DOI 10.37882/2223-2974.2020.12.36

РИСКИ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В ЦИФРОВОМ ГОСУДАРСТВЕННОМ УПРАВЛЕНИИ: ВОПРОСЫ ЭЛЕКТОРАЛЬНОГО ТАРГЕТИРОВАНИЯ[1]

ARTIFICIAL INTELLIGENCE RISKS IN DIGITAL GOVERNANCE: ISSUES OF ELECTORAL TARGETING

N. Toropova
Sh. Guseinov
L. Egorova

Summary: The purpose of this article is to analyze scientific research in the field of risk research during the transition to the digital economy. The reasons for the emergence of possible threats associated with the use of artificial intelligence systems and big data technologies, as well as modern political technologies in the context of the formation of digital socio-political reality are considered. The paper briefly explores targeting technology in its various interpretations in the field of information and communication technologies and political goals. The urgency of changing the model of the organization of state control with the ever-expanding use of big data and artificial intelligence technologies in public administration has been substantiated.

Keywords: digital economy, digitalization risks, public administration, artificial intelligence, targeting, big data, personal data protection.

Торопова Наталья Валентиновна
К.э.н., в.н.с., Финансовый университет при Правительстве Российской Федерации
NToropova@fa.ru
Гусейнов Шахин Рагим оглы
Д.э.н., Московский государственный институт международных отношений МИД России
9585015@mail.ru
Егорова Лариса Ивановна
К.э.н., в.н.с., Финансовый университет при Правительстве Российской Федерации
LIEgorova@fa.ru

Аннотация: Целью настоящей статьи является анализ научных изысканий в области исследования рисков в период перехода к цифровой экономике. Рассматриваются причины возникновения возможных угроз, связанных с использованием систем искусственного интеллекта и технологий больших данных, а также современных политических технологий в условиях становления цифровой социально-политической реальности. В работе кратко исследована технология таргетинга в различных ее интерпретациях в области информационно-коммуникационных технологий и политических целях. Обоснована актуальность изменения модели организации государственного контроля при все расширяющемся использовании технологий больших данных и искусственного интеллекта в государственном управлении.

Ключевые слова: цифровая экономика, риски цифровизации, государственное управление, искусственный интеллект, таргетирование, большие данные, зашита персональных данных.

ВВЕДЕНИЕ

По мере того, как технологии искусственного интеллекта все больше входят во все сферы жизни общества, выявляется все больше рисков, вызванных их внедрением и применением, которые становятся все актуальнее. Решение этих проблем и рисков во взаимосвязи с нормативно-правовыми решениями, разработками, ориентированными на этические и социальные установки, имеет решающее значение успешного принятия систем искусственного интеллекта в политической жизни, в государственном секторе и обществе.

Повсеместное использование в современной повседневной деятельности информационно-цифровых технологий дает предпосылки для трансформации модели контроля основываясь на данных интеллектуальных информационных систем и построенных систем управления рисками.

В условиях цифровизации экономика РФ необходимо поддерживать способность сохранять стабильное состояние и сбалансированность процессов, не теряя систему эффективного управления. В этой связи управление рисками приобретает особое значение, встает вопрос о необходимости создания на государственном уровне систем безопасности, основанных на превентивном подходе к поставленным задачам, использовании технологий больших данных (Big Data) и систем искусственного интеллекта в структурные элементы государ-

1 Статья подготовлена в рамках выполнения Государственного задания 2020 г. по теме: «Выявления рисков государства и общества в условиях цифровизации».

ственных услуг и бизнес-сервисы [1].

В новых условиях цифровой трансформации субъект мониторинга рисков фактически становится участником процессов — объектов контроля. Это становится возможным, потому что информационные системы могут включать в свои процессы функцию мониторинга, проводя, тем самым, отслеживание проводимых операций. Информационные системы сегодня содержат данные о всей деятельности объектов контроля, что является «цифровым профилем объектов контроля» [2].

Результатом этих действий становится формирование условий для эффективного обнаружения нарушений, и, кроме того, использование предлагаемой формы контроля, как регулярное и систематическое наблюдение (анализ и прогнозирование действий подконтрольной сферы, и всех ее объектов, не взаимодействуя с ними). Проводимый мониторинг помогает эффективно реагировать на возникающие риски, не допуская действий, которые могут привести к отклонениям, либо оповещая о возникновении тенденции к появлению отклонения и сбое установленного режима деятельности объектов мониторинга.

Цифровизация мониторинга обеспечивает его непрерывность, наибольший диапазон и прозрачность функционирования объектов контроля, а также подотчетность действий контролирующих органов, что поможет снизить давление на объект контроля и создает условия для эффективного реагирования на риски проявления нарушений.

