УДК 347.121

О. В. Епархина **https://orcid.org/0000-0002-2793-7608**

Цифровые права граждан и их защита в постковидном обществе

Для цитирования: Епархина О. В. Цифровые права граждан и их защита в постковидном обществе // Социально-политические исследования. 2020. № 3 (8). С. 20–37. DOI 10.20323/2658-428X-2020-3-20-37

В статье рассмотрены содержательное наполнение понятия «цифровых прав» граждан и проблемы их восприятия и защиты во время пандемии 2020 года. Неразработанность нормативной базы в данной сфере и актуализация темы защиты прав в условиях ускоренной цифровизации приводят к необходимости рассмотрения существующих международных стандартов их защиты, а также возможностей использования инструментов различных международных правозащитных организаций для этой цели. Автором представлен краткий обзор угроз приватности данных в цифровой среде, появляющихся в условиях роста пандемии, проанализирован опыт разных стран по работе с цифровыми личными данными и возникающие в связи с этим сложности. Показаны различия в политике конфиденциальности цифровой личной информации в разных странах. В качестве основы для создания в будущем нормативной базы, регулирующей цифровые права граждан и обработку личных данных в европейских странах, используется Общий регламент защиты персональных данных (GDPR). Однако в связи с тем, что регулирование такого рода отношений находится пока в начальной стадии развития, наиболее значимую роль могут сыграть активность общественных организаций, международных структур, специализирующихся на защите прав человека в целом.

Ключевые слова: цифровизация общества, стандарт GDPR, правозащитные организации, сфера защиты цифровых прав граждан.

O. V. Eparkhina

Digital rights of citizens and their protection in a post-covid 19 society

In article research intention of digital rights of sitizen and some problems of it perception and protection during the pandemic 2020. Weakness of low base in this sphere and actualization of right's protection during fast digitalization of society lead us to research international standards of right's protection and to research some possibilities of different international human rights organizations. The author presents brief field of privacy data threats in digital society in pandemic situation. There's analyzed the experience of different countries with digital personal data and some problems in this work. There're some differences in digital personal data policy in different countries. As a base of creation a future low about work with digital personal data and digital rights of sitizen, european countries use GDPR. But regulation of this field is take-off now, the most important role have an active public organizations and international human rights organizations.

Key words: digitalization of society, GDPR, human rights organizations, digital rights of sitizen protect.

Актуальность проблемы защиты цифровых прав граждан

Коронавирус беспрецедентно ускорил цифровую трансформацию во всем мире, для борьбы с ним используют IT-технологии, искусственный интеллект и Big Data. Различные страны используют многообразные подходы к привлечению цифровых технологий для мониторинга населения. Среди них – слежение за зараженными или нарушившими карантин людьми, распознавание лиц, беспилотные устройства, отслеживание мобильного трафика и геолокации пользователей и много других способов вмешательства в личную жизнь людей. В связи с пандемией и принимаемыми мерами по мониторингу населения факты ограничения прав и свобод граждан зафиксированы в России, Китае, Израиле, Австрии, Германии, Великобритании, Италии, Иране, Сингапуре, Великобритании, Южной Корее и в других странах. Многие правительства используют массовое наблюдение за людьми с помощью городских камер наблюдения и устройств видеофиксации, расположенных в жилых домах, транспорте и других местах для того, чтобы выявлять нарушителей карантина. Часто разрешается отслеживание передвижения граждан с помощью сетей мобильной связи, GPS в автомобилях, фиксирование локализации транзакций по картам и счетам и т. п. Это приводит не только к нарушению прав человека, но и к изменению его сознания, формированию новой гражданской идентичности. В большей степени это касается молодежи, но и старшее поколение испытывает существенные сложности при осознании возникающих проблем. Поэтому необходимо комплексное изучение этой проблемы в рамках системного и институционального подходов, а также комбинированных методологий. В качестве методологической основы постановки проблемы в данной статье использованы работы О. Коряковцевой, Т. Трофимовой, А. Ломовцевой, А. Мкртумовой, Н. Городновой, Д. Скипина, И. Роженцова, Л. Сморгунова, В. Фролова, Д. Каминченко [Коряковцева, 2019; Городнова, 2019; Мкртумова, 2019; Сморгунов, 2018; Фролов, 2019].

Государственные органы в таких условиях получают практически неограниченный доступ ко всему объему персональных данных людей. При этом разработкой соответствующих технологий занимаются преимущественно частные компании – как крупные, так и средние. И эти компании также имеют доступ к базам личных данных граждан. Например, в Китае люди с повышенной температурой выявлялись в общественных местах с помощью устройств для измерения температуры, в том числе встроенных в шлемы представителей правоохра-

нительных органов, была разработана технология распознавания лиц в масках. Компания Hanvon утверждает, что создала устройство для увеличения процента распознавания лиц, носящих хирургические маски, до 95 % [Поллард, 2020]. В Израиле был разработан план использования индивидуального наблюдения по телефону, чтобы предупреждать пользователей о опасности смешивания с людьми, которые потенциально могут быть носителями вируса [Лоран, 2020]. На Тайване инфицированным лицам выдается мобильный телефон и записывается их местоположение по данным GPS, с тем чтобы полиция могла отслеживать их передвижения и следить за тем, чтобы они не удалялись от места изоляции [Лоран, 2020]. В Италии разработано приложение для смартфона, с помощью которого можно проследить маршрут зараженного вирусом человека и предупредить людей, контактировавших с ним [Обзор, проведенный секретариатом CAHAI, 2020]. США обратились к компаниям с просьбой предоставить доступ к агрегированным и анонимным данным, особенно в отношении мобильных телефонов, для борьбы с распространением вируса [Ромм, 2020].

