Генеральная Ассамблея

Distr.: General
17 May 2019
Russian
Original: English

Совет по правам человека
Сорок первая сессия
24 июня – 12 июля 2019 года
Пункт 3 повестки дня
Поощрение и защита всех прав человека, гражданских, политических, экономических, социальных и культурных прав, включая право на развитие

Права на свободу мирных собраний и на свободу ассоциации

Доклад Специального докладчика по вопросу о праве на свободу мирных собраний и праве на свободу ассоциации*

Резюме

В настоящем докладе Специальный докладчик по вопросу о правах на свободу мирных собраний и ассоциации, Клеман Ниалетсосси Вуле, рассматривает возможности и вызовы в области прав на свободу мирных собраний и на свободу ассоциации в цифровой век. Специальный докладчик ставит перед собой задачу выработать рекомендации относительно того, как наилучшим образом сохранить и максимально эффективно использовать эти возможности и снизить риски.

Специальный докладчик приходит к выводу о том, что международное право защищает права на свободу мирных собраний и ассоциации независимо от того, осуществляются ли они лично, с помощью современных технологий или технологий, которые будут изобретены в будущем. Существующие международные нормы и принципы в области прав человека должны не только определять поведение государств, но и служить основой, которая определяет то, какие разработки будут осуществлять цифровые технологические компании, как они будут реализовывать контроль и управление цифровыми технологиями.

* На основании достигнутой договоренности настоящий доклад издается позднее предусмотренного срока его публикации в связи с обстоятельствами, не зависящими от представляющего доклад лица.

GE.19-08114 (R) 280519 310519

1908114

I. Введение

1. Настоящий доклад представляется Совету по правам человека на его сорок первой сессии Специальным докладчиком по вопросу о правах на свободу мирных собраний и ассоциации в соответствии с резолюциями Совета по правам человека 15/21 и 32/32. В разделе II Специальный докладчик представляет обзор своей деятельности за период после представления его доклада Совету по правам человека 18 июня 2018 года. В разделах III и IV он останавливается на вопросах осуществления прав на свободу мирных собраний и ассоциации в цифровой век. В разделе V приводятся выводы и рекомендации.

2. Цифровая эпоха открывает новые горизонты для осуществления прав на свободу мирных собраний и ассоциации. Можно привести многочисленные примеры по всему миру, которые демонстрируют мощь цифровых технологий в руках людей, стремящихся объединить свои усилия по продвижению демократии, мира и развития. Вместе с тем цифровая революция несет с собой новые риски и угрозы для этих основных прав.

3. Специальный докладчик описывает то, как за последнее десятилетие государства использовали технологии для того, чтобы заглушить голоса диссидентов, политической оппозиции, правозащитников, активистов и протестующих, вести за ними слежку и подвергать запугиванию, а также для манипулирования общественным мнением. Правительства все чаще требуют отключать Интернет, а также блокировать интернет-сайты и ресурсы в преддверии таких важнейших моментов проявления демократии, как выборы и протестные акции. Активизация деятельности по разработке законов и стратегий, направленных на борьбу с киберпреступностью, также открывает дверь для использования цифровых технологий как инструмента наказания и слежки за активистами и участниками протестов во многих странах мира. Несмотря на то, что цифровые технологии могут применяться для поддержки терроризма, подстрекательства к насилию и манипулирования выборами – и это является реальной и серьезной глобальной проблемой, – такие угрозы нередко служат предлогом для того, чтобы затормозить становление нового цифрового гражданского общества.

4. В то же время такие доминирующие онлайновые платформы, как «Фейсбук», «Твиттер» и «Ютьюб», превратились в организации, способные контролировать возможность людей пользоваться правами на свободу мирных собраний и ассоциации, при этом они, располагая огромной властью, могут самостоятельно решать, предоставлять или нет людям и представителям гражданского общества доступ к демократическому пространству.

5. Возможности и угрозы, которые создают цифровые технологии для осуществления права на свободу собраний и ассоциации, будут нарастать по мере разработки и распространения новых технологий, включая Интернет вещей и искусственный интеллект. Опираясь на документы, подготовленные другими соответствующими мандатариями специальных процедур[1], Специальный докладчик в настоящем докладе ставит перед собой задачу выработать рекомендации относительно того, как наилучшим образом сохранить и максимально эффективно использовать возможности этих технологий и снизить связанные с ними риски. Настоящий доклад не претендует на исчерпывающий характер. Скорее, он имеет целью представить первоначальный обзор наиболее актуальных проблем, которые будут более подробно рассмотрены в будущих докладах и сообщениях.

6. Для подготовки настоящего доклада Специальный докладчик использовал полученные от общественности материалы и проводил публичные консультации. В ноябре 2018 года он обратился с призывом представить материалы для доклада. На момент публикации доклада было получено 10 представлений от организаций гражданского общества, 2 представления от цифровых технологических компаний и 2 – от правительств. Специальный докладчик провел совещание на уровне экспертов

[1] См., например, A/HRC/17/27, A/71/373, A/HRC/23/40 и A/HRC/38/47.

в Женеве 11 и 12 октября 2018 года. Он также организовал региональные консультации с организациями гражданского общества в Бангкоке (21 декабря 2018 года), Бейруте (18 января 2019 года) и Мехико (24 и 25 января 2019 года), Кремниевой долине, Калифорния, Соединенные Штаты Америки (27–30 января 2019 года) и Найроби (21 и 22 февраля 2019 года). Он провел встречи на уровне экспертов в Копенгагене (6 марта 2019 года) и организовал консультации с участием представителей правительств в Женеве (20 марта 2019 года). Кроме того, 18 и 19 декабря 2018 года в Бангкоке он организовал совместную консультацию со Специальным докладчиком по вопросу о поощрении и защите права на свободу мнений и их свободное выражение Дэвидом Кайем.

II. Деятельность Специального докладчика

A. Посещения стран

7. Специальный докладчик посетил Тунис с 17 по 28 сентября 2018 года (см. A/HRC/41/41/Add.3) и Армению с 7 по 16 ноября 2018 года (см. A/HRC/41/41/Add.4). Он благодарит правительства обеих стран за сотрудничество до и во время поездок.

B. Сообщения

8. За период с 1 апреля 2018 года по 25 апреля 2019 года Специальный докладчик направил в общей сложности 130 сообщений 60 государствам. Его замечания по направленным государствам сообщениям и полученным ответам содержатся в добавлении к настоящему докладу (A/HRC/41/41/Add.1).

C. Участие в различных мероприятиях

9. В числе многих мероприятий, в которых принял участие Специальный докладчик, следует отметить следующие:

a) ознакомительную поездку в Бразилию с 16 по 20 июля 2018 года;

b) организованную Швейцарским агентством по развитию и сотрудничеству конференцию по проблемам сужения пространства и создания стимулирующей среды для гражданского общества, которая состоялась в Берне 13 и 14 сентября 2018 года;

c) шестьдесят третью сессию Африканской комиссии по правам человека и народов, состоявшуюся в Банжуле 24–26 октября 2018 года, и шестьдесят четвертую сессию Комиссии, состоявшуюся в Шарм-эш-Шейхе, Египет 24 апреля 2019 года;

d) сессию на глобальном Саммите правозащитников под названием «Сделаем наше пространство снова великим: пути решения проблем, связанных с сужением гражданского пространства, рестриктивными законами и ограничениями в области финансирования – фактическое положение дел и основные вопросы для обсуждения в ближайшие 20 лет», которая состоялась в Париже 30 октября 2018 года;

e) конференцию «Угрозы пространству для гражданского общества», состоявшуюся в Центре глобальных проблем при Утрехтском университете, Нидерланды, 21 ноября 2018 года;

f) Форум по вопросам предпринимательской деятельности и прав человека, состоявшийся в Женеве 26–28 ноября 2018 года;

g) мероприятие Международной организации франкоязычных стран в ознаменование семидесятой годовщины Всеобщей декларации прав человека, которое было проведено в Нью-Йорке 10 декабря 2018 года;

h) региональные диалоги с правительствами и организациями гражданского общества из Азиатско-Тихоокеанского региона о последствиях ограничения гражданского пространства, свободы мнений, их выражения и свободы собраний и выборов, которые были организованы Азиатским форумом по правам человека и развитию и состоялись в Бангкоке 20–21 декабря 2018 года;

i) ежегодную конференцию Норвежской ассоциации неправительственных организаций (НПО) «Фривилигет Норге» с темой «Могут ли НПО спасти демократию?», состоявшуюся в Осло, 14 февраля 2019 года;

j) международную конференцию по проблемам совместной борьбы за свободу гражданского пространства, которая состоялась в Копенгагене 4 и 5 марта 2019 года;

k) 172-ю сессию Межамериканской комиссии по правам человека, которая проходила в Кингстоне 6–10 мая 2019 года.

III. Международно-правовая основа прав на свободу мирных собраний и ассоциации в цифровой век

A. Обязательства государств

10. Права на свободу мирных собраний и ассоциации закреплены в статье 20 Всеобщей декларации прав человека и в статьях 21 и 22 Международного пакта о гражданских и политических правах. Совет по правам человека подчеркнул, что государства обязаны уважать и в полной мере защищать эти права в Интернете и вне его[2]. Генеральная Ассамблея также призвала все государства «обеспечивать, чтобы те же права, которые люди имеют вне интернет-пространства, включая права на свободу выражения мнений, мирные собрания и ассоциацию, также в полной мере защищались в интернет-пространстве в соответствии с нормами и стандартами в области прав человека»[3].