Однако, мониторинг должен оставить за собой правовосстановительные функции при сбое механизма предупреждения. Регулярный мониторинг в цифровом пространстве процессов объекта контроля, позволяет применять совокупность индикаторов нарушений и рисков, которые максимально способствуют предотвращению вероятных нарушений, оперативно информируя контролирующий орган об уже совершенных нарушениях.

Совершенствование информационно-коммуникационных технологий и распространение цифровых платформ формируют необходимость дополнять эти преобразование существенными «аналоговыми дополнениями», такими как — нормативная база, позволяющая использовать Интернет для инновационных решений, формирования цифровых навыков, позволяющих людям использовать возможности цифровых технологий, а также подотчетность учреждений, гарантирующих быстрое реагирование государственных органов на потребности и повышение благосостояния граждан.

Таким образом, государственное управление сталкивается с двумя задачами одновременно: оно не может препятствовать внедрению новых технологий и в то же время должно снижать риски, связанные с появлением цифровых тенденций.

Следует отметить, что, несмотря незначительные долгосрочные государственные инвестиции в исследования и разработки, цифровизация в значительной степени является результатом деятельности организаций, принадлежащих частному сектору экономики. Тем не менее, единовременное внедрение инновационных цифровых технологий, широкое применение новых источников данных/информации и использование новейших аналитических методов открывают значительные возможности для:

- повышения эффективности и совершенствования общественного порядка;
- оценки инновационных методов и воздействия цифровизации на общественно-экономические отношения;
- расширения участия граждан и заинтересованных сторон (стейкхолдеров) в разработке и реализации стратегии цифровой экономики [6].

Степень реализации этих возможностей зависит от готовности государства внедрять и распространять цифровые технологии, его способности получить своевременный доступ к надежным данным, которые часто находятся в руках частного сектора, и от того, насколько успешно решаются вопросы защиты личных данных и кибербезопасности. Указом Президента РФ в июле 2020 года определены Цели развития Российской Федерации на период до 2030 года, и в рамках цели «Цифровая трансформация» одним из показателей, характеризующих ее достижение является достижение «цифровой зрелости» ключевых отраслей экономики и социальной сферы, в том числе здравоохранения и образования, а также государственного управления. В тоже время нельзя не отметить доклад Организации экономического сотрудничества и развития (ОЭСР) за 2018 год, где обозначены четыре области, в которых цифровая трансформация может значительно улучшить разработку и реализацию государственной политики в сфере цифровизации.

Одна из обозначенных областей представляет собой необходимость повышения эффективности реализации и проведении целевого анализа существующих результатов.

Растущая способность систем искусственного интеллекта отслеживать результаты, например, с помощью инновационных и скоординированных технологий распознавания и доступности данных, которые ранее не могли

быть изучены всесторонне или которые могут быть изучены только при значительных административных затратах, позволяют более эффективно применять существующие правила и сокращают затраты на целевой анализ результатов цифровизации. В финансовом секторе стало возможным осуществлять мониторинг финансовых процессов с высокой точностью и периодичностью, которые не были доступны, что позволило лучше внедрить существующие правила на финансовом рынке и улучшить управление государственными финансами в целом. В области сельского хозяйства дистанционное распознавание и цифровая идентификация земель позволяет государствам направлять прямые субсидии фермерам и осуществлять другие меры регулирования, связанные с устойчивым социально-экономическим развитием сельских территорий. Растущие проблемы современной политики цифровизации включают неизбежность возникновения вопросов, связанных с защитой личных данных, остаются серьезными проблемами для дифференциации и таргетирования политики, например, социальной или образовательной сферах.

Например, такой механизм информационно-психологического воздействия, как таргетинг, который позволяет выделить из всей имеющейся аудитории часть, которая удовлетворяет определенным критериям (целевую аудиторию), и оказать воздействие именно на нее, то есть, персонифицированное воздействие на конкретных людей с учетом их индивидуальных характеристик. Таргетинг угрожает конфиденциальности, осуществляя сбор и консолидацию персональных данных о гражданах в массовом масштабе, что позволяет делать выводы о предпочтениях и интересах, особенно при микротаргетинге. Более точечный вид таргетирования - микротаргетинг главным образом адаптирован к индивидуальным гражданам и более эффективен, однако, нельзя не отметить риски для граждан [3]. Личная жизнь может быть нарушена, т.к. с помощью этих технологий действиями людей можно манипулировать. Сгенерированная информация формирует угрозы, одна из которых неприкосновенность частной жизни. Однако, если человек подозревает, что его посещения веб-сайтов отслеживается, то он может перестроить свое поведение, чтобы избежать внимания, или совсем отказаться от посещения ранее интересовавших его сайтов [4]. Такое поведение проблематично для компаний, создающих собственную базу данных на основе использования интернета физическими или юридическими лицами.

