Организация Объединенных Наций A/76/220

Генеральная Ассамблея

Distr.: General
23 July 2021
Russian
Original: English

Семьдесят шестая сессия
Пункт 75 b) предварительной повестки дня*
Поощрение и защита прав человека: вопросы прав человека, включая альтернативные подходы в деле содействия эффективному осуществлению прав человека и основных свобод

Право на неприкосновенность частной жизни

Записка Генерального секретаря

Генеральный секретарь имеет честь препроводить Генеральной Ассамблее доклад, подготовленный Специальным докладчиком по вопросу о праве на неприкосновенность частной жизни Джозефом А. Каннатачи, представленный в соответствии с резолюцией 28/16 Совета по правам человека.

* A/76/150.

21-10203X (R) 170821 190821

Доклад Специального докладчика по вопросу о праве на неприкосновенность частной жизни Джозефа А. Каннатачи

Резюме

В настоящем докладе Специальный докладчик по вопросу о праве на неприкосновенность частной жизни Джозеф А. Каннатачи стремится пролить дополнительный свет на то, как можно вести борьбу с пандемией, обеспечивая при этом право на неприкосновенность частной жизни. Опираясь на доклад Специального докладчика, представленный Генеральной Ассамблее в 2020 году (A/75/147), он предлагает в этот раз более взвешенный анализ, поскольку накопленный к настоящему времени больший объем данных позволяет точнее оценить текущую ситуацию с пандемией коронавирусного заболевания (COVID-19). Специальный докладчик, в частности, изучает влияние мер по борьбе с COVID-19 с точки зрения защиты данных, технологий и наблюдения за людьми, и отмечает, что текущие меры, принимаемые государствами для борьбы с распространением COVID-19, продолжают оказывать негативное влияние на осуществление права на неприкосновенность частной жизни, права личности и других взаимосвязанных прав человека. В докладе содержатся рекомендации государственным и негосударственным структурам, касающиеся укрепления прав на неприкосновенность частной жизни и прав личности, обеспечения детям доступа к онлайн-образованию, защиты конфиденциальности личных данных, а также обеспечения прозрачности и сбора данных.

I. Введение

1. Хотя пандемия коронавирусного заболевания (COVID-19) продолжается, се годня в нашем распоряжении имеется больше материала, помогающего понять, как в процессе борьбы с пандемией лучше увязывать право на неприкосновенность частной жизни с эффективными санитарно-эпидемиологическими мерами.

2. Вопрос, поставленный в докладе Специального докладчика Генеральной Ассамблее в 2020 году (A/75/147) — о законности, соразмерности и необходимости нарушений права на неприкосновенность частной жизни в условиях пандемии и их степени , — был призван определить наилучший подход к нынешней и будущим пандемиям. Ответ на него так и не был получен. Ощущается нехватка точных, сопоставимых данных, а недостаточная готовность государств к пандемии и слабые места в механизмах обеспечения подотчетности в сочетании с их политическим контекстом лишь усугубили такое отсутствие прозрачности.

3. Тем не менее цель настоящего доклада — пролить свет на то, как можно вести борьбу с пандемией, обеспечивая при этом право на неприкосновенность частной жизни. Он в значительной степени основан на итогах общественных консультаций по COVID-19, организованных Специальным докладчиком совместно с Глобальной ассамблеей по вопросам неприкосновенности частной жизни и Организацией экономического сотрудничества и развития, которые прошли в период с 21 по 23 июня 2021 года, а также на материалах других исследований[1].

II. Право на неприкосновенность частной жизни, права личности и коронавирусная инфекция

4. Многие меры, принятые государствами для сдерживания распространения COVID-19, негативно повлияли на осуществление права на неприкосновенность частной жизни и других прав человека. Негативные последствия усугубляются существующим структурным неравенством, социальной изоляцией и лишениями. Этот санитарно-эпидемиологический кризис наглядно продемонстрировал взаимозависимость государственного и корпоративного секторов, а также связь между полом, расой, этнической принадлежностью, социально-экономическим положением и состоянием здоровья. Хотя меры по сдерживанию распространения вируса, включавшие ограничения прав человека, затронули всех граждан, на определенные слои общества они оказали несоразмерно сильное воздействие.[2]

5. Специальный докладчик призывает смотреть на неприкосновенность частной жизни шире, чем просто на вопросы конфиденциальности информации[3] и наблюдения за гражданами, уделяя особое внимание положительному, стимулирующему влиянию права на неприкосновенность частной жизни на присущее человеку достоинство, его роли в осуществлении других прав человека и значимости для развития личности любого человека. Это согласуется с подходом,

[1] Ценный вклад в составление и редактирование настоящего доклада внесли проф. Элизабет М. Кумбс, г-н Кетан Мод и г-н Халефом Абраха.

[2] “Epidemics have gendered effects” Clare Wenham, Associate Professor of Global Health Policy, London School of Economics and Political Science, cited by Martha Henriques, 13 April 2020. См. www.bbc.com/future/article/20200409-why-covid-19-is-different-for-men-and-women.

[3] Иногда этот термин ошибочно приравнивается к более узкому термину «конфиденциальность данных».

согласно которому неприкосновенность частной жизни рассматривается не как отдельное право человека, существующее в вакууме, а в контексте его связи с другими правами, особенно с теми, осуществление которых оно стимулирует или обеспечивает иным образом. Таким образом, неприкосновенность частной жизни является важной предпосылкой права на беспрепятственное развитие личности, конкретно закрепленного в статье 22 Всеобщей декларации прав человека 1948 года: «Каждый человек… имеет право … на осуществление необходимых для поддержания его достоинства и для свободного развития его личности прав». Статья 29 Декларации также защищает право на развитие личности: «Каждый человек имеет обязанности перед обществом, в котором только и возможно свободное и полное развитие его личности». Один из наиболее показательных примеров увязки права на неприкосновенность частной жизни с правом на защиту личности в работе Организации Объединенных Наций с момента опубликования Декларации можно найти в резолюции 34/7 Совета по правам человека о праве на неприкосновенность частной жизни в цифровой век, в которой Совет признает, что «право на неприкосновенность частной жизни может способствовать осуществлению других прав и свободному развитию личности и самосознания человека, а также способности человека участвовать в политической, экономической, социальной и культурной жизни, и с обеспокоенностью отмечая, что нарушения или ущемление права на неприкосновенность частной жизни могут негативно сказываться на осуществлении других прав человека, в том числе права свободно выражать свои мнения и беспрепятственно придерживаться их и права на свободу мирных собраний и ассоциации». Таким образом, в процессе сбора затрагивающих права человека полных данных о нем, необходимых для успешного принятия мер по борьбе с COVID, следует учитывать ряд прав, которые тесным образом переплетаются во все более сложный клубок бла годаря применению целого ряда технологий, в частности, бла годаря доступу в Интернет, возможностям фотографии и телефонии, которые объединены в одном устройстве – современном смартфоне.

6. Как четко указано в тексте, первый доклад Специального докладчика о пандемии COVID-19, как и настоящий документ, неизбежно носит промежуточный характер, опираясь на эмпирические данные, которые имелись спустя всего четыре месяца с начала пандемии. Основная цель доклада заключалась в том, чтобы обозначить соответствующие органы и правовую основу для реализации санитарно-эпидемиологических мер и обеспечения права на неприкосновенность частной жизни. В этом докладе не раскрывалось влияние противопандемийных мер на все аспекты права на неприкосновенность частной жизни и различное влияния мер, предпринимаемых в связи с COVID, на разные группы общества, особенно на те из них, которые находятся в уязвимом и маргинальном положении. Эти важные вопросы отражают качество общества и его институтов управления. Успех или провал усилий по обеспечению учета всех прав человека в процессе борьбы с пандемией является мерой этого качества.

7. В докладе, представленном Специальным докладчиком Совету по правам человека в 2021 году (A/HRC/46/37)[4], подчеркивается влияние COVID-19 на частную жизнь детей. Закрытие школ затронуло примерно 90 процентов учащихся по всему миру. Загрузки образовательных приложений в 2020 году выросли на 90 процентов по сравнению со средним недельным значением конца 2019 года.

8. Переход к обучению в режиме «онлайн» усилил существующий дисбаланс сил во взаимоотношениях между компаниями, занимающимися образовательными технологиями, и детьми, а также между правительственными органами,

[4] A/75/147.

детьми и родителями. Правительства ряда стран отменили законы о защите детских данных, обеспечивающих неприкосновенность частной жизни детей. В других регионах, например, в некоторых австралийских штатах, в государственных школах не существует защиты прав детей на неприкосновенность частной жизни, хотя к цифровой информации об успеваемости детей широкий доступ имеют и негосударственные субъекты. Эта цифровая информация позволяет, в частности, узнать мыслительные способности ребенка, прогнозируемый путь в системе образования, степень его интереса к учебе, скорость реакции, а также то, сколько он читает и какие видеоматериалы смотрит.

9. Нельзя отделить борьбу с пандемией от образования, равно как нельзя игнорировать связь между образованием, неприкосновенностью частной жизни и борьбой с пандемией. Когда пандемия вынуждает проводить все больше уроков в режиме «онлайн», влияние на неприкосновенность частной жизни может быть хоть и скрытым, но довольно существенным. Это подтверждает тот факт, что в большинстве стран образование является обязательным с раннего возраста, и большинство детей и родителей не могут оспаривать правила конфиденциальности, устанавливаемые компаниями, которые занимаются образовательными технологиями, или отказаться предоставлять данные, несмотря на обоснованные опасения. Например, проведенный в конце 2020 года анализ 496 образовательных приложений в 22 странах показал, что многие из них собирают данные, позволяющие идентифицировать устройства, 27 приложений получают данные о местоположении пользователя, а 79 из 123 приложений, протестированных вручную, обмениваются данными пользователей с третьими сторонами, например, с партнерами из рекламной сферы. Указываются угрозы безопасности данных. Компания "Майкрософт", например, сообщила о 5,7 миллионах инцидентов, связанных с вредоносными программами, с которыми столкнулись пользователи ее образовательного программного обеспечения в период с 24 августа по 24 сентября 2020 года.[5]

10. На первый взгляд простые меры по сдерживанию коронавируса привели к непредвиденным последствиям, некоторые из которых актуальны для защиты неприкосновенности частной жизни человека. Установление разных дней, когда мужчины и женщины могут покидать свои дома по важным делам, таким как приобретение продуктов питания и получение медицинских услуг[6], отрицательно сказалось на сообществах трансгендеров.[7] Ограничение свободы передвижения людей по половому признаку увеличивает риски для лесбиянок, геев, бисексуалов, трансгендеров и интерсексов (ЛГБТКИ), которых сотрудники безопасности и полиции могут целенаправленно выявлять и подвергать насилию во время проверки документов. С момента начала пандемии закрепляющие гендерную принадлежность медицинские услуги, от которых может зависеть жизнь человека, во многих государствах часто исключались из числа жизненно важных.

