множества государственных ведомств и компаний частного сектора, что представляется нелегкой для достижения задачей, учитывая различия в ценностях и повестках дня западных демократий и авторитарных государств по данному вопросу.

Битва за то, кто управляет Интернетом, отражает более широкую геополитическую борьбу за ценности и влияние между авторитарными государствами и западными демократиями. Китай, Россия и Иран, в частности, выражают озабоченность по поводу децентрализованного регулирования Интернета, отчасти в качестве реакции на то, что ведущими силами Интернета являются США и другие западные демократии. Децентрализованный Интернет противоречит стремлению указанных стран централизованно управлять информацией и коммуникациями. Одной из стран, где технологические платформы США обладают очень малой властью и влиянием, является Китай, который защитил свой внутренний интернет—рынок от иностранных конкурентов и создал собственный набор социальных сетей, включая Twitter-подобные Sina Weibo и WeChat / Weixin, которые напоминают WhatsApp. Цензура изначально встроена в эти платформы, поскольку операторы платформ должны отслеживать онлайн-контент и удалять оскорбительные сообщения, иначе они рискуют потерять свои лицензии на эксплуатацию.

На международной арене Китай активно выступает за кибер-суверенитет[6] и экспортирует свою модель обширной цензуры и автоматизированных систем отслеживания в значительную группу стран.

Freedom on the Net («Свобода в сети») сообщила, что в прошлом году Китай принимал представителей СМИ из 36 государств на семинарах по своей системе цензуры и надзора, при этом среди представленных стран были и такие, где в значительной степени подавляются гражданские свободы (Египет, Ливия, Саудовская Аравия и Филиппины).

Западные демократии, хотя и якобы привержены гражданским свободам, также испытывают проблемы с выработкой последовательной нормативной политики в области управления и

регулирования. Озабоченность по поводу неприкосновенности частной жизни, вмешательства в выборы и распространения насильственного, экстремистского и вредного контента в Интернете привели к тому, что несколько стран, включая Великобританию, Францию и Германию, предложили законы, разрешающие цензуру и удаление контента способами, которые непреднамеренно ограничивают

6 Кибер-суверенитет - это утверждение права каждого государства контролировать Интернет в пределах своих границ. Государства оправдывают эту концепцию, утверждая, что им должно быть разрешено осуществлять контроль над информационными и коммуникационными технологиями и расширять свои возможности для наблюдения, чтобы гарантировать мирное, безопасное, релевантное или соответствующее информационное пространство.

свободу самовыражения. Например, в апреле 2019 года британское правительство предложило широкие новые полномочия по удалению “вредного” контента из Интернета, что легко может быть использовано в качестве предлога для цензуры.

В то же время США, Израиль и несколько европейских стран имеют опыт экспорта технологий наблюдения правительствам с плохими показателями соблюдения прав человека, что ослабляет их возможность бросить вызов действиям Китая. В июне 2018 года ряд государств — членов Европейского союза, включая Великобританию, Польшу, Швецию и Ирландию, попытались заблокировать ограничения на экспорт оборудования для наблюдения в страны, нарушающие права человека.

Напротив, Европейский союз был в авангарде защиты конфиденциальности благодаря введению законов о защите данных в 2018 году, бросив вызов монополии американских технологических гигантов.[7] ЕС также стремится установить глобальные стандарты в отношении этических и правовых рамок ИИ, особенно там, где он используется государственными органами – в здравоохранении, полиции и на транспорте.

ВОЗМОЖНОСТИ ДЛЯ ДЕЙСТВИЙ

РЕГУЛЯТОРНЫЕ ИННОВАЦИИ

Гражданское общество играет решающую роль в информировании правительства об усилиях по разработке законодательства и норм в области использования ИИ как в государственном, так и в частном секторе. Однако сфера нормотворчества в области Интернета относительно молода, и многое еще предстоит сделать для укрепления потенциала более широкого круга акторов

гражданского общества по защите гражданских свобод в цифровой среде посредством нормотворчества и адвокации.