11. В предыдущих докладах мандатарий отмечал, что цифровая технология является составной частью осуществления прав на свободу мирных собраний и ассоциации[4]. Технология служит средством содействия осуществлению прав на свободу собраний и ассоциации как в реальной жизни, так и виртуальном пространстве, где сами эти права можно активно использовать[5]. Действительно, такие технологии являются полезным инструментом, когда нужно оперативно и эффективно организовать большую группу людей с небольшими затратами, а также создают виртуальную площадку для групп населения, которые подвергаются маргинализации со стороны общества и сталкиваются с ограничениями в условиях реальной жизни[6]. Мандатарий призывает государства обеспечить, чтобы все лица имели доступ к Интернету и могли использовать его в целях осуществления этих прав и чтобы ассоциациям[7] и собраниям[8] в интернет-пространстве оказывалось содействие в соответствии с международными стандартами в области прав человека. Совет по правам человека отметил, что, хотя под собранием обычно понимается физический сбор людей, понятие защиты прав человека, в том числе прав на свободу мирных собраний, выражения мнений и ассоциации, может также применяться к аналогичному взаимодействию, происходящему в сетевом режиме[9].

[2] См. резолюцию 38/7 Совета по правам человека.
[3] См. резолюцию 73/173 Генеральной Ассамблеи.
[4] См. A/HRC/20/27 и A/HRC/38/34.
[5] A/HRC/29/25/Add.1, пункт 53.
[6] См. A/HRC/35/28.
[7] A/HRC/20/27, пункт 52.
[8] A/HRC/29/25/Add.1, пункт 34.
[9] См. резолюцию 38/11 Совета по правам человека.

12. Несмотря на то, что эти права не являются абсолютными, свободу доступа и использования цифровых технологий для осуществления прав на свободу мирных собраний и ассоциации следует рассматривать в качестве правила, ограничение которого должно быть исключением. Общая норма должна состоять в том, чтобы разрешать открытое и свободное использование Интернета и других цифровых средств[10]. В резолюции 15/21 Совета по правам человека ясно говорится о том, что эти права могут подлежать некоторым ограничениям, «которые предусмотрены законом и необходимы в демократическом обществе в интересах национальной и общественной безопасности, для охраны общественного порядка (ordre public), охраны здоровья общества или нравственности или для защиты прав и свобод других лиц[11]. Когда такие ограничения имеют место, «государства обязаны доказывать их необходимость и принимать только такие меры, которые требуются для достижения законных целей с точки зрения обеспечения непрерывной и эффективной защиты прав по Пакту. Ни при каких обстоятельствах ограничения не могут применяться или осуществляться таким образом, чтобы это нарушало существо признанного в Пакте права[12].

13. Государства несут не только отрицательное обязательство воздерживаться от неоправданного нарушения права на свободу мирных собраний и ассоциации, но и положительное обязательство поощрять и защищать эти права в соответствии с международными стандартами в области прав человека[13]. Это означает, что правами на свободу мирных собраний и ассоциаций пользуются все люди без какого бы то ни было различия, как-то в отношении расы, цвета кожи, пола, языка, религии, политических и иных убеждений, национального или социального происхождения, имущественного положения, рождения или иного обстоятельства (пункт 1 статьи 2 Международного пакта о гражданских и политических правах)[14].

14. В цифровую эпоху позитивное обязательство содействовать осуществлению прав на свободу мирных собраний и ассоциации включает в себя усилия с целью «преодолеть цифровые разрывы, включая межгендерный цифровой разрыв, и расширить использование информационно-коммуникационных технологий в целях поощрения полного осуществления прав человека для всех»[15]. Обязательство по защите требует принятия позитивных мер с целью недопущения действий, совершаемых негосударственными субъектами, включая коммерческие предприятия, которые могут неоправданно препятствовать осуществлению прав на свободу мирных собраний и ассоциации[16].

15. В тех случаях, когда права на свободу мирных собраний и ассоциации неправомерно ограничиваются, жертвы должны иметь возможность реализовать свои права на эффективные средства правовой защиты и получение возмещения. Совет по правам человека призывает государства «обеспечивать, в соответствии со своими международными обязательствами, эффективные средства правовой защиты в случае нарушений прав человека, в том числе нарушений, связанных с Интернетом»[17].

16. Нарушения права на свободу мирных собраний и ассоциации может также препятствовать осуществлению других прав человека как в сети, так и вне ее. Они

[10] A/HRC/23/39, пункт 76.

[11] См. резолюцию 15/21 Совета по правам человека.

[12] См. Комитет по правам человека, замечание общего порядка № 31 (2004) о характере общего юридического обязательства, налагаемого на государства – участники Пакта, пункт 6.

[13] A/HRC/17/27, пункт 66; и A/HRC/29/25/Add.1.

[14] См. также статью 26 Пакта.

[15] Резолюция 38/7 Совета по правам человека, пункт 5. Это также находит свое отражение в Повестке дня в области устойчивого развития на период до 2030 года, которая содержит обязательство «существенно расширить доступ к информационно-коммуникационным технологиям и стремиться к обеспечению всеобщего и недорогого доступа к Интернету в наименее развитых странах к 2020 году» (целевой показатель 9.C) и «активнее использовать высокоэффективные технологии, в частности информационно-коммуникационные технологии, для содействия расширению прав и возможностей женщин» (целевой показатель 5.B). См. также A/HRC/35/9.

[16] См. пункт 2 статьи 2 Пакта; и Комитет по правам человека, замечание общего порядка № 31.

[17] См. резолюцию 38/7 Совета по правам человека.

включают право на неприкосновенность частной жизни и право на свободу мнений и их свободное выражение, которое неразрывно связано с осуществлением прав на свободу мирных собраний и ассоциации. Могут быть также затронуты и другие права, в частности экономические, социальные и культурные права.

B. Роль и обязанности бизнеса

17. В эпоху цифровых технологий осуществление права на свободу мирных собраний и ассоциации попало в значительную зависимость от коммерческих предприятий, чьи правовые обязательства, политика, технических стандартов, схемы и алгоритмы финансирования могут неблагоприятно воздействовать на осуществление этих свобод. В частности, онлайновые платформы и компании-операторы социальных сетей имеют мощные рычаги воздействия на то, как используются и осуществляются право на свободу мирных собраний и право на свободу ассоциации, особенно в странах, где «внесетевое» осуществление прав на свободу мирных собраний и ассоциации в значительной степени ограничено. В то же время эти платформы также стали новым инструментом для преследования и слежки за представителями гражданского общества.

18. Глобальные рамки для оценки того, как компании, занимающиеся цифровыми технологиями, соблюдают права человека, сформулированы в Руководящих принципах предпринимательской деятельности в аспекте прав человека[18]. В руководящих принципах 11–24 подчеркивается, что коммерческим предприятиям «следует соблюдать права человека», имея в виду, что им следует избегать нарушений прав человека других людей и устранять те неблагоприятные последствия нарушений прав человека, к которым они причастны. Для того чтобы выполнить это обязательство, предприятиям следует разработать правозащитную политику и процессы, включая политическое обязательство выполнять свою обязанность уважать права человека; внедрить процессы должной осмотрительности применительно к защите прав человека для выявления, предотвращения, смягчения последствий и представления отчетности о том, как они устраняют неблагоприятное воздействие на права человека; и процедуры, позволяющие нейтрализовать[19] любое неблагоприятное воздействие на права человека, которые они вызвали или которому они способствовали.

19. В этой связи мандатарий разделяет мнение Специального докладчика по вопросу о поощрении и защите права на свободу мнений и их свободное выражение, который указал, что «право прав человека предоставляет компаниям инструменты для формулирования и разработки политики и процессов, обеспечивающих соблюдение демократических норм и противодействие авторитарным требованиям»[20]. В том же ключе Совет по правам человека признает, что «международное право прав человека должно служить ориентиром для субъектов частного сектора и являться основой для их политики»[21].

20. Со своей стороны, государства несут обязательства по защите прав человека и по предотвращению нарушений в отношении действий или бездействия таких третьих сторон, как предприятия. Принцип 1 Руководящих принципов предусматривает, что «государства в пределах своей территории и/или юрисдикции должны обеспечивать защиту от нарушений прав человека третьими сторонами, включая предприятия». Это требует принятия необходимых мер, направленных на предупреждение и расследование таких нарушений, наказание за них и компенсацию ущерба посредством эффективной политики, законодательства, нормативного регулирования и судопроизводства[22].

[18] A/HRC/17/31.
[19] A/72/162, пункт 86 c).
[20] См. A/HRC/38/35.
[21] См. резолюцию 38/7 Совета по правам человека.
[22] См. A/HRC/17/31.

IV. Возможности и проблемы в области осуществления прав на свободу мирных собраний и ассоциации в цифровой век

A. Цифровые возможности

21. Цифровые технологии открывают широкие возможности для осуществления прав на свободу мирных собраний и ассоциации. Выступая одновременно в качестве инструментов, с помощью которых эти права могут осуществляться «вне сети» и пространства, где люди могут активно проводить сетевые собрания и создавать ассоциации[23], цифровые технологии значительно расширяют возможности отдельных лиц и групп гражданского общества в области организации и мобилизации людей, поощрения прав человека и осуществления инноваций в интересах социальных перемен.

22. Роль социальных сетей в организации уличных протестов хорошо известна. Так, в ходе посещения Армении в 2018 году Специальному докладчику рассказали о ключевой роли социальных медиа-платформ, сайтов прямого вещания и коммуникационных приложений в «бархатной» революции 2018 года, которая привела к отставке премьер-министра. С помощью хэштегов #MyStep и #MerzhirSerzhin велся обмен информацией и работа по мобилизации граждан и получения их поддержки в обход контролируемых правительством средств массовой информации. Движение #BlackLivesMatter за расовое равенство началось с использования хэштега для мобилизации граждан на массовые протесты в Соединенных Штатах и в других частях мира против полицейского насилия и системного расизма в отношении лиц африканского происхождения. Многие молодежные движения во всем мире опираются на поддержку социальных сетей, как показывают движение #RoadSafetyMovement в Бангладеш, кампания #FeesMustFall в Южной Африке и глобальные движения #FridaysForFuture и #ClimateStrikes.

