Генеральная Ассамблея

Distr.: General
28 May 2019
Russian
Original: English

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

Слежение и права человека

Доклад Специального докладчика по вопросу о поощрении и защите права на свободу мнений и их свободное выражение*

Резюме

Слежение за отдельными лицами – зачастую журналистами, активистами, оппозиционерами, критиками и другими лицами, которые осуществляют свое право на свободу выражения мнений, – как было показано, приводит к произвольным задержаниям, иногда пыткам и, возможно, внесудебным казням. Такое слежение процветает в условиях слабого контроля за экспортом и передачей технологий правительствам, проводящим хорошо известную политику репрессий. В настоящем докладе Специальный докладчик сперва определяет проблему целенаправленного слежения, возникающую в связи с обязательствами, возложенными на государства правом прав человека, и соответствующими обязательствами компаний. Затем он предлагает правовые и политические рамки для регулирования, обеспечения подотчетности и транспарентности в сфере частной индустрии слежения. В заключение докладчик призывает ужесточить регулирование экспорта технологий слежения и ввести более строгие ограничения на их использование, а также безотлагательно ввести мораторий на глобальную продажу и передачу средств в сфере частной индустрии слежения до тех пор, пока не будут предусмотрены строгие гарантии в области прав человека для регулирования такой практики и обеспечения законного использования этих средств правительствами и негосударственными субъектами.

* Настоящий доклад был представлен после установленного срока, с тем чтобы отразить в нем самую последнюю информацию.

GE.19-08652 (R) 140619 170619

1908652

Содержание

I. Введение

1. Генеральная Ассамблея осудила незаконное или произвольное слежение и перехват сообщений как «крайне интрузивные действия», нарушающие основные права человека (см. резолюции 68/167 и 71/199 Генеральной Ассамблеи). Однако незаконное слежение продолжается без каких-либо явных ограничений. В материалах, представленных для настоящего доклада, подробно изложены отдельные случаи использования правительствами программного обеспечения для слежения, разработанного, продаваемого и поддерживаемого частными компаниями. Слежение за конкретными лицами – зачастую журналистами, активистами, оппозиционерами, критиками и другими лицами, которые осуществляют свое право на свободу выражения мнений, – как было показано, приводит к произвольным задержаниям, иногда пыткам и, возможно, внесудебным казням. Такое слежение процветает в условиях слабого контроля за передачей технологий правительствам, проводящим хорошо известную политику репрессий. Рынок окутан тайной; на самом деле наши знания об этой проблеме существуют главным образом благодаря работе неправительственных исследователей в области цифровой криминалистической экспертизы и неустанному освещению этой проблемы организациями гражданского общества и средствами массовой информации.

2. Учитывая достаточно высокую степень серьезности данной проблемы, Специальный докладчик завершает настоящий доклад призывом не только ужесточить регулирование экспорта технологий слежения и ограничения на их использование, но и безотлагательно ввести мораторий на глобальную продажу и передачу средств в сфере частной индустрии слежения до тех пор, пока не будут предусмотрены строгие гарантии в области прав человека в целях регулирования такой практики и обеспечения законности использования этих средств правительствами и негосударственными субъектами.

3. Специальный докладчик предлагает правовые и политические рамки для регулирования, обеспечения подотчетности и транспарентности в сфере частной индустрии слежения. Он начинает с определения проблемы, акцентируя внимание на целенаправленном слежении и оставляя в стороне вопрос о массовом перехвате, сборе и хранении личных данных (что часто называют «массовым слежением»). Затем он перечисляет обязательства, которые возлагает на государства право прав человека, и связанные с этим обязанности компаний. В части IV докладчик предлагает рамки для совершенствования существующего законодательства и политики путем включения защиты прав на свободу мнений и их свободное выражение на основе существующих норм международного права прав человека. В заключение он формулирует рекомендации для ключевых субъектов.

4. При подготовке настоящего доклада было получено 11 представлений от государств и 33 – от представителей гражданского общества. В декабре 2018 года в Бангкоке состоялись двухдневные консультации с экспертами, организованные Управлением Верховного комиссара по правам человека. Представленные материалы и высказанные в ходе консультаций мнения кратко резюмируются в добавлении к настоящему докладу[1].

II. Правительства и частная индустрия слежения

5. Мы живем в эпоху легкодоступных и труднообнаружимых средств цифрового слежения, которыми можно легко злоупотребить. В 2013 году предыдущий мандатарий Франк Ла Рю в своем новаторском докладе о слежении отметил, что слабая нормативно-правовая база создала благодатную почву для произвольных и незаконных нарушений прав на неприкосновенность частной жизни и свободу мнений

[1] Я хотел бы выразить особую благодарность Амосу То, Дезире Мюррей, Кристине Бутойю, Мэтью Марколи и Кьюли Парк из Лаборатории международного правосудия Ирвинской школы права Калифорнийского университета за их содействие в подготовке настоящего доклада и добавления к нему.

и их свободное выражение (A/HRC/23/40, пункт 3). В следующем году Верховный комиссар по правам человека в своем первом докладе о неприкосновенности частной жизни в цифровую эпоху сделал вывод о том, что отсутствие подотчетности в вопросах незаконного цифрового слежения является совокупным результатом отсутствия адекватного национального законодательства и/или правоприменения в данной области, слабых процедурных гарантий и неэффективного надзора (A/HRC/27/37, пункт 47).

6. Некоторые государства разрабатывают средства целенаправленного слежения силами своих собственных ведомств и министерств, другие перепрофилируют уже существующие «готовые к употреблению» продукты программного обеспечения, изначально разработанные в преступных целях, а третьи могут приобретать технически сложное коммерческое шпионское программное обеспечение на международном рынке услуг слежения[2]. В настоящем докладе Специальный докладчик уделяет особое внимание последней категории средств. Цифровое слежение более не является прерогативой стран, располагающих ресурсами для проведения массового и целенаправленного слежения с помощью собственных средств. В игру вступил частный сектор, который оказался без какого-либо надзора и действует с почти полной безнаказанностью. По данным «Прайвеси интернэшнл», в 2016 году насчитывалось более 500 компаний, которые занимаются разработкой, маркетингом и продажей продукции такого рода правительственным покупателям[3].

Виды слежения, которые рассматриваются в настоящем докладе

7. В настоящем докладе Специальный докладчик уделяет основное внимание технологиям, которые позволяют субъекту получить скрытый доступ к цифровым сообщениям, результатам работы, истории просмотров в интернет-браузере, исследованиям, данным о местоположении и онлайновой и оффлайновой деятельности отдельных лиц. Ниже описаны основные технологии и способы целенаправленного слежения.

Вмешательство в работу компьютера

8. С помощью технологий слежения можно получить несанкционированный доступ к компьютеру или персональной сети отдельного лица. Возможности такого вмешательства весьма широки[4]. Например, в 2017 году в Соединенных Штатах Америки апелляционный суд рассматривал дело о слежении на территории Соединенных Штатов Америки в интересах иностранного государства[5]. Речь идет о гражданине Соединенных Штатов Америки, родившемся в Эфиопии и проживающем в штате Мэриленд, который оказывал техническую помощь членам общины эфиопской диаспоры. Агенты правительства Эфиопии изначально отправили активисту документ, заразивший его компьютер интрузивной формой вредоносного программного обеспечения под названием «FinSpy», которое поставляется на рынок немецко-британской компанией «Гамма груп»[6]. Программное обеспечение «FinSpy» предположительно записывало интернет-видеозвонки, сохраняло электронные письма и другие сообщения этого человека и его семьи, в том числе фиксируя нажатия клавиш, и отправляло данные обратно на серверы, расположенные в Эфиопии[7].

[2] Citizen Lab, *Communities @ Risk: Targeted Digital Threats Against Civil Society* (Toronto, Monk School of Global Affairs, University of Toronto, 2014), Executive Summary, pp. 8–11.

[3] Представление «Прайвеси интернэшнл», стр. 1 текста оригинала.

[4] См., например, Ronald J. Deibert, *Black Code: Inside the Battle for Cyberspace* (Toronto, Signal, 2013), pp. 186–190.

[5] *Doe v. Federal Democratic Republic of Ethiopia*, 851 F.3d 7 (D.C. Cir. 2017).

[6] Информационные материалы о «FinSpy» можно найти в публикации на «Wikileaks» под названием «The spy files: remote monitoring and infection solutions: FINSPY».

[7] Более подробная информация в связи с этими утверждениями содержится в *first amended complaint, Doe v. Federal Democratic Republic of Ethiopia* (18 July 2014).

Взлом мобильных устройств

9. С помощью продуктов сферы частных услуг слежения также возможно взламывать мобильные устройства напрямую. Классическим примером является шпионское программное обеспечение «Pegasus», разработанное компанией «НСО груп», и его предполагаемое использование в Мексике – весьма поучительным. С 2015 года многие из числа тех, кто был связан с освещением коррупции и торговли наркотиками, стали получать на свои мобильные устройства текстовые сообщения или ссылки, причем некоторые источники казались вполне уместными и предлагали подробные сведения об объектах внимания. Подобные сообщения получали журналисты, политики, следователи Организации Объединенных Наций, правозащитники и другие лица. Канадская научно-исследовательская и правозащитная организация «Ситизен лэб» обнаружила, что при переходе по ссылке загружалось шпионское программное обеспечение «Pegasus», которое заражало устройство и позволяло осуществлять дистанционный мониторинг за объектом. «Ситизен лэб» выявила, что программное обеспечение «Pegasus» используется в качестве средства слежения за отдельными лицами в 45 странах, включая Бахрейн, Саудовскую Аравию, Того, Соединенное Королевство Великобритании и Северной Ирландии и Соединенные Штаты Америки[8].