7 Европейский союз предпринял некоторые действия, в том числе оспорил в судебном порядке монополию Google и потребовал, чтобы корпорация Apple выплатила правительству Ирландии 13 миллиардов евро в качестве неуплаченных налогов.

Адвокация новых средств правовой защиты

СОВЕРШЕНСТВОВАНИЕ ЗАЩИТЫ ДАННЫХ

Всеобъемлющие законы о защите данных, которые должны применяться как к правительству, так и к частному сектору, могли бы устранить многие риски для прав человека, связанные с ИИ. Одной из моделей является Общее положение о защите данных Европейского союза (GDPR), одна из самых сильных и всеобъемлющих попыток регулировать сбор и использование персональных данных как правительствами, так и частным сектором. GDPR устанавливает ограничения на обработку данных в зависимости от допустимости целей, обеспечивая защиту конфиденциальности данных. Дополнительно есть требование о согласии на регистрацию, что ограничивает использование персональных данных для обучения систем ИИ. Права, предусмотренные GDPR и аналогичными законами, обеспечивают основу для предотвращения неподотчетного использования ИИ, влияющего на права индивидуума, обеспечивая при этом определенный уровень контроля над персональными данными и подотчетности за использование ИИ и систем машинного обучения.*

БОРЬБА С ДЕЗИНФОРМАЦИЕЙ

Эксперты по цифровым правам призывают принять законы, которые предписывали бы, чтобы все автоматизированные учетные записи были четко помечены, чтобы указать источник рекламы, ее финансирование и сферу ее охвата. Это может помешать целенаправленной цифровой политической

рекламе и расширению бот-сетей.**

* См.: Human Rights in the Age of Artificial Intelligence Access Now, ноябрь 2018, стр. 30-31 GDPR был принят Европейским союзом в 2016 году и вступил в силу 25 мая 2018 года в 28 государствах-членах ЕС.

** См.: https://luminategroup.com/storage/275/Digital-Democracy-Charter.pdf

Группы гражданского общества выиграют от обучения и инструментов, которые позволят им защищать гражданское пространство на национальном уровне в отношении технологических инициатив правительства, таких, как национальные стратегии в области ИИ или законы о надзоре, а также на десятках форумов с участием многих заинтересованных сторон, где обсуждаются глобальные правила и нормы.[8] Примером может служить недавнее сотрудничество между МЦНП и Глобальным инкубатором цифровой политики Стэнфорда по проведению первого технического лагеря для защитников гражданского пространства. Особая поддержка необходима для обеспечения участия в форумах заинтересованных сторон представителей гражданского общества из стран с репрессивными правительствами, особенно из Китая и России.

Вопросы конфиденциальности, защиты данных и борьбы с дезинформацией могут быть решены гражданским обществом посредством требований о принятии новых правовых рамок.

УЧАСТИЕ ГРАЖДАНСКОГО ОБЩЕСТВА В РАЗРАБОТКЕ ТЕХНОЛОГИЙ

Эксперты по правам человека также призвали к гораздо большему гражданскому участию в разработке ИИ, чтобы гарантировать то, что механизмы соблюдения прав человека будут заложены изначально - от разработки и до внедрения.

> ### ПРАВА ЧЕЛОВЕКА ПРИ РАЗРАБОТКЕ ИИ
>
> Специальный докладчик ООН по поощрению и защите права на свободу мнений и их свободное выражение Дэвид Кей и Access Now рекомендуют консультироваться с гражданским обществом во время оценки воздействия на права человека, которая будет проводиться на протяжении всего жизненного цикла ИИ, от концепции до внедрения.[9] В число тех, с кем проводятся консультации, должны входить правозащитники и представители маргинализированных или недостаточно представленных конечных пользователей. Результаты оценок воздействия на права человека и консультаций с общественностью должны быть обнародованы.

8 Регуляторные механизмы обсуждаются в многосторонних органах, таких, как Международный союз электросвязи, в инженерных группах, таких как Инженерная рабочая группа Интернета, в системе ООН по правам человека, в нормативных органы, таких как Форум по управлению Интернетом или ОЭСР, в организации по доменным именам, напр., в Корпорация по управлению доменными именами и IP-адресами (ICANN) или в региональных реестрах.

