***П.А. Барахвостов**, доцент*
barakhvostov@yandex.by
БГЭУ (Минск)

COVID-19 И ФЕНОМЕН ЦИФРОВОГО АВТОРИТАРИЗМА

Цифровые технологии дали правительствам всего мира инструменты для адаптации государственной политики к изменяющимся условиям и, в то же время, предоставили беспрецедентные возможности осуществления контроля над населением. Использование цифровых информационных технологий для реализации всеобъемлющего, эффективного и незаметного государственного надзора и манипулирования гражданами получило название цифрового авторитаризма.

Цифровой авторитаризм принимает множество форм: от отключения Интернета и кибератак до целевого наблюдения с использованием социальных сетей, искусственного интеллекта и программного обеспечения для распознавания лиц.

Еще несколько лет назад, исследуя данное явление, обращались к примеру Китая [2]. Однако пандемия COVID-19 резко изменила ситуацию. Одним из ее наиболее заметных последствий стало массовое применение информационных технологий для сбора информации о распространении вируса и физиологическом состоянии граждан, что свидетельствует о «диффузии» практик цифрового авторитаризма. Более тридцати стран приняли меры по цифровому надзору за населением, двадцать две из них Freedom House относит к демократиям. Эти меры включают контроль перемещений и контактов в условиях повышенной угрозы заражения, что предполагает использование систем видеонаблюдения и программ распознавания лиц, в том числе, людей в масках, беспилотных летательных аппаратов, данные о применении мобильных телефонов, браслеты с биометрическими трекерами. При этом мировые лидеры в сфере информационных технологий Apple и Google поддержали данную политику и, в целях привлечения как можно большего количества пользователей к программе отслеживания, достигли беспрецедентных договоренностей по ликвидации технических препятствий для обмена данными между платформами iOS и Android [1].

Наиболее широко для отслеживания населения используются мобильные приложения. Это стало возможным ввиду удешевления и, соответственно, широкого использования гражданами смартфонов. В КНР, например, мобильные приложения интегрированы с базами данных Министерства транспорта, железных дорог, управления гражданской авиации и государственной комиссии по здравоохранению. В Сингапуре мобильные приложения анализируют близость устройства по данным протокола беспроводной связи Bluetooth без учета личности пользователя и перемещений. Данные отправляются органам власти не на постоянной основе, а лишь в случае подтверждения диагноза у

какого-либо пользователя и с его согласия, а не востребованные в течение двадцать одного дня данные автоматически удалятся.

Среди стран, использующих данную практику, не только автократии (такие как Китай и Сингапур, быстро адаптировавшие и расширившие существовавшие в этих странах технологии цифрового наблюдения для мониторинга COVID-19), но и признанные демократии. В апреле 2020 г. Норвежский институт общественного здравоохранения запустил мобильное приложение Smittestopp («остановка заражения»), предназначенный для сбора геолокационных данных о перемещениях пользователей, чтобы помочь властям отследить распространение COVID-19. Это приложение было квалифицировано Amnesty International (2020) как одно из самых агрессивных в мире для отслеживания контактов COVID-19 [1].

Тем не менее, к мобильным приложениям наибольшее количество вопросов в связи с проблемой сохранения конфиденциальности. Несмотря на подтверждение большинством демократических правительств своей приверженности ее обеспечению, проблемы остаются. Например, анонимные данные подвержены риску повторной идентификации, и хотя они могут храниться в пользовательских телефонах, а не централизованно, есть опасения, что данные можно взломать.

Отметим различные позиции правительств демократий в отношении цифрового надзора. Норвежские власти, например, признали, что преимуществ Smittestopp недостаточно, чтобы оправдать его чрезмерное проникновение в частную жизнь граждан. В целом, четырнадцать стран отказались от слежки за распространением COVID-19 посредством мобильных приложений. Однако пятнадцать государств их уже запустили.

В связи с этим возникает угроза того, что после окончания пандемии правительства не захотят отказываться от новых возможностей наблюдения, которые предлагают эти приложения, сохранив сбор личных данных на длительный период. Тем более, что есть прецеденты: Патриотический акт США, принятый в 2001 г. в ответ на террористические атаки 11 сентября 2001 г., предоставил правительству широкие полномочия по надзору за населением. Однако эти полномочия остаются и сегодня, несмотря на отсутствие какой-либо угрозы иностранного нападения на Соединенные Штаты. В Великобритании правительство уже заявило, что планирует хранить собранную информацию до двадцати лет с невозможностью удаления ее по запросу [4]. Правозащитные организации выразили опасения, что данные могут быть использованы для других целей: предоставлены рекламным агентствам, которые сотрудничают с фармацевтическими и медицинскими учреждениями, страховым компаниям для отслеживания истории болезни при принятии решений. Базы данных, содержащие сведения о личностях с привязкой к мобильному телефону, также представляют ценность для рынка потребительских товаров. Все это нарушит равные права при ведении бизнеса. Однако наибольшую обеспокоенность вызывает возможность использования технологии распознавания лиц и

обязательного сбора конфиденциальных данных для борьбы с политическими оппонентами.