11. С неприкосновенностью частной жизни также связаны физическая неприкосновенность и автономия человека. Домашнее помещение по самой своей природе лучше защищает частную жизнь от посторонних, однако необходимость находиться в нем постоянно во время пандемии может создать проблемы

[5] См. Quentin Palfrey and others, “Privacy considerations as schools and parents expand utilization of Ed Tech apps during the COVID-19 pandemic”, International Digital Accountability Council, 1 September 2020. URL: https://digitalwatchdog.org/wp-content/uploads/2020/09/IDAC-Ed-Tech-Report-912020.pdf.

[6] К этим странам относятся, в частности, Панама и Перу. URL: www.reuters.com/article/us-health-cronavirus-peru-idUSKBN21K39N, апрель 2020.

[7] Гендерная идентичность подпадает под действие принципов неприкосновенности частной жизни. См. Комитет по правам человека, *Г. против Австралии*, (CCPR/C/119/D/2172/2012), п. 7.2.

по другим причинам. Сообщалось о росте числа случаев бытового гендерного насилия со стороны интимных партнеров и членов семьи во время карантина.[8] Для некоторых детей карантинные меры увеличили риск подвергнуться физическому или психологическому насилию дома и ограничили возможность контакта со взрослыми, которым они могли бы сообщить о таком насилии.[9]

12. Оценка ситуации с правами человека до начала и во время пандемии могла бы снизить указанные выше риски, и поэтому в будущем она должна стать важным направлением работы, имеющим политическое значение.

III. Неприкосновенность частной жизни, иные права человека и коронавирусная инфекция

13. Пандемия заставила обратить внимание на вопросы прав и их места в демократии. В 10 из 13 стран, в которых опрос проводился как в 2020, так и в 2021 году, ощущение социального раскола с начала пандемии существенно усилилось.[10] Например, хотя паспорта вакцинации призваны расширить возможность пользования правами и ослабить ограничения на поездки, их не могут получить те, кто не имеет доступа к вакцинам, не может быть вакцинирован по медицинским показаниям или решил не проходить вакцинацию. Доля мирового населения, которая в сумме попадает в эти категории, в настоящее время очень велика.[11]

14. Люди по всему миру по просьбе своих правительств пожертвовали частью своей частной жизни и свобод, с тем чтобы победить коронавирус. Меры, принятые различными странами, затронули свободу выражения мнений (57 стран); свободу собраний (147 стран); а также право на неприкосновенность частной жизни (60 стран).[12] Давно назрела необходимость провести оценку соразмерности и необходимости этих посягательств на права людей.

15. Поскольку меры эпидемиологического надзора за распространением COVID-19 сохраняются и даже расширяются, правительственные органы получают более широкий доступ к личным данным, позволяющим узнать местонахождение, историю болезни и другую конфиденциальную информацию о жизни и финансовом положении людей. Похоже, что некоторые государства не готовы отказаться от своих новых полномочий и инструментов контроля за населением после того, как санитарно-эпидемиологический кризис отступит. В Китае применение приложения, разработанного для отслеживания распространения коронавируса, в некоторых городах переводится на постоянную основу. Еще большее беспокойство вызывает тот факт, что «новая система использует программное обеспечение для введения карантина и, по-видимому, отправляет личные данные в полицию, что является тревожным прецедентом автоматизированного

[8] См. COVID-19 and increase in gender-based violence and discrimination against women, Joint call by the EDVAW Platform of independent United Nations and regional expert mechanisms on violence against women and women's rights on combating the pandemic of gender-based violence against women during the COVID-19 crisis, 20 July 2020. URL: https://rm.coe.int/edvaw-statement-covid-19-and-vaw-final/16809efd2c.

[9] A/HRC/46/19, пункт 17.

[10] См. опрос исследовательского центра «Пью», проведенный в период с 1 февраля по 26 мая 2021 года с охватом 18 850 взрослых респондентов в 17 странах с развитой экономикой. URL: www.pewresearch.org/fact-tank/2021/06/24/eu-seen-favorably-across-17-advanced-economies-but-views-vary-on-its-coronavirus-response/.

[11] См. OECD, "Access to COVID-19 vaccines: global approaches in a global crisis", OECD Policy Responses to Coronavirus (COVID-19) (18 March 2021).

[12] См. International Center for Not-for-Profit Law, COVID-19 Civic Freedom Tracker. URL: www.icnl.org/covid19tracker/?issue=5.

контроля за обществом». [13] Хотя эти риски, как утверждается, особенно актуальны в Азии,[14] во всех странах, в том числе в демократических, власти могут использовать личные данные в политических целях, что будет сопровождаться ограничением действия прав человека. Чрезвычайные меры по борьбе с пандемией создают риски, требующие принятия чрезвычайных мер защиты[15].

IV. Защита данных, технологии, эпидемиологический надзор и коронавирусная инфекция

16. Данные, связанные с COVID-19, – это данные о состоянии здоровья человека, которые являются первой категорией персональных данных, требующих особого уровня защиты в соответствии с международным, региональным и национальным законодательством. Хотя общая концепция защиты данных о здоровье человека уже стала предметом всеобъемлющих рекомендаций[16] и подробного пояснительного меморандума[17], представленного Специальным докладчиком Генеральной Ассамблее в октябре 2019 года, по оценкам, примерно 75 процентов государств-членов Организации Объединенных Наций в значительной мере не удовлетворяют стандартам, изложенным в этих документах. Все имеющиеся данные свидетельствуют о том, что эти проблемы усугубились в связи с пандемией COVID-19.

17. Эффективное реагирование на санитарно-эпидемиологический кризис требует не только сбора и использования конфиденциальных данных, но и надежных гарантий неприкосновенности частной жизни. Однако во многих случаях системы, ограничивающие возможность обработки данных конкретными медико-санитарными целями, отсутствовали и продолжают отсутствовать.

18. Во многих странах отсутствуют гарантии прозрачности процедур обработки данных и защиты от утечки данных. В других случаях существующие требования, предъявляемые к защите данных, не соблюдаются: например, цифровой COVID-сертификат Европейского союза, предложенный Европейской комиссией 17 марта 2021 года, через год после объявления пандемии в марте 2020 года, не прошел оценку на возможные последствия его использования: «ввиду срочности вопроса оценка возможных последствий Комиссией не проводилась».[18]

19. Такие недостатки подрывают санитарно-эпидемиологические усилия и доверие к ним со стороны общества. Шестьдесят процентов американцев, например, считают, что отслеживание властями местонахождения людей с помощью

[13] Paul Mozur, Raymond Zhong and Aaron Krolik, “In Coronavirus fight, China gives citizens a color code, with red flags”, *The New York Times*, 1 March 2020, обновлено 28 января 2021 года.

[14] См. Sofia Nazalya, “Human Rights Outlook 2020”, 30 September 2020.

[15] См. Graham Greenleaf, “COVID-19: the available evidence … and a little bit of hindsight”, 23 June 2021.

[16] www.ohchr.org/Documents/Issues/Privacy/SR_Privacy/UNSRPhealthrelateddataRecCLEAN.Pdf.

[17] www.ohchr.org/Documents/Issues/Privacy/SR_Privacy/MediTASFINALExplanatoryMemoradum1.pdf.

[18] См. Explanatory Memorandum to European Union Commission’s proposal, sect. 3. URL: eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021PC0130.

их мобильных телефонов вряд ли помогло бы сдержать распространения COVID-19.[19]

20. Данные необходимы для принятия многих мер по борьбе с пандемией, и время показало, что COVID-19 перерос также в «кризис данных». Персональные данные и данные о здоровье человека обрабатывают как правительственные органы, так и технологические компании, что вызывает сомнения по поводу необходимости и пропорциональности сбора данных, методов сбора, безопасности хранения и вторичного использования этих данных.[20] Представители ЛГБТКИ-сообщества особенно обеспокоены возможностью передачи медицинских данных без их согласия.[21] Из-за пандемии COVID-19 почти половина (48 процентов) австралийцев в настоящее время сильнее озабочены вопросами защиты информации о своем местонахождении, а три четверти (75%) считают, что COVID-19 не освобождает бизнес или правительственные органы от исполнения своих традиционных обязанностей в соответствии с законами о неприкосновенности частной жизни.[22]

Технологии

21. Технологии, используемые для борьбы с пандемией, делятся на четыре большие группы:

a) инструменты отслеживания контактов и социального дистанцирования, основанные на контроле расстояния между людьми с использованием технологии Bluetooth;

b) коды быстрого считывания (QR) или штрих-коды, используемые для контроля посещающих общественные места;

c) получение доступа к данным геолокации с использованием архива данных вышек сотовой связи или Глобальной системы позиционирования (GPS) для предупреждения людей о возможной близости к тем, у кого тест на COVID-19 дал положительный результат;

d) приложения для записи на вакцинацию или для загрузки сертификатов о прохождении вакцинации.

22. Отсутствуют данные, подтверждающие надежность некоторых технологий. Имеются основания утверждать, что используемые технологии ненадежны. Например, в Израиле люди успешно оспаривали объявленные им карантинные меры, в которых использовалась триангуляция вышек сотовой связи. Из 20 000 человек, подавших жалобы против предписаний об изоляции, 54 процента (примерно 12 000) выиграли дело.[23] В Соединенных Штатах Америки Американский союз гражданских свобод сообщил, что данные вышек сотовой связи неточны.[24]

23. Недостаточно ненадежным было признано и отслеживание дистанции между людьми с использованием технологии Bluetooth. В исследовании,

[19] Опрос проводился исследовательским центром «Пью» в апреле 2020 года. URL: www.pewresearch.org/fact-tank/2020/05/04/how-americans-see-digital-privacy-issues-amid-the-covid-19-outbreak/.

[20] Там же.

[21] A/HRC/40/63 2019, пункт 84.

[22] Office of the Australian Information Commissioner, 2020.

[23] “Over 12,000 mistakenly quarantined by phone tracking, Health Ministry admits”, *The Times of Israel*, 14 July 2020).

[24] См. Jay Stanley and Jennifer Stisa Granick, “The limits of location tracking in an epidemic” (8 April 2020).

посвященном использованию в Германии, Италии и Швейцарии технологий отслеживания дистанции между людьми в трамваях при помощи технологии Bluetooth, было установлено, что надежность обнаружения контакта сродни отправке уведомлений методом случайного отбора.[25] Надежность связана с мощностью сигнала, на которую влияют такие факторы, как различия между разными моделями/версиями мобильных телефонов; изменения в относительной ориентации мобильных телефонов; поглощение сигнала человеческими телами или объемными предметами; и отражение радиоволн от стен, полов и кресел.