9 См.: https://undocs.org/A/73/348 29 августа 2018, стр. 20-21; Human Rights in the Age of Artificial Intelligence, (Права человека в век ИИ) Access Now, ноябрь 2018, стр. 32.

АЛЬТЕРНАТИВНЫЕ ТЕХНОЛОГИЧЕСКИЕ И БИЗНЕС-МОДЕЛИ

Наконец, растет движение активистов за цифровые права, которые утверждают, что единственный способ устранить вредные последствия цифровых технологий и использовать их возможности для общественного блага - это передать властные полномочия относительно данных от централизованных платформ их пользователям. Хотя все большее внимание уделяется концепции технологии, служащей общественным интересам, предлагаемые подходы неоднозначны.

ДАННЫЕ, ЦИФРОВАЯ ИНФРАСТРУКТУРА И УСЛУГИ ВО БЛАГО ОБЩЕСТВА

Тим Бернерс-Ли, изобретатель Всемирной паутины, экспериментирует с новой архитектурой под названием Solid, в которой пользовательские данные остаются под контролем пользователя и передаются приложениям, когда это необходимо, то есть, не принадлежат этим платформам.

Британский аналитический центр, Институт исследований государственной политики (IPPR), является одним из многих аналитических центров, призывающих к реформам, которые организуют данные и цифровую инфраструктуру в качестве общественного блага. IPPR рекомендует перейти от условий “монопольного загона данных” к “цифровому содружеству”, где огромный потенциал социально генерируемых данных помогает развивать благосостояние, креативность и потенциал всего общества. IPPR предлагает несколько мер, в том числе: (1) усиление законодательства о конкуренции; (2) регулирование платформ-гигантов в качестве провайдеров коммунальных услуг; и (3) создание цифровой государственной службы, которая управляет хранением и продуктивным использованием общедоступных данных и контролирует создание национального портала данных.

В The Case for Digital Public Infrastructure («Доводы за цифровую общественную инфраструктуру») ученый в области цифровых медиа и активист защиты цифровых прав Итан Цукерман приводит аргументы в пользу решения проблем, возникающих в связи с существующими платформами и их бизнес-моделью, посредством технологических инноваций, а не регулирования. Он призывает правительства и благотворительные организации финансировать углубленные исследования влияния социальных сетей на здоровье людей и на гражданское здоровье в более широком смысле, которые затем могли бы быть использованы для поддержки непосредственно экспериментирования или принятия норм. Например, если исследование продемонстрирует, что радикализация проистекает из взаимодействия в комментариях к видео, эксперименты по модерации дебатов вокруг данного видео могут быть более эффективными, чем регулирование.

УГРОЗЫ ГРАЖДАНСКОМУ ПРОСТРАНСТВУ В ИНТЕРНЕТЕ

ДАВЛЕНИЕ НА СВОБОДУ СЛОВА, СОБРАНИЙ И ОБЪЕДИНЕНИЯ

В этом разделе более подробно рассматривается воздействие цифровых технологий на гражданское пространство, а также реагирование на него гражданского общества и ИТР.

В отчете 2018 года «Злонамеренное использование ИИ» предсказывается, что ИИ будет занимать видное место в сфере безопасности будущего, и что в срочном порядке можно и нужно сделать больше для предотвращения его использования злоумышленниками. Некоторые комментаторы[10] утверждают, что директивным органам еще предстоит серьезно разобраться с репрессивными последствиями ИИ и его влиянием на формирование мнений и собрания в контексте растущего авторитаризма и отступления от демократических принципов.

УСИЛЕНИЕ ЦЕНЗУРЫ

Отмечается рост требований государств к компаниям по борьбе с террористическим контентом, разжиганием ненависти и фейковыми новостями, но не существует четких определений того, что охватывают эти проблемы; также отсутствуют стандарты их решения. Фильтрация ненавистнических высказываний может вызвать массовую негативную реакцию в авторитарных условиях, когда правительства направляют или участвуют в разжигании ненависти по отношению к определенным группам.

