



Генеральная Ассамблея

Distr.: General
1 March 2023
Russian
Original: English

Совет по правам человека

Пятьдесят вторая сессия

27 февраля — 31 марта 2023 года

Пункт 3 повестки дня

**Поощрение и защита всех прав человека,
гражданских, политических, экономических,
социальных и культурных прав,
включая право на развитие**

Последствия разработки, использования и передачи новых технологий в контексте борьбы с терроризмом и пресечения и предотвращения насильственного экстремизма

Доклад Специального докладчика по вопросу о поощрении и защите прав человека и основных свобод в условиях борьбы с терроризмом Финнулы Ни Илан***

Резюме

В настоящем докладе Специальный докладчик по вопросу о поощрении и защите прав человека и основных свобод в условиях борьбы с терроризмом Финнула Ни Илан рассматривает проблемы и последствия разработки, использования и передачи новых технологий в контексте борьбы с терроризмом и насильственным экстремизмом для прав человека. Специальный докладчик признает способность новых технологий позитивно преобразовывать жизнь и содействовать полной реализации прав человека, равенства и достоинства человека, а также значительный потенциал новых технологий для устранения пробелов в области прав человека наиболее маргинализированных и уязвимых групп населения. К сожалению, в то же время во всем мире новые технологии неправомерно применяются для ограничения и нарушения прав человека.

В настоящем докладе освещаются способы, с помощью которых борьба с терроризмом и обеспечение безопасности часто используются для политического и юридического обоснования внедрения технологий, связанных с высоким риском и высоким уровнем вмешательства, под предлогом наличия исключительных угроз и с обещанием строго ограниченного применения. В докладе показано, что такие обоснования и ограничения редко соблюдаются и что утверждение об исключительном использовании таких технологий в ответ на кризисы в области безопасности является химерой, когда в реальности имеет место их широкое и

* Настоящий доклад был представлен после истечения установленного срока в целях включения в него самой последней информации.

** Приложение к настоящему докладу распространяется в том виде, в котором оно было получено, и только на том языке, на котором оно было представлено.



массовое использование без надлежащих ограничений, связанных с правами человека или верховенством права. Применение таких технологий, включая биометрические технологии, технологии наблюдения и технологии беспилотных летательных аппаратов, оказывает серьезное негативное воздействие на осуществление прав человека во всем мире. Специальный докладчик подчеркивает риски для прав человека, связанные с разработкой, внедрением и передачей этих технологий на международном уровне. Она также глубоко обеспокоена дискриминационными элементами, свойственными их разработке и внедрению. Негативные последствия включают прямые нарушения не допускающих отступлений прав, целостность которых подрывает новыми технологиями в отсутствие какого-либо значимого правового надзора, и безнаказанность как государственных, так и негосударственных субъектов, использование и передача которыми таких технологий связаны с систематическим нарушением прав. Воздействие на права человека по всему миру разрушительно, в частности воздействие на осуществление прав на неприкосновенность частной жизни, свободу выражения мнений, ассоциации и участие в политической жизни. Главный тезис Специального докладчика заключается в том, что неправомерная практика прочно вошла в сферу борьбы с терроризмом и насилием и экстремизмом именно потому, что в отсутствие согласованного международного определения этих явлений предлагаемые государствами определения служат для продвижения различных интересов, лишь немногие из которых касаются прав человека и верховенства права. Она призывает ввести мораторий на использование определенных технологий, включая глобальный запрет на смертоносные автономные системы вооружений. В частности, Специальный докладчик требует от государств-членов прекращения и отказа от передачи таких технологий государствам, которые ранее, как доказано, нарушили права человека, что подтверждается резолюциями Совета по правам человека и Генеральной Ассамблеи, а также выводами договорных органов Организации Объединенных Наций по правам человека. Поддерживая Верховного комиссара Организации Объединенных Наций по правам человека, она призывает ввести мораторий на передачу технологий наблюдения. Она также предлагает версию глобальной нормативной базы по использованию технологий наблюдения.

I. Деятельность Специального докладчика

1. Специальный докладчик по вопросу о поощрении и защите прав человека и основных свобод в условиях борьбы с терроризмом Финнула Ни Илан представила свой доклад о влиянии борьбы с терроризмом на миротворчество, миростроительство, сохранение мира, предотвращение и разрешение конфликтов Генеральной Ассамблее в октябре 2022 года¹.

2. Специальный докладчик продолжает уделять приоритетное внимание позитивному и активному взаимодействию с государствами-членами на национальном уровне. Она совершила конструктивные визиты на Мальдивы (15–24 мая 2022 года)² и в Боснию и Герцеговину (13–20 января 2023 года)³. В июле 2022 года она посетила Многопрофильную комплексную миссию Организации Объединенных Наций по стабилизации в Мали с учебным визитом рабочего характера. В марте 2022 года, после выхода ее доклада о последующей деятельности по совместному исследованию 2010 года о глобальной практике в связи с тайным содержанием под стражей в условиях борьбы с терроризмом⁴, правительство Соединенных Штатов Америки направило предварительное предложение обсудить возможную техническую поездку в центр содержания под стражей в бухте Гуантанамо, Куба, с уделением особого внимания вопросам переселения/репатриации бывших заключенных и прав человека жертв и семей жертв событий 11 сентября 2001 года. После продолжительных и конструктивных обсуждений она посетила место содержания под стражей 6–10 февраля 2023 года, а другие аспекты визита будут реализованы до апреля 2023 года. По завершении технической поездки будет представлено заявление по ее итогам.

3. Она сохраняет приверженность активному взаимодействию с различными субъектами гражданского общества, тем самым обеспечивая, чтобы опыт борьбы с терроризмом и практики обеспечения безопасности на местах были полностью интегрированы в ее работу. 9 мая 2022 года, в преддверии Международной конференции высокого уровня по правам человека, гражданскому обществу и противодействию терроризму, Специальный докладчик и Испания совместно организовали в Малаге семинар для представителей гражданского общества. В серии консультаций для подготовки итогового документа гражданского общества, который будет включен в официальный итоговый документ Конференции, приняли участие представители гражданского общества из 43 стран. Кроме того, Специальный докладчик при поддержке Германии и Испании приступила к проведению глобального исследования о воздействии контртеррористических мер на гражданское общество и гражданское пространство и выпустила серию короткометражных фильмов, документирующих воздействие контртеррористических мер на субъектов гражданского общества по всему миру.

4. Она считает своей приоритетной задачей оказание государствам технической помощи и представление соображений относительно законодательства по борьбе с терроризмом. С 2021 года она провела обзоры законодательства или законодательных изменений в Австрии, Алжире, Беларуси, Бразилии, Венесуэле (Боливарианская Республика), Гаити, Дании, Зимбабве, Китае, Мали, Нидерландах, Никарагуа, Новой Зеландии, Сальвадоре, Соединенном Королевстве Великобритании и Северной Ирландии, Таджикистане, Таиланде, Турции, Узбекистане, Франции и Шри-Ланке, а также в Европейском союзе.

5. Она выпустила документы с изложением позиции по вопросам влияния контртеррористических санкций на права человека и международно-правовые обязательства государств с особым упором на режимы санкций, предусмотренные

¹ A/77/345.

² См. A/HRC/52/39/Add.1 и Add.2.

³ См. <https://www.ohchr.org/en/press-releases/2023/01/bosnia-and-herzegovina-divisive-post-conflict-politics-and-failure-address>.

⁴ A/HCR/49/45.

резолюциями 1267 (1999) и 1988 (2011) Совета Безопасности⁵, о последствиях лишения гражданства в контексте борьбы с терроризмом для прав человека с особым акцентом на ситуацию в северо-восточной части Сирийской Арабской Республики⁶, о последствиях мер по борьбе с финансированием терроризма для прав человека и верховенства права⁷, о регулировании международной торговли технологиями шпионских программ для борьбы с терроризмом⁸ и об использовании вооруженных беспилотных летательных аппаратов⁹.

6. Она по-прежнему является членом Целевой группы Глобального договора Организации Объединенных Наций по координации контртеррористической деятельности и глубоко привержена подходу «Единой Организации Объединенных Наций» к борьбе с терроризмом с учетом прав человека, как это утверждено в Глобальной контртеррористической стратегии Организации Объединенных Наций. Специальный докладчик поддерживает позитивное сотрудничество с Группой разработки финансовых мер борьбы с отмыванием денег. Она приняла участие в трех заседаниях Межамериканского комитета по борьбе с терроризмом. За прошедший год она неоднократно выступала с брифингами перед региональными группами, включая Организацию исламского сотрудничества, Африканский союз, Европейский союз и Группу государств Латинской Америки и Карибского бассейна, а также участвовала в работе специальной сессии Контртеррористического комитета в Мумбаи и Нью-Дели, Индия.

II. Разработка, использование и передача новых технологий в контексте борьбы с терроризмом и предотвращения и пресечения насилиственного экстремизма

7. Общеизвестно, что новые технологии могут принести огромную пользу, обеспечивая и продвигая человеческое достоинство, способствуя устойчивому развитию и повышению уровня жизни, улучшая здравоохранение, углубляя связи и коммуникацию, содействуя новым образовательным возможностям и доступу к образованию, а также повышая безопасность и эффективность общин. Эти преимущества, если они распределяются равномерно, прозрачно и без дискриминации, могут сделать технологию партнером в поощрении и защите гражданских, политических, экономических, социальных и культурных прав народов всей планеты.

8. К сожалению, потенциальное положительное воздействие новых технологий на права человека еще далеко не является реальностью. Напротив, новые технологии, особенно цифровые, меняют способы ущемления и нарушения прав человека во всем мире. Ряд мандатариев специальных процедур и Верховный комиссар Организации Объединенных Наций по правам человека рассмотрели вопрос о пересечении цифровых технологий с правами человека, в том числе в продвижении дискриминационного обращения с людьми по расовым и ксенофобским мотивам и социальной изоляции¹⁰. Признавая и подтверждая эту важную предшествующую работу, в настоящем докладе Специальный докладчик рассматривает вопрос о пересечении борьбы с терроризмом и предупреждения и пресечения насилиственного экстремизма с использованием новых технологий. Она также должным образом учитывает общесистемный стратегический подход и «дорожную карту» Организации

⁵ См. <https://www.ohchr.org/sites/default/files/2022-03/position-paper-unrct-on-unsc-use-of-ct-targeted-sanctions.pdf>.

⁶ См. <https://www.ohchr.org/en/special-procedures/sr-terrorism/return-and-repatriation-foreign-fighters-and-their-families>.