23. Сегодня отдельные лица могут использовать интернет-пространство для участия в виртуально связанном гражданского обществе. К примеру, женщины-активисты используют Интернет для установления контактов и обмена информацией о стратегиях, в том числе через границы, и в качестве организационной площадки[24]. Пожалуй, наиболее ярким недавним примером является движение #MeToo. В 2017 году жертвы сексуального насилия стали использовать социальные медиа, чтобы рассказать о личном опыте пережитых сексуальных домогательств и надругательств и призвать к обеспечению гендерного равенства на рабочем месте под хэштегом #MeToo. В течение года, как сообщалось, этот хэштег был использован в социальных сетях более 19 млн раз[25] как жертвами сексуального насилия, так и сторонниками движения. Несмотря на то, что это движение зародилось в Соединенных Штатах, к нему также присоединились женщины во Франции (#BalanceTonPorc), арабских странах (#AnaKaman), Индии (#MeTooIndia), Украине (#IAmNotAfraidToSayIt) и Мексике (#MeTooMexico).

24. Благодаря технологиям шифрования, псевдонимности и другим элементам безопасности лица, принадлежащие к группам меньшинств, могут находить друг друга и создавать сообщества. Совет по правам человека особо отмечает, что «технические средства обеспечения безопасности и защиты конфиденциальности электронных сообщений, в том числе меры по шифрованию и обеспечению анонимности, могут играть важную роль для обеспечения осуществления прав человека, в частности прав на неприкосновенность частной жизни, свободное выражение мнений и свободу мирных собраний и ассоциации»[26]. Специальный докладчик утверждает, что это

[23] См. A/HRC/29/25/Add.1.

[24] A/HRC/35/9, пункты 23–24.

[25] Исследовательский центр Пью, “How social media users have discussed sexual harassment since #MeToo went viral”, 11 October 2018.

[26] См. резолюцию 38/7 Совета по правам человека.

относится и к организации и функционированию ассоциаций. Эти инструменты предоставляют людям и субъектам гражданского общества безопасное интернет-пространство, чтобы собираться вместе и устанавливать связи с другими членами их группы, а также организовывать и координировать мероприятия без неправомерного вмешательства третьих сторон и правительств[27].

25. За счет использования социальных сетей, платформ для электронных петиций и краудфандинга организации гражданского общества имеют возможность охватывать новые аудитории, распространять информацию, привлекать новых членов и находить средства в таких формах, которые ранее были невозможными или чрезвычайно дорогостоящими. Например, после землетрясения в Мексике в 2018 году группа граждан организовались в сети через #Verificado19S[28], чтобы давать достоверную информацию и оказывать помощь жертвам необходимыми ресурсами. В Турции такие организации, как Oy ve Ötesi, используя инструменты социальных сетей, смогли заручиться поддержкой более 60 000 добровольцев для наблюдения за более чем 130 000 урн для голосования в ходе всеобщих выборов в ноябре 2015 года. В Соединенных Штатах за одни выходные Американский союз защиты гражданских свобод собрал млн долларов в виде онлайновых пожертвований в поддержку своей деятельности в интересах прав иммигрантов. Аналогичным образом, после того, как в Российской Федерации были введены строгие ограничения в отношении доступа гражданского общества к иностранным ресурсам, правозащитная организация «ОВД-Инфо» использовала краудфандинг для мобилизации поддержки и сбора небольших частных пожертвований от российских граждан[29]. Кроме того, цифровые технологии становятся все более важным инструментом для профсоюзов для выполнения своих основных функций, в том числе для организации протестов, поддержания связи со своими членами и предоставления площадки для обсуждения и принятия решений[30].

26. Многие группы гражданского общества используют технологии для поиска инновационных подходов для решения социальных проблем. Например, в проекте Landmark[31] предоставляются общедоступные карты местности и другие важные данные о земле, которые находятся в коллективном владении и используются коренными народами и местными общинами во всем мире для обеспечения их защиты. В рамках проекта Eyewitness (свидетель)[32] разработаны технологии, повышающие потенциал субъектов гражданского общества и отдельных лиц в плане документирования и регистрации нарушений прав человека. Разработка программного обеспечения с открытыми исходными кодами и бесплатных типовых программных блоков были в основном инициированы организациями гражданского общества, такими как Mozilla Foundation и Wikimedia. В целях повышения защищенности цифровых сообщений группами гражданского общества были разработаны такие платформы, как Signal и Crabgrass. Создание местных сетей в поселениях беженцев и общинах коренного населения служит еще одним примером инновационного подхода гражданского общества к решению социальных проблем.

27. Цифровые технологии должны рассматриваться властями в качестве «замечательной возможности взаимодействия с широкой и разнообразной аудиторией до начала и в ходе проведения мирных собраний с целью информирования ее о своей роли и функциях и в конечном итоге − для установления и укрепления доверия среди населения»[33]. Аналогичным образом, государства должны признать важность технологий для содействия осуществлению прав людей на участие общественности. Специальный докладчик приветствует усилия правительств многих стран по созданию

[27] См. A/HRC/29/32 и A/HRC/38/35/Add.5.

[28] #Verified19S.

[29] A/HRC/35/28, пункт 62.

[30] Jeffrey M. Hirsch, “Worker collective action in the digital age”, *West Virginia Law Review*, vol. 117 (2015), pp. 921–959; и Klaus Schoemann, “Digital technology to support the trade union movement”, *Open Journal of Social Sciences*, vol. 6, No. 1 (2018), pp. 67–82.

[31] См. www.landmarkmap.org.

[32] См. www.eyewitnessproject.org.

[33] A/HRC/23/39, пункт 74.

онлайновых площадок, через которые заинтересованные лица могут представлять свои подписи и вести сбор подписей под петициями в отношении государственных стратегий и законодательных действий.

28. Эти примеры свидетельствуют о широте сферы использования цифровых технологий для осуществления прав на свободу мирных собраний и ассоциации, а также о взаимосвязи между реальным и виртуальным пространством. Специальный докладчик подчеркивает, что права на свободу мирных собраний и ассоциации часто беспрепятственно осуществляются как в виртуальном, так и в реальном пространстве. Так, например, многие ассоциации имеют офисы, где люди встречаются друг с другом в реальной жизни. В то же время они используют цифровые технологии для осуществления повседневной деятельности и в качестве площадки для проведения онлайновых дискуссий и собраний. Аналогично этому ассоциации, которые главным образом функционируют в интернет-пространстве, могут также проводить очные обсуждения и собрания. Масштабы деятельности в реальном и виртуальном пространстве зависит от членского состава, стратегий и целей ассоциации. Проще говоря, международное право защищает права на свободу мирных собраний и ассоциацию, независимо от того, осуществляются ли они лично, с помощью современных технологий или технологий, которые будут изобретены в будущем[34].

B. Тенденции в государственных ограничениях

29. Специальный докладчик выражает обеспокоенность по поводу различных мер и методов, которые используются государствами для контроля и ограничения доступа к использованию цифровых технологий для осуществления прав на свободу собраний и ассоциации. Все чаще принимаются законы, криминализирующие онлайновый контент, что оказывает значительное сдерживающее воздействие на информационно-пропагандистскую деятельность и мобилизацию людей для участия в тех или иных мероприятиях. Во многих странах используются такие меры, как отключение коммуникационных сетей и сервисов в ходе выборов и публичных демонстраций, а также блокировка веб-сайтов, принадлежащих группам гражданского общества, включая правозащитные организации. Демонстрируя изощренную способность быстрого освоения новых технических средств, некоторые государства, а также злонамеренные третьи стороны, все чаще используют цифровые технологии для слежения за деятельностью и преследования в сети представителей гражданского общества, правозащитников, политических лидеров оппозиции и организаторов мирных публичных собраний. Все это значительно сокращает пространство, в котором люди могут отстаивать и продвигать общие интересы. В частности, Совет по правам человека обеспокоен «новой тенденцией к дезинформации и неоправданным ограничениям, препятствующим пользователям Интернета иметь доступ к информации или распространять информацию в ключевые политические моменты, что влияет на возможности организации и проведения собраний»[35].

30. В настоящем разделе анализируются эти действия государств для определения того, насколько они соответствуют статьям 21 и 22 Пакта, а также проверяются соответствующие аналитические критерии, изложенные в этих статьях.

1. Законность

31. Как уже отмечалось, любое ограничение права на свободу мирных собраний и права на свободу ассоциации должно иметь правовую основу (т. е. «соответствовать закону» или быть «предусмотрено законом» соответственно), которую равным образом должны иметь мандат и полномочия ограничивающего органа[36]. Сам по себе

[34] Douglas Rutzen and Jacob Zenn, “Assembly and association in the digital age”, *International Journal of Not-for-Profit Law*, vol. 13, issue 4 (December 2011), p. 67.

[35] См. резолюцию 38/11 Совета по правам человека.

[36] Статья 21 Пакта предусматривает, что осуществление права на мирные собрания не подлежит никаким ограничениям, кроме тех, которые налагаются в соответствии с законом. В пункте 2

закон должен быть достаточно точным, с тем чтобы давать человеку возможность оценить, является ли его поведение нарушением закона, а также предусматривать возможные последствия любого такого нарушения[37].