Модерация контента может также использоваться для цензуры в отношении маргинализированных групп и умиротворения нелиберальных или авторитарных правительств. Контент, предназначенный для того, чтобы быть противоречивым, гиперболическим, сатирическим или ироничным, также может подвергаться ненадлежащей цензуре со стороны людей или автоматизированного мониторинга, заточенных на отслеживание оскорбительного контента.

10 Стивен Фельдстин сообщает, что начиная с 1989 года всенародные акты неповиновения и поражения на выборах стали наиболее распространенными причинами ухода диктаторов; в период 1946-1988 гг. таковыми были перевороты. Он утверждает, что, поскольку самые серьезные угрозы выживанию авторитарных режимов исходят от недовольного населения на улицах или на избирательных участках, автократы используют цифровую тактику для мониторинга, слежки и преследования движений гражданского общества, а также для искажения выборов в качестве стратегий перемен, что являются экономически эффективным и несет меньший политический риск. Он также отмечает, что у демократических правительств может быть стимул использовать ИИ для мониторинга деятельности политических оппонентов и гражданского общества и принятия упреждающих мер против потенциальных угроз своему нахождению у власти. Наконец, правительства, которые зависят от китайских технологий для контроля над своим населением, будут испытывать растущее давление с целью согласования своей политики со стратегическими интересами Китая. См: Feldstein, Steven. The Road to Digital Unfreedom: How Artificial Repression is Reshaping Repression, Journal of Democracy, January 2019.

БЕСПРЕЦЕДЕНТНЫЙ ГОСУДАРСТВЕННЫЙ НАДЗОР

Системы машинного обучения уже могут выводить или прогнозировать содержание высококонфиденциальной информации из неконфиденциальных данных. Заглядывая в будущее, власти могли бы собирать данные, которые мы продуцируем онлайн с помощью наших телефонов и других устройств, а также использовать технологии распознавания лиц в общественных местах для мониторинга, идентификации или определения местоположения определенных лиц или групп. Это можно было бы использовать для позитивных целей — улучшения общественного транспорта, — но также и для целенаправленной и массовой слежки. По данным Access Now, 50% взрослых в США уже находятся в базах данных распознавания лиц правоохранительных органов, а Китай может стать первой страной, разработавшей полностью централизованную систему распознавания лиц.[11].

ОГРАНИЧИТЕЛЬНОЕ ВОЗДЕЙСТВИЕ ИИ НА ПРОТЕСТЫ

Цензура с поддержкой искусственного интеллекта может использоваться для удаления контента, который способствует организации собраний и сотрудничества. Благодаря данным спутниковых снимков, включая тепловые карты[12], камеры с функцией распознавания лиц и местоположение мобильного телефона, ИИ также может использоваться для предоставления подробной информации для прогнозирования и срыва собраний. Технология распознавания лиц в общественных местах также может оказать сдерживающее воздействие на собрания, поскольку многие люди полагаются на анонимность, обеспечиваемую массовыми протестами, чтобы собираться публично и выражать свои взгляды.

Проблема «упреждающей» полицейской деятельности, равно как и практика вынесения приговоров в сочетании с расовыми предубеждениями в системе уголовного

> **Поскольку многие люди полагаются на анонимность, обеспечиваемую массовыми протестами, технология распознавания лиц в общественных местах может оказать сдерживающее воздействие на осуществление свободы собраний**

11 См.: Human Rights in the Age of Artificial Intelligence, Access Now, November 2018, p 21

12 Тепловое картирование включает в себя обнаружение и усиление сигналов, посылаемых с мобильных устройств, для создания “тепловой карты”, которая указывает, где собираются протестующие.

правосудия, хорошо задокументирована. Данная проблема, скорее всего, проявится снова в отношении меньшинств и маргинализированных групп, заподозренных в инакомыслии и протестах. Наблюдение за движением Black Lives Matter и недавнее использование технологии распознавания лиц против протестующих в Индии, выступивших против антимусульманского законодательства, наглядно проиллюстрировали наслоение упомянутых факторов.