Эпидемиологический надзор на основе имеющихся данных

24. «Надзор» — это специальный термин, используемый в эпидемиологических исследованиях и мероприятиях по сдерживанию распространения заболевания. Он также используется применительно к действиям по обеспечению безопасности, связанным, например, со сбором информации и с решением правоохранительных задач. Использование в обеих целях, т.е. в медико-санитарных и в целях обеспечения безопасности, должно быть необходимыми и соразмерными.

25. Необходимость защиты здоровья граждан потребовала от стран прибегнуть к эпидемиологическому надзору для отслеживания распространения инфекции путем:

a) отслеживания контактов в ручном режиме, как на Мальте;[26]

b) использования технологий Bluetooth, GPS, отслеживания с помощью вышек сотовой связи и штрих-кодов/QR-кодов в мобильных телефонах и переносных устройствах в системах, специально разработанных для использования в условиях эпидемий, как, например, в Республике Корея;

c) использования вышек сотовой связи и других источников триангуляции данных, первоначально созданных для ведения скрытой борьбы с терроризмом, но трансформированных для нужд борьбы пандемией, как, например, в Израиле;

d) обязательной проверки на наличие штрих-кодов и QR-кодов при посещении общественных мест, [27] как в Австралии;

e) введения паспортов вакцинации, например, на основе Регламента Европейского Союза о цифровых COVID-сертификатах, с 1 июля 2021 года[28].

26. Процессы сбора и обработки данных из этих источников различаются во всем мире с точки зрения типа собираемых данных, места их хранения, лиц, имеющих к ним доступ, и автономии лиц, чьи данные собираются. Большая часть данных является результатом применения технологий, а также вкладом в процессы с их использованием. Технологическая структура важна с точки

[25] См. Douglas J. Leith and Stephen Farrell, “Measurement-Based Evaluation of Google/Apple Exposure Notification application programme interface for Proximity Detection in a Light-Rail Tram” (2020) PLOS One, vol. 15, e0239943.

[26] Jessica Arena, “What is contact tracing and how is Malta doing it?” *Times of Malta*, 23 March 2020.

[27] См., например, Government of South Australia, “COVID SAfe Check-In” (URL: www.covid-19.sa.gov.au/business-and-events/covid-safe-check-in) and New South Wales Government, “Setting up electronic check-in and QR codes” (URL: www.nsw.gov.au/covid-19/covid-safe/customer-record-keeping/setting-up-electronic-check-and-qr-codes) .

[28] См. https://ec.europa.eu/info/live-work-travel-eu/coronavirus-response/safe-covid-19-vaccines-europeans/eu-digital-covid-certificate_en

зрения доступных гражданам возможностей распоряжаться различными аспектами своего права на неприкосновенность частной жизни.

27. Приложения для отслеживания контактов используют централизованный или децентрализованный подход к данным, будь то для отслеживания контактов или регистрации вакцинации. Централизованный и децентрализованный подходы различаются в первую очередь тем, где хранятся данные и каким способом они обрабатываются. При централизованном подходе, независимо от того, где генерируются данные пользователей, они хранятся и обрабатываются на центральном сервере, управляемом органами здравоохранения, или на серверах частной компании, выбранной правительственными органами.

28. В случае использования приложений для отслеживания контактов, серверы вычисляют постоянно актуализируемые оценки рисков для всех соответствующих пользователей и решают, с какими затронутыми пользователями следует связаться. При регистрации вакцинации серверы хранят данные о запланированных датах вакцинации, типах используемых вакцин и статусе вакцинации каждого человека для административных целей.

29. Централизованные системы позволяют властям анализировать собранные данные, чтобы получить, в частности, представление о распространении пандемии, наиболее сильно пострадавших районах и об уровне охвата населения вакцинацией. Это облегчает распределение ресурсов на основе выбранных приоритетов.

30. В Австралии, например, существует две централизованных системы: приложение для отслеживания расстояния между людьми, работающее на основе технологии Bluetooth (COVIDSafe), и программа контроля входа в общественные места на основе QR-кодов. Приложение COVIDSafe было внедрено путем принятия специального законодательства о гарантиях соблюдения права на неприкосновенность частной жизни. Программа контроля посещений на основе QR-кодов не подкреплена отдельным законодательством, а опирается исключительно на ранее принятые нормативные документы в области медико-санитарного регулирования и действующий Закон «О неприкосновенности частной жизни» 1988 года. Этот недостаток вызывает опасения, поскольку в Австралии отсутствуют конституционные гарантии права на неприкосновенность частной жизни.

31. Республика Корея, имеющая прежний опыт борьбы со вспышкой ближневосточного респираторного синдрома (MERS) в 2015 году, пошла по пути централизованного контроля, используя для этой цели документацию медицинских учреждений, данные систем GPS, транзакций по картам и информацию систем видеонаблюдения.[29] Этот подход позволил определить маршруты передвижения пациентов и риск заражения для окружающих, распределить их контакты на близкие и случайные, а также выбрать тип карантинных мер по отношению к тем, кто вступал в контакт с инфицированными.

32. Аргентина также создала централизованную базу данных для хранения информации, собираемой бла годаря приложению Cuidar, созданному на основании административного решения от 23 марта 2020 года.[30] Установка данного приложения является добровольной для жителей Аргентины, но обязательной для прибывающих из-за границы, а все данные, получаемые бла годаря

[29] См. “Contact transmission of COVID-19 in South Korea: novel investigation techniques for tracing contacts” *Osong Public Health and Research Perspectives*, vol. 11, No. 1 (2020), pp. 60–63.

[30] URL: www.boletinoficial.gob.ar/detalleAviso/primera/227116/20200324 (на испанском языке).

технологии Bluetooth, являются доступными для национальных и местных органов власти.

33. В связи с использованием централизованной архитектуры, в том числе в Австралии, Израиле и Республике Корея, возникает обеспокоенность по поводу защиты и безопасного хранения конфиденциальной информации, в том числе данных о здоровье человека, а также реальной угрозы того, что эта информация может повторно использоваться в централизованных базах данных органов власти и корпораций для иных целей, в том числе для осуществления надзора в политических и коммерческих целях.

34. Граждане не доверяют властям, создающим большие базы персональных данных. Например, большинство австралийцев (60 процентов) согласны с тем, что для борьбы с COVID-19 и ради всеобщего блага необходимо в определенной мере пожертвовать неприкосновенностью частной жизни, если это носит временный характер. Однако свыше половины населения (54 процента) се годня озабочено защитой своей личной информации в связи с теми мерами, которые принимаются для борьбы с COVID-19, больше чем прежде; при этом 26 процентов населения се годня обеспокоены этой проблемой в гораздо больше степени.[31]

35. Децентрализованные приложения предоставляют пользователям больший контроль над своей информацией. Она хранится в их телефонах, а не в центральной базе данных, к которой имеют доступ органы власти или другие организации. Примером широко распространенного децентрализованного подхода является программный интерфейс приложения "Google-Apple Exposure Notification System", в котором уведомления о риске заражения не обрабатываются через центральную базу данных, а автоматически запускаются в локальном режиме на телефонах пользователей.

36. Некоторые страны используют сочетание централизованных и децентрализованных мер. В Сингапуре были созданы переносные устройства отслеживания, оснащенные системой Bluetooth, регистрирующие все контакты с находящимися поблизости устройствами и сохраняя эти данные в течение 25 дней перед удалением.[32] Результатом применения такого подхода стала разработка приложений для мобильных телефонов, позволяющих отслеживать контакты, объявлять карантинные меры, выявлять симптомы заражения и предоставлять информацию о пандемии. Уже в августе 2020 года насчитывалось 46 таких приложений.[33]

37. Скрещивание такой технической архитектуры зависит от того, являются ли принятые технологии обязательными или же добровольными. Приложение можно считать добровольным, если у пользователя есть возможность:

a) вообще не устанавливать приложение;

b) отключить функциональность Bluetooth/GPS;

c) использовать приложение, но отказаться сообщать о положительном диагнозе.

38. Хотя первоначальная реакция на приложения для добровольного отслеживания контактов в Израиле и Австралии была положительной, в конечном итоге

[31] См. 2020 Australian Community Attitudes to Privacy Survey. URL: www.oaic.gov.au/engage-with-us/research/australian-community-attitudes-to-privacy-survey-2020-landing-page/2020-australian-community-attitudes-to-privacy-survey/.

[32] См. “TraceTogether, safer together”. URL: www.tracetogether.gov.sg/.

[33] См. Hanson John Leon Singh, Danielle Couch and Kevin Yap, “Mobile health apps that help with COVID-19 management: scoping review”, *JMIR Nursing*, vol. 3, No. 1 (2020), e20596.

этими приложениями воспользовался лишь небольшой процент населения. В Австралии в соответствии *с Законом 2020 года «О внесении поправок в Закон о неприкосновенности частной жизни (медико-санитарной информации о контактах)»* («Закон о COVIDSafe»), требование принуждать к использованию приложения COVIDSafe считается правонарушением[34], и первоначальная общественная реакция на него оказалась положительной. Однако, несмотря на положительную оценку со стороны 70% опрошенных, в настоящее время приложение «отнюдь не похоронено». [35] Власти австралийских штатов, похоже, в большей степени полагаются на систему обязательного контроля граждан при посещении общественных мест с использованием QR-кодов. Республика Корея является примером проявления национальной политической инициативы, с самого начала пойдя по пути обязательного отслеживания местоположения, и, по мнению некоторых, ее успешная борьба с пандемией объясняется обязательным характером избранных мер.[36]

39. Согласие и возможность отозвать его являются неотъемлемой частью права на неприкосновенность частной жизни. Реализация данного права невозможна, если требование использовать приложения для отслеживания контактов носит обязательный характер. Принудительные меры также повышают риск того, что органы власти и корпорации будут неправомерно использовать данные, собранные в целях борьбы с пандемией, путем «постепенного усиления надзора» или перепрофилирования данных для использования в иных целях в отсутствии у поставщиков данных возможности удалить их из баз данных.

Выход за рамки допустимого?

40. Многие страны оказались недостаточно подготовлены к росту заболеваемости и смертности. Некоторые и них посчитали необходимым устранять риски для здоровья и жизни своих граждан любыми доступными средствами. Сознательно или неосознанно власти некоторых государств при принятии мер «вышли за рамки допустимого» с точки зрения прав человека и тех принципов, которые считаются правильными и приемлемыми в демократических обществах.