32. В различных странах все чаще принимаются законы, устанавливающие уголовную ответственность за доступ к цифровым средствам и их использование. Эти законы предусматривают уголовную ответственность в зачастую расплывчатой и нечеткой форме, что создает возможность произвольного и дискреционного толкования и порождает правовую неопределенность. Они, по сути, не соответствуют правовым стандартам в отношении допустимых ограничений, предусмотренных в статьях 21 и 22 Пакта. В качестве примера можно привести законы о борьбе с киберпреступностью, терроризмом, законы о слежке и законы, запрещающие протесты.

Законы о борьбе с киберпреступностью

33. К примеру, запрет на использование электронных устройств «в целях разрушения гармоничных отношений в обществе, дестабилизации, подрыва основ общества, посягательства или нарушения правопорядка»[38], который содержится в принятом в 2018 году Законе о цифровой безопасности в Бангладеш, предоставляет должностным лицам излишнюю свободу действий для определении того, что является незаконным действием, а также возможность возбуждать уголовное преследование, исходя из произвольных и субъективных оснований. Власти могут приравнивать призывы к мирных собраниям в социальных сетях с созданием нестабильности или разрушением гармоничных отношений в обществе. Другие законы о противодействии киберпреступности наделяют правительства широкими полномочиями блокировать веб-сайты, которые критически отзываются об органах власти, в частности веб-сайты правозащитников[39], на основе широко определенной концепции национальной безопасности.

Законы о борьбе с терроризмом

34. Мандатарий неоднократно высказывал обеспокоенность по поводу слишком общих формулировок, которые часто используются в антитеррористическом законодательстве[40]. Хотя Специальный докладчик сознает, что государства заинтересованы в защите национальной и общественной безопасности, которые являются законными основаниями для ограничения свободы ассоциации и собраний, эти законы зачастую сформулированы так, что создают возможность для злоупотреблений. Так, во многих из них в определении терроризма используются такие общие и субъективные концепции, как «повсеместный террор с помощью политического экстремизма», «серьезные общественные беспорядки»[41], «нарушение функционирования общественных служб», «провоцирование насилия в ходе демонстраций» и «запугивание населения, угрожающее солидарности» страны[42]. Из-за невнятности концепций чрезвычайно трудно определить с разумной степенью определенности, какое поведение (в сети или вне ее) будет квалифицировано как «терроризм». В особенно уязвимое положение попадают организации и отдельные лица, которые, как считается, поощряют или пропагандируют взгляды и убеждения, не разделяемые большинством населения или неблагоприятные для властей. Это оказывает на них значительное сдерживающее воздействие и исключает их из цифрового пространства.

статьи 22 закреплено, что «пользование этим правом не подлежит никаким ограничениям, кроме тех, которые предусматриваются законом».

37 A/HRC/20/27, пункт 16; и A/HRC/31/66, пункт 30.

38 See BGD 4/2018, accessible from https://spcommreports.ohchr.org/Tmsearch/TMDocuments.

39 См., например, EGY 13/2017.

40 A/HRC/26/29, пункт 59.

41 См. BRA 8/2015.

42 Asian Forum for Human Rights and Development (Forum-Asia), *Instruments of Repression: A Regional Report on the Status of Freedoms of Expression, Peaceful Assembly, and Association in Asia*, pp. 84 and 89.

Законы о слежке

35. Мандатарии подчеркивают, что слишком широкие и нечеткие законы о слежке часто не позволяют выбрать конкретное лицо в качестве объекта для слежения на основе обоснованных подозрений[43]. Так, например, принятый в 2016 году Закон о правовом регулировании следственных полномочий Соединенного Королевства Великобритании и Северной Ирландии содержит туманные формулировки, которые позволяют властям выбирать в качестве объекта слежения группу или категорию людей без необходимости индивидуальной идентификации каждого отдельного объекта[44]. Другие виды законодательства о слежке наделяют государства широчайшими правами контролировать сетевую деятельность граждан. В качестве примера можно привести законопроект Австралии о внесении изменений в законы, регулирующие деятельность в сфере телекоммуникаций, и другое законодательство, который включает положения, которые наделяют власти неограниченными полномочиями заставлять компании предоставлять органам безопасности доступ к зашифрованным пользовательским данным и ослаблять средства криптографической защиты данных[45]. Риски злоупотребления увеличиваются с учетом того, что многие существующие законы и нормативные положения о слежке не поспевают за быстрыми изменениями в технических средствах наблюдения и их потенциальными возможностями.

Законы о средствах массовой информации и борьбе с «фальшивыми новостями»

36. В ходе консультаций с организациями гражданского общества была выражена обеспокоенность по поводу туманных формулировок Камбоджийского межведомственного указа (пракас) № 170 от 28 мая 2018 года, который запрещает сетевую деятельность, «направленную на создание хаоса в обществе». Это положение предоставляет властям чрезмерную свободу действий, чтобы запрещать самые разные виды онлайн-деятельности, включая рассылку фото- и видеоматериалов о неправомерных действиях полиции в отношении демонстрантов, распространение сообщений с призывами к участию в мирных демонстрациях и политический активизм. Правила также предусматривают суровые меры наказания, и организации гражданского общества рискуют попасть в черный список за распространения запрещенных материалов, что является несоразмерным и несовместимым с правом на свободу ассоциации. Кроме того, эти ограничения были введены посредством указа правительства, что ко всему прочему ставит вопрос о законности[46].

Законы о демонстрациях

37. К примеру, принятый в Российской Федерации «закон Яровой» вносит в Уголовный кодекс чрезмерно широкие изменения, запрещающие «побуждение, вербовку или вовлечение иным способом» других лиц в организацию «массовых беспорядков»[47]. Публикация заявлений в Интернете считается отягчающим обстоятельством. В том же ключе в Казахстане Уголовный кодекс запрещает предоставление «помощи» «незаконным» собраниям, в том числе «с использованием средств коммуникации»[48]. Широкая формулировка этих положений неоправданно ограничивает права на свободу мирных собраний, ассоциации и выражения мнений, потенциально квалифицируя в качестве преступления распространение, обсуждение, поиск или отсылку к информации о протестном мероприятии.

[43] См. A/HRC/35/28/Add.1.
[44] Там же.
[45] См. AUS 5/2018.
[46] Межамериканская комиссия по правам человека, “Second report on the situation of human rights defenders in the Americas” (OEA/Ser.L/V/II. Doc. 66), para. 165.
[47] См. RUS 7/2016.
[48] A/HRC/29/25/Add.2, пункт 57.

2. Законная цель

38. Ограничения прав на свободу мирных собраний и ассоциации должны преследовать законную цель. Законными целями в Пакте признаются только следующие: «государственная или общественная безопасность, общественный порядок (ordre public), охрана здоровья и нравственности населения или защита прав и свобод других лиц». Государства не могут ссылаться на допустимые основания для сокрытия незаконных целей.

Квалификация онлайновой деятельности в качестве уголовного преступления

39. Криминализация онлайновой деятельности отдельных лиц и организаций является тенденцией во многих странах мира[49]. Людей часто обвиняют в совершении нечетко определенных преступлений, предусмотренных в законах о противодействии терроризму, киберпреступности и антипротестных законах. Так, во Вьетнаме правозащитник был арестован и предстал перед судом за комментарии в Интернете, якобы содержащие критику правительства[50]. В Боливарианской Республике Венесуэла за совершение преступления подстрекательства к насилию был осужден лидер политической оппозиции, призывавший к антиправительственным выступлениям в социальных сетях[51]. В Объединенных Арабских Эмиратах были арестованы и предстали перед судом правозащитники по обвинению в «распространении в Интернете ложной и недостоверной информации в целях разжигания ненависти и внесения раскола в общество»[52], а также за использование социальных сетей «в целях создания угрозы государственной безопасности и оскорбления правителей» в соответствии с положениями Закона о борьбе с киберпреступностью[53]. В Египте были арестованы и привлечены к уголовной ответственности активисты за «членство в организации, учрежденной в нарушение Конституции» и за «подрыв государственных институтов» в отместку за высказывания в социальных сетях[54]. В Саудовской Аравии один из учредителей Саудовской Ассоциации за гражданские и политические права, как сообщалось, был приговорен к восьми годам тюремного заключения и запрету на поездки в течение восьми лет за «нарушение статьи 6 Закона о киберпреступности путем настраивания общественного мнения против правителей страны и подписания размещавшихся в онлайновом режиме заявлений с призывами к проведению демонстраций», а также за «нежелание выполнять судебное постановление о запрещении деятельности» Саудовской Ассоциации за гражданские и политические права[55]. В Саудовской Аравии женщины-правозащитники, протестующие против запрета на вождение для женщин, были привлечены к судебной ответственности по делам, связанным с терроризмом, в том числе за «подстрекательство к протестам», «попытки возбуждения общественного мнения» и «разжигание протестов и публикацию сообщений в социальных сетях»[56].

40. Несмотря на то, что государства, выдвигая такие обвинения, часто ссылаются на национальную безопасность и общественный порядок, на самом деле уголовное преследование слишком часто используется для борьбы с инакомыслием и контроля онлайнового пространства, что не является законной целью правительства и представляет собой прямое нарушение статей 21 и 22 Пакта. Ни один человек не должен нести уголовную, гражданскую или административную ответственность за организацию, поддержку или участие в мирной демонстрации протеста[57] или за создание и управление ассоциацией для достижения законной цели. Инакомыслие

[49] A/71/373, пункты 29–35.
[50] См. VNM 1/2017.
[51] См. Рабочая группа по произвольным задержаниям, мнение № 26/2014.
[52] См. ARE 1/2018.
[53] См. ARE 5/2013.
[54] См. EGY 4/2017.
[55] См. SAU 4/2016.
[56] См. SAU 11/2018, а также SAU/1/2017.
[57] A/HRC/31/66, пункт 27.