УВЕЛИЧЕНИЕ ОБЪЕМА ДЕЗИНФОРМАЦИИ

Мы живем в эпоху информационных войн, когда репрессивные государства осознают, что манипулирование с помощью цифровых платформ может быть гораздо более мощным инструментом для достижения своих целей, чем подавление или слежка. Все большее число государств решают свои задачи, используя различные инструменты для распространения дезинформации, включая ботов на базе ИИ[13], дипфейки,[14] и манипулирование алгоритмами социальных сетей для вмешательства в выборы[15] и подрыва общественного доверия к информации, базирующейся на фактах.

Если платформы не будут успешно пресекать эти методы распространения дезинформации, доверие общественности к легитимности выборов, а также к традиционным СМИ и гражданскому обществу может еще больше снизиться. Девальвация понятий истины и факта создает серьезные проблемы для гражданского общества, поскольку его способность адвокации социальных перемен зависит от легитимности приводимой аргументации. Забегая вперед, отметим, что существуют опасения, что дипфейки могут быть использованы для разжигания дискриминации, насилия и конфликтов, равно как и для дискредитации активистов и лидеров, особенно женщин, путем создания компрометирующих изображений.

ПЛАТФОРМЫ, КУРИРУЮЩИЕ ДОСТУП К ИНФОРМАЦИИ[16]

Технологические платформы будут продолжать играть роль контролеров допуска к информации о гражданском обществе посредством кураторства, ранжирования информации на основе интересов пользователей и наборов данных, а также модерации контента. Практически не изучалось, как кураторство влияет на свободу

13 Чат-бот - это устройство, которое общается с людьми с помощью текста или аудио. Чат-бот на базе ИИ - это более совершенная версия, которая использует обработку естественного языка (NLP) и машинное обучение (ML), чтобы лучше понимать намерения человека и обеспечивать более естественное общение на уровне, близком к человеческому.

14 Дипфейки - это фото или видео, которые изменяются с помощью нейронных сетей и машинного обучения, что делает их реалистичными и затрудняет обнаружение подделки.

15 Стратегии включают использование крупномасштабных атак по генерированию информации, управляемых ботами, для засорения информационных каналов ложной или просто отвлекающей информацией, что затрудняет получение реальных данных.

16 Machine made goods: Charities, Philanthropy & Artificial Intelligence Доклад Фонда помощи благотворительным организациям от 2018 г. предоставляет всесторонний обзор практических и этических последствий использования новых технологий для филантропии.

объединения, в том числе на то, как системы определяют, каким группам и проблемам гражданского общества уделяется особое внимание в Интернете. Растущее использование нетрадиционных интерфейсов, таких как Алекса - цифровой помощник на Амазоне - может усилить этот эффект, поскольку интерфейсы предоставляют пользователям информацию о проблемах и организациях на основе существующих предпочтений. В результате, может быть затруднено общение ОГО с потенциальными сторонниками.

ВОЗМОЖНОСТИ ДЛЯ ДЕЙСТВИЙ

ПРОТИВОДЕЙСТВИЕ СЛЕЖКЕ

До недавнего времени деятельность в области противодействия слежке ограничивалась расследованием и разоблачением европейских, американских и израильских технологических компаний, поставлявших шпионские программы репрессивным режимам.

Привлечение компаний к ответственности представлялось затруднительным до октября прошлого года, когда WhatsApp подал беспрецедентный иск против израильской фирмы по производству кибероружия - группы NSO - обвинив ее в том, что она стоит за секретными атаками на более чем 100 правозащитников, юристов, журналистов и ученых, совершенных в течение двух недель в прошлом году. Судебный иск, организованный при поддержке Citizen Lab, знаменует собой важный позитивный шаг вперед в области защиты прав человека в Интернете и может создать необходимый юридический прецедент.