Социальная инженерия

10. Использование многих технологий, описанных выше, сопровождается применением стратегий, направленных на то, чтобы заставить жертву непреднамеренно скачать на свое устройство вредоносное программное обеспечение. Например, жертве отправляют электронное письмо с вредоносной ссылкой от лица ее контакта или обманом убеждают ее, что ссылка доброкачественна и связана с ее работой, правозащитной деятельностью или личными делами. К примеру, сотрудник «Международной амнистии» получил в «WhatsApp» сообщение, которое исследователи приписывают шпионскому программному обеспечению «Pegasus», с призывом осветить протест – сообщение содержало ссылку, по которой якобы можно найти дополнительную информацию[9]. В результате перехода по ссылке на его устройство, вероятно, было бы загружено шпионское программное обеспечение.

Слежение за сетями

11. Некоторые технологии для целенаправленного слежения задействуют сети. Например, российская Система технических средств для обеспечения функций оперативно-розыскных мероприятий предусматривает возможность установки на телекоммуникационных сетях устройства, которое позволяет прослушивать телефонные разговоры. Данная система производится и поставляется на рынок частной компанией и широко используется в Российской Федерации и за ее пределами – в Центральной Азии. К примеру, компания «Протей» производит оборудование для таких технологий системы, как прослушивание разговоров и перехват сообщений в Интернете, которое применяется в Узбекистане и Казахстане[10].

Распознавание лиц и аффекта

12. Технология распознавания лиц направлена на захват и определение черт лица, что может сопровождаться профилированием отдельных людей на основе их этнической принадлежности, расы, национального происхождения, пола и других характеристик, которые часто являются основанием для незаконной дискриминации[11]. Распознавание аффекта призвано определить чувства, эмоции или намерения человека

[8] See Bill Marczak and others, “Hide and seek: tracking NSO Group’s Pegasus spyware to operations in 45 countries”, Citizen Lab, 18 September 2018.

[9] See Bill Marczak, John Scott-Railton and Ron Deibert, “NSO Group infrastructure linked to targeting of Amnesty International and Saudi dissident”, Citizen Lab, 31 July 2018.

[10] Andrei Soldatov and Irina Borogan, *The Red Web: The Struggle Between Russia’s Digital Dictators and the New Online Revolutionaries* (New York, PublicAffairs, 2015), pp. 190–191.

[11] См., например, представление «Интернет лэб», стр. 6 текста оригинала; и представление Центра по изучению Интернета и общества, стр. 12 текста оригинала.

по его выражению лица с помощью весьма сомнительных систем классификации[12]. Пожалуй, ни одна другая среда не демонстрирует всестороннюю интрузивность этих технологий лучше, чем Китай. Согласно заслуживающим доверия сообщениям, правительство Китая применяет технологию распознавания лиц и камеры наблюдения по всей стране, с тем чтобы «отслеживать исключительно уйгуров на основании их внешности и фиксировать их передвижения для отслеживания и учета»[13]. Большая часть технологий, используемых правительством, как представляется, производится внутри страны как государственными, так и частными предприятиями[14].

Ловушки международного идентификатора абонента мобильной связи (IMSI) («Stingray»)

13. Ловушки международного идентификатора абонента мобильной связи (IMSI) имитируют расположенные поблизости вышки сотовой связи и перехватывают сообщения и данные о местоположении, передаваемые с помощью личных устройств связи. Такие ловушки широко используются во всем мире, нередко правоохранительными органами и разведывательными службами. Одна из частных компаний в Соединенном Королевстве предположительно продавала такие ловушки и другое шпионское программное обеспечение Филиппинам – в этой связи многие опасаются, что данные средства использовались для отслеживания потребителей наркотиков и мониторинга за ними в ходе широко критикуемой правительственной войны против наркотиков[15].

Глубинный анализ сетевых пакетов

14. Глубинный анализ сетевых пакетов позволяет осуществлять мониторинг, анализ и перенаправление трафика, проходящего через коммуникационные и интернет-сети. Эта технология также может использоваться для перенаправления пользователей на зараженные вредоносным программным обеспечением сайты и блокировки пользовательского доступа к определенным веб-сайтам. По сообщениям, такие устройства были установлены в сети «Тюрк Телеком» и применялись, чтобы перенаправлять пользователей из Турции и Сирийской Арабской Республики на загрузку шпионского программного обеспечения при попытке загрузить нужные программные приложения[16].

Государственно-частное сотрудничество

15. На рынке средств цифрового слежения правительства и частный сектор тесно сотрудничают. Правительствам порой не хватает сил собственных министерств и ведомств, чтобы удовлетворить свои потребности. А частные компании обладают необходимыми для удовлетворения этих нужд стимулами, опытом и ресурсами. Существуют глобальные и региональные торговые выставки, которые организуются специально для того, чтобы правительства и частные компании нашли друг друга – механизм похож на работу служб знакомств[17]. Здесь они могут подобрать подходящего партнера. Но проявляют ли компании какую-либо должную осмотрительность, чтобы оценить степень уважения покупателями прав человека – неизвестно.

[12] AI Now Institute, *AI Now Report 2018* (New York, New York University, 2018), pp. 13–14.

[13] См. Paul Mozur, “One month, 500,000 face scans: how China is using A.I. to profile a minority”, *New York Times*, 14 April 2019.

[14] Представление «Хьюман райтс ин чайна», стр. 2–3 текста оригинала. См. также A/HRC/39/29, пункт 14.

[15] См. Sofia Tomacruz, “You think your data, communication devices are safe? Think again”, Rappler, 17 March 2018.

[16] См. Bill Marczak and others, “Bad traffic: Sandvine’s PacketLogic devices used to deploy government spyware in Turkey and redirect Egyptian users to affiliate ads?”, Citizen Lab, 9 March 2018.

[17] См., например, www.issworldtraining.com; и Patrick Howell O’Neill, “ISS World: the traveling spyware roadshow for dictatorships and democracies”, Cyberscoop, 20 June 2017.

16. Продавцы могут иметь благие намерения. Возможно, компании искренне верят в то, что их продукция используется уполномоченными государственными органами для «законного перехвата сообщений» обоснованных объектов слежения с разрешения судебных или других независимых субъектов. Однако это не может быть точно известно, поскольку каждый аспект такого сотрудничества – начиная с проявления должной осмотрительности и продажи и заканчивая оказанием поддержки конечным пользователям – обычно осуществляется в условиях ограниченного надзора и транспарентности. Фактически, почти вся общедоступная информация о частной индустрии слежения была получена благодаря криминалистической экспертизе таких неправительственных и научных учреждений, как «Ситизен лэб», а также журналистским расследованиям[18].

17. Особенно сомнительна репутация так называемого «рынка уязвимостей». Известно, что правительства и частные субъекты приобретают у исследователей в области безопасности данные об уязвимостях в безопасности общедоступного программного обеспечения: уязвимостях «нулевого дня», с помощью которых можно получить доступ к личным сообщениям и устройствам[19]. Пока производитель устройства или программного обеспечения не знает об этих уязвимостях, их можно использовать в качестве отправной точки для слежения. Когда правительства и компании не раскрывают информацию о таких уязвимостях, они ставят под угрозу безопасность конечных пользователей, в том числе клиентов из государственного и частного секторов, которые хранят в базах данных, разработанных частными компаниями, чувствительные финансовые и медицинские данные, а также данные о сотрудниках или данные, связанные с правоохранительной деятельностью. На сегодняшний день не достигнуто согласия относительно того, обязаны ли правительства и компании разглашать информацию об уязвимостях, а продажа таких уязвимостей не регулируется. По сути дела, в результате сложившейся ситуации не только развился рынок уязвимостей с высокой стоимостью, но и многие правительства и компании стали ревностно охранять свои знания об уязвимостях в надежде использовать их в наступательных целях[20].

18. Очевидно также, что государственно-частное сотрудничество не заканчивается в момент продажи и передачи продукта. В результате утечки документов выяснилось, что компании, работающие в частной индустрии слежения, оказывают послепродажную поддержку. Например, в 2014 году компания «ФинФишер», как сообщается, заключила с правительственными заказчиками «годовой(ые) контракт(ы) на поддержку» для обеспечения технической модернизации и технического обновления продуктов и предоставления других форм поддержки клиентов[21]. Они также проводят обучение по вопросам оптимизации своего вредоносного программного обеспечения в целях получения несанкционированного доступа к цифровым сообщениям, компьютерным устройствам и Wi-Fi сетям объектов слежения[22].

19. Компании и правительства стран их происхождения тесно связаны друг с другом, равно как и компании и покупатели. Некоторые из этих компаний имеют весомый голос в вопросах режима экспортного контроля своих стран и подрывают

[18] История частного слежения – это также и история критической важности свободных и независимых исследований и средств массовой информации. Те, кто занимается подобными расследованиями, также подвергают себя риску стать объектами слежения. См., например, Raphael Satter, “Undercover agents target cybersecurity watchdog”, Associated Press, 26 January 2019.

[19] См. Privacy International, “Exploiting privacy: surveillance companies pushing zero-day exploits”, 7 February 2018.

[20] См. обсуждение в представлении Сары МакКьюн, стр. 2–4 текста оригинала; Centre for European Policy Studies, *Software Vulnerability Disclosure in Europe: Technology, Policies and Legal Challenges* (Brussels, June 2018); и Sven Herpig and Ari Schwartz, “The future of vulnerabilities equities processes around the world”, Lawfare, 4 January 2019.

[21] См. Privacy International, “Six things we know from the latest FinFisher documents”, 15 August 2014.

[22] Ibid.

попытки укрепить эти режимы. Например, согласно заслуживающим доверия утверждениям, в 2016 году под давлением лоббистов от индустрии слежения некоторые формы технологий слежения были исключены из предложенного Европейским союзом перечня дополнений к перечню товаров и технологий двойного назначения, подлежащих экспортному контролю[23]. В ходе недавних переговоров по вопросу режима экспортного контроля Европейского союза интересы бизнеса, по всей видимости, повлияли на решение существенно ограничить включение гарантий прав человека в предложенные нормативные изменения, несмотря на широкое согласие относительно их принятия в Европейском парламенте[24].