является легитимной частью осуществления прав на свободу мирных собраний и ассоциации и должно защищаться в интернет-пространстве и в реальной жизни[58].

Произвольное блокирование онлайнового контента

41. Полное блокирование веб-сайтов правозащитных организаций и политических оппозиционных партий становится все более распространенным явлением во многих регионах мира, в том числе в странах Ближнего Востока и Северной Африки. Например, в Объединенных Арабских Эмиратах и Саудовской Аравии власти регулярно блокируют веб-сайты, содержащие критические материалы. Особенно часто репрессивные меры принимаются в отношении интернет-ресурсов, принадлежащих организациям гражданского общества и правозащитным группам, таким как кампания #Women2Drive Саудовской Аравии, сайт которой был заблокирован в 2013 году. Аналогичным образом египетские власти заблокировали несколько веб-сайтов правозащитных организаций[59]. «Великий китайский сетевой щит» систематически блокирует тысячи веб-сайтов и онлайновых ресурсов за пределами Китая, содержащих такие ключевые слова, как «демократия» и «права человека»[60].

42. Веб-сайт отдельного человека или ассоциации является важным средством для человека или ассоциации, которое позволяет: отстаивать свои взгляды и принципы; поднимать вопросы, вызывающие озабоченность у общественности, и участвовать в публичных дебатах; сообщать о нарушениях прав человека; публиковать исследования; искать, получать и распространять всякого рода информацию и идеи; создавать коалиции и сети с другими организациями, в том числе из-за рубежа; участвовать в деятельности по сбору средств; привлекать новых членов и добровольцев; и укреплять сотрудничество с международными и региональными правозащитными органами. В целом блокирование веб-сайтов является крайней, непропорциональной мерой, которая серьезно ограничивает возможности для осуществления этой деятельности и поэтому подрывает осуществление права на свободу собраний и ассоциации. Во многих случаях эти меры, как представляется, неправомерно используются для подавления инакомыслия и, по своей сути, не могут быть оправданы осуществлением какой-либо законной цели. Специальный докладчик считает, что запрещение человеку или ассоциации публиковать материалы в сети «только на том основании, что в нем может содержаться критика в адрес правительства или политико-социальной системы, сторонником которой оно является»[61] идет вразрез с правами на свободу мирных собраний, ассоциации и выражения мнений.

Спонсируемые правительством троллинг и кибератаки

43. Ряд государств задействует технологии для наблюдения и препятствования работе правозащитников и представителей гражданского общества. Методы могут быть разными. Среди них можно назвать взлом телефонов и компьютеров, угрозы расправой и изнасилованием, распространение отредактированных фотоматериалов, временное блокирование счетов, кражу хэштегов, распространение теорий заговора, обвинения в измене и поддержку крайних дискриминационных воззрений. Хотя Специальный докладчик сознает, что эти деяния совершаются не только государствами, правительства несут ответственность в этом контексте за привлечение третьих сторон и поощрение их действий.

44. Эти посягательства являются прямым нарушением прав граждан на свободу мирных собраний и ассоциации, поскольку они не могут быть оправданы осуществлением какой-либо законной цели в демократическом обществе. Их цель состоит в обратном: запугать представителей гражданского общества, подорвать их

[58] A/HRC/20/27, пункт 84.

[59] См. EGY 13/2017.

[60] Организация «Фридом Хаус», Freedom on the Net 2018, см. https://freedomhouse.org/report/freedom-net/freedom-net-2018. См. также Rebecca MacKinnon, *Consent of the Networked: The Worldwide Struggle for Internet Freedom* (Basic Books, 2012), pp. 31–47.

[61] A/66/290, пункт 39.

авторитет и легитимность и лишить их аудитории, необходимой для мобилизации людей в цифровом пространстве. Эти посягательства подрывают способность организаций и активистов гражданского общества распространять и получать информацию и общаться с другими людьми. Они создают стимулы для самоцензуры, угрожая физической безопасности и неприкосновенности личности.

45. К примеру, троллям дается указание распространять пропаганду, изолировать или заглушать критические мнения и препятствовать антиправительственным движениям, одновременно с этим усиливая сигналы официальных властей и увеличивая число их сторонников[62]. Так, в Омане власти «систематически взламывают и захватывают сетевые аккаунты и наводняют такие социальные сети, как Twitter, бесконечным потоком хэштегов со ссылками, тем самым срывая дискуссии по конкретным вопросам»[63].

46. Другим примером этой тенденции служит использование коммерческого шпионского ПО типа FinFisher и Pegasus для организации кибератак против представителей гражданского общества. Хорошо задокументированы случаи использования шпионских программ Pegasus против активистов и правозащитников в Бахрейне, Казахстане, Мексике, Марокко, Саудовской Аравии, Объединенных Арабских Эмиратах и других странах[64]. Эти кибератаки позволяют взламывать их устройства и мониторить в режиме реального времени их сообщения, местонахождение и деятельность[65], причем объекты атаки могут находится как на территории государства, так и за границей[66].

47. Еще один метод состоит в проникновении в группы в социальных сетях и на форумах и отслеживании сетевой активности гражданского общества, становясь «другом» активистов. Анализ открытых источников также позволяет в порядке упреждающих действий срывать мирные протесты путем ареста организаторов, которые обмениваются сообщениями и планируют свои акции в Интернете.

48. Особую опасность эти нападения представляют для женщин, а также лесбиянок, гомосексуалистов, бисексуалов, транссексуалов и интерсексуалов. Например, правительство Египта, как сообщалось, выявляло и арестовывало активистов лесбиянок, гомосексуалистов, бисексуалов, транссексуалов и интерсексуалов, проникая на их ресурсы и осуществляя слежку за их деятельностью на сетевом ресурсе Grindr[67]. Власти Бразилии использовали Tinder в целях налаживания связей с последующим наблюдением за женщинами-активистами, участвующими в протестах[68]. В Таиланде против женщин-правозащитников велась мощная кампания по дискредитации и травле, при этом им угрожали расправой в блогах и в социальных сетях[69]. Эти посягательства осуществляются, в частности, путем распространения отретушированных изображений обычно сексуального и гендерного характера; распространения дискредитирующей информации, зачастую полностью состоящей из вредных и отрицательных гендерных стереотипов; отправки агрессивных ненавистнических посланий с угрозами насилия в социальных сетях, включая призывы к групповому изнасилованию и убийству; и вмешательства в частную жизнь, включая взлом компьютеров и телефонов членов семьи и разглашения и публикации номера телефона, домашнего адреса, личных и семейных фотографий. Мандатарий поддерживает выводы Специального докладчика по вопросу о насилии в отношении женщин, его причинах и последствиях о том, что сетевые злоупотребления в

[62] Institute for the Future, “State-sponsored trolling: how governments are deploying disinformation as part of broader digital harassment campaigns” (2018).

[63] A/HRC/29/25/Add.1, пункт 34.

[64] См., например, the Citizen Lab, “Hide and seek: tracking NSO Group’s Pegasus spyware to operations in 45 countries”.

[65] См. LBN 2/2018.

[66] Резюме независимых судебных экспертов, представленное по делу *John Doe a.k.a. Kidane v. Federal Democratic Republic of Ethiopia*, рассматриваемому Апелляционным судом Соединенных Штатов по округу Колумбия.

[67] Article 19, “Apps, arrests and abuse in Egypt, Lebanon and Iran”, February 2018.

[68] Privacy International, “State of privacy Brazil”.

[69] См., например, THA 6/2017.

отношении женщин представляют собой прямое посягательство на роль женщин и их полноценное участие в публичной жизни и что они должны надлежащим образом расследовались и пресекаться[70].

3. Необходимость и соразмерность в защите законной цели

49. Согласно статье 21 и пункту 2 статьи 22 Пакта, ограничения свободы собраний и ассоциации должны быть необходимыми и соразмерными в демократическом обществе в интересах государственной или общественной безопасности, общественного порядка, охраны здоровья или нравственности населения или защиты прав и свобод других лиц. Как уже указывалось в рамках данного мандата специальной процедуры, слово «необходимые» означает, что «для вмешательства» должна существовать насущная общественная потребность. В тех случаях, когда возникает такая насущная общественная потребность, государства должны обеспечить, чтобы любые ограничительные меры не выходили за рамки того, что приемлемо в демократическом обществе, которое «существует лишь при наличии плюрализма, терпимости и широты взглядов»[71]. Ответственность за установление этого основания всегда возлагается на государство.

50. Государства часто препятствуют осуществлению права на свободу собраний и ассоциации в сети с помощью ограничений, которые не являются ни необходимыми, ни соразмерными с учетом конкретных называемых угроз. В качестве примера этого можно привести нарушение работы сети, санкционированные государством блокировки сетевого контента, введение налогов на социальные медиа, а также слежку с использованием цифровых технологий.

Сбои в работе сети

51. Согласно имеющимся данным[72], в связи с публичными манифестациями и мирными протестами были зафиксированы как минимум 40 сетевых сбоев в 2018 году, 37 – в 2017 году и 27 – в 2016 году. Наиболее часто такие сбои происходят в Азии и в Африке, при этом случаи отключения Интернета и запрета социальных сетей также имели место в Индии[73], Исламской Республике Иран[74], Чаде[75], Камеруне[76] и Того[77]. Только в Индии в период между 2016 и 2018 годами было зафиксировано 64 сбоя в работе Интернета в связи с проведением демонстраций. О перебоях в работе сети во время проведения мирных собраний сообщалось и в других регионах мира, что свидетельствует о том, что это становится опасной глобальной тенденцией. С 2016 года также растет количество сбоев в работе сети и запретов социальных медиа в ходе выборов, что серьезно сказывается на присутствии в публичной сфере оппозиционных политических партий и общественных движений, а также их способности отмобилизовывать своих сторонников в решающий момент. Эти меры сужают возможности правозащитников осуществлять свою деятельность и документировать нарушения прав человека[78].