⁷ См. <https://www.ohchr.org/sites/default/files/2022-06/2022-06-13-SRCT-HR-CFT-Position-Paper.pdf>.

⁸ См. <https://www.ohchr.org/sites/default/files/documents/issues/terrorism/sr/2022-12-15/position-paper-unrct-on-global-regulation-ct-spyware-technology-trade.pdf>.

⁹ См. <https://www.ohchr.org/en/special-procedures/sr-terrorism/activities>.

¹⁰ См. A/HRC/48/76.

Объединенных Наций по поддержке развития потенциала в области искусственного интеллекта (ИИ)¹¹.

9. Она обращает внимание на то, как задачи обеспечения безопасности и обоснования борьбы с терроризмом используются в поддержку разработки, использования и передачи новых технологий, включая, в частности, биометрические технологии, ИИ, беспилотные летательные аппараты (дроны) и средства наблюдения. Специальный докладчик осуждает то, как под видом предупреждения терроризма используются новые технологии, которые на практике ведут к существенному подрыву прав отдельных лиц и общин. Технологии, связанные с высоким риском, были внедрены через так называемый «черный ход», что было подкреплено призывами к обеспечению безопасности, но в действительности они ослабляют более широкую коллективную безопасность и подрывают поощрение и защиту прав человека. Некоторые государства, в которых происходят вопиющие нарушения прав человека, во многих из которых отсутствуют основные законодательные или судебные меры защиты, получили карт-бланш на доступ к технологиям, связанным с высоким риском, которые используются этими же государствами для подавления законного инакомыслия, правозащитной деятельности, в том числе в интересах женщин и детей, юридического представительства, самовыражения журналистов и гуманистической деятельности.

10. Она признает угрозу, которую терроризм представляет для отдельных лиц, общин и обществ. Специальный докладчик глубоко осознает страдания, которые приносят неизбирательные акты политического насилия, направленные против гражданского населения, а ее приверженность оказанию помощи жертвам терроризма, их семьям и общинам непоколебима. Она продолжает оказывать давление на государства и многосторонние институты с тем, чтобы они конструктивно рассматривали и устранили межсекторальные причины терроризма и комплексного насилия, включая вооруженные конфликты¹².

11. Однако она осуждает распространение близорукой концепции безопасности, которая сопровождает особенно ограничительный подход к борьбе с терроризмом, в том числе в рамках многосторонних институтов. Анализ террористической угрозы в национальных контекстах, а также в органах Организации Объединенных Наций по борьбе с терроризмом страдает от привычного отсутствия целостного подхода к причинно-следственным связям, пересекающимся формам и взаимосвязанным проявлениям насилия. Разработчики политики, напротив, предпочитают упрощенные, избитые стереотипы о причинах насилия и предлагают ответные меры, которые просто не работают. Практика борьбы с терроризмом и неполный анализ причин терроризма содействуют неприемлемой неспособности адекватно противодействовать терроризму и комплексному насилию по всему миру. Ответные меры на основе ненадлежащего анализа причинно-следственных связей и выборочных данных, зачастую повышают, а не снижают уровень насилия. Именно в такой среде происходит внедрение новых технологий, часто сенсационно представляемых как «решение» проблемы терроризма, определение которого не является достаточным или просто отсутствует. По мнению Специального докладчика, уместность, необходимость и дополнительные преимущества новых технологий следует подвергать более тщательному изучению, прежде чем с энтузиазмом и безоговорочно внедрять их в контекстах борьбы с терроризмом. Необходимо задать фундаментальные вопросы о том, будут ли такие технологии способствовать защите прав человека, верховенству права и равенству в сфере, которая все больше определяется ущемлением человеческого достоинства, или ставить их под угрозу.

12. Она выделяет три конкретные тенденции, характеризующие использование новых технологий в борьбе с терроризмом и предупреждении и пресечении насилиственного экстремизма. Первая — это использование терроризма в качестве политического обоснования для внедрения технологий, связанных с высоким риском, при этом оправдание исключительности мер проникает в правовые и политические

¹¹ СЕВ/2019/1/Add.3.

¹² См. А/77/345.

дебаты. Сюда относится практика применения исключений, связанных с национальной безопасностью и/или борьбой с терроризмом, в законодательстве, регулирующим новейшие технологии. Вторая связана с отсутствием последовательного анализа и практики в области прав человека при разработке, использовании и передаче новых технологий. Поверхностная и показная ссылка на права человека является характерной чертой этого тренда. Результат — полный провал в регулировании технологий, связанных с высоким риском, что влечет за собой глобальные негативные последствия для прав человека и международного правопорядка. Третья включает предсказуемый и неявный переход от первоначального исключительного использования новых технологий в узких контекстах безопасности к широкому использованию, импорту и нормализации применения этих технологий в повседневной жизни.

13. В настоящем докладе Специальный докладчик уделяет особое внимание двусторонней и многосторонней передаче технологий в сфере борьбы с терроризмом, подчеркивая неспособность государств и многосторонних институтов создать надежные системы надзора и контроля для предотвращения злоупотреблений. Глубокую озабоченность вызывает очевидное нежелание регулировать практику частных организаций, включая многонациональные корпорации, которые нарушают права человека. В докладе содержится ряд конкретных и выполнимых рекомендаций, которые основаны на предыдущих рекомендациях по выполнению Руководящих принципов предпринимательской деятельности в аспекте прав человека (включая использование проекта «Би-тех» Управления Верховного комиссара Организации Объединенных Наций по правам человека (УВКПЧ)) и укреплению других договорных механизмов и механизмов экспортного регулирования.

14. К сожалению, сама Организация Объединенных Наций, похоже, занимается поддержкой и оказанием технической помощи в борьбе с терроризмом и наращиванием потенциала в области новых технологий с помощью программ, которые не в полной мере реализуют обязательства по обеспечениюнойной осмотрительности в вопросах прав человека и, по всей видимости, систематически недооценивают риски злоупотреблений. Структуры Организации Объединенных Наций должны осуществлять наращивание потенциала и оказание технической помощи с использованием технологий, связанных с высоким риском, включая ИИ, биометрию и кибербезопасность, в контексте борьбы с терроризмом в соответствии с нормами международного права прав человека, беженского и гуманитарного права, а также политикиной осмотрительности в вопросах прав человека. Они также должны руководствоваться стратегией Генерального секретаря по новым технологиям, заявленная цель которой — определить, каким образом система Организации Объединенных Наций будет поддерживать использование этих технологий для ускорения реализации Повестки дня в области устойчивого развития на период до 2030 года и содействовать их увязке с ценностями, закрепленными в Уставе Организации Объединенных Наций, Всеобщей декларации прав человека, а также нормах и стандартах международного права. Она поддерживает призывы в первую очередь к критическому диалогу между технологическими и телекоммуникационными компаниями, экспертами Организации Объединенных Наций по правам человека и гражданским обществом при обеспечении надежного многостороннего подхода к регулированию, основанного на участии многих заинтересованных сторон. Этот диалог должен быть полностью согласован с практическими регуляторными мерами по внедрению правозащитного подхода в процесс разработки, использования и передачи новых технологий. В настоящем докладе содержатся конкретные рекомендации на этот счет.

15. Специальный докладчик подчеркивает роль ускорителя, которую сыграл Совет Безопасности в актуализации и узаконивании широкого использования новых технологий в борьбе с терроризмом посредством резолюций, принятых в соответствии с главой VII Устава¹³. Она согласна с мнением о том, что Совету следует использовать свои возможности в области регулирования борьбы с терроризмом с осторожностью,

¹³ См. A/73/361.

осмотрительностью и самоограничением и избегать чрезмерного охвата, характерного для всех резолюций начиная с резолюции 1373 (2001)¹⁴. Специальный докладчик отмечает недавнее рассмотрение Контртеррористическим комитетом вопроса об использовании террористами беспилотных летательных аппаратов, информационно-коммуникационных технологий и новых методов онлайн-платежей и сбора средств. В этом контексте Индия как председатель Комитета способствовала проведению содержательного и широкого диалога с многочисленными заинтересованными сторонами и экспертами, включая независимых представителей гражданского общества. Она высоко оценивает всеобъемлющий процесс, который привел к принятию (не имеющей обязательной силы) Делийской декларации о противодействии использованию новых и новейших технологий в террористических целях¹⁵, и призывает нового председателя, Объединенные Арабские Эмираты, придерживаться аналогичного подхода и внедрить принцип инклюзивности в регуляторную работу Комитета. Декларация представляет собой прогресс в признании связи прав человека и регулирования чувствительных и опасных технологий. Тем не менее Специальный докладчик очень обеспокоена тем, что в Декларации не рассматривается более широкий контекст злоупотребления государствами вооруженными беспилотными летательными аппаратами, неправомерного использования мер по борьбе с финансированием терроризма для репрессий в отношении представителей гражданского общества и гуманитарных организаций, а также широко распространенного злоупотребления государствами технологиями наблюдения. Совету Безопасности и Исполнительному директорату Контртеррористического комитета следует действовать очень осторожно и избегать принятия любых узко сформулированных нормативных указаний, даже в качестве мягкого права. Руководство Организации Объединенных Наций по этим технологиям будет сильно обеднено, если разговор о регулировании будет вести исключительно или в первую очередь контртеррористический орган, действующий в ограниченных рамках, упуская более широкий многосекторальный и многоаспектный контекст, который необходим для регулирования или руководства и основан на уважении верховенства права и соблюдении Устава. Она обеспокоена тем, что такое руководство будет создавать препятствия для достижения юридически обязательного прогресса по этим вопросам на параллельных форумах или в рамках других более крупных многосторонних процессов или подрывать его.

16. Например, Совет Безопасности в своей широкой резолюции 2396 (2017) потребовал от государств (в соответствии с главой VII) разработать системы сбора биометрических данных в контексте борьбы с терроризмом, создав глобальный мандат по сбору, хранению, использованию и передаче биометрических данных высокого риска, при этом практически не проводя внешних консультаций между техническими экспертами и другими заинтересованными сторонами (включая затронутые государства)¹⁶. Феномен иностранных боевиков (террористов), как правило, прибывавших из Ирака и Сирийской Арабской Республики, послужил основанием для создания этого мандата. Не следует преуменьшать масштаб проблем в области политики и обеспечения безопасности в то время (2014 год), когда спецслужбы указывали на перемещение (потенциально) сотен боевиков, связанных с признанными террористическими группами. Но обширный глобальный мандат по сбору биометрических данных о каждом человеке, пересекающем границу, основанный на этой конкретной и целенаправленной региональной угрозе, заставляет задуматься о соразмерности ответных мер. По сей день нет точных глобальных данных о количестве фактических пересечений границы иностранными боевиками (террористами), несмотря на то что на феномен пересечения ссылаются для оправдания введения глобального мандата по сбору биометрических данных и других мер обеспечения

¹⁴ См. Eric Rosand, Alistair Millar and Naureen Chowdhury Fink, “Counter-terrorism and the United Nations Security Council since 9/11: moving beyond the 2001 paradigm”, Securing the Future Initiative, September 2022.

