ПРОЦЕССЫ ЦИФРОВИЗАЦИИ В НА ФОНЕ ВСЕМИРНОЙ ПАНДЕМИИ И ПРАВА ЧЕЛОВЕКА НА НЕПРИКАСНОВЕННОСТЬ ЧАСТНОЙ ЖИЗНИ

Қаражан Бекмырза Серікұлы

bkarazhan@mail.ru
Докторант кафедры международного права
ЕНУ им. Л.Н.Гумилева, Нур-Султан, Казахстан

Всемирная пандемия COVID-19, более известная как коронавирус, привнесла в жизнь обычных граждан и стран непредвиденные вызовы и угрозы. Все мировое сообщество, включая Всемирную организацию здравоохранения, озаботилось вопросом дальнейшего нераспространения столь опасного вируса .По данным ВОЗ по миру на конец августа 2020 года было зарегистрировано почти 25 миллионов подтвержденных случаев заболевания, включая более восемьсот тридцати тысяч летальных исходов [1].

Стремясь ограничить количество новых заражений, правительствам пришлось прибегнуть к чрезвычайным мерам, включая во многих случаях объявление чрезвычайного положения. Казахстан в этом деле не стал исключением. Постановлением Президента

Республики Казахстан от 15 марта 2020 года на территории страны было введено чрезвычайное положение [2]. Были введены специальные ограничительные меры, такие как приостановление деятельности крупных торговых объектов, перевод образовательных услуг, работу большей части государственных служащих на дистанционный режим и.т.д. Длительное нахождение населения в карантине вынудило людей обратить взоры на различные технологий, позволяющих работать дистанционно.

Тревожная ситуация с общественным здравоохранением в этих странах во многом оправдывает введение конкретных ограничительных режимов. Однако, не стоить забывать, что государства должны при этом обеспечить защиту всех прав человека, включая права на неприкосновенность частной жизни и защиту данных, которые закреплены во многих международных договорах по правам человека.

В отличие от наших некоторых соседей, Республика Казахстан пока что не участвует в международных соглашениях по защите персональных данных. Однако, в рамках Совета Европы уже имеется такой международный документ. Конвенция о защите частных лиц в отношении автоматизированной обработки данных личного характера 1981 года устанавливает высокие стандарты защиты персональных данных, которые совместимы и согласованы с другими фундаментальными правами [3].Существует еще модернизированная версия данной конвенции, которая именуется как Конвенция 108+. В соответствии с ней, крайне важно, чтобы принципы защиты данных соблюдались даже в особо сложных ситуациях, и поэтому обеспечивается информирование субъектов об обработке связанных с ними персональных данных; обработка персональных данных осуществляется только в случае необходимости, в соответствии с законной преследуемой цели; оценка воздействия проводится до начала обработки; обеспечивается конфиденциальность и принимаются соответствующие меры для защиты безопасности данных, в частности, когда они связаны с особыми категориями данных, такими как данные, связанные со здоровьем.

Одним из основных принципов защиты данных, предусмотренных Конвенцией 108+, является принцип законности, согласно которому обработка данных может осуществляться либо на основании согласия субъекта, либо на каком-либо другом основании, установленном законом. Следует отметить, в Пояснительном Докладе к Конвенции 108+ предусмотрено такая законная основа, в частности, включает обработку данных, необходимую для жизненно важных интересов индивидов, и обработку данных, осуществляемую на основе общественных интересов, таких как случай мониторинга опасной для жизни эпидемии [4].

Например, право на защиту данных не препятствует органам общественного здравоохранения предоставлять список медицинских работников (имена и контактные данные) организациям, которым поручено распространение масок. Также нельзя утверждать, что право на защиту данных несовместимо с эпидемиологическим мониторингом. Таким образом, использование информации о местах массового скопления людей, нарушающих требования по ограничению движения или информации для мониторинга за перемещением лиц из сильно зараженной территории, не будет препятствием требованиям по защите данных.

Согласно статье 11 Конвенции 108+ исключения должны быть «предусмотрены законом, уважать сущность основных прав и свобод и являются необходимой и соразмерной мерой в демократическом обществе» [5].В случае применения ограничений эти меры должны приниматься исключительно на временной основе и только в течение периода времени, явно

ограниченного чрезвычайным положением. Также очень важно, чтобы были приняты конкретные меры безопасности и были даны заверения в том, что персональным данным предоставляется полная защита.