41. Доступные методы надзора «по санитарно-эпидемиологическим причинам», а также для сбора информации или обеспечения безопасности иногда сливаются и размываются, теряя важные отличительные признаки и различия. В условиях появления добровольных вариантов, поддерживаемых гражданами, такое поведение государств демонстрирует, как правом на неприкосновенность частной жизни и автономию граждан можно пренебречь.

---

[34] См. статью 94H *Закона 2020 года «О внесении поправок в Закон о неприкосновенности частной жизни (медико-санитарной информации о контактах)»*:

94H. Требование использовать приложения «COVIDSafe».

1) Лицо совершает правонарушение, если оно требует от другого лица:

a) установить приложение «COVIDSafe» на устройство связи; или

b) использовать приложение «COVIDSafe» на устройстве связи; или

c) дать свое согласие на отправку данных COVID-приложения с устройства связи в национальное хранилище данных «COVIDSafe».

Наказание: Заключение под стражу сроком на 5 лет или 300 единиц наказания, или и то, и другое.

[35] Paul M. Garrett and Simon J. Dennis, “Australia has all but abandoned the COVIDSafe app in favour of QR codes (so make sure you check in)”, *The Conversation*, 1 June 2021.

[36] См. Kyung Sin Park, “Korea’s COVID-19 success and mandatory phone tracking” (opennet, 20 October 2020).

Израиль

42. Проиллюстрировать попытку пренебречь правами можно на примере действий правительства Израиля, объявившего 19 марта 2020 года чрезвычайное положение в стране на основе Постановление об общественном здравоохранении 1940 года. [37] Министерство здравоохранения утвердило приложение «HaMagen», которое собирает данные о перемещениях и местоположении пользователей и хранит их во внутренней памяти их сотовых устройств, если только пользователи не предпочтут отправить эти данные в Министерство здравоохранения, где к ним будут иметь доступ сотрудники, представители и поставщики услуг. Таким образом, данное приложение являлось как децентрализованным, так и (добровольно) централизованным.

43. Одновременно с этим правительство Израиля наделило Службу безопасности Израиля полномочиями запрашивать и получать у поставщиков телекоммуникационных услуг данные с вышек сотовой связи без согласия тех, за кем ведется наблюдение. Провайдеры телекоммуникационных услуг были вынуждены отслеживать передвижение тех людей, о которых было известно, что они инфицированы, по записям вышек сотовой связи на основании двух указов о чрезвычайных ситуациях, опубликованных в середине марта 2020 года и наделявших полицию полномочиями запрашивать такие данные в целях определения местонахождения пациентов, проводить выборочные проверки тех лиц, которые были отправлены на карантин, и отслеживать их перемещения в течение срока до 14 предыдущих дней.[38] В апреле 2020 года используемый метод надзора был признан Верховным судом Израиля недействительным, что заставило правительство принять новый закон, который предоставлял бы законные основания для наделения Службы безопасности полномочиями продолжать отслеживать инфицированных в соответствии с законом об Службе безопасности Израиля. В июле 2020 года был принят временный закон о полномочиях Службы безопасности Израиля.

44. В начале 2021 года временная поправка к Постановлению об общественном здравоохранении 1940 года разрешила передачу личной информации о непривитых лицах сотрудникам муниципалитетов, а также органов образования и социального обеспечения. В начале марта 2021 года Верховный суд страны запретил применение закона для организации массового надзора, а затем приостановил действие указанной поправки.

45. Кроме того, сообщалось, что данные о вакцинации использовались для проведения крупных популяционных исследований без согласия населения; придания огласке путей заражения; использования дронов для мониторинга соблюдения домашнего карантина; привлечения компаний, занимающихся генетическими данными, к проведению тестирования на COVID-19 и выноса на обсуждение проекта закона о передаче эпидемиологической информации в полицию.[39]

46. Децентрализованное приложение HaMagen, выпущенное Министерством здравоохранения, вначале было встречено положительно и помогло выявить 30% первоначальных случаев, но затем его применение резко упало из-за утраты обществом доверия к тому, что это приложение обеспечивает неприкосновенность

[37] Greenleaf, “COVID-19: the available evidence … and a little bit of hindsight” (см. сноску 15).

[38] См. David M. Halbfinger, Isabel Kershner and Ronen Bergman, “To track Coronavirus, Israel moves to tap secret trove of cellphone data”, *The New York Times*, 16 March 2020.

[39] Prof. Yuval Shany, Israel’s response to the COVID-19 pandemic: Right to Privacy Aspects, Federmann Cyber Security Research Centre, Hebrew University of Jerusalem; “COVID-19: the available evidence … and a little bit of hindsight” (см. сноску 15).

частной жизни.[40] Меры, предпринимаемые Службой безопасности для отслеживания контактов, по-видимому, имели ограниченную эффективность в силу следующих причин:

a) отсутствия прозрачной информации о преимуществах программы Службы безопасности в абсолютном и сравнительном выражении;

b) технологического уклона в сторону ложного завышения числа случаев заражения.

47. Система, используемая в Израиле, спроектирована по образцу системы противодействия терроризму и основана на соответствующих технологиях. Сообщалось, что с середины марта 2020 года Служба безопасности Израиля помогает правительству Израиля в проведении эпидемиологических расследований, предоставляя Министерству здравоохранения маршруты перемещения переносчиков коронавируса и списки лиц, с которыми они находились в тесном контакте. Информация поступает из базы метаданных Службы безопасности. С марта правительство Израиля пытается усилить парламентский надзор за деятельностью по сбору информации о населении. В отличие от Франции, Нидерландов и Соединенного Королевства Великобритании и Северной Ирландии, Израиль не имеет независимого предусмотренного законом «экспертного органа», способного выступать в качестве независимого надзорного органа, дополняющего работу парламентского комитета. Поэтому сохраняются серьезные сомнения в способности тщательно и эффективно контролировать подобную деятельность спецслужб. Спустя примерно год после того, как подобные посягающие на неприкосновенность частной жизни технологии стали применяться в Израиле для борьбы с пандемией, Верховный суд 1 марта 2021 года дал окончательную оценку выходу Израиля за рамки допустимого, запретив правительству широко использовать систему отслеживания носителей коронавируса с помощью мобильных телефонов, назвав эту меру серьезным нарушением гражданских свобод.[41] Специальный докладчик обращает внимание на сообщения о том, что такие действия, в случае Израиля, также сдерживают разработку приложений, обеспечивающих неприкосновенность частной жизни, и проведение эпидемиологических расследований, и считает, что использование контртеррористических полномочий в чисто санитарно-эпидемиологических целях противоречит международному праву прав человека и создает опасный прецедент.

Республика Корея

48. Правительства других стран, например Республики Корея, также заставляли поставщиков телекоммуникационных услуг отслеживать передвижение лиц, об инфицировании которых была получена информация.[42] Такой надзор был построен на использовании приложения для смартфона вместе с технологиями, традиционно применяемыми в правоохранительных органах и в борьбе с терроризмом, объединяя несколько источников личных данных для построения картины передвижения человека, таких как:

a) операции по кредитным и дебетовым картам, которые могут дать представление о том, где человек делал покупки или где он питался, и каким образом он перемещался по транспортной сети;

[40] Например, см. Mitnick J, “How Israel’s COVID contact tracing app rollout went wildly astray” (CIO, 7 November 2020).

[41] См. Maayan Lubell, *Israeli Supreme Court bans unlimited COVID-19 mobile phone tracking*. URL: www.reuters.com/article/us-health-coronavirus-israel-surveillanc-idUSKCN2AT279.

[42] См. Park, “Korea’s COVID-19 success and mandatory phone tracking” (см. сноску 36).

b) данные журналов регистрации местоположения телефона, полученные от операторов мобильной связи, которые дают приблизительное представление о том, в каком районе находится человек, когда он подключается к разным телефонным вышкам;

c) подробная информация, полученная при помощи разветвленной сети камер наблюдения.

49. Прежде всего следует отметить, что в большинстве известных случаев меры, которые принимались в Республике Корея для борьбы с пандемией COVID-19 и затрагивали право на неприкосновенность частной жизни, имели под собой правовую основу. Они были предусмотрены законом. Поэтому, как всегда, встает вопрос: были ли (являются ли) эти меры необходимыми и соразмерными в демократическом обществе?

50. Чтобы точно ответить на этот вопрос, важно подробно проанализировать, что на самом деле произошло в Республике Корея. Используемые технологии, безусловно, оказались эффективными, позволив существенно сократить количество времени, необходимого для определения очага инфекции и способов ее распространения.

51. С началом распространения COVID-19 правительство Республики Корея преобразовало разрабатываемую им информационную платформу «Умный город» в инструмент санитарно-эпидемиологического надзора. Корейское агентство по контролю и профилактике заболеваний разработало Систему поддержки эпидемиологических расследований – платформу, которая позволяет органам общественного здравоохранения быстро собирать и анализировать данные для отслеживания подтвержденных случаев COVID-19. Система начала работать 26 марта 2020 года, всего через два месяца после первого подтвержденного случая заболевания COVID-19 в стране. С помощью данной системы, после того, как Агентство подтверждает отдельный случай COVID-19, уполномоченные органы запрашивают данные о местонахождении каждого пациента, которые соответствующим образом заносятся в систему согласно Закону страны о контроле и профилактике инфекционных заболеваний. Затем система проводит анализ данных отслеживания в режиме реального времени, который, в сочетании с традиционными опросами для выяснения имевших место контактов, позволяет, с одной стороны, быстро отследить контакты, а с другой, выявлять очаги пандемии. Система дала возможность отслеживать и анализировать подтвержденные случаи COVID-19 менее чем за 10 минут, а не за день или более, как это было до ее внедрения. Конфиденциальность и безопасность данных гарантируются за счет того, что только аналитики Агентства, обладающие необходимыми юридическими полномочиями, могут получить доступ к системе, а также посредством регистрации каждого случая входа в систему для выявления возможных случаев несанкционированного использования данных. Чтобы свести к минимуму объем собираемых личных данных, был установлен максимальный 14-дневный период сбора данных для каждого такого случая, равный продолжительности инкубационного периода заболевания. К тому же система носит временный характер: по окончании пандемии COVID-19 вся личная информация будет уничтожена.[43]

52. Создание описанной выше системы поддержки эпидемиологических расследований стало первой из ряда технологических мер, принятых правительством. Во-вторых, Республика Корея использует приложение для смартфонов,

[43] См. Jiyeon Kim and Neil Richards “South Korea’s COVID success stems from an earlier infectious disease failure”, 29 January 2021. URL: https://slate.com/technology/2021/01/south-korea-mers-covid-united-states-democracy.html.