Забегая вперед, отметим, что проблема слежки и защиты частной жизни в общественном и частном пространстве требует гораздо большего внимания со стороны гражданского общества. Примеры нового мышления по этому вопросу включают программу Фонда цифровой свободы по защите цифровых прав в будущем, в которой исследуется, как защитить данные, собранные детскими игрушками и устройствами, и как не допустить, чтобы государства брали на себя хакерские функции для взлома подключенных бытовых устройств. Что касается

Стратегии противодействия надзору на местном уровне

MediaJustice в Окленде разоблачает применение слежки в отношении цветного населения и движения Black Lives Matter, чья кампания «Защити наше движение» направлена на защиту активистов, борющихся за расовую и экономическую справедливость в цифровую эпоху. Предлагаемая поддержка включает в себя веб-центр обмена информацией, предлагающий активистам самую актуальную и полезную информацию о защите устройств и данных.

Crypto-Harlem проводит бесплатные публичные семинары по вопросам конфиденциальности, защиты от слежки и цифровой безопасности для жителей Нью-Йорка.

практической безопасности, международные организации, включая Frontline Defenders и The Engine Room, предлагают обучение по цифровой безопасности для правозащитных организаций, но в обеспечении защиты сообществ или движений от цифрового наблюдения сохраняются огромные пробелы. Новаторская работа в США с активистами борьбы за расовую справедливость расширяет наше представление о том, что возможно.

ВОССТАНОВЛЕНИЕ ДОВЕРИЯ К СМИ И ФАКТАМ

Роль цифровых технологий в подрыве доверия к СМИ и демократии привлекла значительное внимание со стороны государств, медийных организаций и гражданского общества, хотя проблема продолжает опережать масштабы ответных мер.

Были вложены средства в инициативы по повышению медиаграмотности, в частности в веб-сайты и инструменты для проверки фактов, такие как PolitiFact.com, FullFact.org, и BBC Reality check. Несмотря на свою полезность, эффективность данных инициатив вызывает сомнение, поскольку они действуют на уровне доказанных фактов, а не эмоций или настроений, разжигание которых является козырной картой пропаганды.

Повышение прозрачности СМИ в отношении того, как они собирают, сообщают и распространяют новости, раскрытие информации о том, кто платит за рекламу, регулирование политической рекламы и инвестиции в независимые СМИ и журналистские расследования могут быть более эффективными способами укрепления или восстановления доверия к СМИ и демократии.

СОЗДАНИЕ ПУБЛИЧНОГО ДИСКУРСА О ВЛИЯНИИ НОВЫХ ТЕХНОЛОГИЙ:

Группам по защите гражданских свобод и цифровых прав традиционно плохо удавалось заручиться поддержкой общественности в вопросах конфиденциальности и данных – то ли из-за недостаточной заинтересованности, то ли в силу сложности связанных с этим вопросов. Тем не менее, озабоченность общественности по поводу вмешательства в выборы и, в последнее время, использование технологий

Использование ИИ для оказания помощи протестующим в режиме реального времени

ОВД-Инфо - независимый российский правозащитный проект, который собирает информацию об арестах во время публичных протестов и других формах политических репрессий. В 2017 году ОВД-Инфо создал специальный Telegram-бот, который позволяет пользователям добровольно сообщать о своих арестах и любом другом взаимодействии с правоохранительными органами и получать немедленные консультации по своим юридическим правам. Более 8000 человек зарегистрировались для получения информации через этот бот. Когда в 9 сентября 2018 г. россияне вышли на улицы в знак протеста против предложенных пенсионных реформ, 1200 человек были арестованы в 38 городах, и 184 из них сообщили о своем аресте в ОВД-Инфо.

распознавания лиц предоставляют беспрецедентную возможность привлечь внимание к проблеме злоупотреблений с использованием ИИ.

The Great Hack («Великий взлом») - документальный фильм сети Netflix 2019 г., в котором основное внимание уделяется манипулированию данными избирателей и вмешательству в президентские выборы в США в 2016 году, а также успех книги американской ученой Шошаны Зубофф The Age of Surveillance Capitalism[17] («Эпоха капитализма слежки»), демонстрирует, что можно привлечь общественный интерес к таким сложным вопросам, как искусственный интеллект, слежка и цифровая экономика.