20. В последних докладах также отмечается, что многие лица, обладающие специальными знаниями и опытом в области разведки и правоохранительной деятельности, переходят с государственной службы на работу в частный сектор. В результате этого круговорота кадров бывшие правительственные эксперты могут оказывать поддержку частным субъектам, инструменты которых могут быть использованы для нарушения прав человека[25]. В публикации агентства «Рейтер» 2019 года сообщалось, что несколько бывших сотрудников Агентства национальной безопасности Соединенных Штатов Америки перешли на работу в частную компанию, чтобы оказывать поддержку программе радиоэлектронной разведки Объединенных Арабских Эмиратов под кодовым названием «Проджект рэйвен»[26]. Упомянутые сотрудники, как сообщается, использовали свои знания и опыт для слежения за политическими оппонентами властей Объединенных Арабских Эмиратов и использования технологий в отношении граждан Соединенных Штатов Америки. Правительственное регулирование «круговорота кадров» в частной индустрии слежения представляется в лучшем случае малоэффективным и, вероятно, во многих, если не в большинстве, правовых системах отсутствует.

III. Правовые рамки

A. Обязательства государств

21. Объекты слежения являются жертвами нарушения их прав на неприкосновенность частной жизни и свободу мнений и их свободное выражение независимо от того, приносят ли усилия по мониторингу какие-либо результаты или нет[27]. Право на неприкосновенность частной жизни будет по-настоящему нарушено в том случае, если объект слежения не будет знать о неудавшейся или удавшейся попытке получения несанкционированного доступа. Естественно, правительства, как правило, ищут средства получения несанкционированного доступа, о котором объект не будет знать. Однако крайне важно рассматривать такое вмешательство как часть общих усилий, которые повлекут за собой последствия для объекта. Попытка слежения – и успешное слежение – в незаконных целях могут быть использованы для того, чтобы подавить инакомыслие, запретить критику или наказать независимое освещение нарушений (и источники такого освещения)[28]. Санкции могут применяться не к объекту, а к его сети контактов. В странах, где происходит повсеместное

[23] См. Reporters Without Borders, “International regulations: broken or blocked by lobbies”, 14 March 2017.

[24] См. Daniel Moßbrucker, “Surveillance exports: how EU Member States are compromising new human rights standards”, netzpolitik.org, 29 October 2018.

[25] См. Privacy International, “Switching hats: why South Africa’s surveillance industry needs scrutiny”, 14 December 2016; и Alex Kane, “How Israel became a hub for surveillance technology”, The Intercept, 17 October 2016.

[26] См. Christopher Bing and Joel Schectman, “Inside the UAE’s secret hacking team of American mercenaries”, Reuters, 30 January 2019; Robert Chesney, “Project Raven: what happens when U.S. personnel serve a foreign intelligence agency”, Lawfare, 11 February 2019; и представление Сары МакКьюн, стр. 7–8 текста оригинала.

[27] Представление Лаборатории глобального правосудия Школы права Нью-Йоркского университета, стр. 6 текста оригинала.

[28] См. представление Фонда по правам человека.

противоправное слежение, сообщества, за которыми идет слежение, знают или подозревают о таких попытках, что в свою очередь формирует и ограничивает их способность осуществлять права на свободу выражения мнений, ассоциации, религиозных убеждений, культуры и т. д. Иными словами, вмешательство в частную жизнь посредством целенаправленного слежения направлено на пресечение осуществления права на свободу выражения мнений.

22. Нет необходимости дублировать большое количество материалов по правам человека, которые уже были представлены предыдущими Специальными докладчиками, другими мандатариями, Верховным комиссаром, Советом по правам человека, Комитетом по правам человека и другими, где они выделяли следующие ключевые особенности правовых рамок в области прав человека, которые предусматривают защиту от целенаправленного слежения.

23. Во-первых, Международный пакт о гражданских и политических правах и Всеобщая декларация прав человека защищают права каждого человека на неприкосновенность частной жизни, свободу мнений и их свободное выражение. В статье 19 каждого из указанных документов закреплено право каждого человека беспрепятственно придерживаться своих мнений и искать, получать и распространять всякого рода информацию и идеи, независимо от государственных границ и способов. Пункт 1 статьи 17 Пакта, которая повторяет статью 12 Декларации, гласит, что «никто не может подвергаться произвольному или незаконному вмешательству в его личную и семейную жизнь, произвольным или незаконным посягательствам на неприкосновенность его жилища или тайну его корреспонденции».

24. В цифровую эпоху возникает тесная взаимосвязь между неприкосновенностью частной жизни и свободой выражения мнений, при этом неприкосновенность частной жизни в Интернете помогает обеспечить осуществление права на свободу мнений и их свободное выражение (A/HRC/29/32; и A/HRC/23/40, пункт 24). Статья 17 Пакта предусматривает, что меры посягательства на право на неприкосновенности частной жизни допустимы только при условии, что они «санкционированы национальным законодательством, которое является доступным, четким и которое соответствует требованиям Пакта», «отвечают требованиям необходимости и соразмерности» и преследуют «законную цель» (A/69/397, пункт 30). В статье 19 закреплена трехчастная формула, согласно которой ограничения должны быть установлены законом и являться необходимыми для защиты прав или репутации других лиц, национальной безопасности или общественного порядка, здоровья или нравственности населения[29]. Комитет по правам человека подчеркнул, что эти принципы означают по меньшей мере следующее:

a) установлены законом/законность: любое ограничение должно быть сформулировано достаточно четко, с тем чтобы дать лицу возможность соответствующим образом следить за своим поведением, а информация о нем должна быть доступна широким слоям населения. Любое ограничение не может быть чрезмерно расплывчатым или чрезмерно широким и в результате наделять должностных лиц неограниченными дискреционными полномочиями[30];

b) необходимость и соразмерность: на государство возлагается бремя доказывания прямой и непосредственной связи между формой выражения и угрозой и того, что ограничение, которое государство намерено ввести, представляет собой наименее ограничительное средство из числа тех, с помощью которых может быть достигнут желаемый результат такого рода[31];

c) обоснованность: в пункте 3 статьи 19 устанавливаются конкретные ограничения в отношении интересов, которые могут оправдывать ограничения. Ввиду характерной для государств тенденции оправдывать ограничения, особенно

[29] Подробное разъяснение относительно трехчастной формулы, представленной в статье 19, можно найти в замечании общего порядка № 34 (2011) Комитета по правам человека о свободе мнений и их выражения, пункты 5–9 и 22–36; и A/HRC/38/35.

[30] Замечание общего порядка № 34, пункт 25.

[31] Там же, пункты 34–35.

целенаправленное слежение, соображениями национальной безопасности Специальный докладчик пришел к выводу, что это обоснование должно использоваться лишь в случаях, когда на карту поставлены интересы всего государства, что тем самым исключает введение ограничений исключительно в интересах правительства, режима или какой-либо влиятельной группировки (A/71/373, пункт 18).

25. Комитет по правам человека воплотил эти принципы на практике в своих заключительных замечаниях 2017 года по шестому периодическому докладу Италии в соответствии с Международным пактом о гражданских и политических правах (CCPR/C/ITA/CO/6, пункт 36). Он определил, что осуществление права на неприкосновенность частной жизни требует создания надежных, независимых систем надзора за слежением, перехватом сообщений и взломом, в том числе путем обеспечения обязательного участия судебных органов в выдаче разрешения на принятие таких мер и предоставления пострадавшим эффективных средств правовой защиты в случаях злоупотребления, в том числе, если это возможно, направления им последующего уведомления о том, что за ними установлено слежение или что их данные были перехвачены (там же, пункт 37). Эти принципы также нашли свое отражение в резолюции Генеральной Ассамблеи 73/179, где отмечается, что слежение за цифровыми сообщениями должно осуществляться с соблюдением международных обязательств в области прав человека и соответствующих правовых рамок, которые должны быть доступными для общественности, ясными, точными, всеобъемлющими и недискриминационными.

26. Эти принципы применимы во всех случаях целенаправленного слежения, однако они имеют особую силу в случае выражения мнений в интересах общества. Целенаправленное слежение стимулирует самоцензуру и прямым образом подрывает способность журналистов и правозащитников проводить расследования, а также выстраивать и поддерживать отношения с источниками информации (A/HRC/38/35/Add.2, пункт 53). Комитет подчеркнул, что ограничения ни при каких условиях не могут служить оправданием для того, чтобы заставить замолчать каких-либо защитников многопартийной демократии, демократических принципов и прав человека[32]. Посягательства на права человека в связи с осуществлением его права на свободу выражения мнений не могут быть оправданы положениями пункта 3 статьи 19[33]. Далее Комитет обратил отдельное внимание на важность защиты журналистов и лиц, которые занимаются сбором и анализом информации о ситуации в области прав человека и публикуют доклады по правам человека, в том числе судьи и адвокаты[34]. Эти меры защиты распространяются на конфиденциальность источников, которые, как подчеркивается в международных и региональных правозащитных механизмах (в африканской, европейской и межамериканской системах), должны быть защищены законом (A/70/361, пункт 5).

27. В дополнение к первоочередным обязательствам не вмешиваться в частную жизнь и не ограничивать свободу выражения мнений государства также обязаны защищать отдельных лиц от вмешательства третьих сторон. В соответствии со статьей 2 Международного пакта о гражданских и политических правах, где отражены основные обязанности государств-участников, каждое государство-участник обязано уважать и обеспечивать всем находящимся в пределах его территории и под его юрисдикцией лицам права, признаваемые в настоящем Пакте[35]. Пункт 2 статьи 17 Пакта гласит, что каждый человек имеет право на защиту закона от незаконного вмешательства в его частную жизнь. Однако неясно, обеспечивают ли государства в

[32] Замечание общего порядка № 34, пункт 23.

[33] Там же.

[34] Там же.

[35] См. также замечание общего порядка № 31 (2004) Комитета по правам человека о характере общего юридического обязательства, налагаемого на государства – участники Пакта. Следует отметить, что в замечании общего порядка № 31 статья 17 о неприкосновенности частной жизни отдельно упомянута в качестве примера статьи, в которой на государства-участники возлагаются позитивные обязательства принимать меры в отношении деятельности частных лиц или организаций.