чтобы контролировать соблюдение правил лицами, находящимися на изоляции или на карантине – теми, у кого подтверждено наличие заболевания COVID-19, теми, кто находился в тесном контакте с лицами, чей диагноз был подтвержден, а также лицами, прибывающими из-за рубежа. Во время пандемии Республика Корея не закрывала своих границ для иностранцев, въезжающих в страну. Вместо этого она разработала специальные въездные процедуры, требующие от въезжающих в страну соблюдения 14-дневного карантина и бесплатного тестирования на COVID-19 в целях предотвращения распространения заболевания. Приложение Self-Quarantine Safety Protection обеспечивает двустороннюю связь, позволяя человеку, находящемуся на карантине, сообщать о любых симптомах заболевания, а уполномоченному сотруднику отслеживать соблюдение карантина посредством получения данных о местоположении через GPS при наличии согласия человека. Мониторинг соблюдения карантина через приложение настоятельно рекомендуется, но не является обязательным. За теми лицами, у кого нет смартфонов, или за теми, кто не соглашается на использование приложения, уполномоченный сотрудник может следить с помощью традиционного метода – телефонных звонков. Тем не менее показатель использования приложения на 1 сентября составил 91,8%, и как граждане Республики Корея, так и путешественники могут быть спокойны и уверены в том, что те люди, которые могут стать распространителями COVID-19, будут соблюдать все необходимые меры самоизоляции.[44]

53. Нижеследующее резюме объясняет некоторые из причин, по которым Специальный докладчик считает, что сбор значительного объема персональных данных ради борьбы с пандемией COVID-19 в определенные периоды времени, особенно в период с января по июнь 2020 года, не был ни необходимым, ни соразмерным:

> раскрытие данных отслеживания контактов (где, когда и как долго такой контакт имел место) помогает людям самостоятельно идентифицировать потенциальные близкие контакты с людьми, у которых подтверждено наличие инфекции. Однако раскрытие информации о местонахождении может представлять опасность для неприкосновенности частной жизни, давая представление о важных местах посещения и обычном поведении человека. Риски для частной жизни в значительной степени зависят от характера мобильности человека, на которую влияют некоторые региональные и политические факторы (например, тип жилья, близлежащая инфраструктура и распоряжения о социальном дистанцировании). Кроме того, результаты показывают, что раскрытые данные, полученные в результате отслеживания контактов в Республике Корея, часто включают излишнюю информацию, например, подробные демографические сведения (возраст, пол, национальность), сведения о социальных связях (родительский дом) и информацию о рабочем месте (название компании). Раскрытие таких персональных данных уже идентифицированных лиц может оказаться бесполезным для отслеживания контактов, целью которого является выявление еще не известных лиц, которые могли находиться в тесном контакте с людьми с подтвержденным диагнозом. Другими словами, для целей отслеживания контактов не столь полезно раскрывать личный профиль лица с подтвержденным диагнозом и его социальные связи, например информацию о его семье или знакомых. Подробные сведения о местоположении рабочего места можно не указывать, поскольку в большинстве случаев с сотрудниками легко связаться по внутренним каналам связи; исключительным случаем может оказаться ситуация, когда есть опасения по поводу потенциального

[44] Там же.

вторичного группового заражения. Точно так же нет необходимости раскрывать подробную информацию о поездках лиц, въезжающих в страну из-за рубежа (которая не была указана в основных сведениях), например, номер рейса прибытия и цель/продолжительность зарубежной поездки.[45]

54. Осуждая вышеупомянутый, на первый взгляд ненужный и несоразмерный, сбор персональных данных, Специальный докладчик также обращает внимание на продолжающиеся последовательные попытки южнокорейского правительства и других институтов усилить защиту конфиденциальности, несмотря на принимаемые для борьбы с COVID-19 меры. Например:

a) в июне и октябре 2020 года Центры по контролю и профилактике заболеваний выпустили руководство с рекомендацией не публиковать сведения о возрасте, поле, национальности, месте работы, истории поездок или местожительстве пациента, хотя некоторые местные органы власти по-прежнему раскрывают некоторые отдельно взятые истории поездок, несмотря на указание не делать этого. Сохраняются опасения по поводу сбора и обработки конфиденциальных персональных данных, которые могут раскрывать сугубо личную информацию, такую как, сексуальная ориентация и личные отношения человека;

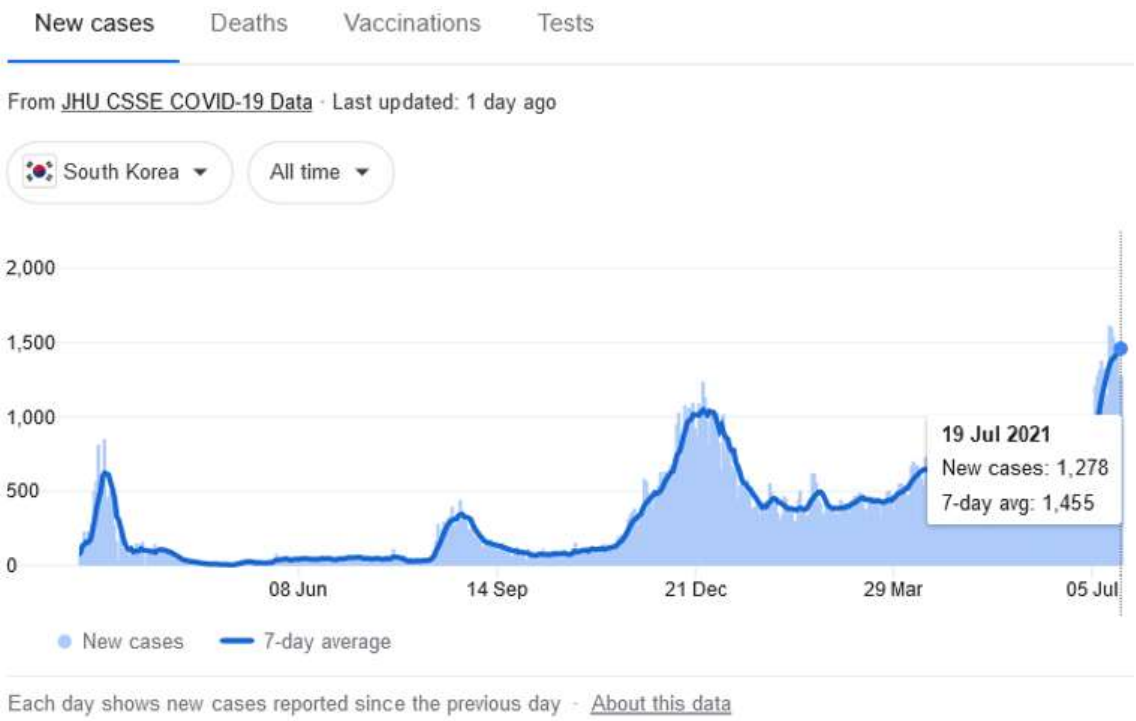
b) в марте 2021 года правительство Республики Корея обратилось к общественности с просьбой в интересах конфиденциальности использовать зашифрованные личные номера вместо номеров телефонов при регистрации входа в рестораны, кафе и так далее, в рамках мер по предотвращению распространения COVID-19. В феврале 2021 года правительство ввело новую меру для защиты права на неприкосновенность частной жизни, позволяющую людям использовать зашифрованные личные номера для посещения таких мест. Зашифрованный номер состоит из комбинации четырех цифр и двух букв, и его нельзя использовать для совершения телефонных звонков или отправки текстовых сообщений. Власти вправе расшифровать этот номер только в том случае, если возникнет острая необходимость связаться с владельцем номера по причинам, связанным с вирусом.

55. Специальный докладчик приходит к выводу, что в своих попытках бороться с COVID-19 правительство Республики Корея приняло ряд мер, которые нарушают право на неприкосновенность частной жизни и которые в некоторых случаях не были ни необходимыми, ни соразмерными. Однако в большинстве, если не во всех таких случаях, правительство осознавало, что допустило ошибку, и попыталось исправить ошибки посредством принятия корректирующих мер (см. примеры выше).

56. На рисунке показаны три волны распространения COVID-19 во время пандемии в Республике Корея с марта 2020 года по 19 июля 2021 года.

[45] См. Gyuwon Jung and others, “Too much information: assessing privacy risks of contact trace data disclosure on people with COVID-19 in South Korea”, *Frontiers in Public Health*, 18 June 2020. URL: www.ncbi.nlm.nih.gov/pmc/articles/PMC7314957/ и www.frontiersin.org/articles/10.3389/fpubh.2020.00305/full.

Статистика



Источник: Университет Джонса Хопкинса.

57. На рисунке видно, что, хотя уровень заражения после третьей волны в январе 2021 года существенно снизился к марту и апрелю 2021 года, он оставался на уровне предыдущего максимального пика первой волны, имевшей место в марте 2020 года, то есть составлял примерно 530 новых случаев в день. Однако к 19 июля 2021 года уровень заражения достиг самых высоких за все время показателей — примерно 1300 новых случаев заражения в день. На момент представления настоящего доклада (20 июля 2021 года) точные причины такого уровня заражения, несмотря на все действующие меры, нарушающие право на неприкосновенность частной жизни, не были ясны. На данном этапе можно сделать лишь предварительные выводы, поскольку для получения окончательных выводов требуется больше данных за более длительный период времени. Таким образом, окончательный вердикт касательно того, были ли какие-либо (или все) меры, затрагивающие право на неприкосновенность частной жизни, предпринятые Республикой Корея в связи с пандемией COVID-19, необходимыми и соразмерными, еще не вынесен. Всё это затрудняет ответ на вопрос, что позитивного можно найти (и можно ли найти вообще) в подходе правительства к обеспечению неприкосновенности частной жизни в контексте пандемии, за исключением уменьшения объема собираемых персональных данных в качестве корректирующей меры в 2020 и 2021 годах.

58. В Нигерии объявление общенационального карантина привело к смертоносным репрессиям и нарушениям прав человека, среди которых нарушения права на неприкосновенность частной жизни, по всей видимости, оказались наименее смертоносными по сравнению с другими серьезными негативными последствиями. Сообщалось, что силовые структуры Нигерии, помимо

ограничений свободы передвижения, производили незаконные аресты и задержания, занимались вымогательством, и захватом и конфискацией имущества[46].

59. Сингапур также может служить примером ситуации, в которой был допущен выход за рамки допустимого без острой на то необходимости, что довольно наглядно иллюстрирует проблему "ползучего" расширения полномочий. «Общественная поддержка была сильно подорвана после того случая, когда власти раскрыли в январе (2021 года), что полиция использовала данные приложения в целях расследования убийства – всего спустя несколько месяцев после того, как ответственный министр пообещал, что эти данные будут использоваться исключительно в целях сдерживания эпидемии COVID. Правительство принесло извинения, что происходит довольно редко. Но вместо того, чтобы отказаться от этой идеи, оно планирует официально оформить право полиции получать доступ к таким данным в отдельных случаях, внеся на рассмотрение в парламент проект соответствующего закона».[47] Согласно новым поправкам к Закону о *COVID-19 (Временных мерах)* 2020 года, принятым Парламентом Сингапура в феврале 2021 года, персональные данные, собираемые программами цифрового отслеживания контактов в период пандемии, могут использоваться исключительно в целях отслеживания контактов с зараженными лицами, если только они не требуются правоохранительными органами для расследования «серьезных преступлений».[48]

Кто в доме хозяин?