Для раннего выявления заболевших граждан и предупреждения их контактов с окружающими можно использовать продвинутые системы видеоаналитики, обычные смартфоны и фитнес-трекеры. В скором времени в офисах и на производствах могут появиться системы позиционирования персонала, сигнализирующие о нарушении безопасной дистанции между сотрудниками. В случае обнаружения первых симптомов или заражения у отдельного сотрудника, работодатель может быстро идентифицировать его местоположение и получить историю всех его контактов с другими сотрудниками.

В Китае уже существуют прототипы мобильного приложения для выявления симптомов COVID-19 по голосу человека. Алгоритм с помощью искусственного интеллекта определяет состояние пациента в соответствии с голосовыми маркерами по различным заболеваниям (респираторные, кардиологические или болезни, связанные с поведенческими расстройствами, такими как депрессия). Это приложение может использоваться для удаленной диагностики и мониторинга, для того чтобы предотвратить распространение заболевания и перегрузку национальной системы здравоохранения. В Сингапуре идет работа над платформой, которая создается для проверки собственных симптомов на риск заражения COVID-19 [Обзор, проведенный секретариатом CAHAI, 2020]. Это приложение призвано помочь специалистам отслеживать распространение коронавируса, а также оценить вероятность заражения для отдельных граждан. Приложение просит пользователей заполнить данные, включая возраст, пол, даже

почтовый индекс, а также ответить на вопрос о наличии хронических заболеваний, таких как сердечные заболевания, астма и диабет. Затем приложение просит всех, кто предоставил информацию, каждый день выделять максимум минуту для того, чтобы сообщить о своем самочувствии [Ляпунов, 2020]. Во многих странах беспилотники с помощью видеокамер отслеживают нарушителей режима карантина в общественных местах.

Разрабатывается и программное обеспечение для анализа распространения коронавируса и для контроля за социальным поведением граждан во время пандемии: Google проводит анализ данных о местоположении с миллиардов телефонов пользователей его платформы – это самый большой общедоступный набор данных, который помогает органам здравоохранения оценить, соблюдают ли люди указания по местоположению и подобные приказы по всему миру, чтобы остановить вирус. Стали обыденной практикой браслеты для контроля перемещений людей в карантине. Это специальное устройство, которое может отслеживать мобильный сигнал людей, находящихся дома на карантине. В случае если гражданин выключит телефон или выйдет из дома, устройство автоматически сообщит в полицию о нарушении. В Китае работает платформа с информацией о зонах с повышенным риском заражения COVID-19. Она использует информацию из официальных источников и отмечает на реальных картах места и целые зоны, непосредственно связанные с повышенным риском заражения новым коронавирусом (на основании официально подтвержденных случаев заражения) [Якобович, 2020].

Как отмечают специалисты Pandemic Big Brother [РосКомСвобода, 2020], в Европе намечается глобальный тренд на коронавирусные приложения, которые отслеживают круг контактов заболевших. Но если в Европе установка приложений носит рекомендательный характер, то в Азии ситуация противоположная. Например, в Китае ввели так называемые «коды здоровья», которые сканируются практически во всех публичных местах. В Индии также разрабатывают подобные приложения, одно из которых решили сделать обязательным на территории всей страны. В Индии рассматривают возможность использования дронов с функцией распознавания лиц и интегрированных с местной системой цифровой идентификации, которая насчитывает более 1 млрд пользователей. «Приложение, разработанное для отслеживания людей с COVID-19 и симптомами других респираторных заболеваний, неоправданно нарушает конфиденциальность пользователей, погрязло в недостатках и технических проблемах и должно быть немедленно прекращено», – отмечают эксперты Human Rights Watch [РосКомСвобода, 2020]. В Южной Корее передается предупреждение

органам здравоохранения через приложения в случае несоблюдения карантина, когда зараженные или контактировавшие с ними лица находятся в общественных местах (транспорт, торговый центр). По итогам отслеживания тестировались все потенциально зараженные. Сейчас власти активно выявляют тех, кто посещал места массового скопления людей, в метро установлены устройства для распознавания лиц тех, кто не использует маски, не соблюдает социальную дистанцию. Для остальных граждан приложения не используются [РосКомСвобода, 2020].

Приложениями для контроля местоположения должны были в марте 2020 г. пользоваться иностранцы, прибывающие на территорию страны, оно выполнено на корейском и английском языках и кроме функции слежения дает доступ к информации по профилактике, лечению и возможности заражения. Отслеживаются звонки, выходы из дома и посещение мест массового скопления.

Особый интерес в начале пандемии с точки зрения соблюдения цифровых прав представляла даже не китайская система отслеживания контактов, а британская. Особенностью Великобритании является уже имевшийся обширный опыт цифровизации: она начала переход на цифровые паспорта задолго до начала пандемии. В начале июля 2018 года стало известно о создании в Британии единой базы биометрических данных граждан страны. За счет этого проекта власти хотели упростить поиск преступников и ускорить работу пограничников. Министерство внутренних дел Великобритании опубликовало Biometrics Strategy, в котором описывается план по созданию базы данных, в которую войдут ДНК, отпечатки пальцев, фотографии лиц и, возможно, даже образцы голоса жителей страны. Предполагалось, что информация будет доступна полиции, миграционным службам и работникам паспортного контроля в аэропортах. Уже в 2018 году были собраны данные (включая изображения лиц) на 12,5 млн человек. Во время пандемии вся эта система начала активно использоваться.