¹⁵ См. <https://www.un.org/securitycouncil/ctc/news/delhi-declaration-countering-use-new-and-emerging-technologies-terrorist-purposes-now-available>.

¹⁶ См. A/73/361.

безопасности, предусматривающих вмешательство¹⁷. В результате сбор биометрических данных на границах, который первоначально был оправдан террористической угрозой, функционирует как способ регулирования потоков мигрантов¹⁸ и предоставления данных наблюдения государствам и действует как механизм социального контроля. Требование резолюции 2396 (2017) о сборе биометрических данных отличается отсутствием конкретики в области прав человека и верховенства права и удручаает наличием пробелов в области прав человека. Внедрение такого сбора биометрических данных при лишь поверхностном надзоре за соблюдением прав человека способствует существованию серьезной глобальной проблемы, связанной с систематическим злоупотреблением контртеррористическими мерами¹⁹. Неспособность установить связи между глобальными мандатами по борьбе с терроризмом и внутренней практикой обеспечения безопасности является основным недостатком ООН-оцентричной концепции безопасности, которая подрывает более широкие усилия Организации Объединенных Наций в области развития, управления и обеспечения верховенства права. Вызывает обеспокоенность тот факт, что региональные органы не предпринимают достаточных усилий для устранения пробелов в области прав человека и верховенства права.

17. Она отмечает, что многие новые технологии включают сложные системы, которые несут в себе риски для защиты прав, в особенности уязвимых групп населения. В этой сфере основные проблемы в области прав человека включают неспособность учитывать особые характеристики систем, связанных с высокими рисками, системную девальвацию рисков дискриминации и неравенства, а также отсутствие подходов к управлению рисками, основанных на правах человека. Кроме того, политическое стремление к снижению риска или готовность ввести мораторий на использование ряда технологий, связанных с особо высокими рисками, невелики. Напротив, преобладает попустительское отношение к разработке и использованию частным сектором новых технологий в контексте безопасности. По сути, учитывая отсутствие согласованного на международном уровне определения терроризма²⁰ и укоренившиеся и систематические злоупотребления законами и практикой борьбы с терроризмом и обеспечения безопасности на национальном уровне, использование новых технологий в этой проблематичной сфере создает сложный и межсекторальный комплекс вызовов в области прав человека.

A. Биометрия

18. Биометрия — это научная дисциплина, связанная с измерениями и показателями биологических или поведенческих характеристик, которые являются общими для всех людей и в то же время высоко репрезентативными для каждого отдельного человека, что позволяет идентифицировать конкретное лицо. Такие маркеры могут быть связаны с физиологическими характеристиками человека, такими как отпечатки пальцев или ладоней, ДНК, а также лицо, радужная оболочка или сетчатка глаза (т. е. биологическая биометрия). Другие связаны с поведенческими моделями, например распознавание человека по его походке (поведенческая биометрия или «бихевиометрия»). Поскольку биометрические идентификационные признаки являются одновременно уникальными для человека и стабильными во времени, они представляют собой исключительно полезный инструмент для точной и эффективной идентификации и аутентификации. Однако эти характеристики также

¹⁷ См. резолюцию Совета Безопасности 2482 (2019).

¹⁸ Специальный докладчик признает усилия по обеспечению ответственного использования сбора биометрических данных на границах в отношении мигрантов. См. International Organization for Migration, “IOM and biometrics: supporting the responsible use of biometrics”, November 2018; и Katia Lindskov Jacobsen, “Biometric data flows and unintended consequences of counterterrorism”, *International Review of the Red Cross*, No. 916-917 (February 2022).

¹⁹ См. A/HRC/40/52; см. также сообщения OTH 229/2021, ISR 11/2021, IRL 3/2022 и CHN 12/2022. Со всеми сообщениями и ответами на них, упомянутыми в настоящем докладе, можно ознакомиться URL: <https://spcommreports.ohchr.org/Tmsearch/TMDocuments>.

²⁰ E/CN.4/2006/98 (пп. 26–50 и 72).

делают такие данные особенно уязвимыми²¹, что создает необходимость в надежных системах хранения и обработки данных для снижения риска несанкционированного доступа²².

19. Средства сбора биометрических данных стали стандартным инструментом правоохранительных и административных органов в различных контекстах, включая гражданскую идентификацию, уголовное правосудие и пограничный контроль. Специальный докладчик напоминает, что, несмотря на успешное использование таких средств в законных общественных интересах, они также применялись в связи с грубыми нарушениями прав человека, преступлениями в форме зверства, репрессивными и авторитарными режимами²³.

20. Специальный докладчик, среди прочего, выразила обеспокоенность по поводу сбора биометрических данных уязвимых групп населения и лиц в различных контекстах. Сбор биометрических данных населения в зонах конфликтов, в том числе в Ираке и Афганистане, вызывает серьезную озабоченность²⁴, в том числе в связи с передачей биометрических данных, собранных в рамках борьбы с терроризмом, непосредственно в руки террористических групп или террористов, признанных таковыми Организацией Объединенных Наций²⁵. Мандатарии специальных процедур и Комитет по ликвидации расовой дискриминации выразили обеспокоенность относительно использования таких технологий в Синьцзян-Уйгурском автономном районе в контексте применения Китаем Закона о борьбе с терроризмом и мер по его реализации в регионе²⁶. Среди ряда мер, вызывающих серьезную озабоченность в контексте прав человека, сообщения указывают на факт проведения властями массового сбора биометрических данных (таких, как образцы ДНК, отпечатки пальцев, сканы радужной оболочки глаза и группа крови) жителей региона. Использование биометрических данных в Сомали и Израилем на оккупированной палестинской территории вызывают аналогичные опасения²⁷.

21. Она подчеркивает, что пандемия коронавирусной инфекции (COVID-19) ускорила сбор биометрических данных и привела как к еще большему расширению чрезвычайных полномочий, так и к нормализации использования этой практики, включая применение биометрических технологий, разработанных для целей борьбы с терроризмом и обеспечения безопасности, для борьбы с глобальной пандемией, что непропорционально сильно затронуло религиозные, этнические и расовые меньшинства, другие уязвимые группы и экономически и социально маргинализированные слои общества²⁸. Использование биометрических технологий, разработанных для борьбы с терроризмом, в целях регулирования наиболее маргинализированных общин во время пандемии должно волновать все заинтересованные стороны.

²¹ Международная организация по стандартизации определяет биометрическую характеристику как биологическую и поведенческую характеристику лица, из которой могут быть извлечены отличительные, повторяемые биометрические признаки для целей биометрического распознавания (ISO/IEC 2382-37:2017(en)).

²² Krisztina Huszti-Orbán and Fionnuala Ní Aoláin, “Use of biometric data to identify terrorists: best practice or risky business?”, University of Minnesota, 2020.

²³ United States Holocaust Memorial Museum, “Tattoos and numbers: the system of identifying prisoners at Auschwitz”, Holocaust Encyclopedia.

²⁴ См. United States Government Accountability Office, “DOD biometrics and forensics: progress made in establishing long-term deployable capabilities, but further actions are needed”, report to congressional committees GAO-17-580 (August 2017); и Electronic Privacy Information Center, “Iraqi biometric identification system” (URL: <https://epic.org/privacy/biometrics/iraq.html>).

²⁵ После вывода коалиционных сил из Афганистана в августе 2021 года в руки талибов попали биометрические устройства, оставленные американскими войсками, вследствие чего они получили доступ к обширным персональным биометрическим данным.

²⁶ См. сообщения CHN 18/2019 и CHN 14/2020; и [CERD/C/CHN/CO/14-17](#), п. 40 б).

²⁷ См. Keren Weitzberg, “Biometrics and counter-terrorism: case study of Somalia”, Privacy International, May 2021; и сообщение ISR 11/2021.

²⁸ Fionnuala Ní Aoláin, “Exceptionality: a typology of COVID-19 emergency powers”, *UCLA Journal of International Law and Foreign Affairs*, vol. 26, issue 2 (2022).

22. Все более активное использование биометрических технологий — и злоупотребление ими — в контексте борьбы с терроризмом опирается на целый ряд резолюций Совета Безопасности. В своей резолюции 2396 (2017) Совет потребовал от государств «разрабатывать и внедрять системы сбора биометрических данных» «для ответственного и надлежащего выявления террористов, включая иностранных боевиков-террористов». В той же резолюции Совет особо потребовал от государств разрабатывать и внедрять системы сбора таких данных, включая отпечатки пальцев, фотографии, данные распознавания лиц и другие соответствующие идентификационные биометрические данные²⁹.

23. Этот согласованный политический курс на всеобъемлющий сбор биометрических данных не подкреплен необходимой работой по созданию надлежащего всемирного нормативно-правового режима. Действительно, вместо того чтобы возглавить комплексные усилия по согласованию набора надежных международных правил и стандартов в отношении сбора биометрических/идентификационных данных, основные усилия в системе Организации Объединенных Наций были направлены на создание потенциала для содействия такому сбору. Эта программа — Программа Организации Объединенных Наций по борьбе с передвижениями террористов — предусматривает оказание технической помощи и поддержки государствам-членам в сборе наборов данных, содержащих предварительную информацию о пассажирах и записи их регистрации, применительно ко всем авиапассажирам на международном уровне на основе программного обеспечения Организации Объединенных Наций goTravel, которое Организация Объединенных Наций предоставляет государствам в качестве стандартного инструмента для сбора, обмена и анализа данных³⁰.