Необходимо отметить еще одну угрозу, касающаяся утечки данных, так получая собранную информацию от хакеров или иных лиц, можно составить требуемый для систематизирования или деления на группы, образ клиента (потребителя), учитывая его религиозные, политические, эстетические, сексуальные, и, наконец, гастрономические предпочтения. Потеря конфиденциальности может привести к негативным последствиям, а далее и к манипулированию [5]. В период предвыборных компаний заинтересованная партия может направить целенаправленную информацию на конкретных избирателей, манипулируя ими для минимизации участия в выборах, или наоборот, активизируя участие выбранных групп в избирательной компании, что может способствовать искажению информации и препятствовать общественному обсуждению. Например, используя интеллектуальные технологии в телевизорах т.н. «автоматическое распознавание контента» и получив доступ к шаблонам просмотра телевизионных программ, далее определив поведенческие данные личности, можно максимально использовать возможности широкого набора элементов персонифицированных сообщений для отдельных избирателей. Необходимо при этом учитывать еще один вид политического таргетирования - таргетированные санкции, которые представляют собой еще одни инструмент дифференцированного политического влияния, сосредоточенный на политических лидерах или их отдельных сторонниках, поддерживаемых ими коммерческих компаниях, секторах национальной экономики, либо на территориях, находящихся под контролем противодействующих законодательной власти групп[7].

Искусственный интеллект и другие автоматизированные системы смогут формировать прогнозы поведения электората и оказывать воздействие на о принятие решений без какого-либо контролирующего механизма. Распространение практики таргетирования создает противодействие для формирования системы политического надзора. За адресной политической рекламой в Интернете стоит комплексная и непрозрачная корпоративная деятельность. Data-аналитики и фирмы, работающие с цифровыми медиа, ведут свою деятельность непосредственно в политических партиях, участвующих в выборах, для проведения онлайн-кампаний. Подробности их деятельности зачастую неясны - на кого именно работают эти компании, чем они занимаются и как они это делают, часто является тайной. Задача надзорных органов состоит в создании условий для обеспечения большей прозрачности в отношении того, как ваши данные собираются и используются политическими партиями и компаниями, с которыми они работают. Очевидно, что реализация политических интересов повсеместно превратилась в сложную игру с данными, принимая во внимание, что во многих странах по-прежнему отсутствует или недостаточно развита практика законодательных и регулирующих механизмов, обеспечивающих защиту данных и конфиденциальность, нельзя не отметить, что такой уровень генерации и обработки данных, особенно персональных данных, таких как политические взгляды или этническая принадлежность поможет привлекать аудиторию с помощью подходящей политической рекламы [10].

В заключении хотелось бы отметить, что цифровые технологии в том числе системы искусственного интеллекта, технологии больших данных расширяют спектр инструментов политики, доступных правительствам, и могут снизить стоимость экспериментов и оценки результатов. В больших городах цифровые камеры, которые автоматически считывают количество автомобилей, въезжающих в зону скопления, делают более реалистичным проектирование, внедрение и проверку платежных систем для входа в районы, где вероятнее всего возникнут пробки. Сравнение данных о пробках с данными об использовании общественного транспорта на электронных картах позволяет оценить влияние политики городского планирования или транспортного поведения населения. В области образования мониторинг учебной деятельности студентов позволил некоторым странам выявить устаревшие элементы в разработке учебных программ и привел к экспериментам с новыми областями образования. В других областях (например, таких, как охрана природы) искусственный интеллект используется для разработки недорогих технологий распознавания образов, которые позволяют широкому кругу заинтересованных сторон играть более важную роль и вносить вклад в достижение важных целей государственной политики [8].

Цифровые технологии позволяют разработчикам политических программ быть более активными и реагировать на обнаружение и быстро меняющуюся действительность, будь то с точки зрения рисков или возможностей. В то же время расширенный анализ может способствовать более надежному прогнозированию реакции на определенные политические меры, чем раньше. Цифровая трансформация усиливает коллективное участие государства, граждан, гражданского общества, профсоюзов и частного сектора в разработке и реализации политики. Для государства цифровые платформы являются экономическим инструментом для изучения мнений и взглядов общества и для вовлечения заинтересованных сторон в разработку, реализацию и мониторинг политики цифровизации. Тем не менее, возможность прямого взаимодействия с государством вызывает необходимость большей подотчетности государства и быстрого реагирования на потребности пользователей.