В феврале 2017 года британская Правительственная цифровая служба (Government Digital Service, GDS; отвечает за проекты электронного правительства Великобритании) обнародовала национальную стратегию цифровых преобразований, в рамках которой планируется обновить устаревшие ИТ-системы, более эффективно использовать данные и создать единые платформы для государственных услуг, способствовать развитию услуг, оказываемых государственными органами (например, планируется наладить взаимодействие органов соцобеспечения с налоговой системой), и усилению кибербезопасности. В рамках национальной стратегии цифровых преобразований сначала планируется изменить оказываемые гражданам государственные услуги, затем пре-

образовать сами государственные органы с цифровой точки зрения и все правительство целиком. Еще одним элементом программы цифровой трансформации государственных услуг является увеличение числа API-интерфейсов и расширение их функциональности внутри и за пределами электронного правительства. К примеру, бухгалтеры смогут автоматически подавать налоговые декларации с разрешения своих клиентов. На уже существующей технологической базе британскому правительству, вероятно, удастся достаточно оперативно создать систему мониторинга за перемещениями зараженных COVID-19 лиц и соблюдением ими режима самоизоляции. По сути, британская модель – это не сбор данных, а технологическое решение для оптимизации работы с уже имеющимися у государственных органов данными. Пандемия дала толчок усовершенствованию технической базы уже запущенной цифровизации.

Существует явная тенденция к сохранению этих технологий в постковидном обществе. Государство является главной заинтересованной стороной, стремящейся к их сохранению, однако, определенную роль играют и корпорации, производящие и использующие системы контроля в своих целях. Большинство стран использует подобные технологии для отслеживания контактов заболевших людей, но часто отслеживаются и покупки, в частности, покупки медикаментов, любые выходы на улицу, телефонные звонки и т. п.

В целом, технологии слежения можно свести к следующему:

− использование камер и систем уличного видеонаблюдения с системой распознавания лиц;

− использование дронов для отслеживания перемещений;

− использование приложений в телефоне;

− использование отслеживающих устройств, в том числе отслеживающих перемещения по данным GPS;

− фиксирование локализации транзакций по картам и счетам;

− отслеживание мобильного трафика;

− раскрытие доступа к базам данных персонала компаний для отслеживания перемещений и соблюдения дистанции;

− фиксирование температуры и иных симптомов заболеваний без уведомления человека.

Представленный выше перечень далеко не полный из возможных направлений мониторинга и отслеживания. Данные могут собираться как на заболевших людей, так и на круг их близких контактов, и даже на любых подозрительных с точки зрения власти лиц. При этом нет никакой гарантии локального хранения данных, их безопасного использования и дальнейшего удаления. COVID-19 выявил, что цифровизация зачастую способствует социальной изоляции, ставит под угрозу жизни и здоровье бедных и

пожилых. По мнению экспертов, есть основания говорить о digital-эксклюзии многих групп населения; так, в частности, пандемия показала, что нуждающаяся группа населения тратит значительную часть дохода на доступ к интернету в ущерб повседневным нуждам и покупке продуктов. Кроме того, пандемия выявила недостаток персональных данных многих людей в электронной среде, так как они не пользуются услугами интернета. Особой опасности в условиях такой эксклюзии подвергаются пожилые люди, инвалиды, женщины в ситуации домашнего насилия, когда эти группы не только оказываются отрезанными от систем жизнеобеспечения, но и подвергают угрозе свои жизни и жизни детей при невозможности сообщить об этом [Guardian, 2020]. Вероятно, обеспечение населения интернетом должно стать зоной ответственности правительств, но пока неясно как это осуществить технически. На сегодняшний день рассматриваются возможности средств массовой информации, социальных сетей и соседских сообществ для улучшения этой ситуации.

Еще одним риском является обнаружившаяся угроза утечки персональных данных: в кризисной ситуации государство четко осознало, что не обладает достаточно надежными механизмами защиты данных.

Таким образом, страны используют различные стратегии, и часто они обусловлены спецификой менталитета населения, волевой позицией государства, и практически везде пока отсутствует четкая и ясная нормативно-правовая база для действия систем контроля за гражданами.

Интерес в решении этого вопроса представляет и кластерный подход. Этот подход позволяет учитывать миграционный фактор для стран с высокой миграционной нагрузкой: – если у мигрантов нет постоянной работы, им предлагают выйти в качестве волонтеров в дома престарелых, где эпидемиологическая ситуация тяжела, и тогда, безусловно, необходимо их отслеживание, поскольку эти люди могут переходить из учреждения в учреждение, что способствует распространению инфекции. Но, с другой стороны, это ведет и к дискриминации цифровых прав определенных групп населения.

Нормативная база

На сегодняшний день значительных изменений в правовом поле рассмотренных стран, регламентирующих доступ к персональным данным, еще не произошло, но их следует ожидать в ближайшие месяцы. В частности, нормативная база в европейских странах будет по-прежнему ориентироваться на нормы и принципы GDPR.

Общий регламент защиты персональных данных (GDPR) обеспечивает Постановление Европейского Союза, с помощью которого Европейский парламент, Совет Европейского Союза и Европейская комиссия усиливают и унифицируют за-

щиту персональных данных всех лиц в Европейском Союзе. Постановление также регламентирует экспорт данных из зоны Евросоюза. GDPR направлен, прежде всего, на то, чтобы дать гражданам контроль над собственными персональными данными, и на упрощение нормативной базы для международных экономических отношений путем унификации регулирования в рамках ЕС [GDPR, 2020].