24. Особые опасения Специального докладчика в отношении Программы и поддерживаемой ею системы сбора персональных данных включают следующее: а) сбор данных в принципе, учитывая степень детализации, которую эти данные, в особенности данные записи регистрации пассажиров, предоставляют о жизни субъектов данных; б) то, как сбор, по определению и неизбежно, происходит в отношении всех пассажиров без разбора, что ставит под сомнение его необходимость и соразмерность; с) продолжительность периода хранения, что позволяет использовать такие данные не только для сверки со списками наблюдения для определенных рейсов, но и в качестве долгосрочной записи поведения отдельного лица, из которой можно извлечь подробную информацию; и д) трансграничный обмен данными между ведомствами разных стран создает особые риски, касающиеся различных стандартов соблюдения прав человека на международном уровне. Специальный докладчик глубоко обеспокоена неверным/дискриминационным принятием решений на основе алгоритмов при сборе предварительной информации о пассажирах и записей регистрации пассажиров; она подчеркивает влияние использования или передачи этих технологий на свободу передвижения, право на выезд и право на убежище; и отмечает незаконное целевое использование данных государствами, которым они передаются, и совершенно неадекватные средства правовой защиты в случае нарушений прав человека, которые имеют место в контексте использования таких данных³¹. Она указывает на ограниченное взаимодействие Программы с правозащитными структурами Организации Объединенных Наций. Она призывает провести независимую проверку Программы, чтобы убедиться в добросовестности применяемое ее рамках практики и передачи технологий в том, что касается прав человека, защиты данных и верховенства права.

²⁹ Было выпущено руководство Организации Объединенных Наций по использованию биометрических данных в борьбе с терроризмом, однако, по оценке Специального докладчика, оно требует значительного пересмотра для учета аспектов прав человека и рисков, связанных с широким использованием государствами биометрических данных.

См. https://www.unodc.org/pdf/terrorism/Compendium-Biometrics/Compendium-biometrics-final-version-LATEST_18_JUNE_2018_optimized.pdf.

³⁰ См. <https://learnt.unocit-connectandlearn.org/course/index.php?categoryid=35> и <https://www.un.org/cttravel/goTravel>.

³¹ OHCHR, “Principles and guidelines on human rights at international borders” (October 2014), p. 13.

25. В том же ключе Специальный докладчик испытывает серьезную озабоченность относительно роли и влияния Института биометрических данных³², расположенного в Соединенном Королевстве, организации, связанной с промышленностью и правительствами, которая продвигает стандарты и практику, но является исключительно закрытой и недоступной для субъектов гражданского общества и правозащитников.

26. Она также подчеркивает свою глубокую озабоченность по поводу обмена биометрическими данными, который настоятельно поощряется международным сообществом. Одним из ярких мотивов нормативного регулирования борьбы с терроризмом является акцент на сотрудничество между государствами для продвижения предполагаемых совпадающих интересов в борьбе с терроризмом³³. Обмен данными является «черным ящиком» в практике международного права, при этом имеется мало информации о том, происходит ли обмен биометрическими данными и какого типа, а также, что в большей мере относится к практической стороне вопроса, о содержании соглашений об обмене данными. По большей части неизвестно, учитываются ли вообще соображения прав человека в таких соглашениях. Специальный докладчик подчеркивает существующее в настоящее время противоречие между неоднократными призывами Генеральной Ассамблеи и Совета по правам человека к сотрудничеству между государствами в борьбе с терроризмом, содержащимся в документах, начиная с Глобальной контртеррористической стратегии и заканчивая резолюциями³⁴, и абсолютным отсутствием указаний, что такое сотрудничество должно осуществляться в соответствии с обязательствами государств в области прав человека, в том числе в отношении права на неприкосновенность частной жизни.

B. Беспилотные летательные аппараты

27. Еще одна область, в которой очевидна тенденция к тому, что сомнительные, а иногда и незаконные тактики и технологии, изначально разработанные для исключительных и конкретных целей борьбы с терроризмом и обеспечения национальной безопасности, нормализуются и используются на регулярной основе, — это беспилотные летательные аппараты (БПЛА). Технология БПЛА распространяется с поразительной скоростью. Использование вооруженных БПЛА во всем мире, как в рамках официальных вооруженных конфликтов в конкретных географических точках, так и в рамках заявленной борьбы с терроризмом, остается предметом серьезных споров и представляет собой постоянный риск для гражданского населения и проблему для защиты прав человека. Удары дронов направлены как против целей в зонах боевых действий во время конфликта, так и против отдельных лиц в так называемых «целенаправленных убийствах» вне географических рамок текущего конфликта. Многие из этих конфликтов стоят особняком, поскольку они рассматриваются не как традиционные международные вооруженные конфликты, а как театры контртеррористических операций и мероприятий. Развитие технологии БПЛА неразрывно связано с военным потенциалом и поражающим действием³⁵, а удары БПЛА постоянно оправдываются борьбой с терроризмом. Использование дронов подвергается резкой критике, в том числе со стороны Специального докладчика по вопросу о внесудебных казнях, казнях без надлежащего судебного разбирательства или произвольных казнях и бывшего Специального докладчика по вопросу о поощрении и защите прав человека и основных свобод в условиях борьбы с терроризмом³⁶. Специальный докладчик присоединяется к этим осуждениям и оспаривает законность экстерриториального использования боевых БПЛА

³² См. <https://www.biometricsinstitute.org/>.

³³ Резолюция 2482 (2019) Совета Безопасности, п. 15 с), и резолюции Генеральной Ассамблеи 75/291, п. 30, и 60/288, приложение, разд. II, пп. 3–5.

³⁴ См. резолюцию 76/169 Генеральной Ассамблеи и резолюцию 51/24 Совета по правам человека.

³⁵ Imperial War Museum, “A brief history of drones”. URL: <https://www.iwm.org.uk/history/a-brief-history-of-drones>.

³⁶ См. A/HRC/44/38, A/HRC/25/59, A/HRC/14/24/Add.6 и A/68/389.

и многочисленных нарушений прав человека, к которым приводит использование их в таких целях. Она выражает глубокое беспокойство по поводу ускоренного внедрения дронов, действующих «за пределами видимости», в целях предотвращения терроризма. Она предостерегает от сохранения условий, способствующих терроризму, когда применение силы пагубно, неподотчетно, неизбирательно на практике и обусловлено высокомерием, которое обесценивает жизнь людей на местах³⁷.

28. Несмотря на предпринимавшиеся в течение последнего десятилетия попытки призвать государства согласовать, принять и соблюдать единые стандарты законного использования вооруженных дронов, ощутимого прогресса добиться не удалось. Государства продолжают применять эту технологию в качестве средства для целенаправленного убийства предполагаемых террористов за рубежом, как в пределах, так и за пределами формальных границ вооруженного конфликта. Кроме того, многие государства начали расширять использование вооруженных беспилотных летательных аппаратов в пределах своих собственных границ, и были разработаны новые технологии, включая нано-БПЛА, дроны, вооруженные несмертельным оружием, и смертоносные БПЛА, не несущие зажигательных устройств, что вызывает новые проблемы в области прав человека. Специальный докладчик подчеркивает нехватку комплексного регулирования в этой инновационной сфере, включая абсолютное отсутствие механизмов защиты и обеспечения соблюдения прав человека.

29. Она напоминает о работе предыдущих мандатариев в отношении использования вооруженных дронов. В своем докладе Генеральной Ассамблеи за 2013 год³⁸ Бен Эммерсон проанализировал десятки ударов, нанесенных с 2001 по 2013 год по различным локациям, от Афганистана до оккупированной палестинской территории, и подчеркнул, что развертывание вооруженных БПЛА не является прозрачным, что, по словам Верховного комиссара Организации Объединенных Наций по правам человека, «создает вакuum ответственности и отрицательно оказывается на способности жертв требовать компенсации»³⁹. В своем докладе Совету по правам человека за 2014 год г-н Эммерсон подчеркнул срочную и настоятельную необходимость достижения консенсуса между государствами по целому ряду вопросов для продвижения защиты прав человека и гуманитарного права⁴⁰. Специальный докладчик повторяет призыв Генерального секретаря к глобальному запрету на смертоносные автономные системы оружия⁴¹.

30. Она подчеркивает, что целесообразность международных правовых норм законного применения силы не является абстрактным вопросом или вопросом, не связанным с оценкой прав человека при нанесении смертоносных ударов БПЛА. В соответствии с основным принципом международного права прав человека, применение смертоносной силы для лишения человека права на жизнь должно осуществляться во всех случаях не произвольным образом. Как отметил Комитет по правам человека в своем замечании общего порядка № 36 (2019), право на жизнь — «высшее право, отступление от которого не допускается даже в ситуациях вооруженного конфликта и во время других ситуаций чрезвычайного положения в государстве, при которых жизнь нации находится под угрозой», а лишение жизни является произвольным, «если оно противоречит международному праву или внутригосударственному праву». Комитет далее отметил, что «применение смертоносной силы, совместимое с международным гуманитарным правом и другими применимыми нормами международного права, в целом не является произвольным», и поэтому «государства-участники должны, как правило, раскрывать критерии применения смертоносной силы в отношении лиц или объектов, нападения на которые предположительно повлекут за собой лишение жизни, включая правовое основание для конкретных нападений... обстоятельства, при которых применялись соответствующие средства и методы ведения войны, и были ли рассмотрены менее

³⁷ См. Atef Abu Saif, *The Drone Eats With Me: A Gaza Diary* (Boston, Beacon Press, 2016).

³⁸ A/68/389.

³⁹ Там же, п. 41.

⁴⁰ A/HRC/25/59, п. 71.

⁴¹ См. <https://www.un.org/sg/en/content/sg/statement/2018-11-11/allocution-du-secretaire-general-au-forum-de-paris-sur-la-paix>.

опасные альтернативы»⁴². Если государства полагаются на предполагаемые обоснования, которые не находят адекватной поддержки в международном праве, то в результате такие действия, по определению, нарушают основополагающий принцип прав человека о недопустимости произвола. Она глубоко обеспокоена тем, что современное экстерриториальное использование вооруженных дронов подразумевает произвольное применение силы согласно международным нормам в области прав человека.

31. За последние пять лет технология БПЛА прошла тот же уже привычный путь от поля боя к тылу, который наблюдается в методах охраны правопорядка и области вооружений в целом. Этот переход от обоснования использования в контексте конфликта и борьбы с терроризмом к «регулярному» правоприменению отражает последовательную картину, выявленную в настоящем докладе, когда подходы, изначально оправданные исключительными целями борьбы с терроризмом, надежно инкорпорируются в местную, внутреннюю и «обычную» правовую систему. В частности, после принятия в 2016 году Федеральным управлением гражданской авиации США правила, разрешающего развертывание БПЛА в гражданском воздушном пространстве страны⁴³, использование дронов национальными правоохранительными органами, сначала в США, а затем и во всем мире, быстро распространилось. Исследования показывают, что в настоящее время более 1000 департаментов полиции в США используют технологию БПЛА⁴⁴. В Великобритании их используют по меньшей мере 40 полицейских подразделений⁴⁵. БПЛА применяет полиция Китая, причем Синьцзянское бюро общественной безопасности наладило партнерство с компанией DJI — ведущим мировым производителем дронов, который занимает более 75 процентов рынка дронов⁴⁶. Их также используют полицейские силы в Австралии и Израиле, а также в Африке, Европе, Персидском заливе и Северной и Южной Америке⁴⁷.