Как показывает изучение этой проблематики, сегодняшнее цифровое внедрение систем искусственного интеллекта позволяет протестировать тысячи вариантов сообщений, оценить, как каждый из пользователей реагирует на них, и изменить контент в режиме реального времени и в различных СМИ, чтобы ориентировать и установить для конкретных избирателей. Данные, доступные для этого процесса, значительны, персонифицированы и содержат личную информацию, которая выходит далеко за рамки обычных представлений, включая поведенческие предпочтения, шаблоны просмотра телепрограмм и психографические модели. Растущее преобладание политического аппарата Big Data может также открыть новую эпоху кампаний, действующих на постоянной основе, когда отдельные лица и группы по всей стране постоянно отслеживаются, подвергаются таргетированию и управляются.

Разработка законодательных и регулирующих механизмов поможет ослабить некоторые из наиболее недопустимых видов использования социальных сетей недобросовестными кампаниями и другими участниками, однако они вряд ли каким-либо образом ограничат основные принципы современной практики политической рекламы. Поскольку, каждый технологический лидер устанавливает свой собственный набор внутренних политик в отношении рекламы, в настоящее время отсутствуют четкие общеотраслевых нормативы, применимые ко всем участникам цифровой экосистемы. Несмотря на то, что платформенные компании могут вносить корректировки, предполагающие надежные гарантии сохранения конфиденциальности, другие участники очень сложной инфраструктуры маркетинга больших данных могут предложить множество способов обойти эти ограничения.

Тем не менее, внедрение в качестве обязательного условия требования к раскрытию информации для цифровых медиа, должны быть гораздо более полными, т.е. должно требоваться полное раскрытие всех использованных ими методов рекламы и данных (например, отслеживание между устройствами, двойное моделирование, геолокация, измерения, нейромаркетинг), а также другие варианты рекламы, доставляемой через мобильные приложения подобные AI-приложениям [4].

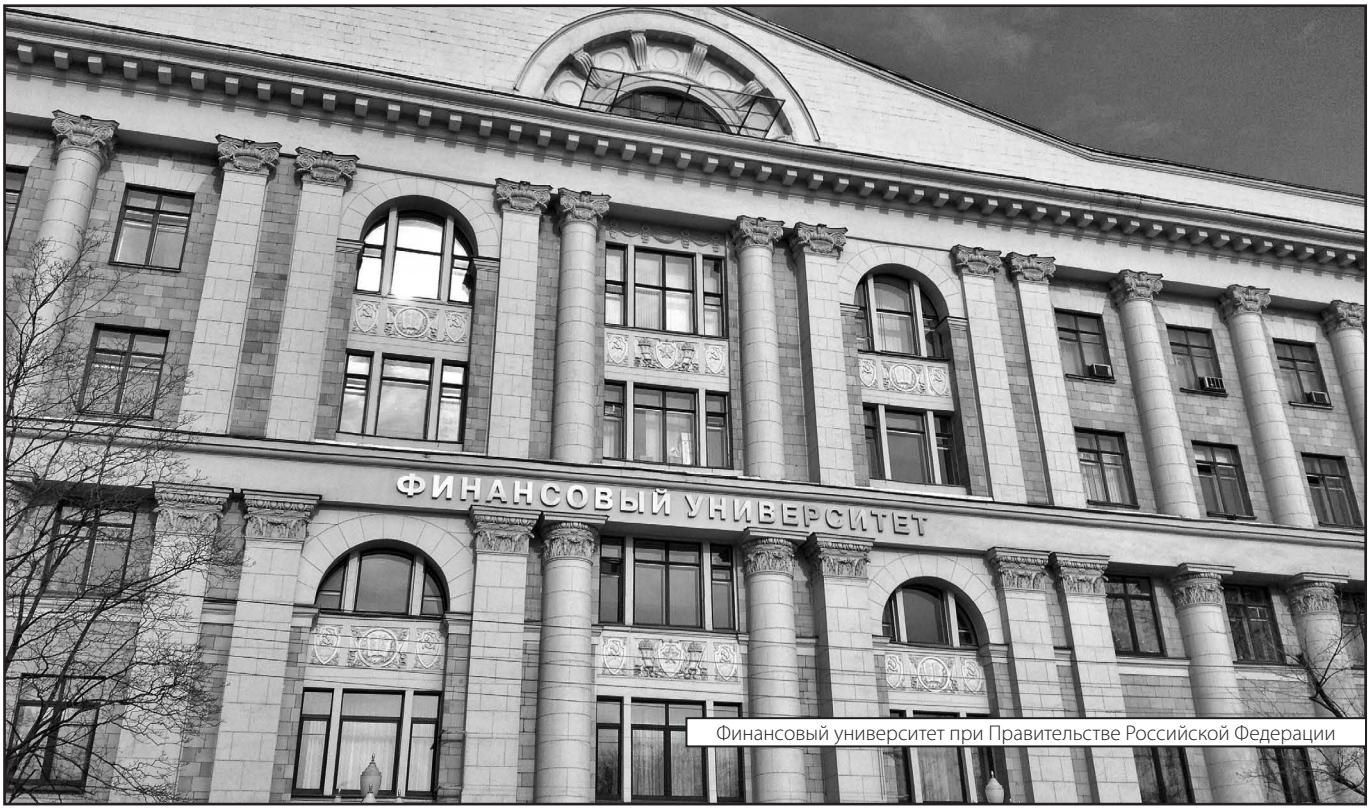
В первую очередь стоит уделить больше внимания использованию данных и методам таргетирования, обозначая различия между политической рекламой для граждан, которая поможет стимулировать их активность и такой, как как удержать от участия в голосовании и принижения роли реализации избирательного права. Кроме того, очевидно, что политическим партиям должно быть запрещено вести активные действия по получению беспрепятственного доступа к данным профиля избирателя, установив ограничения по источникам и объему данных. Это имеет особое значение в то время, когда большинство стран испытали «взрывное» воздействие от внедрения новых цифровых технологий во всех сферах жизнедеятельности созданное пандемией коронавируса Covid-19.