Именно эти нормы определяют базовый подход к пониманию сущности персональных данных. Например, человек может быть идентифицирован с использованием фамилии, идентификационного номера, данных о местоположении, а также при помощи характерных для данного лица физических, физиологических, генетических, духовных, экономических, культурных факторов и т. п. [GDPR, 2020].

GDPR сегодня усиливает существующие и вводит новые права граждан ЕС, а также дает гражданам больше контроля над своими личными данными [GDPR, 2020]:

− более легкий доступ к их данным, включая предоставление дополнительной информации о том, как обрабатываются эти данные, и обеспечение доступности этой информации ясным и понятным образом;

− право на переносимость данных – изменение правил передачи персональных данных между поставщиками услуг;

− право на забвение («право на удаление персональных данных») – когда человек больше не хочет, чтобы его персональные обрабатывались и нет законных оснований для их сохранения, то данные будут удалены;

− право знать, если данные пользователя были взломаны – компаниям и организациям придется незамедлительно информировать людей о нарушениях безопасности данных. Они также обязаны уведомить соответствующий орган по надзору за защитой данных.

GDPR также разрабатывает расширенную линейку инструментов гражданам Евросоюза для реализации своих прав, упрощая механизмы обращения в надзорные органы, например, жалобы в электронном виде.

Отметим, что под действие закона GDPR попадает полностью или частично автоматизированная обработка персональных данных граждан на территории Европейского Союза и за его пределами физическими или юридическими лицами, государственными органами, другими институтами и организациями. На сегодняшний день в связи с пандемией началось расширение списка особо охраняемых персональных данных, куда входят раса и национальность, политические взгляды, вероисповедание, сексуальная ориентация, биометрические данные – физические, физиологические или поведенческие признаки физического лица, при помощи которых воз-

можно однозначно идентифицировать человека (изображение человеческого лица, отпечатки пальцев, сетчатка глаза, запись голоса и т. п.), данные о здоровье, генетические данные – унаследованные или приобретенные генетические признаки физического лица, предоставляющие уникальную информацию о физиологии или здоровье, а также соответствующие биологические образцы [GDPR, 2020].

Необходимо ориентироваться также на стандарты, касающиеся защиты данных, такие как Конвенция 108(+) Совета Европы в части использования биометрических данных, геолокации, распознавания лиц или использования данных о здоровье. Использование чрезвычайных мер должно осуществляться на основе всесторонних консультаций с органами защиты данных и при уважении достоинства и частной жизни пользователей. Следует учитывать различные предвзятости при проведении различных видов операций по надзору, поскольку они могут привести к значительной дискриминации [Кан, 2020].

Реакция общества, правозащитных структур и международных организаций

В настоящее время существует несколько форматов выявления общественных оценок нарушений цифровых прав граждан:

− *проведение кросскультурных опросов населения по восприятию систем слежения и нарушений прав человека*. Этот формат пока недостаточно востребован в связи с тем, что пандемическая ситуация еще продолжается, эксклюзивные группы, в наибольшей степени страдающие от нее, пока недоступны, а серьезных запросов на проведение таких исследований не поступало. Однако такие цели уже поставлены в Швеции и Великобритании.

− *онлайн проекты по фиксации нарушений прав человека в ситуации мониторинга населения*. Пока наиболее интересным проектом является Pandemic Big Brother. Активисты, представители коммерческих компаний и правозащитники в РФ в лице таких организаций как АНО «Информационная культура», Центр цифровых прав, Роскомсвобода, Лаборатория цифровых прав активно обсуждают российский и зарубежный опыт в этой сфере и выявляют пути их решения. Так, «Роскомсвобода» совместно с партнерами провела Privacy Day 2020 [РосКомСвобода, 2020] и презентовала проект общественного мониторинга нарушений прав на частную жизнь, свободу слова, тайну связи Pandemic Big Brother. Данный трансграничный и мультиязычный проект общественного мониторинга отражает ограничение цифровых прав и свобод пользователей во время пандемии в разных странах. Проект доступен на русском, английском, французском и немецком языках. Его партнеры – правозащитные организации из Белоруссии, Украины, Кыргызстана, Казах-

стана, Великобритании, США и других стран. Цель проекта – отследить, снимут ли ограничительные меры после пандемии. **Задачами проекта являются** общественный мониторинг соблюдения цифровых прав, сбор аналитической и новостной информации, освещение ситуации по цифровым правам по всему миру, отслеживание действий властей после окончания пандемии.

Проект выглядит, как карта мира, и все страны обозначены тремя цветами. Серый означает, что информации по стране нет, желтый – есть вероятность ограничительных мер, но пока они не введены, красный – ограничения уже в действии. Зеленым в дальнейшем отметят страны, где ограничения после пандемии сняли, а коричневым – те места, где меры останутся.

На карте отмечаются следующие нарушения:

− слежка через мобильные телефоны и госсервисы;

− цензура (борьба с фейками);

− административное и уголовное преследование за публикации;

− ограничение доступа к официальной информации;

− контроль через дроны;

− видеонаблюдение и распознавание лиц;

− отключение или принудительное замедление интернета.

По мнению авторов проекта, ограничения должны вводиться с соблюдением следующих принципов: добровольность; законность; открытость; наличие временных рамок; достижение цели; инфобезопасность; отсутствие дискриминации; общественное участие.