32. Примечательно, что в ряде национальных контекстов обоснованием такого использования служат задачи обеспечения национальной безопасности и борьбы с терроризмом, которое считается необходимым для противодействия внутреннему терроризму или защиты критически важной инфраструктуры от террористических атак. Первое поколение БПЛА, используемых правоохранительными органами внутри страны, выполняло только функции наблюдения. Они были фактически летающими в небе камерами видеонаблюдения. Однако нынешнее поколение, как правило, оснащается такими усовершенствованными функциями, как тепловидение и ночное видение, автоматическое слежение за целью, громкоговорители и прожекторы. Производители дронов разработали модели, предназначенные для полиции, которые оснащены несмертоносным оружием. Французские производители БПЛА продают правоохранительным органам модели, которые могут нести до 18 гранат со слезоточивым газом⁴⁸. Южноафриканский производитель БПЛА Desert Wolf разработал дрон с мощными пейнтбольными стволами, способными стрелять твердыми гранулами, шариками с краской или перцовым спреем⁴⁹. «Продажа» такого

⁴² Комитет по правам человека, замечание общего порядка № 36 (2019), пп. 2, 12 и 64.

⁴³ См. <https://www.faa.gov/newsroom/faa-doubles-blanket-altitude-many-uas-flights?newsId=852644>.

⁴⁴ См. <https://atlasofsurveillance.org/atlas>.

⁴⁵ См. Chris Cole and Jonathan Cole, “Benchmarking police use of drones in the UK”, UK Drone Watch, 2 November 2020.

⁴⁶ См. United States Department of the Treasury, “Treasury identifies eight Chinese tech firms as part of the Chinese military-industrial complex”, 16 December 2021; и Blake Schmidt and Ashlee Vance, “DJI won the drone wars, and now it’s paying the price”, Businessweek, 26 March 2020.

⁴⁷ См. Christof Heyns, “Human rights and the use of autonomous weapons systems (AWS) during domestic law enforcement”, Human Rights Quarterly, vol. 38, No. 2, pp. 350–378; и Australian Federal Police, “Australia and Sri Lanka strengthen ties over aerial drone surveillance”, 9 April 2021.

⁴⁸ См. Christian Enemark, “Armed drones and ethical policing: risk, perception, and the tele-present officer”, Criminal Justice Ethics, vol. 40, issue 2, pp. 124–144. См., например, Drone Volt’s Hercules 10 tear gas model (URL: <https://www.aeroexpo.online/prod/drone-volt/product-180237-28892.html>).

⁴⁹ См. Leo Kelion, “African firm is selling pepper-spray bullet firing drones”, BBC News, 18 June 2014.

оружия напрямую связана с определением внутренних рисков и вызовов национальной безопасности как внутри страны, так и за ее пределами. Специальный докладчик напоминает предприятиям, что они несут ответственность за соблюдение всех международно признанных прав человека. Они должны избегать нарушения прав человека других и устранять неблагоприятные последствия оказанного ими воздействия. По существу, государства должны привлекать предприятия к ответственности за нарушения прав человека. В разделе II Руководящих принципов предпринимательской деятельности в аспекте прав человека представлено авторитетное руководство для всех предприятий по выполнению этой обязанности⁵⁰.

33. По мере совершенствования технологии БПЛА операторы, вероятно, перейдут на микро- или нанодроны, что повлечет за собой глубокие последствия для прав человека в результате их более легкого внедрения и возможностей проникновения. БПЛА Black Hornet («Черный шершень»), разработанный норвежской компанией Prox Dynamics, в настоящее время официально используется примерно 20 вооруженными силами, включая морскую пехоту США, британскую армию и вооруженные силы Австралии, Германии, Турции Франции, Южной Африки и других стран. Он весит менее 20 граммов, помещается в одной руке и летает практически бесшумно. Современные модели могут быть оснащены камерами для съемки движущихся и неподвижных объектов, а радиус действия составляет 1,6 км. За последние пять лет вооруженными силами были внедрены тысячи этих микродронов⁵¹.

34. Кроме того, Специальный докладчик глубоко обеспокоена использованием БПЛА для наблюдения за протестами. Она вновь подчеркивает, что это согласуется с более широкой тенденцией, которую она выявила: кратковременное исключительное использование определенных технологий и их быстрое перерождение в обычную государственную практику. Помимо очевидных последствий для частной жизни, свободы собраний, свободы выражения мнений и права на участие в политической жизни, использование дронов в сочетании с принудительной силой полиции поднимает вопросы произвольного задержания, свободы и безопасности человека, а также права на жизнь.

35. Учитывая, что национальные технологии БПЛА развиваются в направлении наделения их вооружением, необходимо обеспечить, чтобы рамки защиты прав человека, которые затрагиваются при операциях, ставящих под угрозу права объекта на безопасность и/или жизнь, стали частью стандартных оперативных процедур правоохранительных органов во всем мире. Следует извлечь уроки из негативных последствий использования беспилотных летательных аппаратов в контексте борьбы с терроризмом, и применить их к потенциальному использованию дронов в национальной правоохранительной деятельности. Первая часть — обязательства правоохранительных органов проводить предварительное планирование, а не просто использовать беспилотные летательные аппараты в качестве стандартной практики или по желанию сотрудников. Обязательства, связанные с планированием потенциально опасных операций, были подчеркнуты в прецедентном праве, например в деле Европейского суда по правам человека *МакКанн и другие против Соединенного Королевства*. В этом деле Суд постановил, что риск для жизни должен подвергаться «самому тщательному изучению, особенно в случае преднамеренного применения смертоносной силы, принимая во внимание не только действия представителей государства, которые фактически применяют силу, но и все сопутствующие обстоятельства, включая такие вопросы, как планирование и контроль

⁵⁰ A/HRC/48/31, п. 11.

⁵¹ См. [https://www.flir.co.uk/news-center/military/flir-wins-additional-\\$15.4m-contract-for-black-hornet-nano-uav-systems-for-u.s.-army-soldier-borne-sensor-program/](https://www.flir.co.uk/news-center/military/flir-wins-additional-$15.4m-contract-for-black-hornet-nano-uav-systems-for-u.s.-army-soldier-borne-sensor-program/); [https://www.flir.fr/news/press-releases/flir-systems-awarded-\\$89-million-contract-from-french-armed-forces-to-deliver-black-hornet-personal-reconnaissance-system/](https://www.flir.fr/news/press-releases/flir-systems-awarded-$89-million-contract-from-french-armed-forces-to-deliver-black-hornet-personal-reconnaissance-system/); и <https://www.regjeringen.no/en/aktuelt/droner/id2924942/?fbclid=IwAR0-IEUzOY5c5gorr6nY0-xBcqyGfgpCzzWQxb55Xgg9OniVOkKThv1Fumw.>

рассматриваемых действий»⁵². Факторы, которые необходимо учитывать при планировании, отмечены Комитетом по правам человека в пункте 12 его замечания общего порядка № 36, который гласит, что любое действие, которое влечет за собой риск смерти или серьезного ранения, «должно быть строго необходимым с учетом угрозы».

36. Если БПЛА будут использоваться таким образом, что возникает риск смерти или серьезного ранения, то государственные правоохранительные органы должны быть готовы выполнить свое обязательство в соответствии с правом прав человека по проведению надлежащего расследования (что признано на международном уровне Комитетом по правам человека⁵³, Межамериканским судом по правам человека⁵⁴ и Африканской комиссией по правам человека и народов⁵⁵). Ключевые аспекты обязательства по проведению расследования были официально изложены в пересмотренной версии Миннесотского протокола по расследованию предположительно незаконного лишения жизни. Эти аспекты включают следующее:

- a) расследование должно быть оперативным;
- b) расследование должно быть эффективным и тщательным;
- c) расследования и проводящие их лица также должны быть независимы от неправомерного влияния, а следователи должны быть беспристрастными и всегда действовать непредвзято;
- d) расследования нарушений должны быть прозрачными, в том числе благодаря их открытости для контроля со стороны широкой общественности и семей жертв.

37. Очевиден риск того, что технология БПЛА, используемая в контексте правоохранительной деятельности, выйдет за пределы этой сферы и будет использоваться в других контекстах и другими субъектами. Мы уже видели это в контексте борьбы с терроризмом. Распространение технологии БПЛА стимулируется основной группой государств, но они не могут быть уверены в том, что смогут контролировать ее дальнейшее рассеивание. Значительную озабоченность Специального докладчика вызывает процесс, посредством которого Организация Объединенных Наций и государства сотрудничают, предоставляют технические консультации и наращивают потенциал по всему миру, в том числе посредством передачи технологий, таких как БПЛА⁵⁶. Государства могут осуществлять передачу технологий намеренно и осознанно, но они также могут делать это из-за несоблюдения политикиальной осмотрительности, что позволяет осуществлять случайную, незапланированную или скрытую передачу технологий и средств. Государства, обладающие мощными инструментами, несут большую ответственность за их сохранность и предотвращение их попадания в другие руки. Продвигая использование таких технологий в государствах, Организация Объединенных Наций также должна выполнять такие обязательства, как политика политической осмотрительности в вопросах прав человека. Положение дел в государствах в области контроля над технологией БПЛА оставляет желать лучшего. Как отметил Специальный докладчик по вопросу о внесудебных казнях, казнях без надлежащего судебного разбирательства или произвольных казнях, согласно сообщениям, по меньшей мере 20 негосударственных субъектов, включая Ливийскую национальную армию, Харакат Тахрир аш-Шам, Палестинский исламский джихад, венесуэльских военных дезертиров, Рабочую партию Курдистана (РПК), группу «Мауте», Картель Нового поколения Халиско, движение «Аль-Хуси» и ИГИЛ, получили вооруженные и невооруженные

⁵² European Court of Human Rights, *McCann and others v. the United Kingdom*, Application No. 18984/91, Judgment, 27 September 1995, para. 150.

⁵³ Замечание общего порядка № 31, пп. 15 и 18.

⁵⁴ *Montero Aranguren et al (Detention Center of Catsia) v. Venezuela*, Ser.C, No. 150, Judgment, 5 July 2006, para. 66.

⁵⁵ Замечание общего порядка № 3, пп. 2 и 15.