целом позитивную правовую защиту от целенаправленного слежения. Такая защита однозначно предусмотрена в случае транснационального слежения, даже когда оно осуществляется иностранными субъектами в отношении своих собственных граждан[36]. Так, например, в случае с утверждениями о целенаправленном слежении в Мексике Специальный докладчик по вопросу о свободе выражения мнений Межамериканской комиссии по правам человека и Специальный докладчик по вопросу о поощрении и защите права на свободу мнений и их свободное выражение предприняли совместную миссию в эту страну, где они подняли вопрос об использовании правительством шпионского программного обеспечения «Pegasus». Они настоятельно призвали правительство разрешить провести независимое расследование в отношении утверждений о том, что шпионское программное обеспечение использовалось против журналистов (A/HRC/38/35/Add.2, пункты 52–55). На сегодняшний день усилия по расследованию этих утверждений не позволили прояснить ситуацию, несмотря на постановления Национального института по вопросам транспарентности, доступа к информации и защиты личных данных Мексики о том, чтобы правительство раскрыло природу своих контрактов на приобретение программного обеспечения «Pegasus»[37].

28. В Руководящих принципах предпринимательской деятельности в аспекте прав человека: осуществление рамок Организации Объединенных Наций, касающихся «защиты, соблюдения и средств правовой защиты», принятых Советом по правам человека в 2011 году, недвусмысленно указано, что обязанность государства по защите включает обязанность по принятию надлежащих мер для предупреждения и расследования нарушений прав человека, совершаемых третьими лицами, наказания за них и возмещения ущерба (A/HRC/17/31). Руководящие принципы призывают государства-участники осуществлять надлежащий контроль в целях выполнения своих международных обязательств в области прав человека при заключении контрактов с предприятиями или принятии законодательных актов в их интересах для предоставления услуг, которые могут оказать воздействие на осуществление прав человека (там же, стр. 10 текста оригинала).

B. Корпоративная ответственность

29. Поскольку компании, работающие в частной индустрии слежения, действуют под покровом секретности, общественность не располагает никакой информацией о том, какое внимание они уделяют – если вообще уделяют – вопросам воздействия своей продукции на права человека. Сложно поверить в то, что они действительно принимают во внимание такое воздействие, учитывая природу этой индустрии и широкое использование ее продукции в целях, несовместимых с международным правом прав человека. Другими словами, ввиду широкой общественной осведомленности о политике репрессий, которую практикуют многие из их клиентов, компании не могут всерьез утверждать, что не понимают, как их инструменты используются при проведении политики репрессий.

30. Руководящие принципы обеспечивают рамки для оценки того, учитывают ли компании, работающие в индустрии слежения, права тех, против кого используется их продукция и услуги. В частности, в Руководящих принципах уделяется особое внимание программным обязательствам по соблюдению прав человека; процедурам обеспечения должной заботы о правах человека в целях выявления, предотвращения, смягчения последствий и представления отчетности об оказываемом воздействии на права человека; консультациям с затрагиваемыми группами; непрерывному процессу оценки эффективности политики в области прав человека; и эффективным механизмам рассмотрения жалоб от затрагиваемых правообладателей (A/HRC/17/31, пункты 15–25).

[36] См. Nate Cardozo, “D.C. circuit court issues dangerous decision for cybersecurity: Ethiopia is free to spy on Americans in their own homes”, Electronic Frontier Foundation, 14 March 2017.

[37] См. Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, “Fiscalía general de la República tiene oportunidad histórica para acabar con la impunidad en caso Pegasus: Salas Suárez”, 27 March 2019; и Juan Arvizu, “Ordena Inai a PGR abrir contrato de compra de Pegasus”, *El Universal*, 17 April 2018.

31. По всем меркам компании, похоже, не соответствуют даже этим минимальным базовым критериям. У тех немногих компаний, которые опубликовали документы о своей клиентской политике, необходимость соблюдения прав человека была обозначена весьма расплывчато. Например, компания «Хэкинг тим» утверждает, «что перед продажей она изучает потенциальных клиентов на предмет объективных доказательств или обоснованных опасений, что применение технологии "Хэкинг тим" будет способствовать нарушениям прав человека», но при этом компания не объясняет, как используется полученная информация, и даже не указывает, о нарушении каких прав человека может идти речь в контексте их технологий[38]. Компания «НСО груп» утверждает, что работает в соответствии с требованиями Комитета по деловой этике, «в который входят внешние эксперты по различным дисциплинам, включая право и международные отношения», и отмечает, что может расторгнуть договор, если ее продукция используется «ненадлежащим образом»[39]. На своем веб-сайте компания также заявляет, что будет «расследовать любые заслуживающие доверия утверждения об использовании ее продукции ненадлежащим образом», однако там не указано, относятся ли сюда нарушения прав человека[40].

32. Другими словами, компании не раскрывали случаев принятия значимых мер, таких как применение процедур должной осмотрительности, позволяющих выявлять неблагоприятное воздействие на права человека, избегать его оказания или содействия его оказанию в рамках своей деятельности, а также предотвращать или смягчать неблагоприятное воздействие на права человека, которое непосредственно связано с их деятельностью, продукцией или услугами, вследствие их деловых отношений (A/HRC/17/31, приложение, принцип 13). Например, отсутствует какая-либо общедоступная информация, свидетельствующая о том, что оценка соблюдения прав человека является стандартной составляющей должной осмотрительности при продажах и что компании придают решающее значение этим оценкам, и что такие оценки продолжаются на протяжении всего жизненного цикла продукта и любого контракта на послепродажное обслуживание. Действительно, ввиду постоянно увеличивающегося количества доказательств того, что индустрия слежения играет центральную роль в содействии грубым нарушениям прав человека, а также на фоне ее упорного отказа объяснить характер своих гарантий напрашивается вывод о том, что такое саморегулирование на деле отсутствует.

33. В рекомендациях Европейской комиссии по осуществлению Руководящих принципов в секторе информационно-коммуникационных технологий подчеркивается важность «учета прав человека при проектировании»[41]. Ввиду чрезвычайно высокого риска использования продуктов слежения ненадлежащим образом компаниям следует предвидеть неправомерное использование их программного обеспечения и приступить к разработке технических решений в контексте неизбежного негативного воздействия. В качестве многообещающего шага правительство Соединенного Королевства в партнерстве с одной из ассоциаций технологической индустрии подготовило ряд руководящих принципов для индустрии кибербезопасности, в которых подчеркивается важность предотвращения и уменьшения рисков для прав человека «посредством принятия соответствующих проектировочных решений» на самых ранних этапах разработки продукта.

[38] Hacking Team, Customer Policy.

[39] См. заявление «НСО» от 17 сентября 2018 года. Доступно по адресу https://citizenlab.ca/wp-content/uploads/2018/09/NSO-Statement-17-September-2018.pdf. Как утверждает «Ситизен лэб», заявления «НСО» о Комитете по деловой этике напоминают пример внешней группы технических экспертов и юрисконсультов «Хэкинг тим» ... которая рассматривает потенциальные продажи. Эта «внешняя группа», похоже, представляла собой единственную юридическую контору, рекомендации которой «Хэкинг тим» не всегда выполняла (Marczak and others, «Hide and seek»).

[40] См. www.nsogroup.com/about.

[41] См. European Commission, *ICT Sector Guide on Implementing the UN Guiding Principles on Business and Human Rights* (Luxembourg, 2013).

C. Международный и национальный экспортный контроль

34. Экспортный контроль является важным элементом усилий по снижению рисков, связанных с частной индустрией слежения и использованием ее инструментов при проведении политики репрессий. Однако его эффективность ограничена. Во-первых, соответствующий международный режим экспортного контроля – Вассенаарские договоренности о контроле за экспортом обычных вооружений и товаров и технологий двойного назначения, не имеющие обязательной силы, в которых участвуют 42 государства, – призван снизить угрозы региональной и международной безопасности. Это нужная и достойная высокой оценки цель, однако данный механизм плохо подходит для борьбы с угрозами правам человека, которые возникают из-за целенаправленного слежения; действительно, в нем не предусмотрены руководящие принципы или правоприменительные меры, которые касались бы непосредственно нарушений прав человека, возникающих в результате применения средств слежения. Во-вторых, за счет акцента на экспорт невозможно в полной мере решить основную проблему: такие технологии используются против законного выражения мнений, инакомыслия, освещения нарушений и других форм осуществления прав человека.

35. Тем не менее Вассенаарские договоренности способствуют достижению важных целей обеспечения «транспарентности и большей ответственности при передаче обычных вооружений и товаров и технологий двойного назначения». Ожидается, что государства-участники будут применять меры экспортного контроля ко всем товарам и технологиям, включенным в перечень товаров и технологий двойного назначения[42]. В этой связи Вассенаарские договоренности были (или должны быть) интегрированы в национальное законодательство и политику государств-участников и неучаствующих государств; к сожалению, не существует какого-либо механизма обеспечения соблюдения этих Договоренностей, который гарантировал бы их включение в национальное законодательство или их осуществление соответствующими национальными учреждениями.

36. В 2013 году государства-участники добавили в перечень технологий двойного назначения товары и технологии, связанные с «программным обеспечением для получения несанкционированного доступа» и системами слежения за сетевыми сообщениями с помощью интернет-протоколов. Согласно данному перечню, программное обеспечение для получения несанкционированного доступа – это «"программное обеспечение", специально разработанное или измененное таким образом, чтобы избежать обнаружения с помощью "средств мониторинга" или чтобы преодолевать "защитные контрмеры"» и которое либо извлекает данные из компьютера или сетевого устройства, либо изменяет «стандартный ход работы» программы таким образом, чтобы обеспечить возможность «выполнения команд, полученных извне»[43].