Как полагают эксперты, меры по ограничению этих прав в связи с пандемией часто носят избыточный характер и могут остаться в постковидном мире и после пандемии. В частности, вопросы у экспертов вызывает технология распознавания лиц. Пандемия продвинула эту технологию сильно вперед. Еще во время протестов в Гонконге власти не могли идентифицировать людей в медицинских масках. Теперь не помеха даже шлемы, поскольку система ориентируется не только на точки, но и создает 3D-модель головы. Несмотря на свои положительные стороны, распознавание лиц несет и много опасностей. Среди них – незаконный сбор данных, мошенничество, ошибки распознавания (в отношении чернокожих людей до сих пор постоянно происходят сбои) и возможность неавторизованного доступа третьего лица, который ведет к утечкам данных. Массовая слежка со стороны государства не просто нарушает права людей, но и меняет поведение и действия людей, перерастая в психологическую проблему. Другой проблемой является сбор биометрических данных. Особенно активно эта технология реализуется в Китае, США, в последнее время в России и Канаде. Сам Китай как экспортирует технологию, так следит и за своими гражданами. Сейчас в стране установлено

173 млн камер, на систему слежки уже потрачено 200 млрд долл. Однако, существуют и другие варианты поведения: Сан-Франциско и Окленд (США) приняли запрет на эту технологию, позже Калифорния – мораторий на ее использование правоохранительными органами. Порядок же использования распознавания бизнесом строго регламентируется: например, владелец заведения должен повесить крупный значок-предупреждение о видеонаблюдении. В январе этого года Еврокомиссия предложила ввести мораторий на распознавание лиц в публичных местах на 3–5 лет в целях выяснения разумной методологии и оценки воздействия технологии. Чуть позже, однако, она решила не принимать документ и разрешила каждому государству-члену самостоятельно определить, как использовать технологию. В феврале стало известно о планах Европарламента создать панъевропейскую базу данных, что вызвало бурные общественные дискуссии. Пандемия спровоцировала ускорение создания рамочных соглашений по данной технологии, универсальных для всех европейских стран.

– *выявление позиций неправительственных и правозащитных организаций по вопросу нарушения прав человека* в ситуации мониторинга населения. Представители многих неправительственных организаций уже сейчас выступают против внедряемых технологий массового наблюдения. Решения, которые государство принимает сейчас, вводя ограничения базовых прав человека, в том числе и цифровых прав, повлияют на будущую реальность, а в результате на жизнь и здоровье нынешнего и будущих поколений. В дискуссию включились депутаты Европарламента, Совет Европы, международные правозащитные структуры.

На сегодняшний день свои позиции обозначили такие международные организации как European Digital Rights, Privacy International, European Agency for Fundamental Rights, Freedom House и другие. «ЕС был убежищем для незаконных биометрических экспериментов и слежки», – заявили в брюссельской неправительственной организации European Digital Rights [Jakubowska, 2020]. Но Бельгия и Люксембург до сих пор являются единственными государствами, которые считают, что распознавание лиц нарушает национальное законодательство. Исследование этой организации показало, что 80 % европейцев не хотят делиться своими данными с властями. Технологии распознавания лиц могут быть использованы не только для наблюдения, отслеживания или анализа граждан (и оценки их «социального кредита» в китайском стиле), но также и для разблокировки мобильного телефона или банковского перевода. EDRi призвала государства-члены и Европейскую комиссию запретить использование технологий распознавания лиц и биометрической обработки в обще-

ственных местах – как законодательно, так и на практике [Jakubowska, 2020].

«Введение распознавания лиц в городах – это радикальная и антиутопическая идея, которая значительно угрожает нашим свободам и ставит основополагающие вопросы о том, в каком обществе мы хотим жить», – заявил Иоаннис Коувакас из Privacy International [Privacy International, 2020].

В докладе European Agency for Fundamental Rights отмечается, что «внятная правовая база должна регулировать внедрение и использование технологий распознавания лиц» [FRA, 2020].

Другие авторитетные правозащитные организации также отмечают, что необходимо уже сейчас выявлять преимущества и проблемы, появившиеся при использовании цифровых инструментов и искусственного интеллекта для контроля за гражданами. В частности, временные меры по контролю и массовому мониторингу населения с помощью этой технологии не должны считается тривиальными и не должны стать постоянными [Харари, 2020].

Freedom House представила принципы защиты гражданских и политических прав во время пандемии. В частности, отмечено, что меры, предпринимаемые правительствами, носят дискриминационный характер и могут быть сохранены после ликвидации кризиса. Защита гражданских и политических прав в этих условиях должна осуществляться в соответствии с такими принципами как прозрачность, легитимность, соответствие уровню угроз. Эти принципы имеют особое значение при сборе, хранении и использовании персональных данных [Freedom House, 2020].

Отдельно следует рассмотреть позиции ООН, Совета Европы, Европарламента. Верховный комиссар ООН по правам человека Мишель Бачелет также высказала свою позицию: «Я глубоко обеспокоена наделением правительств ряда стран чрезвычайными полномочиями на неопределенный срок и без возможности пересмотра. В некоторых случаях эпидемия используется для оправдания репрессивных изменений в действующем законодательстве, которые после окончания чрезвычайной ситуации сохранятся надолго. Для улучшения ситуации многими государствами было принято решение об ограничении основных прав человека, включая цифровые права и право на передвижение. Мы считаем соблюдение цифровых прав человека основополагающим условием обеспечения неприкосновенности частной жизни, личной и семейной тайны, свободы слова, свободы передвижения, иных прав человека, вне зависимости от чрезвычайности сложившегося положения. Баланс соблюдения прав и свобод человека и ограничительных мер имеет критически важное значение для сохранения психического и эмоционального здоровья нации,

обеспечения чувства безопасности, снижения социальной напряженности в обществе» [Pandemic Big Brother, 2020]. Также ею было отмечено: «Современные технологии должны рассматриваться как средство поддержки свободы коммуникации, информационного взаимодействия и упрощения решения проблем пандемии коронавируса, которое может нести в себе опасность ущемления прав человека. Поэтому мы призываем государства гарантировать использование технологий для отслеживания передвижения и слежения за гражданами (инвазивных технологий слежения) исключительно в соответствии с законодательными ограничениями, позволяющими соблюдать права человека. Подобная гарантия правомерного использования информационных технологий позволит предотвратить злоупотребления и снизить количество административных и уголовных дел в данной сфере. Новые возможности государства, обусловленные совершенствованием технологий и возможностью доступа к информации о геолокации мобильных устройств, создают угрозу неприкосновенности частной жизни, свободе передвижения, выбору места жительства и свободе собраний, и способны подорвать доверие граждан к органам государственной власти» [Pandemic Big Brother, 2020].