При условии, что главенство человека и принятие профессиональных стандартов являются руководящими ценностями в области лечения, обработка данных, связанных со здоровьем, должна гарантировать уважение прав и основных свобод каждого человека, в частности права на неприкосновенность частной жизни и защите личных данных. Рекомендация CM / Rec (2019) 2 относительно данных, связанных со здоровьем, содержит конкретные меры в этом отношении [6]. Его положения об обмене данными между специалистами здравоохранения и между сектором здравоохранения и другими секторами должны, в частности, служить руководством для соответствующих специалистов.

В этой связи, нельзя не упомянуть новый Кодекс Республики Казахстан от 7 июля 2020 года «О здоровье народа и системе здравоохранения», где в пункте 4 статьи 60 говорится, что передача персональных медицинских данных в Национальный электронный паспорт здоровья и электронные информационные ресурсы уполномоченного органа осуществляется без согласия физического лица [7].

Связь с общественностью со стороны органов здравоохранения и государственных органов должна оставаться приоритетом, чтобы обеспечивать защиту, информирование и консультирование общественности. Тем не менее, во время такой коммуникации следует избегать публикации конфиденциальных данных (таких как данные, связанные со здоровьем) конкретных лиц, и рекомендуется, чтобы обработка таких данных производилась только в том случае, если дополнительные технические и организационные меры дополняют эти применяются к не конфиденциальным данным.

Поскольку большие объемы данных и базы данных создаются с использованием преимуществ методов и технологий обработки данных, таких как *BigData* или искусственный интеллект, эти данные должны обрабатываться в таких средах таким образом, чтобы уважать человеческое достоинство и защиту данных. Соответствующее руководство, разработанное Комитетом Конвенции 108 в контексте больших данных и искусственного интеллекта, может быть полезным инструментом как для разработчиков, так и для правительств, чтобы формировать такую обработку таким образом, чтобы защитить от добровольного неправильного использования или непреднамеренных негативных последствий, включая дискриминацию отдельные лица или группы лиц. Этот вопрос приобретает большую актуальность и в нашей стране, поскольку технологии тотального контроля придут к нам в недалеком будущем. Напомним, Президент РК уже проявлял большой интерес китайскому опыту в процессах обеспечения безопасности посредством использования технологии видеонаблюдения производства китайской компании *Hikvision* [8].

Работодатели также столкнулись с трудностями в поддержании своего бизнеса или деятельности, защищая общественность и своих сотрудников, очень часто их сотрудники работают удаленно. Однако такая практика не должна приводить к мониторингу сотрудников, в том числе с помощью видео. При организации работы в таких условиях следует продумать меры ненавязчивого вмешательства. В данных обстоятельствах работодателям, возможно, придется обрабатывать личные или конфиденциальные данные, которые они обычно не обрабатывают (например, данные, связанные со здоровьем). Поэтому следует помнить, что

при этом они должны уважать принципы необходимости, соразмерности и подотчетности, а также должны руководствоваться принципами, разработанными для минимизации любых рисков, которые такая обработка может представлять для прав и основных свобод сотрудников, в частности их прав. конфиденциальности, как это подробно описано в Рекомендации CM / Rec (2015) 5 по обработке персональных данных в контексте занятости. В частности, работодатели не должны обрабатывать персональные данные сверх того, что необходимо для идентификации потенциально уязвимых сотрудников. Если по закону от них требуется раскрыть определенные данные государственным органам по соображениям общественного здравоохранения, им предлагается сделать это в строгом соответствии с основной правовой базой с целью принятия необходимых мер для возврата к «нормальной» обработке (включая безвозвратное удаление) после прекращения действия режима чрезвычайного положения.