60. В апреле 2020 года компании «Гугл» и «Эпл» объявили о совместном проекте, цель которого заключается в том, чтобы дать правительствам и органам здравоохранения возможность использовать технологию Bluetooth для борьбы с распространением вируса. для этого были использованы интерфейсы прикладного программирования и технологии уровня операционной системы, обеспечивающие большую конфиденциальность и защищенность пользователей за счет децентрализованной модели. [49] Инициатива “Google and Apple Exposure Notification” задала тренд использования децентрализованных подходов к отслеживанию технологических контактов через мобильные телефоны из-за их доминирования на рынке смартфонов. Эта технология используется странами по всему миру, включая Австралию, несколько штатов США и большинство государств-членов Европейского Союза. В июне 2020 года правительство Соединенного Королевства было вынуждено резко развернуть свой курс и отказаться от своего тогдашнего приложения для отслеживания коронавируса, перейдя на модель, основанную на технологиях, предлагаемых компаниями «Эпл» и «Гугл».

61. В апреле 2021 года обновление приложения для отслеживания контактов, разработанное для Англии и Уэльса, было заблокировано за нарушение условий

[46] См. Simisola Akintoye, “Privacy implications of national responses to COVID 19 in Nigeria”; De Montfort University; Greenleaf, “COVID-19: the available evidence … and a little bit of hindsight” (см. сноску 15); “Coronavirus: security forces kill more Nigerians than COVID-19”, BBC News, April 2020.

[47] См. Jamie Tarabay and Bloomberg, “Countries vowed to restrict use of COVID-19 data. For one Government, the temptation was too great”, *Fortune*, 1 February 2021.

[48] См. Kirsten Han, “COVID app triggers overdue debate on privacy in Singapore”, Al-Jazeera, 10 February 2021.

[49] См. www.apple.com/mt/newsroom/2020/04/apple-and-google-partner-on-covid-19-contact-tracing-technology/.

соглашения, заключенного с компаниями «Эпл» и «Гугл»[50] Соглашение, которое было подписано всеми органами здравоохранения для получения права использовать технологии компаний «Эпл» и "Гугл" для отслеживания контактов и которое ориентировано на защиту неприкосновенности частной жизни, предусматривало, что программное обеспечение не может использоваться для сбора данных о местоположении. Однако в предлагаемом обновлении пользователей просили загружать регистрационные данные о посещении общественных мест (сканы штрих-кодов) в случае сдачи положительных тестов на вирус.

62. Эти инциденты наглядно демонстрируют мощь крупных технологических компаний. Независимо от юридических формальностей и вопроса о том, какой орган в состоянии гарантировать наибольшую неприкосновенность частной жизни, необходимо обсудить, насколько уместно, чтобы правительственные органы полагались на частный сектор для обеспечения своих граждан необходимыми инструментами санитарно-эпидемиологического контроля, и должен ли этот сектор иметь возможность диктовать условия, на которых он будет поставлять такие инструменты. Франция продемонстрировала, что в состоянии действовать в одиночку, и приложение, запущенное в июне 2020 года, к маю 2021 года установили более 25 процентов населения Франции.[51]

V. Упрощенные решения и иные механизмы борьбы с пандемией

63. Многие страны были плохо подготовлены к введению в кратчайшие сроки таких санитарно-эпидемиологических мер, как социальное дистанцирование, ограничения на поездки и ношение масок. Были приняты упрощенные решения в разных формах и с разными последствиями.

64. К числу механизмов борьбы с пандемией относится, во-первых, объявление чрезвычайных ситуаций. На се годняшний день 108 стран объявили чрезвычайные ситуации[52], с тем чтобы, помимо прочего, сделать обязательным отслеживание контактов. Чрезвычайную ситуацию в стране, объявила, например, Южная Африка, сделавшая это на основании Закона 2002 года «О предупреждении бедствий и ликвидации их последствий».

65. Во-вторых, были предприняты шаги для того, чтобы обойти требования к защите и обеспечению безопасности данных. В Австрии в марте 2020 года в Закон 2012 года «О телематике здравоохранения» были внесены поправки, позволяющие медицинским работникам передавать медицинские и генетические данные по незащищенным каналам, таким как факс или электронная почта[53].

66. В-третьих, было принято новое законодательство. В марте 2020 года Дания приняла Закон «Об эпидемии», ограничивающий:

а) право на проведение собраний путем введения комендантского часа, ограничений на доступ в определенные районы и запрета на проведение

[50] См. “Apple and Google block NHS Covid app update over privacy breaches”, *The Guardian*, 20 April 2021).

[51] См. Reuters, “French COVID tracing app downloaded by 25 per cent of the population – minister”, Reuters staff, 23 May 2021.

[52] По состоянию на 14 июля 2021 года, International Center for Not-for-Profit Law, “COVID-19 Civic Freedom Tracker” (см. сноску 12).

[53] Текст поправки см. www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20008120

собраний и встреч численностью свыше 10 человек в период с 18 марта по 8 июня 2020 года;

b) право на личную свободу путем принудительной госпитализации, изоляции и вакцинации, а задержания лиц без подтвержденной инфекции;

c) право на уважение неприкосновенности частной жизни путем внедрения приложений для отслеживания контактов, обязывающих людей, компании и государственные органы предоставлять данные, связанные с COVID-19, а также программ, использующих такие данные для анализа характера передвижения, в том числе физических лиц.

67. В феврале 2021 года в Закон «Об эпидемии» были внесены поправки, предусматривающие парламентские процедуры и механизмы для контроля принимаемых правил и мер, связанных с вмешательством в частную жизнь, повышение прозрачности процессов и сокращение у органов государственной власти полномочий по своему усмотрению принимать решения, ограничение возможностей принимать принудительные меры в отношении физических лиц, например, закрепление добровольного принципа вакцинации, а также установление судебного контроля за применением мер принуждения, связанных с лишением свободы.

68. В-четвертых, в других странах обеспечение соблюдения санитарно-эпидемиологических требований было возложено, в частности, на правоохранительные органы и гражданские организации. В апреле 2021 года в соответствии с Законом Мальты «Об общественном здравоохранении» руководитель службы общественного здравоохранения делегировал полномочия по обеспечению соблюдения пандемических мер:

a) полиции и сотрудникам местных правоохранительных органов;

b) вооруженным силам Мальты;

c) Транспортной администрации Мальты;

d) Управлению по туризму Мальты;

e) Управлению по охране окружающей среды.

69. Перечисленным должностным лицам было разрешено входить в дома и проводить проверки на основании «полученных сообщений или обоснованного подозрения в том, что несколько человек собрались вместе в нарушение действующих нормативных правил». Эти меры, по-видимому, не обставлялись надлежащими гарантиями, но нарушали принципы необходимости и соразмерности. Поскольку для проникновения в жилище частного лица, как правило, требуется судебный ордер, этот пример демонстрирует перераспределение большого объема полномочий в связи с чрезвычайной санитарно-эпидемиологической ситуацией.

70. О необходимости внимательно анализировать роль и обязанности органов здравоохранения и правоохранительных органов свидетельствуют также призывы правоохранительных органов других стран, таких как Соединенное Королевство, разрешить проникновение в дома тех лиц, которые подозреваются в нарушении карантинных правил, в качестве «полезного инструмента» обеспечения соблюдения карантина.[54]

[54] См. “Police Chief calls for power of entry into homes of suspected lockdown breakers”, Vikram Dodd, *The Guardian*, 5 January 2021.

VI. Прочие соображения

71. Пандемия COVID-19 продолжает набирать обороты, и в этом процессе будут происходить изменения в спорах и дебатах вокруг нее. Одной из тем дискуссий на се годняшний день является противопоставление подхода Европейского союза, ставящего во главу угла защиту права человека на неприкосновенность частной жизни, и подхода, который взят на вооружение в Соединенных Штатах и, отчасти, в Австралии и который отдает приоритет защите прав потребителей. Федеральная торговая комиссия США недавно заострила внимание на вопросах соблюдения права на неприкосновенность частной жизни при использовании таких технологий, как видеоконференцсвязь, образовательные и медицинские технологии, выпустив циркуляры с предупреждением о случаях мошенничества и кражи личных данных после перехода к работе и обучению в цифровом формате.[55]

72. Предыдущие санитарно-эпидемиологические кризисы повлияли на то, как страны ведут борьбу с нынешней пандемией. Например, Республика Корея выбрала обязательные централизованные механизмы отслеживания контактов, имея за плечами опыт борьбы со вспышкой ближневосточного респираторного синдрома (MERS) в 2015 году. Предыдущий опыт заставил страну пересмотреть Закон «О контроле и профилактике инфекционных заболеваний», с тем чтобы защитить людей от разглашения сведений о поле, возрасте, образовании и национальности, но при этом сохранить требование обязательного раскрытия инфекционного статуса.

73. На степень защиты неприкосновенности частной жизни, которую могут обеспечить определенные меры, повлиял и географический размер страны. Небольшие страны имели преимущество в реагировании на некоторые аспекты пандемии: например, несмотря на высокую плотность населения Сингапура, данная страна в дополнение к приложению для смартфонов TraceTogether смогла обеспечить аппаратными токенами физических лиц, не имеющих возможности воспользоваться приложениями для смартфонов.[56] С другой стороны, такие страны, как Индия, с большой территорией и огромной численностью населения, организовали регистрацию на вакцинацию через интернет и с помощью приложения CoWIN (в привязке к номеру телефона человека), что не позволяет записаться на вакцинацию многим людям, не имеющим смартфона или доступа к Интернету. Распределение аппаратных токенов (либо альтернативных или анонимных средств регистрации) требует выпуска многих миллионов токенов, но если этого не делать, то речь пойдет о дискриминации.

74. По сообщениям, Африка, Латинская Америка, Австралия и Индия – это те регионы и страны, хотя и далеко не единственные, где конституционные гарантии и/или надежные национальные законы о защите данных и механизмы надзора отсутствуют и где такое отсутствие подрывает все усилия правительств по обеспечению необходимого доверия граждан к принимаемым санитарно-эпидемиологическим мерам.