37. Подробные сообщения о злоупотреблениях, связанных со слежением, свидетельствуют о том, что режим экспортного контроля, основывающийся на Вассенаарских договоренностях, по сути не ограничивает распространение технологий слежения и их использование при проведении политики репрессий. Трудности, связанные с проведением реформы, проявились, когда попытка европейских парламентариев упрочить защиту прав человека в рамках европейского экспортного законодательства и политики, не увенчалась успехом. В рамках своих усилий они недвусмысленно призывали расширить перечень товаров двойного назначения и ввести режим всеобъемлющего контроля, а также ввести требование учитывать «ситуацию с соблюдением прав человека в стране конечного назначения» технологий слежения[44]. В январе 2018 года в Европейском парламенте состоялось

[42] См. Wassenaar Arrangement, “List of dual-use goods and technologies and munitions list”.

[43] Ibid., p. 221 .

[44] См. See European Commission, “Proposal for a regulation of the European Parliament and of the Council setting up a Union regime for the control of exports, transfer, brokering, technical assistance and transit of dual-use items (recast)”, 28 September 2016; и Lucie Krahulcova, “The European Parliament is fighting to strengthen the rules for surveillance trade”, Access Now, 8 December 2017.

первое чтение данного законопроекта, который первоначально снискал поддержку как инициатива по усилению контроля за экспортом технологий двойного назначения[45]. Однако с того момента по меньшей мере девять государств-членов озвучили критику в отношении данного предложения, выступив за ослабление гарантий прав человека[46]. Сегодня невозможно предсказать дальнейшую судьбу этого законопроекта[47].

38. Даже государства – участники Вассенаарских договоренностей подходят к соблюдению мер экспортного контроля на национальном уровне по-разному. Например, Соединенные Штаты пока не приняли добавления 2013 года, которые касаются программного обеспечения для получения несанкционированного доступа и сетевых систем слежения за коммуникациями с помощью интернет-протоколов[48]. Вместе с тем Министерство торговли Соединенных Штатов проводит широкий обзор существующих рамок, и в соответствии с Законом о реформе системы экспортного контроля 2018 года министерству было поручено запустить межучережденческий процесс создания новых механизмов контроля как за «новыми», так и за «основными» технологиями[49]. В свою очередь Израиль, который не является государством – участником Вассенаарских договоренностей, принял меры экспортного контроля за товарами двойного назначения, предусмотренные Вассенаарскими договоренностями, однако вопросы применения этих мер держатся в тайне[50].

D. Отсутствие средств правовой защиты в случае целенаправленного слежения

39. В рамках обязанности государств уважать и обеспечивать осуществление прав человека пункт 3 a) статьи 2 Международного пакта о гражданских и политических правах накладывает обязательство предоставлять жертвам нарушений доступ к эффективным средствам правовой защиты. В пункте 3 b) статьи 2 указано, что жалобы на такие нарушения должны рассматриваться компетентными судебными, административными или законодательными органами или любым другим компетентным органом, который предусмотрен правовой системой государства. Комитет по правам человека подчеркнул, что органы правоохранения и прокуратуры должны незамедлительно, тщательно и эффективно проводить расследования по заявлениям о нарушениях с помощью независимых и беспристрастных органов[51]. Обязанность по предоставлению эффективных средств правовой защиты также влечет за собой обязательство защищать физических лиц от действий организаций частного сектора, которые приводят к нарушениям, посредством принятия мер должной осмотрительности в целях предотвращения и расследования случаев нарушений, наказания за нарушения или возмещения ущерба, причиненного соответствующими действиями частных лиц или организаций[52].

40. Жертвы целенаправленного слежения не добились больших успехов в своих попытках добиться признания причиненного им ущерба, не говоря уже о возмещении такого ущерба. И это при том, что как Европейский суд по правам человека, так и Верховный комиссар по правам человека пояснили, что сама угроза слежения, даже

[45] Для экскурса в историю законопроекта о вышеупомянутом предложенном регламенте см. EUR-Lex, Doc. 52016PC0616.

[46] Delegations of Cyprus, Czechia, Estonia, Finland, Ireland, Italy, Poland, Sweden and the United Kingdom, “For adoption of an improved EU Export Control Regulation 428/2009 and for cyber-surveillance controls promoting human rights and international humanitarian law globally”, WK 5755/2018 INIT (15 May 2018); и Access Now, “EU: States push to relax rules on exporting surveillance technology to human rights abusers”, 11 June 2018.

[47] См. Catherine Stupp, “Nine countries united against EU export controls on surveillance software”, Euractiv, 11 June 2018; и Moßbrucker, “Surveillance exports”.

[48] Представление «Прайвеси интернэшнл», стр. 5 текста оригинала.

[49] John S. McCain National Defense Authorization Act for Fiscal Year 2019, Public Law No 115–232 (2018).

[50] См. “Israel-U.S. export controls”, export.gov, 20 July 2018. См. также пункт 43 ниже.

[51] Замечание общего порядка № 31, пункт 15.

[52] Там же, пункт 8.

если она скрытая, в совокупности с отсутствием средств правовой защиты может представлять собой посягательство на право на неприкосновенность частной жизни[53].

41. Обращение в суд является ненадежным средством правовой защиты от частных компаний, которые производят и продают средства слежения, и правительств, которые их используют. Отсутствие оснований для подачи исков и отсутствие средств правовой защиты вызывают серьезную обеспокоенность относительно вероятности того, что компании не понесут ответственность за нарушения прав человека. По меньшей мере в восьми странах предполагаемые жертвы обратились в суд или направили официальные жалобы на компании, работающие в частной индустрии слежения, или правительства[54]. Однако на пути успешного судебного разбирательства и подачи официальных жалоб имеются серьезные препятствия, в том числе отсутствие судебного надзора, средств правовой защиты, оснований для подачи исков, правоприменения и механизмов обеспечения сохранности данных.

42. В некоторых ситуациях организации гражданского общества обращаются к правительствам с просьбой расследовать случаи незаконного слежения, однако эти просьбы часто отклоняются. В Соединенном Королевстве организация «Прайвеси интернэшнл» подала в Национальное агентство по борьбе с преступностью уголовный иск против компании «Гамма груп», утверждая, что она нарушила многочисленные национальные законы, когда ее дочерняя компания «ФинФишер» продавала технологии слежения и оказывала помощь правительству Бахрейна[55]. Европейский центр по конституционным правам и правам человека и «Прайвеси интернэшнл» также подали уголовный иск в Мюнхене (Германия) с требованием провести расследование в отношении указанной компании, однако органы прокуратуры отклонили этот запрос[56]. Даже когда государства начинают расследования для определения того, нарушает ли санкционированное правительством слежение нормы в области прав человека или государственные законы, такие расследования могут быть произвольными или дезорганизованными.

43. Альтернативы судебному разбирательству, обеспечивающие средства правовой защиты в соответствии с международным правом прав человека, представляются отсутствующими. Так, например, после того, как сотрудник «Международной амнистии» получил подозрительное сообщение в «WhatsApp», которое предположительно связанно с «Pegasus», организация обратилась в Министерство обороны Израиля с просьбой аннулировать экспортную лицензию, выданную «НСО груп»[57]. В ответ израильское Агентство по контролю за экспортом военной продукции направило письмо, в котором было указано, что агентство не предоставляет сведений о своей политике в отношении выдачи экспортных лицензий или какой-либо иной информации о самих лицензиях[58]. Агентство не подтвердило и не опровергло существование указанной экспортной лицензии, но отметило, «что лицензии на экспорт правительственным клиентам, которые Израиль [Министерство обороны] выдал "НСО груп", соответствуют международным обязательствам»[59]. Отсутствие регионального и международного давления и политика неразглашения информации, оправданная соображениями национальной безопасности, оказываются серьезными препятствиями.

[53] См. Европейский суд по правам человека, *Роман Захаров против России*, жалоба № 47143/06, постановление от 4 декабря 2015 года, пункт 171; и A/HRC/27/37, пункт 20.

[54] См. Siena Anstis, “Litigation and other formal complaints concerning targeted digital surveillance and the digital surveillance industry”, Citizen Lab, 12 December 2018.

[55] См. Privacy International, “Criminal complaint to national cyber crime unit on behalf of Bahraini activists”, 13 October 2014. Судебные иски против «НСО груп» были также поданы в Израиле и на Кипре: см. David D. Kirkpatrick and Azam Ahmed, “Hacking a prince, an emir and a journalist to impress a client”, *New York Times*, 31 August 2018.

[56] См. European Centre for Constitutional and Human Rights, “FinFisher: no investigation into German-British software company”, 12 December 2014.

[57] Представление «Международной амнистии» в рамках УПО, стр. 8 текста оригинала.

[58] Ibid.

[59] Ibid.

44. Организация «Прайвеси интернэшнл» также подала жалобы Национальным координаторам Германии и Соединенного королевства Организации экономического сотрудничества и развития (ОЭСР) на компании «Гамма» и «Тровикор» из-за их предполагаемого участия в целенаправленном слежении за политическими оппонентами правительством Бахрейна[60]. В жалобе на «Тровикор» Национальному координатору Германии было предложено «установить, нарушила ли эта компания Руководящие принципы ОЭСР для многонациональных предприятий вследствие того, что она экспортировала продукцию для слежения в Бахрейн, где власти используют такую продукцию для нарушения прав человека, в том числе для проведения арестов, задержаний и пыток политических оппонентов и диссидентов»[61]. Однако Национальный координатор отклонил эту жалобу по причине отсутствия достаточных доказательств присутствия «Тровикора» в Бахрейне. В практически идентичной жалобе, направленной Национальному координатору Соединенного Королевства, многочисленные организации гражданского общества утверждали, что подобные нарушения были совершены компанией «Гамма»[62]. Национальный координатор принял жалобу к рассмотрению и опубликовал свою предварительную позицию в июне 2013 года, указав, что «несмотря на то, что ни одна из сторон не представила прямых доказательств того, что "Гамма" осуществляла поставки в Бахрейн, представленные доказательства позволяют предположить, что продукция компании могла быть использована против бахрейнских активистов. [Национальный координатор] считает, что это оправдывает вопросы, связанные с обязательствами компании проявлять надлежащую должную осмотрительность и устранять последствия»[63].