52. Специальный докладчик полагает, что отключение сети является явным нарушением международного права и ничем не может быть обосновано. Отключение не отвечает установленным критериям для ограничения права на мирные собрания, содержащиеся в статье 21, и для ограничения права на свободу ассоциации в соответствии с пунктом 2 статьи 22 Пакта. В большинстве случаев распоряжения об отключении сети не имеют под собой правовой основы. В тех случаях, когда правовые основания все же имеются, приказы об отключении часто отдаются на основе общих

[70] См. A/HRC/38/47.
[71] A/HRC/20/27, пункт 17.
[72] Access Now, #KeepitOn campaign, and Shutdown Tracker Optimization Project (STOP).
[73] См. IND 5/2016, IND 3/2017 и IND 7/2017.
[74] См. IRN 1/2018.
[75] См. TCD 3/2016.
[76] См. CMR 1/2018.
[77] См. TGO 1/2017.
[78] A/68/299, пункт 28.

и туманных положений при отсутствии мер надлежащего независимого надзора[79]. Хотя эти меры, как правило, оправдываются соображениями национальной безопасности и охраны общественного порядка, они представляют собой несоразмерное – и, как правило, неэффективное – средство достижения этих законных целей.

53. Эти крайние меры по целому ряду аспектов наносят ущерб правам человека, экономической деятельности, общественной безопасности и работе экстренных служб, который перевешивает предполагаемые выгоды. Перебои в работе сети зачастую приводят к обратному результату, порождая хаос и беспорядки. В контексте протестов и выборов, когда напряженность достигает апогея, эти средства, по сути, необходимы для того, чтобы предотвращать дезинформацию и развеивать слухи, а также для защиты прав на свободу и личную неприкосновенность, поскольку обеспечивают доступ к экстренной помощи и связь с семьей и друзьями[80]. Совет по правам человека выразил глубокую обеспокоенность «мерами, которые в нарушение международного права прав человека имеют своей целью или результатом умышленное недопущение или нарушение доступа к информации или ее распространения в режиме онлайн»[81].

Налог на социальные сети

54. Специальный докладчик обеспокоен тем, что недавнее введение налогов на использование социальных сетей в ряде стран может в гораздо большей степени подрывать возможности уязвимых групп населения в плане реализации свобод ассоциации и собраний, что эти «налоги на социальные сети» могут дать повод для обеспокоенности в отношении необходимости или соразмерности. Так, например, налог на использование социальных сетей в Уганде «соразмерно и негативно влияет на возможность пользователей получать приемлемый по цене доступ к Интернету и, таким образом, необоснованно ограничивает их право на свободу выражения мнений и их права на свободу мирных собраний и ассоциации, что особенно больно бьет по малоимущим гражданам, для которых расходы на покупку трафика объемом в 1 Гбайт в месяц составят около 40% их среднемесячного дохода»[82]. Хотя эти налоги могут быть экономически оправданы, государства должны принимать меры для обеспечения того, чтобы такие налоги не ограничивали в непропорциональной степени возможности людей общаться с другими членами общества и не расширяли цифровой разрыв.

Слежение с использованием цифровых технологий

55. Во всем мире в течение последнего десятилетия ширится излишнее и несоразмерное использование мер слежения. Требование о необходимости предполагает демонстрацию того, каким образом слежение позволит достичь заявленной цели, которая зачастую ставится под угрозу самим фактом применения слежения. Например, такие государства, как Австралия и Соединенное Королевство Великобритании и Северной Ирландии, утверждают, что национальная безопасность или общественный порядок оправдывает ослабление средств криптографической защиты информации[83]. Как подчеркнул Специальный докладчик по вопросу о поощрении и защите права на свободу мнений и их свободное выражение, «в среде экспертов по вопросам информационной безопасности имеется широкий консенсус в отношении того, что такие факторы уязвимости влекут за собой значительные расходы на обеспечение цифровой безопасности в целом, поскольку ими могут воспользоваться несанкционированные третьи стороны, даже если эти средства предназначены исключительно для использования правительственными органами»[84].

[79] См. A/HRC/29/25/Add.2.

[80] Jan Rydzak, Global Network Initiative, “Disconnected: a human rights-based approach to network disruptions”.

[81] См. резолюцию 38/7 Совета по правам человека.

[82] См. UGA 3/2018.

[83] См. A/HRC/35/28/Add.1.

[84] См. A/HRC/38/35/Add.5.

56. Принцип соразмерности требует доказательства того, что применяемая мера является наименее инвазивной. Массовое слежение или сбор и анализ всех коммуникационных метаданных[85], которые явно направлены против ассоциаций между людьми, по своей сути являются несоразмерными[86]. Аналогичным образом, законодательные требования к провайдерам коммуникационных сервисов хранить у себя личные и конфиденциальные данные и регистрировать сим-карты на неизбирательной основе позволяют властям получать доступ к информации, которая не имеет отношения и существенного значения для любого серьезного преступления или конкретной угрозы[87]. Законы об обязательной регистрации сим-карт, в частности, «в сущности требуют от большинства населения раскрывать информацию, позволяющую установить личность» соответствующему государству[88]. Технологии распознавания лиц, которые широко используются в ходе крупных культурно-массовых мероприятий, спортивных состязаний, музыкальных фестивалей и политических митингов, также вызывают обеспокоенность в части соразмерности применения. Аналогичным образом, системы международной идентификации мобильного абонента (IMSI-кетчеры)[89] позволяют странам снимать данные с тысяч мобильных телефонов в конкретном районе или в ходе общественных мероприятий, например политических демонстраций. Такие методы используются для идентификации и слежения за всеми лицами, принимающими участие в конкретных мероприятиях или находящимися в определенных общественных местах[90]. Эти формы идентификации и сбора данных нарушают право людей на анонимность в общественных местах и оказывают значительное «сдерживающее влияние» на решения об участии в массовых мероприятиях[91].

57. Использование шпионских методов для неизбирательной массовой слежки за теми, кто осуществляет свое право на мирные собрания и ассоциации, как в реальном, так и цифровом пространстве, должно быть запрещено. Слежение за людьми, осуществляющими свои права на мирные собрания и ассоциации, может проводиться только на выборочной основе, если имеются разумные основания подозревать их в совершении или умысле на совершение серьезных уголовных преступлений, при этом должны соблюдаться строжайшие правила, исходящие из принципов необходимости и соразмерности и предусматривающие скрупулезный судебный надзор.

C. Цифровые технологические компании – основные проблемы

58. Поскольку такие компании контролируют онлайновые платформы и средства, они обязаны по требованию государства предоставлять доступ к пользовательским данным. В зависимости от обстоятельств такие требования могут принимать форму неофициальных запросов или давления. В тех случаях, когда национальные законы нарушают международные стандарты и нормы в области прав человека, компаниям приходится принимать решения о выполнении конкурирующих правовых обязательств, которые ставят под угрозу соблюдение ими прав человека, а также возможность работы в конкретных странах. Это может приводить к нарушению прав пользователей на мирные собрания и ассоциацию, а также ставить вопрос о транспарентности и подотчетности. Компании по всему миру зачастую не раскрывают надлежащим образом информацию о сборе данных и запросах правительств[92].

[85] Под метаданными понимается относящаяся к сообщениям информация, например о геолокации, продолжительности сообщения и сторонах коммуникативного процесса.

[86] См. резолюцию 34/7 Совета по правам человека.

[87] A/HRC/29/32, пункт 51; и A/HRC/35/22, пункт 20.

[88] Там же.

[89] См. A/HRC/35/28/Add.1.

[90] The Human Rights, Big Data and Technology Project, “The Universal Declaration of Human Rights at 70: putting human rights at the heart of the design, development and deployment of artificial intelligence”, 20 December 2018, p. 31.

[91] Daragh Murray and Pete Fussey, “Bulk surveillance in the digital age: rethinking the human rights law approach to bulk monitoring of communications data”, *Israel Law Review*, vol. 52, issue 1.

[92] Ranking Digital Rights, The Ranking Digital Rights 2018 Corporate Accountability Index, chap. 3, “Inadequate disclosure”.

Доклады о транспарентности, выпущенные крупнейшими глобальными технологическими компаниями из Соединенных Штатов и Европы, дают позитивные примеры, которые следует расширять и совершенствовать.

59. Методы контент-модерирования на онлайн-ресурсах в соответствии с их собственными общественными нормами также вызывают озабоченность в плане соблюдения прав человека, в том числе в отношении права на свободу мирных собраний и ассоциации. В частности, контент-политика социальных сетей отражает различные толкования того, что является приемлемым выражением или поведением, которые могут не отвечать международным стандартам и нормам в области прав человека. Кроме того, методы реализации этой контент-политики посредством модерирования контента могут быть также несовместимы с нормами в области прав человека и ставить вопросы произвольного вмешательства, несмотря на некоторые попытки усовершенствования. Реализация контент-политики также, как представляется, в непропорциональной степени негативно сказывается на тех, кто имеет определенный общественный статус. По сути, опора на пользователей в плане получения сигналов о нарушении общественных норм (т. е. некая форма охраны правопорядка силами местной общественности) в реализации контент-политики ставит под угрозу активистов и тех, кто призывает к мобилизации общественности, в том смысле, что их контент может быть произвольно удален с ресурсов, а аккаунт заблокирован или деактивирован. Те, кто имеет определенный общественный статус, не только чаще чем менее популярные пользователи становятся объектом жалоб (с учетом их известности), но также нередко становятся объектом направленных кампаний, имеющих целью удаление из сети их контента и блокирование аккаунта. Проблема усугубляется использованием для модерирования сетевого контента искусственного интеллекта, поскольку выявление материалов, подлежащих блокировке, все чаще осуществляется с помощью автоматизированных процессов.