ЛИТЕРАТУРА

1. Bennett C.J. & Lyon D. (2019). Data-driven elections: implications and challenges for democratic societies. Internet Policy Review, 8(4). DOI: 10.14763/2019.4.1433 https://policyreview.info/data-driven-elections
2. Mavriki P., Karyda M. (2020) Big Data Analytics: From Threatening Privacy to Challenging Democracy. In: Katsikas S., Zorkadis V. (eds) E-Democracy – Safeguarding Democracy and Human Rights in the Digital Age. e-Democracy 2019. Communications in Computer and Information Science, vol 1111. Springer, Cham. https://doi.org/10.1007/978-3-030-37545-4_1 https://link.springer.com/chapter/10.1007%2F978-3-030-37545-4_1;
3. Bethany Shiner. The legal landscape: Micro-targeted politics and big data. https://www.electoral-reform.org.uk/the-legal-landscape-micro-targeted-politics-and-big-data/;
4. William D. Eggers, David Schatsky, Peter Viechnicki. How artificial intelligence could transform government. https://www2.deloitte.com/us/en/insights/focus/cognitive-technologies/artificial-intelligence-government-summary.html
5. Политический микротаргетинг в Интернете: обещания и угрозы для демократии. Зудервен Боргезиус, Фредерик и Мёллер, Джудит и Крюкемайер, Санне и О Фатхай, Ронан и Ирион, Кристина и Доббер, Том и Бодо, Балаш и де Вризе, Клаас Х., (9 февраля, 2018). Утрехтский обзор права, Vol. 14, № 1, с. 82-96, 2018, https://ssrn.com/abstract=3128787
6. Виловатых А.В. Манипулирование социальным поведением в условиях цифровой среды /А.В. Виловатых// Дискурс-Пи. 2020. Т. 17. № 2 (39). С. 149-164.
7. Шлюндт Н.Ю. Рассуждения о таргетировании в области санкционного инструментария в теории и практике международно-политического влияния /Н.Ю. Шлюндт// Международный журнал гуманитарных и естественных наук. 2018. № 7. С. 96-101.
8. Авдеева И.Л., Головина Т.А., Парахина Л.В. Цифровая трансформация экономических процессов: возможности и угрозы /И.Л. Авдеева, Т.А. Головнина, Л.В. Парахина// Финансовый бизнес. 2020. № 1 (204). С. 3-7.
9. Микрина В.Г. Международно-правовые механизмы защиты трудовых прав домашних работников // Евразийский юридический журнал. 2018. № 3 (118). С. 118-122.
10. Молчаков Н.Ю., Котлова А.В. «Конституционность» политического лидерства в сравнительной перспективе // Социально-политические науки. 2019. № 4. С. 35-40.

© Торопова Наталья Валентиновна (NToropova@fa.ru), Гусейнов Шахин Рагим оглы (9585015@mail.ru),
Егорова Лариса Ивановна (LIEgorova@fa.ru).

Журнал «Современная наука: актуальные проблемы теории и практики»



Финансовый университет при Правительстве Российской Федерации