45. Несмотря на то, что в заключительном докладе Национального координатора содержится ряд рекомендаций, основанных на стандартах в области прав человека, нет никаких свидетельств того, что «Гамма» их выполнила или вообще ознакомилась с этим докладом[64].

IV. Рамки для защиты основных прав человека в случае целенаправленного слежения

46. Недостаточно сказать, что комплексная система контроля и использования технологий целенаправленного слежения не работает. На деле ее практически не существует. В то время как право прав человека предусматривает конкретные ограничения на использование средств слежения, государства практикуют незаконное слежение, не опасаясь каких-либо правовых последствий. Законодательство в области прав человека существует, однако отсутствует какой-либо механизм обеспечения соблюдения ограничений. В этой связи необходимо, чтобы государства в срочном порядке ограничили использование таких технологий только видами законного использования, которые должны сопровождаться самыми строгими формами надзора и разрешения, и чтобы они обусловили участие частного сектора на рынке средств слежения – от исследований и разработок до маркетинга, продажи, передачи и

[60] Согласно веб-сайту организации, основная роль Национального координатора «заключается в повышении эффективности Руководящих принципов путем проведения пропагандистских мероприятий, обработки запросов и содействия решению вопросов, которые могут возникнуть в связи с предполагаемым несоблюдением руководящих принципов в отдельных случаях».

[61] См. Privacy International, “OECD complaint: Trovicor exporting surveillance technology to Bahrain”, 1 February 2013.

[62] См. Privacy International, “German OECD NCP unwilling to investigate role of German company in human rights violations in Bahrain”, 20 December 2013.

[63] United Kingdom, Department for Business Innovation and Skills, “Initial assessment by the UK National Contact Point for the OECD Guidelines for Multinational Enterprises: complaint from Privacy International and others against Gamma International UK Limited, June 2013” (London, 2013), пункт 25.

[64] См. Amitpal Singh, “OECD finds actions of Gamma International to be in violation of human rights”, Citizen Lab, 3 March 2015; и “UK National Contact Point for the OECD Guidelines for Multinational Enterprises – Privacy International and Gamma International UK Ltd: final statement after examination of complaint”, December 2014.

обслуживания – проявлением должной осмотрительности в вопросах прав человека и соблюдением норм в области прав человека.

47. Предыдущий мандатарий настаивал на том, что государствам следует принимать меры по предотвращению коммерциализации технологий слежения, уделяя особое внимание технологическим исследованиям, развитию, торговле, экспорту и использованию этих технологий с учетом возможности их содействия систематическим нарушениям прав человека (A/HRC/23/40, пункт 97). Этот призыв остается настолько же актуальным и сегодня. В настоящем разделе Специальный докладчик рассматривает основные элементы системы защиты отдельных лиц от использования технологий слежения, которые препятствуют осуществлению прав человека. Шаги, предлагаемые в настоящем докладе, требуют действий и практических мер со стороны: государств как пользователей этих технологий и как стран-экспортеров; компаний в соответствии с Руководящими принципами предпринимательской деятельности в аспекте прав человека; государств и компаний, сотрудничающих с гражданским обществом; и Совета по правам человека.

A. Мораторий на экспорт и использование технологий целенаправленного слежения

48. Форматы, в которых частные компании создают, передают и обслуживают – а государства приобретают и используют – технологии слежения, вызывают обеспокоенность. Согласно заслуживающим доверия утверждениям, компании продают свои инструменты правительствам, которые используют их против журналистов, активистов, оппозиционеров и других лиц, которые играют важнейшую роль в демократическом обществе. Некоторые из этих компаний не согласны с такими заявлениями и утверждают, что они не разрешают использовать свою продукцию в противоправных целях, имеют механизмы оценивания продаж «чувствительным» конечным пользователям и соблюдают национальное законодательство стран в сфере экспортного контроля. Не исключено, что компании предпринимают искренние попытки ответить на обвинения в пособничестве репрессиям и злоупотреблениям в результате слежения. Однако нет никаких конкретных причин верить частным компаниям на слово, не подвергая их процедурам публичного раскрытия информации и подотчетности. Серьезность утверждений требует транспарентности в отношениях и процессах компаний, не говоря уже о ряде других шагов, которые описаны ниже.

49. Для принятия шагов, изложенных в настоящем докладе, потребуется время. Тем временем десятки журналистов, активистов, правозащитников и критиков правительств будут уповать на милость правительств, которые чувствуют себя хозяевами положения, имея в своем распоряжении целый арсенал высокоинтрузивных средств слежения. Поэтому крайне важно, чтобы компании немедленно прекратили продажу, передачу и поддержку таких технологий до тех пор, пока они не предоставят убедительных доказательств принятия достаточных мер (как указано ниже) в вопросах должной осмотрительности, транспарентности и подотчетности, с тем чтобы предотвратить или смягчить последствия использования этих технологий для совершения нарушений прав человека. Правительствам следует также незамедлительно ввести мораторий на выдачу лицензий на экспорт технологий слежения до тех пор, пока не будут представлены убедительные доказательства того, что использование этих технологий может быть технически ограничено законными целями, которые соответствуют стандартам в области прав человека, или что эти технологии будут экспортироваться только в страны, где для их использования необходимо получить разрешение независимого и беспристрастного судебного органа, которое выдается в соответствии с надлежащей правовой процедурой и стандартами законности, необходимости и обоснованности. Однако на сегодняшний день появляется все больше доказательств того, что средства слежения, разработанные частными компаниями, используются в явно незаконных целях, что является веским основанием для введения моратория на такую передачу.

B. Обязательства правительств как пользователей технологий слежения

1. Ужесточить национальные законы, ограничивающие применение мер слежения в соответствии с обязательствами по международному праву прав человека

50. В качестве первого шага правительства, применяющие средства слежения, должны обеспечить, чтобы их практика соответствовала национальным правовым рамкам, которые отвечают стандартам, предусмотренным международным правом прав человека. Меры слежения следует легально санкционировать исключительно в случаях наиболее тяжких уголовных преступлений. Для соответствия этим стандартам национальные законы должны:

a) подчеркивать, что каждый человек имеет право не подвергаться незаконному или произвольному вмешательству в его личную жизнь и беспрепятственно придерживаться своих мнений, а также искать, получать и распространять информацию и идеи, независимо от государственных границ и способов;

b) требовать, чтобы любое законодательство, регулирующее слежение, содержалось в четких и общедоступных законах и применялось только при условии необходимости и соразмерности для достижения одной из законных целей, перечисленных в пункте 3 статьи 19 Международного пакта о гражданских и политических правах;

c) обеспечивать, чтобы меры слежения были одобрены для использования против конкретного лица только в соответствии с международным правом прав человека и только с разрешения компетентного, независимого и беспристрастного судебного органа со всеми соответствующими ограничениями по времени, способу, месту и масштабу слежения;

d) требовать, с учетом чрезвычайно высокого риска злоупотреблений, связанных с технологиями целенаправленного слежения, чтобы в отношении санкционированных видов использования применялись подробные требования к ведению отчетности. Удовлетворять запросы о слежении необходимо только в соответствии со стандартными, документально закрепленными правовыми процедурами и посредством выдачи ордеров на применение таких мер. Объектов слежения следует уведомлять о решении санкционировать слежение за ними, как только это не будет представлять серьезной угрозы для цели слежения[65].

51. Государства нередко устанавливают очень высокие требования в отношении бремени доказывания для уголовных расследований, в рамках которых предпринимаются попытки получить доступ к работе журналистов (A/70/361, пункт 24). Технологии слежения часто используются в отношении тех, кто играет важную роль в продвижении демократических ценностей. Специальный докладчик признает, что некоторые государства могут полагать, что существуют ситуации, в которых, например, журналисты прикрываются своей профессией для совершения серьезных уголовных преступлений. По его опыту, подобные утверждения почти всегда являются ложными или преувеличенными. Правительства слишком часто используют такого рода утверждения, чтобы препятствовать журналистике и инакомыслию или чтобы инициировать слежение за журналистами, даже если они не являются подозреваемыми в рамках законного уголовного расследования, что оказывает несоразмерное воздействие на свободную прессу. В этом контексте закон должен по умолчанию запретить использование средств цифрового слежения против отдельных лиц, представляющих средства массовой информации. Разумеется, это не подразумевает наделения журналистов иммунитетом от других форм законного судебного процесса, включая нецифровое слежение. Просто в контексте интрузивных технологий цифрового слежения возможность злоупотреблений или «утечки» материалов законного уголовного расследования в области, связанные с другой

[65] См. “Necessary and proportionate: International Principles on the Application of Human Rights to Communications Surveillance” (May 2014).

журналистской деятельностью, является весьма реальной, и их весьма непросто, если вообще возможно, предотвратить. Весьма вероятно, что сама эта возможность будет отпугивать журналистов от работы над наиболее чувствительными темами, не говоря уже о готовности источников и осведомителей разглашать информацию.

2. Создать общественные механизмы для одобрения использования технологий слежения и надзора за их использованием

52. Судебное разрешение на использование правительством технологий наблюдения является необходимым, но недостаточным. Закупка таких технологий также должна сопровождаться реальным общественным надзором, консультациями и контролем. В Соединенных Штатах в связи с широким использованием технологий слежения правоохранительными органами в последние годы в ряде общин были созданы гражданские советы по надзору для регулирования использования и закупок таких технологий. Например, город Окленд в штате Калифорния принял постановление, в котором содержится ряд требований к процессу закупки технологий слежения, которые государства могли бы использовать[66]. В частности, речь идет о таких требованиях, как:

a) процесс одобрения, осуществляемый соответствующими ведомствами с учетом обязательств государства-участника в области прав человека;

b) информирование общественности о таких закупках посредством регулярных процедур и консультаций по таким вопросам, как последствия таких закупок для прав человека и эффективность данных технологий для достижения поставленных целей;

c) периодическое информирование общественности о выдаче таких разрешений, закупках и случаях использования технологий слежения.

