



Генеральная Ассамблея

Distr.: General
6 September 2017
Russian
Original: English

Совет по правам человека

Тридцать четвертая сессия

27 февраля – 24 марта 2017 года

Пункт 3 повестки дня

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

Доклад Специального докладчика по вопросу о праве на неприкосновенность частной жизни*

Записка секретариата

В своем докладе, подготовленном в соответствии с резолюцией 28/16 Совета по правам человека, Специальный докладчик по вопросу о праве на неприкосновенность частной жизни уделяет основное внимание деятельности по ведению слежки, осуществляемой государственными органами, под национальным и международным углом зрения. Специальный докладчик подробно рассматривает характеристики международно-правовой базы и ее толкование. Кроме того, он описывает текущие события и тенденции, подходы к их исследованию, а также их связь с соблюдением права на неприкосновенность частной жизни и других взаимосвязанных прав человека. Затем он определяет первые подходы к надзору за деятельностью государственных органов по ведению слежки, призванному обеспечить большую неприкосновенность частной жизни. Наконец, Специальный докладчик отчитывается о мерах, принятых за период, рассматриваемый в настоящем докладе.

* Настоящий документ был представлен с опозданием в связи с необходимостью включения в него самой последней информации.



Доклад Специального докладчика по вопросу о праве на неприкосновенность частной жизни

Содержание

	<i>Стр.</i>
I. Введение	3
II. Последние события и тревожные тенденции в области деятельности государственных органов по ведению слежки	7
A. Деятельность государственных органов по ведению слежки и неприкосновенность частной жизни в эпоху цифровых технологий: статус-кво	7
B. Вызовы и тревожные тенденции	10
III. Первые подходы к надзору за деятельностью государственных органов по ведению слежки, призванному обеспечить большую неприкосновенность частной жизни	12
A. Комплексный обзор подходов и тем	12
B. Обсуждение	13
IV. Деятельность Специального докладчика	14
V. Выводы и рекомендации	16

I. Введение

1. В соответствии с резолюцией 28/16 Совета по правам человека Специальный докладчик по вопросу о праве на неприкосновенность частной жизни представляет ежегодные доклады Совету и Генеральной Ассамблее. Настоящий доклад является его вторым докладом Совету. В предыдущем докладе Специальный докладчик изложил план действий из десяти пунктов и стратегию по урегулированию конкретных важных современных проблем в рамках своего мандата через «тематические направления деятельности». Специальный докладчик надеется на то, что благодаря этим инициативам ему удастся внести вклад в соблюдение, защиту и осуществление права на неприкосновенность частной жизни, которому угрожают, в частности, события, происходящие в эпоху цифровых технологий.

2. Недавно Специальный докладчик опубликовал заявление под названием «Запланированные тематические доклады и призыв к проведению консультаций», в котором он рассказал, каким вопросам будет уделено внимание в его нынешнем и будущих докладах, и определил график их представления¹. Это заявление следует рассматривать как постоянно действующее приглашение для всех заинтересованных сторон во всех странах мира, желающих сотрудничать с его мандатом. Все те, кто стремится внести вклад в любые из упомянутых инициатив или каким-либо иным образом принять в них участие, могут связаться со Специальным докладчиком или членами его группы, предпочтительно по электронной почте (srprivacy@ohchr.org), и они получают ответ в кратчайшие сроки.

3. Как отмечалось в резюме выше, настоящий доклад Специального докладчика посвящен первым подходам к надзору за деятельностью государственных органов по ведению слежки, призванному обеспечить большую неприкосновенность частной жизни. Специальный докладчик уже принял ряд мер по данному вопросу в рамках своего мандата и продолжит работу в этом направлении. Для выполнения задач, изложенных в предыдущем докладе (A/HRC/31/64), в частности в отношении сектора, отвечающего за ведение слежки, Специальный докладчик предпринял серьезные усилия для организации Международного форума по надзору за деятельностью по ведению слежки, который был проведен в Бухаресте 11 и 12 октября 2016 года совместно с Объединенным комитетом Палаты депутатов и Сената по парламентскому надзору за деятельностью румынской службы разведки, Специальным комитетом Палаты депутатов и Сената по парламентскому надзору за деятельностью службы внешней разведки и Комитетами по вопросам обороны, общественного порядка и национальной безопасности Палаты депутатов и Сената при участии кафедры информационной политики и управления Мальтийского университета и исследовательской группы по вопросам безопасности, технологий и неприкосновенности частной жизни в электронном пространстве Гронингенского университета в Нидерландах. Хотя перед мероприятием по понятным причинам стояли скромные цели, оно прошло весьма успешно². Таким образом, Специальный докладчик намерен продолжить проводить форум на ежегодной основе, выступая одним из его организаторов.