75. Существующие в некоторых регионах мира надежные законы о защите данных на национальном уровне и сильные, независимые органы, занимающиеся вопросами защиты данных, или иные надзорные органы помогают запустить инициативы по отслеживанию контактов и регистрации на вакцинацию,

[55] См. *Federal Trade Commission*, “One year into COVID-19 pandemic, new Federal Trade Commission staff report highlights agency’s ongoing efforts to protect consumers” (19 April 2021).

[56] “Token Go Where”. См. https://token.gowhere.gov.sg/.

должным образом учитывая необходимость защищать данные граждан и информируя об этой необходимости общество.

76. В результате принятия большинства мер происходит сбор большого объема конфиденциальных данных, и трудно дать оценку тому, является ли такой сбор данных соразмерным. Даже признанные весьма действенными законы о защите данных, такие как Общий регламент Европейского Союза о защите данных, требуют более подробных разъяснений и инструкций для их применения в ситуациях санитарно-эпидемиологического кризиса.

77. Новые системы наложились на уже существующую и без того сложную инфраструктуру информационных технологий. Как отмечает Совет по защите данных Австрии в своей оценке региональной инициативы, «органы власти, занимающиеся вопросами защиты данных во многих странах, не смогли оценить технические аспекты этих систем и также сопровождающих их длинных и технически очень сложных описаний в силу ограниченности времени, ресурсов или опыта».[57]

78. Стратегии, выбранные разными странами по всему миру, в целом неизбежно привели к приостановке действия основных прав и свобод человека. Чрезвычайные меры способствовали быстрой, но не обязательно хорошо продуманной ответной реакции. Приложения для смартфонов или другие инструменты контроля должны быть приемлемыми с правовой точки зрения, технически надежными и одобряемыми обществом, а также должны проходить проверку на предмет соблюдения прав человека, которая в рассматриваемый период очевидно отсутствовала.

79. Общественное доверие влияет на эффективность мер, принимаемых в борьбе против пандемии. Хотя доверие к государству играет большую роль в успешной реализации любой правительственной инициативы, оно особенно необходимо в чрезвычайных ситуациях, таких как пандемия COVID-19. Это особенно важно в случае добровольных мер, эффективность которых зависит от участия самих граждан.

80. Меры, посягающие на неприкосновенность частной жизни, встречают сопротивление. В Соединенных Штатах Америки попытки внедрить программы отслеживания местоположения и централизованные системы встретили решительное сопротивление; по состоянию на июль 2021 года лишь два штата ввели паспорта вакцинации, а многие штаты запретили их.[58] Граждане опасаются, что меры по борьбе с пандемией не будут отменены. Аналогичным образом, большинство австралийцев (60 процентов) согласны с тем, что для борьбы с COVID-19 и ради всеобщего блага необходимо в определенной мере пожертвовать неприкосновенностью частной жизни, если это не примет постоянного характера.[59]

81. Технологии крайне важны для властей в их борьбе за здоровье человека. Тем не менее, в результате их использования надзор за гражданами может стать после пандемии обычным явлением. Например, утвержденные правительством приложения для отслеживания контактов также могут использоваться для получения доступа к личным данным пользователей в качестве инструмента государственного надзора за гражданами. Легитимация посягающих на частную жизнь людей технологий открывает путь к дальнейшим мерам, позволяющим проникать в частную жизнь. Например, под предлогом внедрения приложений и

[57] См. www.bmj.gv.at/dam/jcr:c4b7569c-46c3-4772-bb07-9085f61412a8/Stellungnahme_des_Datenschutzrates_Epidemiegesetz.pdf.

[58] См. Elliott Davis, “Which States Have Banned Vaccine Passports?”, *US News*, 1 June 2021.

[59] Управление Австралийского уполномоченного по вопросам информации.

токенов для мониторинга соблюдения социальной дистанции компании расширили слежку за сотрудниками.

82. Нежелание или неспособность правительственных органов оценивать соразмерность и необходимость принимаемых мер могут быть связаны с "ползучим" расширением функционала технологий и собираемых данных и/или с неэффективностью используемых инструментов.

83. Пандемия вызвала к жизни невиданные ранее проблемы из-за перехода к гибридной рабочей среде, когда работодатели коллективно контролируют своих работников. Меры, принимаемые компаниями для контроля соблюдения социальной дистанции своими сотрудниками, затрагивают их право на неприкосновенность частной жизни. В то время как многие компании были вынуждены приостановить свою деятельность, другим удалось обойти это требование бла годаря тому, что компании потребовали от своих сотрудников носить устройства, предупреждающие о недопустимом физическом сближении. Многие компании се годня проявляют интерес к контролю удаленно работающих сотрудников с помощью программного обеспечения, регистрирующего количество нажатий на клавиатуру, снимки экрана и другую компьютерную деятельность. Эти технологии создают риск "ползучего" усиления надзора, в то время как другие таким же образом изменяют действующие процедуры, передавая считанные с переносных устройств данные мониторинга без какой-либо уважительной причины в централизованную базу вместо того, чтобы хранить их на месте.

84. Пандемия COVID-19 вскрыла недостатки в действующих законах о защите данных, не позволяющие нейтрализовать возникающие риски для личных данных и неприкосновенности частной жизни. Общий регламент о защите данных, который считается эталоном защиты данных во всем мире, не предусматривает возможность подачи коллективных исков, поскольку он касается в первую очередь индивидуальных прав.[60]

VII. Выводы

85. Качество государств, правительств и частных субъектов, в том числе физических, лиц по-настоящему проверяется в чрезвычайных ситуациях.

86. Международные договоры и большинство национальных конституций позволяют государствам временно расширять свои полномочия для реагирования на кризисы, такие как пандемия COVID-19. Пандемия переплела в один клубок проблемы здравоохранения, надзора за гражданами и каждого отдельного человека. Поэтому борьба с ней должна вестись в рамках параметров, установленных для каждой из этих сфер.

87. С точки зрения права на неприкосновенность частной жизни пандемия позволила правительствам и корпорациям чаще вторгаться в жизнь людей, нарушая их право на неприкосновенность частной жизни. Хотя в интересах охраны общественного здоровья некоторых наступлений на права во время пандемии не избежать, на се годняшний день невозможно определить, в какой степени они являлись необходимыми и соразмерными.

88. К сожалению, многие государства противопоставили меры, необходимые для спасения жизней людей, защите неприкосновенности частной жизни. Такой упрощенный взгляд игнорирует то значение, которое люди придают своей частной жизни и необходимости ограничения неоправданных вторжений со стороны

[60] См. Andrew Pakes, “High Visibility and COVID-19: returning to the post-lockdown workplace” (Ada Lovelace Institute, 19 May 2020).

государства и коммерческого сектора в их жизнь. Результатом этого стало сопротивление усилиям правительства, направленным на борьбу с пандемией.

89. В условиях пандемии COVID-19 самые разные страны мира стали искать упрощенные пути реализации национальных санитарно-эпидемиологических стратегий. Одни прибегли к законам о чрезвычайном положении для введения обязательного отслеживанию контактов; другие воспользовались отсутствием действенных законов о защите данных на национальном уровне, в ускоренном порядке развернув программы отслеживание контактов и регистрации вакцинированных лиц, игнорируя при этом право на неприкосновенность частной жизни или другие права человека. В качестве ответа на кризис, который иногда напоминал скорее «рефлекторную реакцию», государства воспользовались законами о чрезвычайных ситуациях и слабостью или отсутствием законов о защите данных. Для ряда государств и правительств важным фактором, по-видимому, были и остаются приближающиеся выборы.[61]

90. Государства-члены используют технологические инструменты для отслеживания инфицированных, обеспечения соблюдения карантинных мер и правил социального дистанцирования, а также для контроля хода вакцинации.

91. В этом контексте страны не были готовы к демонстрации независимости и мощи технологическими компаниями, в том числе к позиции компаний «Эпл» и «Гугл» по вопросу неприкосновенности частной жизни пользователей приложений для отслеживания контактов. В то же время следует признать, что эти две компании, по всей видимости, действовали довольно разумно, желая защитить права на неприкосновенность частной жизни даже в большей степени, чем некоторые государства, которые стремились использовать собираемые данные в своих интересах.

92. Непрекращающаяся пандемия означает, что поощрение и защита права на неприкосновенность частной жизни, а также смежных прав требуют постоянного мониторинга и представления публичной отчетности органами власти на международном, региональном и национальном уровнях.

93. Централизованные подходы, в том числе те, которые используются в Австралии, Израиле и Республике Корея, несут в себе угрозу для неприкосновенности частной жизни, например, с точки зрения защиты и безопасного хранения чувствительной информации, в том числе данных о здоровье человека, а также существования большой вероятности того, что эти данные будут повторно использоваться в централизованных базах данных органов власти и корпораций, и не будут уничтожены после использования. Децентрализованные приложения предоставляют пользователям больше возможностей контролировать свою информацию, поскольку вся контактная информация хранится лишь на телефонах пользователей, а централизованная база данных, доступная правительству или органам власти, отсутствует.

94. Влияние обязательных приложений для отслеживания контактов на неприкосновенность частной жизни очевидно – получение согласия и возможность отозвать его во многих, хотя и не во всех случаях, были признаны законом как неотъемлемая часть права на неприкосновенность частной жизни. Использование принудительных мер также повышают риск того, что органы власти и корпорации будут неправомерно использовать чувствительные данные, собираемые для борьбы с пандемией, путем «ползучего» усиления надзора или использования данных не по назначению в отсутствии у пользователей возможности удалить свои данные из баз данных. Приложения для добровольного отслеживания

[61] См. www.idea.int/news-media/multimedia-reports/global-overview-covid-19-impact-elections.

контактов не получили широкого распространения, как правило, из-за отсутствия у общественности доверия к способности органов власти обеспечивать безопасность и защиту персональных данных.

95. Множество проблем существует также с использованием технологий, включая проблему отсутствия данных, позволяющих оценить точность некоторых технологий. В ходе осуществления большинства обсуждаемых мер собирается большой объем чувствительной информации, и трудно оценить, является ли сбор такого количества данных соразмерным. Хотя технологии играют решающую роль в борьбе с пандемией, они могут превратить практику надзора в будущем в обычное явление. Интенсивный и повсеместный технологический надзор не является панацеей в таких ситуациях, как пандемия COVID-19.

96. С этим связаны также вопросы равенства и защиты неприкосновенности частной жизни работников. Законодательство о защите данных оказалось не лишено недостатков, в том числе положения Общего регламента о защите данных. Требуются более подробные рекомендации в отношении толкования положений закона, а также внесение в них изменений. Эти законы, как правило, касаются индивидуальных прав, а не коллективных требований к соблюдению неприкосновенности частной жизни, которые приобретут дополнительную актуальность с выходом на первый план искусственного интеллекта и перехода в гибридную рабочую среду большего числа работников.