⁵⁶ См. A/76/261.

беспилотные системы⁵⁷. Государства постепенно начинают осознавать последствия использования дронов негосударственными или преступными группами. В апреле 2022 года правительство Соединенных Штатов приступило к реализации национального плана по борьбе с беспилотными авиационными системами, направленный на противодействие злонамеренному применению беспилотников враждебными внутренними субъектами⁵⁸.

C. Искусственный интеллект в борьбе с терроризмом

38. Специальный докладчик отмечает стремительный рост использования ИИ, что ведет к изменению множества областей социальной, экономической, политической и военной деятельности. Она признает, что ИИ обладает свойствами технологии общего назначения, а это значит, что он откроет широкие возможности для применения. Она подтверждает, что государства все активнее внедряют ИИ в сферы правоохранительной деятельности, национальной безопасности, уголовного правосудия и пограничного контроля⁵⁹.

39. В основе разработки и использования ИИ лежат алгоритмы, и в этих условиях ИИ функционирует как инструмент прогнозирования. В контексте борьбы с терроризмом системы ИИ используют большие объемы данных, включая данные за прошлые периоды, данные уголовного правосудия, сведения о поездках и переписку, данные социальных сетей и медицинские данные. Эти технологии могут быть использованы для создания профилей людей, определения мест, которые могут стать местами повышенной криминальной или террористической активности, и для выявления людей как вероятных подозреваемых и предполагаемых рецидивистов⁶⁰. Использование ИИ имеет прямые последствия для человека в плане его взаимодействия с властью государства, включая используемые им средства принуждения. Серьезные последствия такого сбора данных и прогностической деятельности для частной жизни и прав человека затрагивают как допускающие, так и не допускающие отступлений права. Специальный докладчик подчеркивает свою глубокую обеспокоенность тем, что оценки ИИ применяются для инициирования действий государства в контексте борьбы с терроризмом — от обыска, допроса, ареста, судебного преследования и административных мер до более интенсивного и интрузивного наблюдения, в то время как разумные подозрения не должны базироваться исключительно на оценках ИИ, учитывая их вероятностный характер. Она согласна с УВКПЧ в том, что непрозрачность принятия решений на основе ИИ создает исключительные трудности для обеспечения транспарентности и ответственности за нарушения прав человека при его использовании⁶¹.

40. Кроме того, Специальный докладчик глубоко обеспокоена укоренившейся практикой принятия государствами законодательства, освобождающего использование ИИ в военных целях и целях национальной безопасности от обычных режимов надзора. В этой связи она отмечает исключение, содержащееся в предложенном Европейским союзом законе об искусственном интеллекте и в конфиденциальном «нулевом проекте» конвенции Совета Европы об ИИ, правах человека, демократии и верховенстве права. В европейском контексте она решительно предостерегает от полного освобождения от ответственности по соображениям национальной безопасности в законе об ИИ и призывает Европейский союз обеспечить, чтобы такое освобождение было соразмерным и соответствовало действующему законодательству Европейского союза, включая Хартию основных прав. Она рекомендует законодательно обязать такие агентства, как Агентство Европейского союза по сотрудничеству правоохранительных органов (Европол)

⁵⁷ A/HRC/44/38, п. 9.

⁵⁸ См. <https://www.whitehouse.gov/briefing-room/statements-releases/2022/04/25/fact-sheet-the-domestic-counter-unmanned-aircraft-systems-national-action-plan/>.

⁵⁹ См. A/HRC/48/31.

⁶⁰ Там же, п. 23.

⁶¹ См. A/HRC/48/31.

и Европейское агентство пограничной и береговой охраны (Фронтекс), выполнять обязательства в соответствии с Хартсией, поскольку их исключение создаст сферу исключительности, которая послужит пагубным прецедентом на региональном и глобальном уровнях. Специальный докладчик подчеркивает, что системы ИИ, разработанные для военных целей или целей двойного назначения, должны регулироваться законом об ИИ. Она придерживается позиции, что конвенция Совета Европы должна охватывать проектирование, разработку и использование систем ИИ для целей национальной обороны. Исключение этих аспектов фактически приведет к тому, что предлагаемая конвенция не будет затрагивать проблемы прав человека, которые наиболее актуальны в регионе.

D. Наблюдение

41. Специальный докладчик глубоко обеспокоена масштабами нарушений прав человека, вызванных распространением по всему миру и неправомерным использованием сложных технологий кибернаблюдения, применение которых изначально оправдывалось целями борьбы с терроризмом и обеспечения национальной безопасности или предназначалось для их выполнения. Она подготовила для государств-членов документ с изложением позиции по этому вопросу под названием «Глобальное регулирование торговли технологиями шпионского программного обеспечения для борьбы с терроризмом: обзор предложений по ориентированному на права человека подходу»⁶². В приложении к настоящему докладу приводится резюме рекомендаций, содержащихся в документе с изложением позиции, включая необходимые характеристики любой будущей нормативно-правовой базы, направленной на решение проблемы глобальной торговли шпионским программным обеспечением. Специальный докладчик признает, что эти мощные и инновационные технологии могут предоставить правоохранительным органам, военным и службам безопасности эффективные инструменты расследования и мониторинга для пресечения террористического насилия и привлечения виновных к ответственности.

42. Сочетание в XXI веке двух факторов — быстрого повышения мощности и сложности компьютерного оборудования и программного обеспечения и значительного увеличения финансирования и значимости государственных программ борьбы с терроризмом — привело к развитию широкого спектра передовых технологий наблюдения, направленных на борьбу с терроризмом или подходящих для этих целей. Стандартная практика борьбы с терроризмом и проведения уголовных расследований, продвигаемая многосторонними организациями, такими как Совет Европы и Международная организация уголовной полиции (Интерпол), предусматривает наблюдение и сбор данных на регулярной основе с помощью ряда аппаратных и программных средств в целях проведения следственного анализа⁶³. Возможности для такого массового наблюдения как основного инструмента расследования резко возросли благодаря ряду сходящихся тенденций последних лет: стремительному снижению стоимости технологий и хранения данных; повсеместному распространению цифровых устройств и возможностей подключения; и экспоненциальному росту вычислительной мощности компьютеров.

43. Бурное развитие индустрии технологий наблюдения в XXI веке отчасти связано со значительными потоками финансирования в сфере борьбы с терроризмом. Это также стало следствием чрезвычайных полномочий, которые государственные органы присвоили себе на том якобы основании, что задачи борьбы с терроризмом оправдывают повсеместное наблюдение и вмешательство властей как инструмент предупреждения и расследования⁶⁴. В соответствии с фундаментальными моделями использования, выявленными в настоящем докладе, вмешательство обычно

⁶² См. <https://www.ohchr.org/sites/default/files/documents/issues/terrorism/sr/2022-12-15/position-paper-unsrct-on-global-regulation-ct-spyware-technology-trade.pdf>.

⁶³ См. Council of Europe Cybercrime Programme Office, Standard operating procedures for the collection, analysis and presentation of electronic evidence, September 2019.

⁶⁴ A/69/397, п. 19.

представляется как направленное только на определенные группы риска, как правило, нечетко и сомнительно определенные на основе (часто дискриминационных)⁶⁵ допущений о предполагаемом риске причинения вреда в будущем. Такие оценки риска часто базируются на недостаточных или скучных эмпирических данных, а их методологии зачастую имеют недостатки и плохо продуманы для решения поставленной задачи. Отсутствие ясности или точности в этих определениях приводит к тому, что контртеррористические операции выходят за первоначально заявленные границы.

44. Передовые технологии наблюдения, разработанные в целях борьбы с терроризмом и обеспечения национальной безопасности, все чаще становятся предметом озабоченности международной общественности в связи с целым рядом разоблачений, свидетельствующих о том, что такие инструменты фактически используются для шпионажа за политиками, журналистами, правозащитниками, адвокатами и обычными гражданами, не связанными с терроризмом и не представляющими угрозы национальной безопасности. Интрузивные скрытые технологии отслеживания содержания цифровых сообщений и другой информации отдельных лиц, включая метаданные (местоположение, продолжительность, источник и контакты) — широко известные как шпионские программы, — распространились по всему миру, выйдя из-под всякого контроля, и представляют собой существенный риск с точки зрения поощрения и защиты прав человека. Такие глубокие проблемы иллюстрирует скандал, связанный с использованием репрессивными режимами программы слежки Pegasus, произведенной компанией киберразведки NSO Group. Такое использование повлекло расследование со стороны Европейского парламента, а также судебные разбирательства⁶⁶.

45. Влияние наблюдения на многочисленные права человека значительно. Специальный докладчик подчеркивает, что право на неприкосновенность частной жизни функционирует как промежуточное право, защищающее и обеспечивающее многие другие права и свободы, и его защита тесно связана с существованием и развитием демократического общества. В связи с этим она считает рост масштабов использования скрытого наблюдения и сбора информации о контенте и метаданных в целях борьбы с терроризмом в сочетании с бурным развитием недостаточно регулируемых новых технологий большой угрозой для демократических обществ.

46. Ответственность за эти серьезные проблемы лежит не только на частных организациях, которые разрабатывают и либо сознательно предоставляют такие технологии непосредственно режимам, нарушающим права, либо не проявляют должной осмотрительности в отношении конечного использования своей продукции, но и на государственных учреждениях, которые неправомерно используют эти технологии в нарушение международного и внутреннего права, а также на государствах и международных организациях, которые либо активно способствуют попаданию таких технологий в чужие руки, либо, в силу отсутствия жесткого регулирования, не смогли его предотвратить.

47. Если в предыдущие эпохи шпионаж и технологии наблюдения были исключительной прерогативой государственных учреждений и штатных технических специалистов, то в наше время подавляющее большинство средств наблюдения, используемых государственными органами, приобретаются в частном секторе. Среди частных компаний, занимающихся кибербезопасностью и ответственных за инструменты с такими возможностями, — израильские компании NSO, Quadream и Candiru/Saito Tech; британская компания Gamma International; базирующиеся в Германии компании Vilicius Holding и Trovicor; базирующиеся во Франции Qosmos и Amesys; базирующиеся в Италии Area SpA и Hacking Team/Memento Labs; фирма

⁶⁵ A/HRC/43/46, pp. 28–34.

⁶⁶ В марте 2022 года Европейский парламент создал комитет по расследованию использования Pegasus и аналогичных шпионских программ для слежки (см. <https://www.europarl.europa.eu/committees/en/pega/home/highlights>). Что касается судебных разбирательств, см. United States Federal Case No. 19-cv-07123-PJH WhatsApp Inc. et al v. NSO Group Technologies Ltd et al.