«Приложения не могут быть использованы для массового наблюдения. Частные лица будут держать под контролем свои данные. Приложения должны использоваться только во время кризиса и быть деактивированы не позднее, чем по окончании пандемии», – заявил еврокомиссар по вопросам юстиции Дидье Рейндерс депутатам Европарламента [РосКомСвобода, 2020]. Однако защитники конфиденциальности заявили, что реальный риск, вызванный расширением технических решений для наблюдения, заключается в том, что слежка может продолжаться еще долго после того, как пандемия закончится. По словам Фанни Хидвеги из Access Now, «защита цифровых прав также способствует общественному здоровью», но приостановление прав на защиту данных в Венгрии показывает, почему Евросоюз должен действовать активнее в этом вопросе.. Европейская комиссия рассматривает возможность введения временного запрета на использование технологии распознавания лиц [РосКомСвобода, 2020].

Выводы

Таким образом, можно выделить следующие угрозы и риски в сфере цифровых прав граждан, возникшие в ходе пандемии 2020 года:

− угрозы, связанные с процедурами сбора, хранения и обеспечения ограниченного доступа к данным;

− угрозы приватности, риски массовой утечки данных и мошенничества;

− угрозы изменение поведения человека под наблюдением;

− риск незаконных действий государственных органов в отношении персональных данных;

− риск незаконного использования биометрических данных (законодательство не предусматривает хранение или обработку биометрических данных как возможное решение для борьбы с пандемией, обработка биометрических данных законна только с письменного согласия человека или для ряда других случаев, например, для оперативно-розыскных мероприятий);

− непрозрачность и неподконтрольность существующих систем сбора данных для общественности;

− несоответствие оборудования для видеонаблюдения требованиям закона и сертификации;

− риски технических сбоев со стороны государственных сервисов и приложений.

Рассмотренные проблемы должны решаться комплексно в рамках трех направлений:

− информирование общественности об изменениях в цифровых правах;

− взаимодействие со специализированными общественными организациями;

− вынесение проблемы в политическое и правовое поле.

Библиографический список

1. Городнова Н. В. Применение Smart-технологий: оценка влияния на развитие человеческого капитала / Н. В. Городнова, Д. Л. Скипин, И. С. Роженцов // Креативная экономика. 2019. Т. 13, № 10. С. 1837–1858.

2. ИИ и контроль коронавируса Ковид-19 // Обзор, проведенный секретариатом CAHAI. 2020. URL: https://www.coe.int/en/web/artificial-intelligence/ii-i-kontrol-koronavirusa-kovid-19. (Дата обращения: 12.03.2020).

3. Кан А. Ф. Данные отслеживания КОВИД-19 и риски, связанные с надзором, являются более опасными, чем их польза / А. Ф. Кан, Дж. Вейслемляйн // NBC News: сайт. 2020. 19 марта. URL: https://www.coe.int/en/web/artificial-intelligence/ii-i-kontrol-koronavirusa-kovid-19. (Дата обращения: 19.03.2020).

4. Коряковцева О. А. Кризис идентичности молодежи и становление Гражданина / О. А. Коряковцева, Т. В. Бугайчук // Вестник Вятского университета. 2019. №2 (132). С. 91–98.

5. Лоран А. COVID-19: Государства используют геолокацию, чтобы знать, кто соблюдает режим изоляции // Usebk & Rica: сайт. 2020. 20 марта. URL: https://usbeketrica.com/article/covid-19-la-geolocalisation-pour-savoir-qui-respecte-confinement. (Дата обращения: 20.03.2020).

6. Ляпунов К. Роботы против коронавируса. Как цифровизация помогает бороться с COVID-19. LENTA.RU: сайт. 06.04.2020. URL: https://lenta.ru/articles/2020/06/04/robots/. (Дата обращения: 06.04.2020).

7. Мкртумова А. А. Трансформация роли человека в условиях цифровизации экономики // Креативная экономика. 2019. Т. 13, № 6. С. 1163–1168.

8. Поллард М. Даже носящие маски могут быть идентифицированы, утверждает китайская фирма по распознаванию лиц // Рейтер: сайт. 2020. 9 марта. URL:https://www.reuters.com/article/us-health-coronavirus-facial-recognition/even-mask-wearers-can-be-idd-china-facial-recognition-firm-says-idUSKBN20W0WL. (Дата обращения: 09.03.2020).

9. Ромм Т. Правительство США и технологическая индустрия обсуждают способы использования данных о местоположении смартфонов для борьбы с коронавирусом / Т. Ромм, Э. Двоскин, С. Тимберг // The Washington Post: сайт. 2020. 18 марта. URL: https://www.washingtonpost.com/technology/2020/03/17/white-house-location-data-coronavirus/. (Дата обращения: 18.03.2020).