53. Следует поощрять и усиливать общественный контроль за такими закупками, особенно в государствах, которые предоставляют субнациональным органам определенную автономию в вопросах закупки средств поддержания правопорядка. Учитывая явную заинтересованность общественности в сохранении неприкосновенности частной жизнь и безопасности широко доступного коммерческого программного обеспечения, механизмы общественного надзора также должны быть наделены полномочиями определять политику в отношении хранения уязвимостей и их соответствующей разработки для целей использования.

3. Предоставить жертвам национальные правовые средства возмещения ущерба

54. Ввиду описанных выше причин лицам, являющимся объектами незаконного или произвольного слежения, трудно предъявлять иски в отношении правительств. Некоторые из этих препятствий носят структурный характер: например, во многих правовых системах не предусмотрена возможность предъявлять иски к государственным субъектам. Кроме того, как законодательные органы, так и суды могут также запрещать такие иски, если они рассматривают интересы национальной безопасности и правоохранительной деятельности как требующие чрезмерно высокого статуса. Иногда трудности подачи иска обусловлены сложностью и издержками процесса сбора доказательств факта слежения или того, что слежение ведет государственный субъект или даже конкретные государственные учреждения, в отношении которых можно было бы инициировать судопроизводство. Объекты целенаправленного слежения часто не знают о том, что за ними установлено слежение, а если они об этом узнают, то это может быть уже после истечения срока давности[67]. Другими словами, истец крайне редко добивается удовлетворения внутренних судебных исков, связанных с якобы незаконным слежением.

[66] См. American Civil Liberties Union of Northern California, “Oakland becomes latest municipality to reclaim local control over surveillance technologies used by local law enforcement”, 2 May 2018.

[67] См. *Роман Захаров против России*.

55. Государствам, которые действительно обеспокоены злоупотреблением технологиями слежения, следует предпринять шаги, позволяющие предъявлять индивидуальные иски как к государственным, так и к негосударственным субъектам. Для многих государств это обязательно предполагает обеспечение того, чтобы правила, касающиеся юрисдикции, доказательств, соблюдения сроков и других основных пороговых условий, служили достижению соответствующих целей в условиях цифровой эпохи. Им следует, например, обеспечить, чтобы суды могли принимать и рассматривать в качестве доказательств результаты криминалистической экспертизы технических экспертов. В национальном законодательстве следует также определить основания для возбуждения исков против частных субъектов с учетом изменений в структуре корпоративной собственности (известных как процессы «отчуждения» или «передела»), которые зачастую затрудняют попытки потерпевших привлечь виновных к ответственности и добиться возмещения ущерба[68]. Следует также рассмотреть альтернативные формы возмещения ущерба, такие как комиссии по установлению истины, которые позволяют жертвам грубых нарушений прав человека, совершению которых способствует цифровое слежение, представлять показания и которые изучают вопросы причастности корпораций к этим нарушениям.

56. В то же время целенаправленное слежение не всегда ограничено определенной территорией. Когда государства выходят за пределы своих границ при осуществлении целенаправленного слежения, лицам, ставшим объектами такого слежения, может быть трудно предъявлять претензии к государству-правонарушителю. В этих случаях, как и в случае с национальными исками, могут также применяться те же требования, касающиеся бремени доказывания и иных обременений. Кроме того, как отмечалось выше в деле *Доу*, суды могут проявлять нежелание рассматривать иски против иностранных суверенных государств. Хотя правила подачи таких исков различаются, государствам следует толковать нормы суверенного иммунитета таким образом, чтобы их суды могли принимать иски против иностранных правительств.

C. Обязательства правительств, выдающих лицензии на экспорт технологий слежения

57. Решающее слово в сфере контроля за экспортом технологий слежения остается не за Вассенаарскими договоренностями; эффективность контрольных перечней зависит от соответствующих мер на национальном уровне. Кроме того, не все основные страны-экспортеры являются участниками Вассенаарских договоренностей: Израиль, один из основных игроков на рынке технологий слежения, утверждает, что его деятельность «полностью соответствует» требованиям Договоренностей, но, тем не менее, по-прежнему не является государством-участником[69]. Кроме того, охват данного механизма ограничен: несмотря на его важные цели, связанные с обеспечением регионального и международного мира и безопасности, в нем не учитывается проблематика прав человека. Тем не менее, принимая во внимание то, что Договоренности устанавливают стандарты, которые предполагают широкое применение и соблюдение, государствам-участникам следует использовать этот важный форум для введения правозащитных ограничений на передачу технологий слежения.

58. В целях повышения роли Вассенаарских договоренностей в разработке глобальных экспортных стандартов государства-участники могли бы учредить рабочую группу по правам человека, которая могла бы предлагать и рассматривать стандарты экспорта, учитывающие правозащитные аспекты при передаче технологий. Однако независимо от того, будет ли использован формат такой рабочей группы или какой-либо иной механизм, в рамках Вассенаарских договоренностей необходимо предусмотреть положения, в соответствии с которыми лицензирование любой технологии будет зависеть от проведения национального обзора соблюдения прав человека и соблюдения компаниями Руководящих принципов предпринимательской

[68] Представление организации «Эксесс нау», часть I, стр. 8 текста оригинала.

[69] См. Wassenaar Arrangement, “IL – Israel cybersecurity export control policy” (PowerPoint presentation), June 2016.

деятельности в аспекте прав человека, как об этом говорится ниже. Как заявила организация «Прайвеси интернэшнл», государства-участники, а также другие правительства стран-экспортеров должны отказывать в выдаче лицензии «в тех случаях, когда существует значительный риск того, что такой экспорт может быть использован для нарушения прав человека, или когда отсутствует правовой механизм, регулирующий использование технологии слежения, или когда правовые рамки ее использования не соответствуют международному праву или стандартам в области прав человека»[70]. Для обеспечения соблюдения этих требований в тех случаях, когда на этом основании отказывают в выдаче экспортных лицензий, соответствующие технологии должны быть включены в существующие режимы санкций[71].

59. Такие стандарты станут ценным дополнением к Вассенаарским договоренностям, однако способность общественности или конкретных организаций гражданского общества контролировать их осуществление будет зависеть от соблюдения более строгих обязательств по обеспечению транспарентности на национальном и международном уровнях. Договоренности как таковые должны способствовать такой транспарентности путем разработки четких и осуществимых руководящих принципов межправительственного обмена информацией и публичного раскрытия информации, касающихся стандартов лицензирования, решений о выдаче, изменении или отклонении лицензий, случаев или схем неправомерного использования технологий слежения и соответствующих нарушений прав человека, а также режима обращения с цифровыми уязвимостями. Национальное законодательство об экспорте должно также предусматривать выделение достаточных ресурсов для ведения государственного учета и обеспечения доступности решений о выдаче экспортных лицензий, а также уполномочивать соответствующие правительственные учреждения запрашивать мнение общественности и проводить многосторонние консультации при рассмотрении заявок на получение экспортных лицензий. Наконец, государствам следует также создать «безопасные гавани» для проведения исследований в области безопасности и освободить товары и технологии, связанные с шифрованием, от ограничений в рамках экспортного контроля[72].

D. Применение компаниями Руководящих принципов предпринимательской деятельности в аспекте прав человека

60. Учитывая чрезвычайно высокий риск злоупотребления технологиями слежения, национальное законодательство должно запрещать выдачу экспортных лицензий, за исключением случаев, когда компания регулярно доказывает, что она неукоснительно выполняет свои обязательства в соответствии с Руководящими принципами при разработке, продаже, передаче или поддержке таких технологий. Это сделало бы соблюдение Руководящих принципов реальным предварительным условием для выхода компаний на рынок частных услуг слежения. В предыдущих докладах Специальный докладчик пояснил, каким образом сектор информационно-коммуникационных технологий должен выполнять свои обязательства по соблюдению прав человека (A/HRC/35/22, пункты 45–75). Для того чтобы частные компании слежения могли выполнять эти обязанности, они должны разработать как минимум следующее[73]:

а) клиентскую политику, недвусмысленно подтверждающую ответственность компаний за уважение свободы выражения мнений, неприкосновенности частной жизни и соответствующих прав человека в ходе всей своей деятельности, а также то, что соблюдение клиентами международного права прав человека является условием для одобрения и совершения продажи, передачи или заключения договора об оказании поддержки;

[70] Представление «Прайвеси интернэшнл», стр. 8 текста оригинала.

[71] Там же, стр. 3–4 текста оригинала.

[72] Там же, стр. 5 текста оригинала.

[73] Многие из этих стандартов основаны на представлениях, внесенных организациями гражданского общества, с которыми можно ознакомиться в добавлении к настоящему докладу и на веб-сайте Специального докладчика.

b) процедуры должной осмотрительности в области прав человека (такие, как оценка воздействия на права человека), которые проводятся в случае, если компания осуществляет деятельность, затрагивающую свободу выражения мнений и неприкосновенность частной жизни, в рамках разработки, продажи, передачи и обслуживания продуктов и услуг слежения;

c) внутреннюю политику и стандартные договорные положения, устанавливающие четкие и конкретные запреты на адаптирование продукта к специфическим потребностям, выбор объектов слежения, обслуживание или помощь, которые противоречат международному праву прав человека;

d) внутренние процедуры, обеспечивающие учет гарантий прав человека при принятии решений на стадии проектирования и инженерно-технических работ, например с помощью систем выявления случаев ненадлежащего использования и предохранителей, которые срабатывают в случае такого использования;

e) регулярные программы аудиторских проверок и процедуры проверки соблюдения прав человека для обеспечения того, чтобы использование их продукции и услуг соответствовало международному праву прав человека, включая обязательство обнародовать основные выводы по итогам этих аудиторских проверок и процедур контроля;

f) процессы уведомления, которые позволяют оперативно сообщать о ненадлежащем использовании инструментов компании соответствующим государственным надзорным органам (например, национальным правозащитным учреждениям) или межправительственным органам (например, механизмам подачи и рассмотрения жалоб в рамках специальных процедур);

g) прозрачную отчетность, раскрывающую потенциальные возможности использования продукции компании и ее достоинства, а также виды предоставляемой послепродажной поддержки, случаи ненадлежащего использования и данные о количестве и видах продаж правоохранительным, разведывательным и другим государственным органам или их агентам;

h) регулярные консультации с затрагиваемыми правообладателями, группами гражданского общества и организациями по защите цифровых прав относительно текущего или потенциального воздействия продукции и услуг компании и гарантий прав человека, необходимых для предотвращения или смягчения такого воздействия, с особым акцентом на вовлечение лиц, подверженных риску дискриминации или репрессий в результате слежения, таких как расовые и этнические меньшинства и исторически маргинализованные группы;

i) механизмы рассмотрения жалоб, которые позволяют отдельным лицам подавать жалобы на нарушения прав человека в результате использования продукции и услуг компании и которые предусматривают независимую оценку таких жалоб и принятие действенных последующих мер;

j) механизмы правовой защиты, которые позволяют заявителям добиваться компенсации, извинений и других форм возмещения ущерба, в зависимости от обстоятельств, в тех случаях, когда жалобы проходят независимую проверку.