Cytrix, имеющая подразделения в Венгрии, Израиле и Северной Македонии; американские фирмы CyberPoint, Narus (дочерняя компания Boeing), Blue Coat Systems и Cisco Systems; и фирма DarkMatter из Объединенных Арабских Эмиратов. Необходимо в срочном порядке отрегулировать деятельность этих предприятий и транснациональных корпораций в соответствии с обязательствами государств в отношении регулирования предпринимательского сектора, чтобы предотвратить нарушения прав человека.

48. В свете последних разоблачений все большее число представителей международного правозащитного сообщества поддерживают предложение о создании более надежной, соответствующей правам человека нормативно-правовой базы для использования, продажи и передачи технологий наблюдения, а на данный момент — к введению моратория на торговлю такими технологиями и их передачу. Верховный комиссар Организации Объединенных Наций по правам человека призывала к созданию более совершенной, основанной на правах человека системы регулирования торговли шпионскими программами, включая механизмы возложения ответственности за нарушения прав человека на частных производителей шпионских программ посредством «законодательного требования к соответствующим компаниям выполнять свои обязательства в области прав человека, повысить прозрачность в отношении разработки и использования своих продуктов и ввести более эффективные меры подотчетности»⁶⁷. Вместе с тем Верховный комиссар также призывала приостановить торговлю технологиями наблюдения, чтобы дать возможность государствам разработать режим экспорта и контроля, а также укрепить правовую базу, обеспечивающую неприкосновенность частной жизни⁶⁸. Кроме того, Специальный докладчик по вопросу о праве на свободу мнений и их свободное выражение, Специальный докладчик по вопросу о положении правозащитников, Специальный докладчик по вопросу о правах на свободу мирных собраний и ассоциации и члены Рабочей группы по вопросам предпринимательства и прав человека сделали следующее совместное заявление:

В последние годы мы неоднократно были тревогу по поводу опасности, которую представляет технология наблюдения для прав человека. Мы вновь призываем международное сообщество разработать надежную нормативную базу для предотвращения, смягчения и устранения негативного воздействия технологий наблюдения на права человека, а до этого ввести мораторий на их продажу и передачу⁶⁹.

УВКПЧ недавно вновь высказался в поддержку временного моратория в своем докладе 2022 года о праве на неприкосновенность частной жизни в цифровую эпоху⁷⁰. В апреле 2022 года Коста-Рика стала первым государством, присоединившимся к призыву о введении моратория на торговлю технологиями шпионского программного обеспечения⁷¹, а широкая коалиция гражданского общества повторила требование о введении моратория на встрече Всемирного экономического форума, состоявшейся в Давосе, Швейцария, в мае 2022 года⁷².

49. Учитывая глубокую озабоченность относительно этих технологий и прикрытия, которое им дают современные рассуждения на тему борьбы с терроризмом и ее практика, Специальный докладчик согласна с призывами приостановить передачу таких технологий. Она не исключает, что государства могут прийти к мнению об обоснованности постоянного запрета на шпионские программы, но прислушивается к призыву Верховного комиссара проводить исследования и работать над созданием соответствующей правам человека системы регулирования продажи, использования и

⁶⁷ См. <https://www.ohchr.org/en/2021/07/use-spyware-surveil-journalists-and-human-rights-defendersstatement-un-high-commissioner>.

⁶⁸ См. <https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=27455&LangID=E>.

⁶⁹ См. <https://www.ohchr.org/en/press-releases/2021/08/spyware-scandal-un-experts-call-moratorium-sale-life-threatening>.

⁷⁰ A/HRC/51/17, п. 19.

⁷¹ См. <https://www.accessnow.org/costa-rica-first-country-moratorium-spyware/>.

⁷² См. <https://www.accessnow.org/spyware-davos-press-conference/>.

передачи технологий шпионских программ, либо в качестве предвестника такого запрета, либо в качестве средства обеспечения защиты прав человека без необходимости его введения. Документ с изложением позиции Специального докладчика представляет собой новое эффективное предложение по международному регулированию торговли шпионскими программами с целью минимизации рисков для прав человека.

50. В заключение она подчеркивает необходимость независимого надзора за осуществлением наблюдения и сбора данных по соображениям национальной безопасности или борьбы с терроризмом⁷³. Отмечая, что спецслужбы стимулируют и адаптируют технологические изменения и внедряют множество новых технологий, включая машинное обучение, для автоматизированных наступательных и оборонительных операций в компьютерных сетях, Специальный докладчик призывает к существенным государственным инвестициям в развитие потенциала надзора за спецслужбами. Экономия применительно к надзору за осуществлением наблюдения не может быть оправдана с учетом развития технологий наблюдения, поскольку легитимность действий исполнительной власти зависит от эффективного, современного и всеобъемлющего надзора за спецслужбами⁷⁴. Она настоятельно призывает к предоставлению надзорным органам прямого доступа к оперативным системам спецслужб⁷⁵ и разрешения проверять хранящиеся данные на предмет ошибок в заполнении в качестве общей практики. Они также должны участвовать в проверках минимизации данных. Это обеспечит надзор за журналами регистрации разведывательных данных и создаст методы, позволяющие осуществлять надзор, если систематическое выявление закономерностей покажет большое совпадение с незаконным и ненадлежащим использованием баз данных спецслужб. Наконец, она подчеркивает, что необходимо срочно провести отвечающий правам человека обзор сотрудничества спецслужб⁷⁶, который потребует последовательной проверки передаваемых разведданных с помощью таких методов, как предупреждение надзорных органов об обмене данными, последовательная проверка файлов журналов, мониторинг удаления данных и мораторий на обмен разведданными с агентствами-компараторами, которые, как было установлено, постоянно нарушают права человека⁷⁷.

E. Последствия терроризма: жертвы

51. В своей резолюции 42/18 Совет по правам человека предложил Специальному докладчику рассмотреть негативные последствия терроризма. Она была рада представить анализ правовых параметров последствий терроризма в области прав человека в своем докладе Совету за 2021 год⁷⁸. В нем содержится всеобъемлющая обновленная информация о правозащитных обязательствах государств перед жертвами терроризма, а также призыв к государствам принять правозащитный подход и ориентированные на права человека и недискриминационные меры по защите, расследованию, обеспечению средств правовой защиты и участия, а также увековечению памяти жертв терроризма⁷⁹.

⁷³ А/HRC/10/3,пп. 25–78, и А/HRC/14/46.

⁷⁴ См. Kilian Vieth and Thorsten Wetzling, “Data-driven intelligence oversight: recommendations for a system update”, Stiftung Neue Verantwortung, 2019, p. 9.

⁷⁵ Это необходимо для проведения выборочных проверок, внеплановых инспекций и (полу)автоматизированного контроля за обработкой данных спецслужбами.

⁷⁶ В качестве основной проблемы в области прав человека она выделяет тот факт, что, после того как спецслужбы передают данные иностранным партнерам, они теряют контроль над их последующим использованием.

⁷⁷ Она отмечает положительную практику органов по надзору за деятельностью спецслужб Дании и Швеции.

⁷⁸ А/HRC/46/36,пп. 32–38.

⁷⁹ См. Принципы и установки в отношении детей, связанных с вооруженными силами или вооруженными группами (Парижские принципы); и резолюцию СБ ООН 1314 (2000).

52. Пользуясь возможностью, Специальный докладчик хотела бы затронуть еще два вопроса: уникальные потребности и права детей, ставших жертвами терроризма, и необходимость принятия государствами законодательства, отвечающего требованиям прав человека, для защиты прав человека жертв терроризма.

53. Она подчеркивает непреходящие последствия терроризма для жизни детей и обращает особое внимание на обязательства государств использовать Конвенцию о правах ребенка в качестве руководства при решении вопросов, связанных с правами детей, ставших жертвами терроризма. Специальный докладчик подчеркивает, что при принятии мер в отношении таких детей необходимо исходить из наилучших интересов ребенка. Она отмечает, что учитывающие интересы ребенка и гендерную специфику меры по оказанию помощи детям, ставшим жертвами терроризма, в связи с полученными травмами имеют важное значение и недостаточно развиты во многих государствах. Необходимо сосредоточить внимание на вопросах устойчивости к потрясениям, а также на праве на учитывающее потребности ребенка психологическое медицинское обслуживание и образование как на путях, обеспечивающих и поддерживающих долгосрочное восстановление.

54. Специальный докладчик выражает обеспокоенность положением детей, ставших жертвами ИГИЛ в Ираке и Сирийской Арабской Республике, тысячи из которых произвольно удерживаются в лагерях Аль-Холь и Родж на севере Сирийской Арабской Республики. Она подчеркивает, что с детьми, содержащимися в этих лагерях, необходимо обращаться в первую очередь как с жертвами терроризма в соответствии с Конвенцией о правах ребенка, резолюцией 2427 (2018) Совета Безопасности и резолюцией 60/1 Генеральной Ассамблеи. Этим детям отказано во всех мыслимых законных правах на достойную и защищенную жизнь в детстве. Специальный докладчик особенно встревожена положением мальчиков и подростков, содержащихся под стражей на основании предположения о «связи [с террористами]» в так называемых реабилитационных учреждениях, в условиях, которые, по ее мнению, соответствуют определению пыток и других жестоких, бесчеловечных и унижающих достоинство видов обращения и наказания согласно международному праву. Она безоговорочно считает, что государства не могут выбирать жертв терроризма по своему усмотрению, и отказ в защите детей, которые подверглись такому жестокому обращению со стороны признанной террористической группы, подрывает принцип равенства, основополагающий для защиты всех жертв терроризма без дискриминации. Специальный докладчик подчеркивает, что для защиты таких жертв от последствий терроризма и продолжающейся жестокости бессрочного и произвольного содержания под стражей необходимо срочно провести их депатриацию с соблюдением прав человека.

55. В заключение Специальный докладчик переходит к вопросу о внутреннем регулировании терроризма. Она высоко оценивает типовые законодательные положения в поддержку потребностей и защиты прав жертв терроризма, разработанные совместно Межпарламентским союзом, Управлением Организации Объединенных Наций по наркотикам и преступности и Контртеррористическим управлением, которым она была рада оказать техническую помощь и в работу которых внести свой вклад⁸⁰. Специальный докладчик призывает государства принять внутреннее законодательство, ориентированное на права человека, для полной и равной защиты прав всех жертв, включая жертв терроризма.

⁸⁰ См.

https://www.unodc.org/documents/terrorism/Website2021/220204_model_legislative_provisions.pdf.