10. Пандемия и системы распознавания лиц: пора сворачивать? Рос КомСвобода: сайт. 2020. URL: https://roskomsvoboda.org/58723/ https://euobserver.com/coronavirus/148387. (Дата обращения: 20.05.2020).

11. Публичная политика. Институты, цифровизация, развитие : коллективная монография / под ред. Л. В. Сморгунова. Москва : Аспект-пресс, 2018. 249 с.

12. РосКомСвобода: официальный сайт. Москва. URL: http://roskomsvoboda.org/56935/. (Дата обращения: 13.03.2020).

13. Трофимова Т. В. Цифровые технологии в обеспечении деятельности органов государственной власти / Т. В. Трофимова, А. В. Ломовцева // Креативная экономика. 2019. Т. 13, № 2. С. 261-270.

14. Фролов В. Г. Применение методов политико-экономического анализа в целях проведения результативной согласованной промышленной политики в условиях цифровой экономики / В. Г. Фролов, Д. И. Каминченко // Экономика, предпринимательство и право. 2019. Т. 9, №4. С. 289–300.

15. Харари Ю. Н. Мир после коронавируса // The Financial Times: сайт. 2020. 20 марта. URL: https://www.ft.com/content/19d90308-6858-11ea-a3c9-1fe6fedcca75?fbclid=IwAR0N8RvjeYCe9nsadqRh0sh6qse18azhLPnPjPrd3eIe0uLVf4HgOZb2mAs. (Дата обращения: 20.03.2020).

16. Якобович Д. Как бороться с коронавирусом с помощью ИИ и науки о данных // Medium: сайт. 2020. 15 февраля. URL: https://towardsdatascience.com/how-to-fight-the-coronavirus-with-ai-and-data-science-b3b701f8a08a. (Дата обращения: 15.02.2020).

17. GDPR: официальный сайт. URL:https://ogdpr.eu/ru#i-3. (Дата обращения: 16.03.2020).

18. Digital divide 'isolates and endangers' millions of UK's poorest. The Guardian: сайт. 2020. 28 апреля. URL:

http://www.theguardian.com/world/2020/apr/28/digital-divide-isolates-and-endangers-millions-of-uk-poorest. (Дата обращения: 28.04.2020).

19. Freedom House: официальный сайт. URL:https://freedomhouse.org/issues/democracy-during-pandemic. (Дата обращения: 18.03.2020).

20. Fundamental rights implications of COVID-19. FRA. 2020. 20 марта. URL:https://fra.europa.eu/en/themes/covid-19. (Дата обращения: 20.03.2020).

21. Human Rights Watch призывает Россию свернуть «Социальный мониторинг». РосКомСвобода: сайт. 2020. 22 мая. URL: https://roskomsvoboda.org/58842/. (Дата обращения: 22.05.2020).

22. Jakubowska E. COVID-Tech: the sinister consequences of immunity passports. EDRi.org: сайт. 2020. URL: http://edri.org/. (Дата обращения: 20.03.2020).

23. Pandemic Big Brother. Pandemicbigbrother: сайт. 2020. URL: https://pandemicbigbrother.online/ru/. (Дата обращения: 14.04.2020).

24. Privacy Day 2020: пандемия как предлог для нарушений цифровых прав по всему миру. РосКомСвобода: сайт. 2020. URL:https://roskomsvoboda.org/59055/. (Дата обращения: 14.04.2020).

25. Privacy International: официальный сайт. URL: https://www.privacyinternational.org/news-analysis/3858/data-protection-piece-puzzle-do-no-harm-digital-age. (Дата обращения: 01.04.2020).

26. WHO: официальный сайт. Novel Coronavirus 2019/26. 2020. Февраль. URL: https://www.who.int/docs/default-source/searo/whe/coronavirus19/covid-19-sprp-whe-searo-feb-2020.pdf?sfvrsn=9ee49760_2. (Дата обращения: 20.02.2020).

Bibliograficheskij spisok

1. Gorodnova N. V. Primenenie Smart-tehnologij: ocenka vlijanija na razvitie chelovecheskogo kapitala / N. V. Gorodnova, D. L. Skipin, I. S. Rozhencov // Kreativnaja jekonomika. 2019. T. 13, № 10. S. 1837–1858.

2. II i kontrol' koronavirusa Kovid-19 // Obzor, provedennyj sekretariatom CAHAI. 2020. URL: https://www.coe.int/en/web/artificial-intelligence/ii-i-kontrol-koronavirusa-kovid-19. (Data obrashhenija: 12.03.2020).

3. Kan A. F. Dannye otslezhivanija KOVID-19 i riski, svjazannye s nadzorom, javljajutsja bolee opasnymi, chem ih pol'za / A. F. Kan, Dzh. Vejslemljajn // NBC News: sajt. 2020. 19 marta. URL: https://www.coe.int/en/web/artificial-intelligence/ii-i-kontrol-koronavirusa-kovid-19. (Data obrashhenija: 19.03.2020).

4. Korjakovceva O. A. Krizis identichnosti molodezhi i stanovlenie Grazhdanina / O. A. Korjakovceva, T. V. Bugajchuk // Vestnik Vjatskogo universiteta. 2019. №2 (132). S. 91–98.

5. Loran A. COVID-19: Gosudarstva ispol'zujut geolokaciju, chtoby znat', kto sobljudaet rezhim izoljacii // Usebk & Rica: sajt. 2020. 20 marta. URL: https://usbeketrica.com/article/covid-19-la-geolocalisation-pour-savoir-qui-respecte-confinement. (Data obrashhenija: 20.03.2020).