97. Существует острая необходимость в формировании общих принципов обеспечения конфиденциальности данных, которые можно было бы применять ко всем законам, регламентирующим сбор данных для борьбы с пандемией. Эти принципы установят общий, универсальный стандарт работы как для нынешней пандемии, так и для будущих подобных чрезвычайных ситуаций. Такой набор мер был предложен Грэхэмом Гринлифом и адаптирован здесь, чтобы включить в них вопросы, касающиеся адресной защиты персональных данных на основе принципа «проектируемой конфиденциальности».[62]

98. Подготовкой к будущей пандемии лучше заняться прямо сейчас.[63] Вынесенные уроки применимы не только к COVID-19, но и к другим регистрируемым в обязательном порядке и инфекционным заболеваниям и возможным будущим пандемиям.

VIII. Рекомендации

99. Эти рекомендации направлены на обеспечение права каждого человека на неприкосновенность частной жизни во время нынешних и будущих кризисов в области общественного здравоохранения без применения произвольного вмешательства, как указано во Всеобщей декларации прав человека (статья 12), Международном пакте о гражданских и политических правах (статья 17) и выводах договорных органов.

100. Приведенные ниже рекомендации предназначены как для государственных, так и для негосударственных субъектов права.

[62] См. Greenleaf, “COVID-19: the available evidence … and a little bit of hindsight” (см. сноску 15).

[63] См. “The best time to prevent the next pandemic is now: countries join voices for better emergency preparedness” (WHO, 1 October 2020).

Неприкосновенность частной жизни и защита персональных данных

101. **Государства и негосударственные участники процесса должны соблюдать Руководящие принципы предпринимательской деятельности в аспекте прав человека: осуществление рамок Организации Объединенных Наций в отношении «защиты, соблюдения и средств правовой защиты» (A/HRC/41/43, приложение).**

102. **Принимать рекомендации Специального докладчика по вопросу о праве на неприкосновенность частной жизни в целях защиты от посягательств на неприкосновенность частной жизни по гендерному признаку (A/HRC/43/52, пункты 33 и 34).**

103. **Поощрять партнерство с гражданским обществом и промышленностью в целях совместной разработки стратегий и принятия технологических ответных мер.**

104. **Привлекать группы населения, подвергающиеся особому риску, к участию в консультациях по вопросам принятия отдельных мер в области общественного здравоохранения.**

105. **Сокращать количество случаев нарушений неприкосновенности частной жизни вследствие пандемии по гендерному признаку, требуя проведения оценки влияния принимаемых решений на права человека, касающиеся неприкосновенности частной жизни, с учетом гендерных аспектов до принятия каких бы то ни было мер, стратегий и законодательства.**

106. **Регулярно оценивать эффективность мер, принимаемых для привлечения лиц, находящихся в уязвимом и маргинализованном положении, к усилиям, направленным на реагирование и преодоление пандемии.**

Дети

107. **Разрабатывать комплексные образовательные онлайн-планы действий на основе пункта 1) статьи 29 Конвенции о правах ребенка и Руководящих принципов Совета Европы по защите данных детей в образовательной среде.**

108. **Обеспечивать формирование и поддержку соответствующей правовой системы для онлайн-образования.**

109. **Создавать общественную инфраструктуру для некоммерческих образовательных и социальных пространств.**

110. **Обеспечивать справедливую, точную и безопасную обработку персональных данных детей в соответствии с законной правовой базой, используя системы защиты данных, воплотившие в себе лучший передовой практический опыт, такой как, например, Генеральный регламент и Конвенция о защите персональных данных 108+.**

Неприкосновенность частной жизни в информационном пространстве

111. **Учитывать права человека при проектировании, разработке и внедрении технологических подходов к борьбе с пандемией.**

112. **Законодательные меры защиты, основанные на общих принципах с указаниями для конкретных ситуаций, необходимы для всех типов мер, принимаемых в области охраны здоровья в условиях пандемии.**

Специальный докладчик рекомендует использовать 11 общих принципов[64] для централизованных и децентрализованных систем надзора за общественным здравоохранением, а также законодательные меры в отношении инфекционных заболеваний и их применения в оценке политики предотвращения пандемии во всем мире:

a) **с самого начала установить адресную защиту персональных данных на основе принципа «проектируемой конфиденциальности» и «в общепринятом порядке» путем включения комплексной оценки прав человека наряду с оценкой защиты данных для мер в области общественного здравоохранения, уделяя особое внимание вопросам эпидемии и пандемии;**[65]

b) **вопросы, связанные с неприкосновенностью частной жизни, следует учитывать с самого начала реагирования на любую эпидемию или пандемию. Более того, неприкосновенность частной жизни должна являться краеугольным камнем любой национальной стратегии борьбы с эпидемией, хорошо продуманной за годы вперед и выступать в качестве неотъемлемой — и хорошо интегрированной — части упомянутой выше комплексной оценки прав человека;**

c) **включить в закон о конфиденциальности данных региона или отдельной страны четкие и подробные меры контроля;**

d) **более эффективно обеспечить необходимую ясность и правовую базу, чем просто посредством принятия делегированных актов или постановлений, а также достичь большего единообразия в юрисдикции;**

e) **гарантировать доступ к сайтам, мероприятиям, объектам, образованию и так далее во избежание дискриминации;**

f) **защитить, что является жизненно важной задачей, уязвимые группы, на которые оказывают неблагоприятное и дифференцированное воздействие меры эпидемиологического надзора за пандемией;**

g) **свести к минимуму и определить разрешенный объем использования данных по COVID, чтобы гарантировать, что данные по COVID-19 не будут впоследствии использоваться для иных целей;**

h) **установить «целевую спецификацию», как во многих действующих законах о защите данных;**

i) **свести к минимуму сбор данных;**

j) **обеспечить соразмерность мер по сбору данных, разработать общепринятый подход к управлению рисками и оказать помощь в ограничении ущерба, причиненного вследствие утечек данных, кибератак и усиления используемого функционала;**

k) **положения о борьбе с принуждением: требование об использовании или демонстрации доказательств использования должно предотвращаться или строго определяться и содержаться в законодательных актах. Иные требования или просьбы представить сертификаты использования следует предотвращать, квалифицируя такое поведение как правонарушение в соответствии с законодательством. Необходимо обеспечить контроль за исполнением данного правила, а также средства правовой защиты;**

[64] URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3875920.

[65] См. Council of Europe “2020 Digital Solutions to Fight COVID-19 2020”, Data Protection Report October 2020. URL: www.coe.int/en/web/data-protection/-/digital-solutions-to-fight-covid-19-council-of-europe-report-on-data-protection-2020.

l) **необходимо предотвращать «постепенное усиление надзора»: следует избегать ситуаций, как, например, в Сингапуре, который в 2020 году обещал «только отслеживание контактов с инфицированными лицами», а затем в 2021 году отступил от этого правила, разрешив использовать надзор в целях проведения уголовных расследований;**

m) **принцип добровольного участия, необходимого для большинства принимаемых мер по предотвращению пандемии, может работать только в случае наличия доверия со стороны общества. Чтобы обеспечить такое доверие, следует объявить противозаконным дальнейшее распространение надзора на другие области, например, в целях проведения уголовных расследований;**

n) **программа постоянного удаления данных (если данные собираются): само законодательство должно требовать, чтобы любые собранные данные удалялись в течение короткого периода времени, например, по истечении срока инфицирования человека или какого-либо иного доказанного/научно-обоснованного срока;**

o) **оговорка о прекращении срока действия для всей системы и обязательный независимый «аудит прекращения действия» всех систем эпидемических данных должны быть закреплены в законе и должны строго соблюдаться: необходимо установить фиксированный срок или закрепить право проведения независимой оценки целесообразности, чтобы обеспечить прекращение действия всех систем пандемического надзора и прописать в законе требование о проведении независимого аудита;**

p) **надзор и периодическая публичная отчетность, подготовленная независимым органом по защите данных: контроль за этими системами надзора должен быть внешним и независимым;**

q) **прозрачность: необходимые условия должны быть определены в процессе проведения консультаций с экспертами и гражданским обществом. Это может быть представлено в форме выпуска любого исходного кода, используемого для создания систем надзора (например, приложений для отслеживания контактов), проведения всесторонних оценок воздействия на защиту данных и публикации данных об эффективности методов, используемых для надзора за пандемией.**

113. **Постоянный диалог с крупными технологическими компаниями должен дополнять официальные и неформальные публичные дискуссии о роли и ответственности крупных технологических компаний в выполнении своей роли по защите права на неприкосновенность частной жизни во время пандемий.**

Прозрачность и метрики

114. **Полномочия в связи с чрезвычайными ситуациями в области здравоохранения требуют оценки их необходимости и соразмерности. В рамках этой периодической и регулярной оценки:**

a) **Специальный докладчик по вопросам права на неприкосновенность частной жизни, самостоятельно, а также вместе с другими обладателями мандата, должен пересматривать ситуацию, связанную с заболеваниями, подлежащими регистрации, и с инфекционными заболеваниями, уделяя особое внимание, помимо прочего, COVID-19, но не ограничиваясь COVID-19, как минимум, каждые 24–36 месяцев, в целях выявления существующих и возникающих рисков, а также в целях понимания наиболее**

эффективных и благоприятных для соблюдения неприкосновенности частной жизни политических инициатив, которые можно было бы использовать для подготовки к пандемиям в рамках целостного подхода к защите прав человека;

b) **если какая-либо страна примет решение о том, что технологический надзор в ответ на глобальную пандемию COVID-19 является необходимой и целесообразной мерой, то такая страна должна доказать необходимость и соразмерность конкретной принимаемой меры, а также принять закон, который прямо предусматривает применение таких мер надзора, которые содержат обязательные явно выраженные и особые гарантии;**

c) **государства и корпорации должны учитывать права человека при проектировании, разработке и внедрении технологических подходов к борьбе с пандемией, принимая во внимание те огромные последствия, которые имеют цифровые технологии в отношении широкого спектра прав, особенно в части, касающейся неприкосновенности частной жизни;**[66]

d) **государствам и корпорациям следует принять технологический проект, ориентированный на пользователя и обеспечивающий соблюдение прав человека, посредством которого, например, в случае ввода в действие «паспортов вакцинации» путешественники могли бы самостоятельно распоряжаться своими персональными данными для их представления по запросу;**

e) **следует проводить внешний анализ ответных мер государств на пандемию, при этом меры борьбы с пандемией в государствах должны оцениваться наряду с иными внутренними обязательствами стран в области соблюдения прав человека в рамках их регулярных периодических обзоров, проводимых на уровне Организации Объединенных Наций.**

[66] См. A/HRC/46/19.