ПОЗИТИВНЫЕ ТЕНДЕНЦИИ И ИНИЦИАТИВЫ

В течение следующих двух десятилетий всем акторам ОГО необходимо будет научиться эффективно функционировать в цифровом мире. В своем прогнозе по цифровому гражданскому обществу на 2020 год Люси Бернхольц отмечает, что "Эффективными организациями будут те, которые управляют и руководят всеми своими ресурсами — временем, деньгами, персоналом, данными и цифровыми системами — для достижения цели". Цифровые технологии предоставляют возможность акторам ОГО трансформировать свое влияние, повышать прозрачность и доверие, улучшать коммуникации и находить новые источники финансирования.

Поскольку сообщество конструкторов и предпринимателей, думающих о цифровых инструментах, отвечающих гражданским потребностям, остается относительно небольшим, у нас еще нет полного представления о том, что ИИ и цифровые технологии могут сделать для улучшения гражданского пространства. Однако появляются новые идеи и инструменты, которые могли бы повысить эффективность и охват гражданского общества и принести пользу обществу в более широком плане.

ИННОВАЦИИ ДЛЯ ПРОДВИЖЕНИЯ ЦЕЛЕЙ И ЗАДАЧ

ИИ может быть использован благотворительными организациями и ОГО для помощи в продвижении своих целей и задач. Проводимая работа в основном подразделяется на три категории:

1. Улучшение доступа к информации и услугам для пользователей, сталкивающихся с трудностями доступа из–за инвалидности, нарушения зрения или языкового барьера - например, специальные чат-боты, которые предоставляют консультации или услуги;

17 Zuboff, Shoshana. The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power. New York: Public Affairs, 2019

2. Анализ данных с беспрецедентной скоростью и масштабом для ускорения прорывов в области лечения и исследований, а также прогнозирования экстремальных погодных явлений для содействия адаптации к климату, и

3. Использование новых приложений и машинного обучения для защиты гражданских свобод и прав человека – от платформ для улучшения доступа к юридическим консультациям для протестующих и до использования журналистскими расследованиями машинного обучение для сбора больших массивов финансовых данных в целях выявления доказательств отмывания денег и коррупции.

Чтобы воспользоваться этими возможностями, гражданскому обществу необходимо будет решить вопросы о том, кому принадлежат данные, к которым у них есть доступ, получить согласие на использование данных, а также предпринять шаги по улучшению качества и объема данных.

ДЕЦЕНТРАЛИЗАЦИЯ ЦИФРОВОЙ ИНФРАСТРУКТУРЫ

Из множества новых технологий, рассмотренных при подготовке этой статьи, больше всего хайпа и горячих споров вызывает блокчейн[18]. Децентрализованные и неизменяемые характеристики блокчейн означают, что его можно использовать для предотвращения мошенничества и коррупции в различных условиях, включая трансграничные финансовые транзакции, обмен данными и голосование.

Что касается филантропии, блокчейн обеспечивает максимальную степень прозрачности, позволяя отслеживать активы по цепочке транзакций. Хотя идея использования блокчейна для трансграничных пожертвования уже

Из множества новых технологий, рассмотренных при подготовке этой статьи, больше всего хайпа и горячих споров вызывает блокчейн

18 Блокчейн - это распределенный публичный реестр: способ ведения учета транзакций и владения в системе без необходимости в традиционной доверенной третьей стороне

тестируются[19], пока что нет ясности в отношении регулирования блокчейн или криптовалюты для этого вида пожертвований. Существует также серьезная проблема "последней мили": от криптовалюты мало пользы, если вы не можете потратить ее на товары и услуги или конвертировать в традиционную валюту[20].

ТЕХНОЛОГИЯ РЕГИСТРАЦИИ

Благотворительный фонд CAF выделил несколько способов использования ИИ для улучшения регистрации, надзора и соблюдения требований некоммерческими организациями[21]. К ним относятся: использование ИИ для сканирования большого объема финансовых данных для выявления проблем с соблюдением требований на раннем этапе, что позволяет не доводить до использование принудительного правоприменения в качестве инструмента; внедрение законов и нормативных актов в смарт-контракты, регулирующие работу организаций таким образом, чтобы затруднить их нарушение, тем самым сводя к минимуму необходимость принудительного обеспечения соблюдения; запись транзакций в блокчейне, чтобы точная информация о расходах в режиме реального времени была доступна всем, тем самым упраздняя необходимость в ежегодной отчетности.