60. Также используются алгоритмические системы для изменения поисковой доступности и ранжирования информации, т. е. для влияния на то, какой контент видят люди, с кем они общаются и какие группы находят. Это означает, что доставка контента может производится исходя из исторической или предполагаемой политической принадлежности или по другим критериям ассоциации, что может быть полезным качеством для тех, кто стремится адресовать информацию конкретной аудитории и общается с единомышленниками, но одновременно с этом также сопряжено с проблемами. Алгоритмические системы обладают возможностью глушить голос активистов и общественных движений, не давать представителям гражданского общества возможности выйти на более широкую аудиторию, усиливать эффект герметизации информационного пространства, а также воспроизводить стереотипы и дискриминацию в ущерб демократическому развитию. Эти меры также могут оказывать несоразмерное воздействие на и без того маргинализированные или подверженные риску группы населения, включая женщин[93]. Алгоритмические системы непрозрачны и постоянно меняются, затрагивая сетевое присутствие отдельных лиц и групп, «не предоставляя им возможности изучить или понять, почему, каким образом и на каком основании это происходит»[94].

61. Политика и функции, относящиеся к сфере неприкосновенности личной жизни и безопасности сообщений пользователей, могут также влиять на осуществление права на свободу мирных собраний и ассоциации. Лишь немногие цифровые технологические компании позволяют использовать псевдонимы или другие способы сокрытия личности или обеспечивают шифрование сообщений. Специальный докладчик приветствует усилия, предпринимаемые приложением Grindr по разработке и внедрению функций безопасности, с тем чтобы защитить лесбиянок, геев, бисексуалов, трансгендеров и интерсексуалов в Египте, Исламской Республике Иран и Ливане от полицейского террора, пыток и тюремного заключения.

62. Отмечая определенные усилия ряда цифровых технологических компаний по включению права на свободу выражения мнений и права на неприкосновенность

[93] A/HRC/35/9, пункт 41.
[94] A/73/348, пункт 32.

частной жизни в оценки рисков и процедуры должной осмотрительности, Специальный докладчик замечает, что права на свободу мирных собраний и ассоциации не принимаются во внимание. По итогам встреч с представителями цифровых технологических компаний он констатировал, что многие такие компании признают ценность и важность этих прав в демократическом обществе, но до сих пор не взяли на себя соответствующие политические обязательства на высоком уровне.

63. Специальный докладчик призывает технологические компании выполнять их обязанности по уважению международно признанных норм в области прав человека, включая права на свободу мирных собраний и ассоциации. В этом контексте приоритетом для этих компаний должно стать эффективное осуществление Руководящих принципов предпринимательской деятельности в аспекте прав человека. Следует расширять применение моделей, которые включают независимую оценку последствий, таких как модель, продвигаемая Глобальной сетевой инициативой[95]. Технологические компании должны брать на себя политические обязательства уважать права на свободу мирных собраний и ассоциации (в дополнение к существующим обязательствам по соблюдению свободы выражения мнений и права на неприкосновенность частной жизни), проводить надлежащие проверки соблюдения этих основных свобод, в том числе путем регулярных оценок воздействия на права человека, и создания эффективных механизмов правовой защиты в целях предоставления компенсаций и иных форм возмещения в случае нарушений. Государства должны принять и осуществлять законы и стратегии, нацеленные на установление обязательных требований к технологическим компаниям в части проведения проверок в целях выявления, предотвращения и смягчения воздействия на права человека от их деятельности и продуктов, а также представления данных об этом и на создание надежных механизмов транспарентности и правовой защиты. Эти законы и политика должны «преследовать цель обеспечения всеобщего доступа и осуществления прав человека»[96] и соответствовать рекомендациям, содержащимся в международных стандартах и нормах. Они должны приниматься только после проведения всеобъемлющих широких консультаций с соответствующими заинтересованными сторонами.

64. По мнению Специального докладчика, в том, что касается ответов на запросы правительств, модерирования контента и принятия технических решений, включая курирование контента с помощью вычислительных средств, цифровые технологические компании должны руководствоваться международным правом в области прав человека. Это означает, что по отношению к решениям компаний, затрагивающим права на свободу мирных собраний и ассоциации, должны применяться стандарты законности, необходимости и легитимности. Специальный докладчик напоминает о последних докладах Специального докладчика по вопросу о поощрении и защите права на свободу мнений и их свободное выражение по теме модерирования контента онлайновых ресурсов и искусственного интеллекта, в которых подробно говорится о сложности и масштабах этих проблем и предлагаются важные рекомендации[97].

V. Выводы и рекомендации

65. **Эпоха цифровых технологий открывает новые возможности для осуществления прав на свободу мирных собраний и ассоциации, но она также несет с собой новые риски и угрозы для этих основных прав. К примеру, введение государствами строгих правовых ограничений, а также использование практики цифрового слежения несет в себе угрозу ликвидации пространства, в котором**

[95] Глобальная сетевая инициатива представляет собой многостороннюю площадку, созданную в 2008 году «в целях защиты и поощрения свободы выражения мнений и неприкосновенности частной жизни в отрасли ИКТ путем установления глобальных стандартов ответственного принятия корпоративных решений». См. https://globalnetworkinitiative.org/team/our-mission/.

[96] Резолюция 38/7 Совета по правам человека, пункт 18.

[97] A/HRC/38/35, пункт 61.

гражданское общество может коллективно продвигать и защищать общие интересы. Действия и бездействие цифровых технологических компаний усугубляют эти риски и создают новые серьезные вызовы для отдельных лиц и организаций, которые стремятся к осуществлению права на свободу собраний и ассоциации в Интернете и в реальной жизни. Эти вызовы в условиях все более активной цифровизации будут усиливаться.

66. **Международное право защищает права на свободу мирных собраний и ассоциации, независимо от того, осуществляются ли они лично, с помощью современных технологий или технологий, которые будут изобретены в будущем. Существующие международные нормы и принципы в области прав человека должны не только определять поведение государств, но и служить основой, которая определяет то, какие разработки будут осуществлять цифровые технологические компании, как они будут реализовывать контроль и управление цифровыми технологиями.**

67. **Государства должны обеспечивать уважение, защиту и осуществление прав на свободу мирных собраний и ассоциации в правовой базе, политике и на практике в соответствии с нормами международного права. Цифровые технологические компании должны взять на себя обязательство уважать свободу мирных собраний и ассоциации, а также проводить надлежащие проверки, с тем чтобы гарантировать, что они не вызывают нарушения этих прав, не способствуют им и не становятся их соучастниками. В русле выполнения своих соответствующих обязанностей государства и цифровые технологические компании должны соблюдать широко признанные принципы недискриминации, плюрализма мнений, транспарентности, широкого участие заинтересованных сторон и доступа к правосудию.**

68. **В этой связи Специальный докладчик выносит следующие рекомендации:**

A. Рекомендации государствам

69. **Государства должны обеспечивать, чтобы любые вмешательства в осуществление прав на свободу мирных собраний и ассоциации были «предусмотрены законом» и «необходимы в демократическом обществе в интересах национальной и общественной безопасности, для охраны общественного порядка (ordre public), охраны здоровья общества или нравственности или для защиты прав и свобод других лиц»[98]. Ограничения с целью обеспечения «национальной безопасности», «общественной безопасности» и «защиты морали» должны быть четко и точно определены, с тем чтобы не допускать злоупотреблений со стороны властей.**

70. **Государствам следует поощрять и облегчать доступ к цифровым технологиям и не вводить ограничений на их использование для осуществления прав на свободу мирных собраний и ассоциации. Стратегии и применяемые на практике методы должны обеспечивать равный доступ к Интернету и цифровым технологиям, ценовую приемлемость и участие в цифровой эпохе для всех в целях преодоления цифрового разрыва.**

71. **Онлайновые собрания и ассоциации играют особенно важную роль для маргинализированных групп, при этом вмешательство в осуществление прав на свободу мирных собраний и ассоциации может оказывать несоразмерное воздействие на отдельные лица и группы, находящихся в уязвимом положении. При выполнении своих обязательств государства должны обращать особое внимание на то, что ограничения на доступ к цифровым технологиям и их использование могут иметь неодинаковые последствия для расовых и религиозных меньшинств, политических оппонентов и активистов, а также лесбиянок, геев, бисексуалов, трансгендеров и интерсексуалов.**

[98] Резолюция 15/21 Совета по правам человека, пункт 4.

72. **Государства должны обеспечивать наличие эффективных и доступных для всех средств защиты прав на свободу мирных собраний и ассоциации. Средства правовой защиты должны быть доступными, приемлемыми, адекватными и своевременными с точки зрения затронутых правообладателей. Государства должны обеспечить наличие средств правовой защиты с помощью независимых судебных, административных и законодательных органов власти или любых иных компетентных независимых органов, предусмотренных правовой системой.**

73. **Государства должны создавать благоприятную правовую основу для осуществления права на мирные собрания и ассоциации в эпоху цифровых технологий посредством:**

a) отмены или отказа от введения законов, которые могут чрезмерно ограничивать или подрывать права на свободу мирных собраний и права на ассоциации, в том числе законов, запрещающих проведение демонстраций протеста;

b) отмены или изменения любых законов и политики, которые допускают возможность нарушения работы и отключения сети, а также отказа от принятия таких законов и стратегий;

c) пересмотра и изменения законов о киберпреступности, слежении и противодействия терроризму, а также приведения их в соответствие с международными нормами и стандартами в области прав человека, регулирующими права на неприкосновенность частной жизни, право на свободу убеждений и их свободное выражение, право на свободу мирных собраний и права на свободу ассоциации;

d) поощрения и защиты применение надежных средств криптографии и анонимизации, в том числе путем принятия законов, правил и политики, согласно которым только суды, а не правоохранительные органы, обладают полномочиями аннулировать право на анонимность.