Телекоммуникационные компании, онлайн-платформы и поставщики интернет-услуг также активно участвуют в борьбе с распространением COVID-19, и от них все чаще требуется делиться данными подписчиков, личной информацией, которую они собирают, и другими видами информации с государственными органами, чтобы внести заметный вклад в эпидемиологический надзор, включая анализ пространственных данных для определения местонахождения возможно зараженных людей. Аналогичным образом частные и государственные организации могут разрабатывать ИТ-решения для эпидемиологического надзора. Масштабная обработка персональных данных может быть выполнена только тогда, когда на основе научных данных потенциальные преимущества такого цифрового надзора за эпидемией (например, отслеживание контактов) для общественного здравоохранения (например, отслеживание контактов), включая их точность, перевешивают преимущества других альтернативных решений, которые были бы меньше навязчивый. Разработка этих решений для наблюдения должна основываться на предварительной оценке вероятного воздействия планируемой обработки данных на права и основные свободы субъектов данных, а также должна планироваться обработка данных таким образом, чтобы предотвратить или минимизировать риск вмешательство в эти права и основные свободы.

Школы и университеты прилагают все возможные усилия для повышения навыков и ресурсов дистанционного обучения, при этом профессора и учителя сами сталкиваются с проблемой изоляции. При рассмотрении технических решений, направленных на обеспечение непрерывности образовательной работы, следует отдавать предпочтение стандартным конфигурациям, ориентированным на защиту данных, например, в отношении настроек по умолчанию, чтобы использование приложений и программного обеспечения не нарушало права субъектов данных и избежать обработки большего количества данных, чем необходимо для достижения законной цели обеспечения непрерывности обучения. Также крайне важно, чтобы была выбрана надлежащая правовая основа (включая одобрение родителей или законного опекуна, если это необходимо), и чтобы родители извлекали выгоду из максимальной прозрачности в отношении обработки данных их детей. Дополнительные руководящие принципы относительно обработки персональных данных в контексте образования в настоящее время разрабатываются Комитетом Конвенции 108 и будут полезны для практиков и лиц, принимающих решения.

Мир сейчас переживает трудные времена. Ситуация быстро развивается и правительства принимают в меру своих возможностей различные меры для защиты населения. Но они должны делать это, не подвергая общество большему риску, обеспечивая сохранность всех персональных данных индивидов. Только в таких условиях, при полном уважении верховенства закона, прав человека и демократии мир сможет преодолеть эту нелегкую ситуацию.

Список использованной литературы

1. WHO Coronavirus Disease (COVID-19) Dashboard / WHO official website URL: https://covid19.who.int/ (date of access 25.08.2020)

2. Постановление Президента Республики Казахстан «О введении чрезвычайного положения в Республике Казахстан» от 15 марта 2020 года / Официальный сайт Президента Республики Казахстан URL: http://www.akorda.kz/ru/legal_acts/decrees/o-vvedenii-chrezvychainogo-polozheniya-v-respublike-kazahstan (дата обращения: 25.08.2020)

3. Конвенция о защите частных лиц в отношении автоматизированной обработкиданных личного характера 1981 года / Официальный сайт Совета Европы URL: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680078c46 (дата обращения: 27.08.2020)

4. Пояснительный Доклад к Конвенции о защите частных лиц в отношении автоматизированной обработкиданных личного характера 1981 года / Официальный сайт Совета Европы URL: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016800ca434 (дата обращения: 30.08.2020)

5. Конвенция 108+ / Официальный сайт Совета Европы URL: https://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f1 (дата обращения: 30.08.2020)

6. Recommendation CM/Rec(2019)2 of the Committee of Ministers to member States on the protection of health-related data / The official website of European Council / URL: https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=090000168093b26e (date of access 30.08.2020)

7. Кодекс Республики Казахстан от 7 июля 2020 года № 360-VI «О здоровье народа и системе здравоохранения» / Аналитическо-правовая система «Параграф» URL: https://online.zakon.kz/document/?doc_id=34464437#pos=1679;-55&sdoc_params=text%3D%25D0%25BF%25D1%2580%25D0%25B5%25D0%25B7%25D1%2583%25D0%25BC%25D0%25BF%25D1%2586%25D0%25B8%25D1%258F%26mode%3Dindoc%26topic_id%3D34464437%26spos%3D1%26tSynonym%3D1%26tShort%3D1%26tSuffix%3D1&sdoc_pos=0 (дата обращения: 30.08.2020)

8. АсемгульМухиткызы. «Распознает даже людей в масках». Нужны ли Казахстану камеры Hikvision? / Новостной портал Радио азаттык URL: https://rus.azattyq.org/a/kazakhstan-china-survelliance-camera/30210035.html (дата обращения: 30.08.2020)