III. Рекомендации

A. Государства

56. Специальный докладчик рекомендует государствам:

- а) принять всеобъемлющее внутреннее законодательство, защищающее права личности и коллективные права при сборе данных по соображениям национальной безопасности, борьбы с терроризмом или экстремизмом, в том числе насилиственным;
- б) обеспечить, чтобы в своей политике и процедурах использования вооруженных БПЛА как в условиях борьбы с терроризмом и конфликтов, так и вне их, в том числе в экстерриториальных операциях, они строго соблюдали установленные нормы международного права, международного гуманитарного права и международного права прав человека (в зависимости от ситуации), а использование вооруженных дронов в национальном контексте должно регулироваться надежными механизмами надзора в полном соответствии с правом прав человека, причем такой надзор должен применяться на технологически нейтральной основе ко всем разработкам в области технологий БПЛА;
- в) принять всеобъемлющее внутреннее законодательство, которое надлежащим образом защищает право на неприкосновенность частной жизни как основное право, обеспечивающее и поддерживающее защиту других основных прав человека, включая права, не допускающие отступлений. Сюда относится всеобъемлющее законодательство о защите данных;
- г) создать и поддерживать обеспеченный надлежащим финансированием и независимый надзор за новыми технологиями в контексте борьбы с терроризмом и обеспечения безопасности. Это включает создание независимых органов надзора за обеспечением конфиденциальности данных. Параллельно государства должны предоставить органам надзора за деятельностью спецслужб достаточные ресурсы и технологические возможности для изучения широкого использования технологий спецслужбами. Сюда относится прямой доступ к оперативным системам спецслужб, доступ к хранящимся данным, надзор за журналами регистрации разведданных, а также создание механизмов надзора за сотрудничеством спецслужб, о чем говорится в настоящем докладе;
- д) ввести моратории на не учитывающее права человека трансграничное сотрудничество, способствующее передаче технологий, связанных с высоким риском, государствам, в которых наблюдается неудовлетворительная ситуация с соблюдением прав человека или их хроническое нарушение;
- е) предоставлять надлежащие и доступные средства правовой защиты лицам, чья личная информация была неправильно обработана или использована неправомерно в контексте борьбы с терроризмом или предотвращения и пресечения насилиственного экстремизма;
- ж) принять практические законодательные меры для защиты от нарушений прав человека со стороны предприятий технологического сектора;
- и) взять на себя обязательство осуществлять независимый надзор за деятельностью Целевой группы Глобального договора Организации Объединенных Наций по координации контртеррористической деятельности и Контртеррористического управления.

57. Специальный докладчик также призывает:

- a) пересмотреть предлагаемое законодательство Европейского союза по ИИ с целью устранения исключений, связанных с национальной безопасностью;
 - b) повысить прозрачность, инклюзивность и открытость процесса разработки «нулевого проекта» конвенции Совета Европы по ИИ;
 - c) в соответствии с докладом Верховного комиссара, принять на уровне государств надежные режимы экспортного контроля в отношении трансграничной торговли технологиями наблюдения, с тем чтобы предотвратить продажу таких технологий при наличии риска их возможного использования для нарушения прав человека, в том числе в отношении правозащитников и журналистов⁸¹;
 - d) ввести мораторий на использование технологий дистанционного биометрического распознавания в общественных местах по крайней мере до тех пор, пока ответственные органы не смогут продемонстрировать соблюдение стандартов конфиденциальности и защиты данных и отсутствие серьезных проблем в плане точности и последствий дискриминационного характера, а также до тех пор, пока не будут выполнены⁸² все рекомендации, изложенные в пункте 53 j) доклада Специального докладчика по вопросу о поощрении и защите права на свободу мнений и их свободное выражение⁸³.

В. Конкретные рекомендации для Организации Объединенных Наций

58. Специальный докладчик рекомендует:

⁸¹ А/HRC/41/35, п. 49, и А/HRC/44/24, п. 40. В этих докладах Специальный докладчик по вопросу о поощрении и защите права на свободу мнений и их свободное выражение и Верховный комиссар призывали ввести мораторий на выдачу экспортных лицензий на технологии наблюдения.

⁸² A/HRC/48/31, п. 59 д).

A/HRC/44/24.

c) Генеральному секретарю инициировать процесс внутренней проверки и оценки или внешней независимой проверки Программы по борьбе с передвижениями террористов для обеспечения добросовестности применяемой в ее рамках практики и передачи технологий в том, что касается прав человека, защиты данных и верховенства права.

C. Коммерческие предприятия

59. Специальный докладчик подчеркивает, что:

a) предприятия в секторах новых технологий должны открыто осуществлять свою деятельность, на практике руководствуясь международным правом прав человека, и действовать с должной осмотрительностью, чтобы избежать неблагоприятного воздействия на отдельных лиц и общины, в том числе посредством осуществления рамок в отношении «защиты, соблюдения и средств правовой защиты», закрепленных в Руководящих принципах предпринимательской деятельности в аспекте прав человека⁸⁴;

b) предприятия в сфере новых технологий должны осуществлять комплексную политику должной осмотрительности в вопросах прав человека. Она включает проведение оценки рисков фактического и потенциального воздействия на права человека, как прямого, так и косвенного, на всех этапах ведения бизнеса;

c) предприятия, занимающиеся разработкой, использованием и передачей новых технологий, связанных с высоким риском, должны подвергаться более строгому регулированию и надзору со стороны законодательных органов, судов и органов международного регулирования, включая значительные финансовые и административные санкции за несоблюдение надлежащей практикиальной осмотрительности.

⁸⁴ См.

https://www.ohchr.org/sites/default/files/documents/publications/guidingprinciplesbusinesshr_ru.pdf.

Annex

Draft Proposed State Commitments with Respect to the International Trade in Spyware

1. The current response to the challenge posed to human rights by the extremely powerful tools of the contemporary spyware industry is fractured and inadequate. Direct approaches to the voluntary responsibility of corporations developing and selling the technology rely upon the UN Guiding Principles on Business and Human Rights, the effectiveness of which is undermined by the absence of a binding enforcement arm. Domestic private law doctrines form an inconsistent patchwork, with ample room for argument about degrees of responsibility along transnational production chains, how human rights harms equate to (or diverge from) traditional models of physical harm, and how relationships between private entities and foreign sovereign entities ought to be dealt with. They also necessitate victims of unlawful surveillance having the knowledge and the means to use litigation to hold private companies to account. At the same time the export control system was developed for the radically different context of conventional arms. It grants exporting States generous latitude in their decision-making, providing the conditions for confusion, inconsistency, and arbitrage between jurisdictions.
2. All of this means that there is no obvious mechanism for accountability if corporations fail to advert to the harms to which their spyware technology may cause or contribute, and no clear deterrent to prevent producers from developing and trading in such technology without concern for its potential impacts.
3. As a result, the way forward for regulation of the spyware trade requires a novel approach which avoids the gaps in the existing patchwork of purported oversight and accountability methods.
4. A human rights analysis of the use of spyware in the counter-terrorism context suggests that spyware technology must at a minimum: (a) allow for users to specifically target certain data and metadata, rather than automatically monitor and record all data and metadata; (b) avoid automatically accessing data relating to contacts of targeted individuals, unless users specifically require that additional information for investigative purposes; and, in any event, (c) create an indelible, permanent, and uneditable auditable record of what actions have been taken by the user of the spyware, including any interferences/modifications of data/metadata, when those occurred, and by whom they were effected so that the use of the tool can be verified, and its human rights compliance assessed after the fact by judicial authorities. Part of that indelible and uneditable record must be some form of identifier or watermark such that judicial authorities overseeing complaints may verify the producer of spyware alleged to have been used against a victim and the customer to which that spyware was originally supplied and, from such source, can compel disclosure of the auditable record such that the legality of any use complained of can be adequately reviewed. Spyware which fails to display such features cannot, however otherwise tightly regulated, be capable of human rights compliance.
5. It is therefore recommended that States adopt commitments substantively equivalent to the following draft proposals:

'Each State party shall, within two years from the date of their signature, give binding domestic effect to the following obligations (whether through the enactment of domestic legislation or such other steps (if any) as are required under its national law):'

1. Companies domiciled within their jurisdiction are prohibited from manufacturing or offering for sale or other provision spyware technology which fails to display the following cumulative characteristics:

- (a) Not automatically granting access to all data and/or metadata once the spyware infiltrates a network, computer, or device, and instead providing that the user must positively select the types of data and/or metadata for monitoring;

(b) Not automatically granting access to any data and/or metadata regarding contacts of the target network, computer, or device, and instead providing that the user must positively select any contacts for monitoring;

(c) Providing in all cases of use of the spyware that there is created an indelible, permanent, and uneditable auditable record of what actions have been taken by the user of the spyware, including any interferences/modifications of data/metadata, when those occurred, and by whom they were affected. This record must include a record of the producer and customer for the spyware technology, so that judicial authorities may properly be able to identify the producer and purchase of spyware used in any particular instance;

2. Companies domiciled within their jurisdiction are made subject to a binding obligation to undertake a human rights due diligence exercise upon the purchasers, and, if different, the reasonably foreseeable end users, of spyware technology sold. Such human rights due diligence shall be proportionate to the risk of the technology being used by purchasers, or reasonably foreseeable end users, in breach of international human rights law;

3. As a separate and independent obligation, companies domiciled within their jurisdiction are made subject to a binding obligation only to sell spyware technology in circumstances where they can prove that there is no tangible risk of the technology being used by purchasers, or reasonably foreseeable end users, in breach of international human rights law;

4. For the avoidance of doubt, while the fact that such companies have obtained guarantees or assurances of compliance with international human rights law from purchasers, and/or, if different, the reasonably foreseeable end users, may be taken into account in the due diligence exercise and in the companies' assessment of the real risk of breach, the mere fact of such guarantees or assurances will not, of itself, be sufficient to demonstrate compliance with their obligations set out above;

5. As a separate and independent obligation, companies domiciled within their jurisdiction are subject to a binding obligation not to sell spyware to the agencies of any State which is not itself a signatory of this treaty;

6. Breaches of the obligations set out above are to be actionable in the ordinary domestic courts of the State on the application of persons including but not limited to persons capable of demonstrating that they are likely (subject to an appropriate evidential burden) to have been victims of breaches of international human rights law connected with the use of that companies' technology; and

7. In the event that a court determines that a breach has occurred, the persons bringing actions in respect of the same are entitled to such remedies as are available in domestic law adequately to compensate them for the violations of their international human rights which are found to have occurred.