ПОДДЕРЖКА ИДЕИ ГИБКИХ АССОЦИАЦИЙ

Активистка борьбы за демократию Пиа Манчини из Democracy OS экспериментирует с концепцией открытых платформ, которые выступают в качестве финансовых спонсоров для тех, кто хочет самоорганизовываться более гибко, чем это обычно разрешается действующими законами, регулирующими НКО. Платформы будут работать на основе модели доверия между людьми и организациями и действовать как механизм обеспечения прозрачности и подотчетности.

ТЕХНОЛОГИИ ПОДДЕРЖКИ ДВИЖЕНИЙ

Неформальным объединениям и группам, являющимися частью движений, требуется надежное, разнообразное, ориентированное на ценности программное обеспечение, которое обеспечивало бы их безопасность и могло бы успешно использоваться в зонах повышенной опасности. Aspiration Tech является лидером в производстве инструментов, поддерживающих создание движений, включая программное обеспечение с открытым исходным кодом, поддерживающее безопасную связь и совместную работу. В отчете Фонда Форда за 2017 год излагается

19 Крупные международные НПО и агентства по оказанию помощи, такие как ЮНИСЕФ, экспериментируют с использованием блокчейн для своих внутренних денежных потоков. Тем временем стартапы, такие как Disberse, пытаются создать платформы, которые могут использовать технологию блокчейн для повышения эффективности, прозрачности и рентабельности трансграничных платежей.

20 См.: https://www.cafonline.org/about-us/caf-campaigns/campaigning-for-a-giving-world/future-good/blockchain

21 См.: https://www.cafonline.org/about-us/publications/2016-publications/block-and-tackle-using-blockchain-technology-to-create-and-regulate-civil-society-organisations

долгосрочная стратегия оказания помощи в разработке технологий, поддерживающих общественные движения. В отчете определены потребности, в том числе в разработке и распространении программного обеспечения, которое позволяет активистам безопасно просматривать веб-страницы, не идентифицируя себя и свое местоположение при использовании устройств, и децентрализовать хранение данных в разных странах, препятствуя, тем самым, блокировке доступа.

ЗАКЛЮЧЕНИЕ

На пороге новой промышленной революции цифровые технологии уже изменили гражданское пространство и демократию так, как это представлялось бы немыслимым еще десять лет назад. Еще в 2011 году мы рассматривали технологии в первую очередь как силу добра, поскольку социальные сети и приложения для обмена сообщениями способствовали протестному движению на Ближнем Востоке и в Северной Африке. Прошло меньше десяти лет, и мы осознали способность тех же сетей распространять дезинформацию и ненависть. По мере ускорения инноваций разработчики технологий, государства и гражданское общество изо всех сил стараются не отставать от их воздействия на общество.

Гражданское общество призвано сыграть решающую роль в обеспечении того, чтобы цифровые технологии служили общественному благу; посредством реформ, совершенствования управления и в качестве равноправных партнеров в разработке и внедрении новых технологий. Гражданское общество также имеет возможность использовать потенциал ИИ для повышения эффективности и обеспечения соответствия своей инфраструктуры требованиям цифровой эпохи. Для того, чтобы сделать и то, и другое, гражданскому обществу потребуется техническая грамотность, особенно на уровне руководства; нужны правления НКО, поддерживающие перемены; нужна помощь доноров и готовность идти на совместные затраты и риски, связанные с инвестированием в ИИ, с государством и частным сектором.

> **Цифровые технологии уже изменили гражданское пространство и демократию так, как это представлялось бы немыслимым еще десять лет назад.**

ICNL

1126 16th Street NW, Suite 400
Washington, DC 20036 USA

www.icnl.org
facebook.com/ICNLAlliance twitter.com/ICNLAlliance