74. **Отказаться и прекратить применение таких мер, как перекрытие доступа к Интернету и телекоммуникационным услугам. Доступ к Интернету и услугам мобильной телефонной связи должен обеспечиваться в любых обстоятельствах, в том числе во время гражданских беспорядков. Необходимы особые меры для соблюдения, защиты и поощрения доступности и использования цифровых технологий в ходе выборов для целей собраний и ассоциаций.**

75. **Прекратить использование любых мер по блокированию веб-сайтов организаций гражданского общества и правозащитников.**

76. **Запретить использование шпионских методов для неизбирательной массовой слежки за теми, кто осуществляет свое право на мирные собрания и ассоциации, как в реальном, так и цифровом пространстве.**

77. **Отказаться от проведения неправомерного целенаправленного слежения с использованием цифровых средств за представителями гражданского общества, организаторами протестов, меньшинствами и другими лицами, стремящимися осуществить свои права на свободу мирных собраний и ассоциации. Для того чтобы быть допустимыми, меры по целенаправленному слежению должны осуществляться только при условии, что такая деятельность ведется открыто; ограничена по времени; осуществляется в соответствии с установленными международными стандартами правовых норм, законной целью, является необходимой и соразмерной; и подлежит непрерывному независимому контролю, который предусматривает надежные механизмы получения предварительного разрешения, оперативного надзора и проверки. Отдельные лица и группы лиц должны ставиться в известность, если их права нарушаются в результате слежения, при этом должны быть гарантированы эффективные средства правовой защиты.**

78. **Любое применение новых технологий слежения должно также соответствовать вышеупомянутым принципам и стандартам, включая экстерриториальное слежение. Государства должны проводить независимые расследования для изучения обстоятельств применения любых технологий слежения, с тем чтобы общественность могла определить характер и частоту их применения, основания, необходимость и соразмерность такого применения, а также то, является ли использование таких технологий неправомерным или чрезмерным.**

79. **Прекратить применение любых спонсируемых государством методов онлайнового троллинга, запугивания и дезинформации, нацеленных на представителей гражданского общества. Государства должны расследовать эти факты, предоставлять эффективные средства правовой защиты, а также принимать и осуществлять превентивные меры. В этом контексте государствам следует выявлять и устранять гендерные формы онлайнового насилия и барьеры, мешающие женщинам получить доступ к правосудию.**

80. **Государства должны надлежащим образом выполнять свою обязанность по защите от нарушений прав на свободу мирных собраний и ассоциации со стороны коммерческих предприятий путем принятия надлежащих мер, направленных на предупреждение и расследование таких нарушений, наказание за них и компенсацию ущерба посредством эффективной политики, законодательства, нормативного регулирования и судопроизводства. Это включает принятие и осуществление законов и стратегий, имеющих целью установление обязательных требований к технологическим компаниям в части проведения проверок в целях выявления, предотвращения и смягчения воздействия на права человека от их деятельности и продуктов, а также представления данных об этом, и на создание надежных механизмов транспарентности и правовой защиты. Эти законы должны приниматься только после проведения всеобъемлющих широких консультаций со всеми соответствующими заинтересованными сторонами.**

81. **Государства должны подтвердить свою приверженность многостороннему подходу в качестве краеугольного камня процесса управления Интернетом. Эффективное сотрудничество по вопросам, касающимся цифровой сферы, зависит от способности отдельных лиц и групп лиц осуществлять свои права на свободу мирных собраний и ассоциации.**

B. Рекомендации для компаний, действующих в сфере цифровых технологий

82. **Компании должны выполнять свои обязанности по соблюдению международно признанных прав человека, включая права на свободу мирных собраний и ассоциации, путем принятия всех необходимых и законных мер для того, чтобы не вызывать нарушения, не способствовать нарушениям и не становиться соучастниками нарушений этих прав.**

83. **Компаниям следует на высоком уровне взять на себя политические обязательства соблюдать права на свободу мирных собраний и ассоциации, а также признать важность роли гражданского общества в демократии и устойчивом развитии.**

84. **В тех случаях, когда государства требуют от компаний принятия мер по цензурированию, слежению или наблюдению в отношении отдельных лиц или групп, а также предоставления данных, которые они собирают, обрабатывают или хранят, они должны в максимально возможной и допускаемой законом степени стремиться к предотвращению или смягчению негативных последствий их вмешательства для прав человека.**

85. **Компании должны признать международное право в области прав человека в качестве авторитетной основы для обеспечения соблюдения прав на**

свободу мирных собраний и ассоциации в своих продуктах и услугах, а также должны в свете этого оценить свои стратегии. Компании должны обеспечивать, чтобы их политика и правила сообщества были достаточно четкими, доступными и соответствовали международным стандартам в области прав человека. Они должны также представлять более подробные примеры или исследования конкретных примеров того, каким образом они применяют на практике стандарты сообщества, с тем чтобы пользователи понимали условия, при которых может быть предоставлен доступ к их личным данным или информации, ограничен доступ к контенту, заблокирован или ограничен доступ к сервису.

86. **Компании должны проводить надлежащие проверки соблюдения прав человека в целях выявления, предотвращения, смягчения и устранения нарушений прав на свободу мирных собраний и ассоциации, в том числе путем:**

a) проведения оценок воздействия на права человека, которые включают права на свободу мирных собраний и ассоциации, при разработке или изменении своих продуктов и услуг. Процесс оценки воздействия всегда должен включать консультации с представителями гражданского общества и другими экспертами и должен быть утвержден аккредитованной третьей стороной, компетентной в области прав человека;

b) учета выводов по результатам оценок воздействия посредством принятия мер, направленных на: повышение уровня знаний и осведомленности о правах на свободу мирных собраний и ассоциации за счет обучения и подготовки руководящих принципов для руководства, сотрудников и других субъектов, связанных с деятельностью компании, таких как подрядчики; разработку и принятие политики и процедур, которые определяют, каким образом компания будет оценивать и реагировать на требования правительства в отношении введения ограничений на доступ к средствам коммуникации или контента; интеграцию систем раннего предупреждения в бизнес-процессы для выявления и своевременного реагирования на риски в области прав человека; использование своего влияния для оспаривания запросов правительств в отношении мер, которые неправомерно ограничивают права на свободу мирных собраний и ассоциации; оказание поддержки в проведении научных исследований и разработок для поиска соответствующих технологических решений, помогающих бороться с сетевыми преследованиями, дезинформацией и пропагандой, включая инструменты для обнаружения и выявления связанных с государством аккаунтов и ботов; принятие показателей мониторинга, которые включают конкретные проблемы, связанные со свободой мирных собраний и ассоциации.

87. **Компании должны принимать эффективные меры для обеспечения транспарентности своей политики и методов работы, включая применение условий предоставления ими услуг, автоматизированные процессы обзора и соблюдение процессуальных гарантий. В этой связи компании должны регулярно публиковать на своих официальных веб-сайтах информацию о правовом основании запросов правительств и других третьих сторон, количестве и процентной доле удовлетворенных запросов, а также об ограничении и блокировании доступа к контенту или аккаунтам в рамках собственной политики компании и правил сообщества.**

88. **Компании должны ввести независимые механизмы надзора для контроля за результатами решений по модерированию контента, а государствам следует рассмотреть возможность принятия правил, требующих введения такого независимого надзора.**

89. **Компаниям следует создавать в рамках конструктивных консультаций с затрагиваемыми сообществами механизмы рассмотрения жалоб на оперативном уровне, которые были бы открытыми, доступными, а также эффективными с точки зрения процедур и возмещения ущерба.**

90. **Компании должны участвовать и повышать качество участия в осуществлении существующих многосторонних инициатив. Участвующие в реализации этих инициатив компании должны укреплять свою роль в соблюдении прав на свободу мирных собраний и на свободу ассоциации.**

91. **Компаниям следует взаимодействовать с правительствами и гражданским обществом, с тем чтобы разрабатываемые технологии поощряли и укрепляли права человека.**

C. Рекомендации для гражданского общества

92. **Представители гражданского общества должны продолжать поиск инновационных подходов и налаживать партнерские связи с правительствами, компаниями и научными кругами, с тем чтобы разрабатываемые технологии содействовали осуществлению прав на свободу мирных собраний и ассоциации.**

93. **Представители гражданского общества должны обеспечить, чтобы в основе деятельности их организаций лежали цифровая безопасность и цифровая грамотность.**

94. **Представители гражданского общества должны расширять и улучшать систему сбора и документирования данных о цифровых угрозах правам на ассоциацию и собрания, в частности в сфере разработки законодательства, нарушения работы сети, слежения, преследования и кампаний по дезинформации в Интернете. Им следует обмениваться знаниями, поощрять стандарты для сбора данных и сотрудничать в этой деятельности с другими заинтересованными сторонами.**

95. **Все группы гражданского общества, и не только организации, выступающие в защиту цифровых прав, должны оказывать поддержку и участвовать в процессе понимания цифровых угроз пространству для гражданской активности и разрабатывать эффективные меры реагирования на угрозы.**

D. Рекомендация Комитету по правам человека

96. **Учесть содержащуюся в данном докладе информацию в ходе подготовки замечания общего порядка по статье 21 Международного пакта о гражданских и политических правах.**