6. Ljapunov K. Roboty protiv koronavirusa. Kak cifrovizacija pomogaet bo-rot'sja s COVID-19. LENTA.RU: sajt. 06.04.2020. URL: https://lenta.ru/articles/2020/06/04/robots/. (Data obrashhenija: 06.04.2020).

7. Mkrtumova A. A. Transformacija roli cheloveka v uslovijah cifrovizacii jekonomiki // Kreativnaja jekonomika. 2019. T. 13, № 6. S. 1163–1168.

8. Pollard M. Dazhe nosjashhie maski mogut byt' identificirovany, utverzhdaet kitajskaja firma po raspoznavaniju lic // Rejter: sajt. 2020. 9 marta. URL:https://www.reuters.com/article/us-health-coronavirus-facial-recognition/even-mask-wearers-can-be-idd-china-facial-recognition-firm-says-idUSKBN20W0WL. (Data obrashhenija: 09.03.2020).

9. Romm T. Pravitel'stvo SShA i tehnologicheskaja industrija obsuzhdajut sposoby ispol'zovanija dannyh o mestopolozhenii smartfonov dlja bor'by s koronavirusom / T. Romm, Je. Dvoskin, S. Timberg // The Washington Post: sajt. 2020. 18 marta. URL: https://www.washingtonpost.com/technology/2020/03/17/white-house-location-data-coronavirus/. (Data obrashhenija: 18.03.2020).

10. Pandemija i sistemy raspoznavanija lic: pora svorachivat'? Ros KomSvo-boda: sajt. 2020. URL: https://roskomsvoboda.org/58723/ https://euobserver.com/coronavirus/148387. (Data obrashhenija: 20.05.2020).

11. Publichnaja politika. Instituty, cifrovizacija, razvitie : kollektivnaja mono-grafija / pod red. L. V. Smorgunova. Moskva : Aspekt-press, 2018. 249 s.

12. RosKomSvoboda: oficial'nyj sajt. Moskva. URL: http://roskomsvoboda.org/56935/. (Data obrashhenija: 13.03.2020)

13. Trofimova T. V. Cifrovye tehnologii v obespechenii dejatel'nosti organov gosudarstvennoj vlasti / T. V. Trofimova, A. V. Lomovceva // Kreativnaja jekonomika. 2019. T. 13, № 2. S. 261-270.

14. Frolov V. G. Primenenie metodov politiko-jekonomicheskogo analiza v celjah provedenija rezul'tativnoj soglasovannoj promyshlennoj politiki v uslovijah cifrovoj jekonomiki / V. G. Frolov, D. I. Kaminchenko // Jekonomika, predprini-matel'stvo i pravo. 2019. T. 9, №4. S. 289–300.

15. Harari Ju. N. Mir posle koronavirusa // The Financial Times: sajt. 2020. 20 marta. URL: https://www.ft.com/content/19d90308-6858-11ea-a3c9-1fe6fedcca75?fbclid=IwAR0N8RvjeYCe9nsadqRh0sh6qse18azhLPnPjPrd3eIe0uLVf4HgOZb2mAs. (Data obrashhenija: 20.03.2020).

16. Jakobovich D. Kak borot'sja s koronavirusom s pomoshh'ju II i nauki o dannyh // Medium: sajt. 2020. 15 fevralja. URL:

https://towardsdatascience.com/how-to-fight-the-coronavirus-with-ai-and-data-science-b3b701f8a08a. (Data obrashhenija: 15.02.2020).

17. GDPR: oficial'nyj sajt. URL:https://ogdpr.eu/ru#i-3. (Data obrashhenija: 16.03.2020).

18. Digital divide 'isolates and endangers' millions of UK's poorest. The Guardian: sajt. 2020. 28 aprelja. URL: http://www.theguardian.com/world/2020/apr/28/digital-divide-isolates-and-endangers-millions-of-uk-poorest. (Data obrashhenija: 28.04.2020).

19. Freedom House: oficial'nyj sajt. URL:https://freedomhouse.org/issues/democracy-during-pandemic. (Data obrashhenija: 18.03.2020).

20. Fundamental rights implications of COVID-19. FRA. 2020. 20 marta. URL:https://fra.europa.eu/en/themes/covid-19. (Data obrashhenija: 20.03.2020).

21. Human Rights Watch prizyvaet Rossiju svernut' «Social'nyj monitoring». RosKomSvoboda: sajt. 2020. 22 maja. URL: https://roskomsvoboda.org/58842/. (Data obrashhenija: 22.05.2020).

22. Jakubowska E. COVID-Tech: the sinister consequences of immunity passports. EDRi.org: sajt. 2020. URL: http://edri.org/. (Data obrashhenija: 20.03.2020).

23. Pandemic Big Brother. Pandemicbigbrother: sajt. 2020. URL: https://pandemicbigbrother.online/ru/. (Data obrashhenija: 14.04.2020).

24. Privacy Day 2020: pandemija kak predlog dlja narushenij cifrovyh prav po vsemu miru. RosKomSvoboda: sajt. 2020. URL:https://roskomsvoboda.org/59055/. (Data obrashhenija: 14.04.2020).

25. Privacy International: oficial'nyj sajt. URL: https://www.privacyinternational.org/news-analysis/3858/data-protection-piece-puzzle-do-no-harm-digital-age. (Data obrashhenija: 01.04.2020).

26. WHO: oficial'nyj sajt. Novel Coronavirus 2019/26. 2020. Fevral'. URL: https://www.who.int/docs/default-source/searo/whe/coronavirus19/covid-19-sprp-whe-searo-feb-2020.pdf?sfvrsn=9ee49760_2. (Data obrashhenija: 20.02.2020).