Тесным образом с информационными технологиями и цифровизацией связано развитие Интернета и его неотъемлемого сегмента – социальных сетей. В январе 2020 г. наблюдалось столь быстрое распространение слухов и лжи о происхождении, симптомах и средствах лечения COVID-19 в социальных сетях, что в феврале, за несколько недель до объявления пандемии Всемирная организация здравоохранения (ВОЗ) назвала ситуацию «инфодемией», предупредив, что вводящая в заблуждение информация имеет опасные последствия для здоровья людей и подрывает доверие к органам здравоохранения [7]. В связи с этим правительства ряда стран приняли такие меры, как цензура онлайн-контента и введение ответственности, вплоть до уголовной, за распространение «фейковых новостей». Например, когда граждане Китая начали делиться информацией о таинственной болезни в Ухани, онлайн-посты и хэштеги, связанные с болезнями, были быстро удалены, а учетные записи пользователей заблокированы. Facebook, Twitter и Google использовали специальных цензоров и компьютерные алгоритмы, чтобы удалить ложь, связанную с пандемией, запретить мероприятия в нарушение директив о социальном дистанцировании, а также предупреждали пользователей, столкнувшихся с подобным контентом, что он вводит в заблуждение [3]. В ряде государств запрещалась информация о COVID-19, не исходящая от правительства или органов здравоохранения. В частности, в марте 2020 г. в Армении был принят закон, в соответствии с которым любая распространяемая о заболевании информация должна быть подготовлена на основе данных специальной службы экстренной помощи при премьер-министре страны [5].

Крайней формой цензуры, возникшей в связи с COVID-19, стало уголовное наказание за дезинформацию. Данная мера была широко распространена как в автократиях, так и в демократиях. По крайней мере, двадцать четыре страны приняли законы, направленные на препятствование распространению ложной информации, причем в пятнадцати из них это действие карается тюремным сроком. Среди стран ЕС закон о фейковых новостях приняла только Венгрия, хотя в Европейской комиссии раздавались призывы выйти за рамки нынешнего саморегулируемого характера онлайн-СМИ [6].

Кроме того, многие страны ограничили доступ к официальной информации. Так, например, в Грузии введены правила, предусматривающие продление сроков ответа правительства на запросы о предоставлении публичной информации о локализации COVID-19. Правительство Бразилии перестало публиковать данные о случаях COVID-19 и смертей, а Швеция скрыла от общественности ряд правительственных сообщений и информацию о готовности к вирусу.

Таким образом, пандемия способствовала изменению практик управления практически во всех странах. Режим мобилизации потребовал принятия быстрых решений, усиления государственного надзора за населением, частичного ограничения свобод (в частности, свободы передвижения) отдельных личностей

во имя безопасности нации в целом. Принятые экстраординарные меры – в русле политики, проводимой властями автократий. Это свидетельствует о превращении в эпоху коронавируса цифрового авторитаризма в явление мирового масштаба.

Список источников:

1. Eck, K. State surveillance and the COVID-19 crisis/ K. Eck, S. Hatz // J. Human Rights. – 2020. – V. 19, № 5. – P. 603–612.
2. Erixon, F. Digital authoritarianism: Human rights, geopolitics and commerce / F. Erixon, H. Lee-Makiyama // ECONSTOR [Electronic resource]. – Mode of access: https://www.econstor.eu/bitstream/10419/174715/1/ecipe-op-2011-5.pdf. – Date of access: 06.11.2021.
3. Goldsmith, J. Internet speech will never go back to normal / J. Goldsmith, A. Woods // The Atlantic [Electronic resource]. – Mode of access: https://www.theatlantic.com/ideas/archive/2020/04/what-covid-revealedabout-internet/610549/. – Date of access: 10.11.2021.
4. Hern, A. Public Health England will keep personal data of people with coronavirus for 20 years / A. Hern// The Guardian [Electronic resource]. – Mode of access: https://www.theguardian.com/world/2020/may/28/nhs-will-keep-personal-data-of-people-with-coronavirus-for-20-years–uk-test-and-trace-programme. – Date of access: 10.11.2021.
5. COVID-19 Civic Freedom Tracker // ICNL [Electronic resource]. – Mode of access: https://www.icnl.org/COVID19tracker. – Date of access: 01.11.2021.
6. Stolton, S. Regulation Against Fake News 'Very Important,' Reynders Says / S. Stolton // Euractiv [Electronic resource]. – Mode of access: https://www.euractiv.com/section/digital/news/regulation-against-fake-news-very-important-reynders-says/. – Date of access: 11.11.2021.
7. Working Together to Tackle the 'Infodemic' // WHO [Electronic resource]. – Mode of access: https://www.euro.who.int/en/health-topics/Health--systems/pages/news/news/2020/6/working-togetherto-tackle-the-infodemic. – Date of access: 10.11.2021.

***Э.Э. Ермакова**, старший преподаватель*
ermakova.eleonora@gmai.com
БрГТУ (Брест)

ЦИФРОВАЯ ТРАНСФОРМАЦИЯ БИЗНЕС-ПРОЦЕССОВ В РЕСПУБЛИКЕ БЕЛАРУСЬ

На современном этапе переход к инновационному развитию экономики в Беларуси является решающим фактором повышения конкурентоспособности. Инновационное развитие в последние десятилетия связывают с информационными технологиями и определением пути цифровых преобразований.