E. Инициативы по совместному регулированию

61. Описанные здесь подходы государств и компаний могут оказаться недостаточными для решения глобальной проблемы целенаправленного слежения. Им также недостает ряда важных элементов, касающихся представителей гражданского общества, будь то активисты, технические специалисты, ученые, пострадавшие или лица, принадлежащие к более чем одной из этих категорий. Совместное регулирование, предполагающее конструктивное участие представителей государства, бизнеса и гражданского общества, может стать основой для обеспечения подотчетности в области прав человека в частной индустрии слежения. В частности, весьма полезен опыт инициатив по совместному регулированию, которые были

разработаны для обеспечения подотчетности и надзора среди частных охранных компаний. Риски, которые берут на себя частные охранные компании, как и в случае частных компаний в сфере услуг слежения, связаны с неотъемлемым участием этих компаний в осуществлении государственных функций, особенно в области национальной безопасности. Поэтому совместное регулирование деятельности частных охранных компаний требует усилий по информированию сотрудников компаний по вопросам прав человека и создает стимулы для участия многих заинтересованных сторон (сертификация на основе процедур аудита и мониторинга с участием гражданского общества), что могло бы успешно применяться в частной индустрии слежения.

62. В контексте деятельности частных охранных компаний стоит обратить внимание на два аспекта нормативно-правовой базы, регулирующей деятельность частных охранных компаний. В Документе Монтре о соответствующих международно-правовых обязательствах и передовой практике для государств, связанных с деятельностью частных военных и охранных компаний в период вооруженных конфликтов, определены рекомендации в отношении надлежащей практики государств в таких ситуациях[74]. Хотя этот Документ не имеет обязательной силы, он содержит существующие международно-правовые обязательства для частных охранных компаний, а также рекомендации в форме передовой практики для договаривающихся государств, государств территориальной юрисдикции и государств происхождения. Изложенные в Документе Монтре принципы публичного раскрытия информации и проявления должной осмотрительности предшествуют закрепленным в Руководящих принципах обязанностям и отражают их.

63. Подходящей моделью может также служить Международный кодекс поведения частных поставщиков охранных услуг. Данный подход, созданный при поддержке гражданского общества, частного сектора и правительства Швейцарии, является одним из немногих подходов, предусматривающих участие частных охранных компаний. Международный кодекс поведения Ассоциации частных поставщиков охранных услуг представляет собой инициативу с участием многих заинтересованных сторон, в которой участвуют представители государств, частных охранных компаний и организаций гражданского общества. Не имеющий обязательной юридической силы Кодекс призван дополнить мониторинг и надзор, сформулировать международно-правовые обязательства компаний и создать структуру системы подотчетности перед Ассоциацией. Ассоциация состоит из общего собрания, в котором представлены группы заинтересованных сторон, и совета директоров, в состав которого входят 12 избранных членов, представляющих все 3 группы заинтересованных сторон. Примечательно, что членство в Ассоциации зависит от соблюдения Кодекса, включая процедуры сертификации, аудита и проверки.

64. Согласно уставу Ассоциации, основная идея Кодекса заключается в содействии ответственному использованию частных охранных услуг, а также соблюдению международных норм в области прав человека. В самом Кодексе изложены как общие обязательства государств и частных охранных компаний и других частных охранных компаний, так и конкретные принципы поведения в следующих областях: применение силы, содержание под стражей, задержание лиц, пытки и другие наказания, гендерное насилие, торговля людьми, рабство и принудительный труд, дискриминация, идентификация и регистрация сотрудников частных охранных компаний[75].

[74] См. Switzerland, Federal Department of Foreign Affairs, and the International Committee of the Red Cross, “The Montreux Document on pertinent international legal obligations and good practices for States related to operations of private military and security companies during armed conflict” (Berne, 2008).

[75] См. также представление Сары МакКьюн, стр. 10 текста оригинала.

F. Новый акцент в Организации Объединенных Наций на практике слежения

65. Совет по правам человека создал несколько рабочих групп, наделенных мандатом рассматривать ключевые темы, касающиеся осуществления международных норм в области прав человека, что принесло реальную пользу. Совет или его специальные процедуры могли бы рассмотреть вопрос о создании нового механизма для уделения такого внимания конкретным случаям, которое отдельные мандатарии могут быть не в состоянии поддерживать и оценивать. Новая рабочая группа, межмандатная целевая группа или утвержденный план действий могли бы уделять особое внимание жалобам о нарушениях основных прав человека в результате национальной практики слежения, которая затрагивает многие области права прав человека и, следовательно, многие мандаты специальных процедур.

V. Рекомендации

66. **Для государств:**

a) государствам следует незамедлительно ввести мораторий на экспорт, продажу, передачу, использование или обслуживание разработанных частным образом средств слежения до тех пор, пока не будет установлен режим гарантий, предусматривающий защиту прав человека;

b) государствам, закупающим или использующим технологии слежения («государствам-покупателям»), следует обеспечить, чтобы в национальном законодательстве была предусмотрена возможность их использования только в соответствии с правозащитными стандартами законности, необходимости и обоснованности целей, и создать правовые механизмы возмещения ущерба в соответствии с их обязательством предоставлять жертвам нарушений, связанных со слежением, эффективные средства правовой защиты;

c) государствам-покупателям следует также создать механизмы, обеспечивающие одобрение, надзор и контроль за закупками технологий слежения со стороны населения в целом или общин;

d) государствам, экспортирующим или разрешающим экспорт технологий слежения («государствам-экспортерам»), следует обеспечить, чтобы соответствующие правительственные учреждения запрашивали мнение общественности и проводили многосторонние консультации при рассмотрении заявок на получение экспортных лицензий. Все материалы, касающиеся экспортных лицензий, должны храниться в архивах и быть в максимально возможной степени доступными. Государства-экспортеры также должны создать «безопасные гавани» для проведения исследований в области безопасности и освободить товары и услуги, связанные с шифрованием, от ограничений в рамках экспортного контроля;

e) государствам-экспортерам следует присоединиться к Вассенаарским договоренностям и соблюдать их правила и стандарты в той мере, в какой они соответствуют международному праву прав человека;

f) государствам – участникам Вассенаарских договоренностей следует разработать механизм, в соответствии с которым лицензирование любой технологии будет зависеть от проведения национального обзора положения в области прав человека и соблюдения компаниями Руководящих принципов предпринимательской деятельности в аспекте прав человека. Такой механизм можно было бы разработать с помощью специально созданной рабочей группы по правам человека. Кроме того, им следует разработать четкие и осуществимые руководящие принципы в отношении транспарентности и подотчетности в вопросах принятия решений о лицензировании, нарушений прав человека, связанных со слежением, и режима обращения с цифровыми уязвимостями.

67. **Для компаний:**

a) компаниям, работающим в сфере частных услуг слежения, следует публично подтвердить свою ответственность за уважение свободы выражения мнений, права на неприкосновенность частной жизни и смежных прав человека и интегрировать процедуры должной осмотрительности в области прав человека с самых ранних этапов разработки продукции и на протяжении всей своей деятельности. Эти процедуры должны предусматривать учет прав человека при проектировании, регулярные консультации с гражданским обществом (особенно с группами, которые имеют повышенный риск стать объектами слежения) и эффективное представление прозрачной отчетности о предпринимательской деятельности, которая оказывает воздействие на права человека;

b) компаниям следует также предусмотреть надежные гарантии для обеспечения того, чтобы любое использование их продуктов или услуг соответствовало стандартам в области прав человека. Такие гарантии включают в себя договорные условия, которые запрещают адаптирование продукта к специфическим потребностям, выбор объектов слежения, обслуживание или иное использование, которое противоречит международному праву прав человека, а также проектно-технические решения, которые выявляют, предотвращают случаи ненадлежащего использования или смягчают его последствия, а также аудиторские проверки и процедуры контроля за соблюдением прав человека;

c) когда компании выявляют случаи ненадлежащего использования их продукции и услуг, в результате которого нарушаются права человека, они должны незамедлительно сообщать об этом в соответствующие национальные, региональные или международные надзорные органы. Компаниям следует также создать эффективные механизмы рассмотрения жалоб и возмещения ущерба, которые позволят жертвам нарушений прав человека, связанных со слежением, подавать жалобы и добиваться возмещения ущерба.

68. **Для Организации Объединенных Наций: Организации, в частности Совету по правам человека, следует создать рабочую группу или межмандатную целевую группу для мониторинга и представления рекомендаций в отношении тенденций и отдельных случаев нарушений прав человека в результате цифрового слежения.**

69. **Для всех заинтересованных сторон: государствам, частному сектору, гражданскому обществу и другим соответствующим заинтересованным сторонам следует разработать инициативы по совместному регулированию, предусматривающие разработку правозащитных стандартов поведения для частной индустрии слежения, и осуществлять эти стандарты посредством проведения процедур независимого аудита, осуществления инициатив по обучению и программных инициатив.**