¹ Заявление см. по адресу www.ohchr.org/EN/Issues/Privacy/SR/Pages/ThematicReports.aspx и www.privacyandpersonality.org/2016/12/united-nations-mandate-of-the-special-rapporteur-on-the-right-to-privacy-planned-thematic-reports-and-call-for-consultations/.

² Согласно официальному приглашению, направленному государствам, задачи форума заключались в том, чтобы начать открытое и откровенное обсуждение в доверительной обстановке достаточности механизмов надзора; существующих и планируемых мер слежения, которые могут оказывать негативное воздействие на неприкосновенность частной жизни; разницы между избирательным и массовым слежением; пропорциональности подобных мер в демократическом обществе; а также рентабельности и общей эффективности таких мер.

В 2017 году форум планируется провести 20–21 ноября в Брюсселе, и в его организации, помимо прочих, примет участие бельгийское управление по защите данных – Комиссия по вопросам неприкосновенности частной жизни. Предполагается, что благодаря форуму Специальный докладчик сможет лучше выполнить свой мандат, опираясь на практический опыт и оперативные знания большого количества надзорных органов, учрежденных по всему миру. Это поможет Специальному докладчику лучше понять и осмыслить реальные проблемы, связанные со стремлением обеспечить эффективный надзор за деятельностью служб безопасности и разведки, а также потенциальные последствия для неприкосновенности частной жизни. В первом форуме приняли участие почти 70 представителей 26 учреждений из 20 стран. Были представлены независимые надзорные органы, парламентские комитеты, гражданское общество и даже надзорный трибунал. Специальный докладчик считает, что создание более продуманной и более обеспеченной ресурсами системы надзора за ведением слежки является одной из многих взаимодополняющих инициатив, которые могут способствовать улучшению защиты права на неприкосновенность частной жизни по всему миру. По мнению некоторых, это является одним из самых многообещающих направлений конкретной работы по защите неприкосновенности частной жизни. В этом еще предстоит убедиться. Хотелось бы надеяться, что проведение серии ежегодных форумов поможет отследить передовую практику и обмениваться ей и тем самым существенно укрепить механизмы надзора во многих государствах-членах. Следует также надеяться на то, что механизмы надзора будут опираться на прочный фундамент подробно прописанного и строгого национального законодательства, в котором будут предусмотрены только пропорциональные меры, необходимые демократическому обществу, и закреплены соответствующие гарантии. Законодательство также должно обеспечивать эффективный надзор за деятельностью правоохранительных органов и служб безопасности и разведки со стороны надзорных структур, наделенных необходимыми ресурсами и независимостью. По итогам обсуждений на ежегодных форумах Специальный докладчик планирует в рамках своего мандата сформулировать рекомендации, направленные на поощрение и защиту неприкосновенности частной жизни, в том числе в свете трудностей, связанных с новыми технологиями.

4. Что касается деятельности по ведению слежки, то Специальный докладчик уделил особое внимание не только механизмам надзора, но и, насколько это было возможно, появляющимся во всем мире соответствующим новым законопроектам и докладам об использовании методов слежки и злоупотреблении ими.

Кроме того, Специальный докладчик по мере возможности осуществляет на глобальной основе мониторинг соответствующих новых законопроектов и докладов об использовании методов слежки и злоупотребления ими. Таким образом, запрашивая разрешения на официальное посещение стран, одним из главных предметов своего внимания он видит деятельность, связанную со слежкой. Об этом свидетельствует, в частности, выбор им стран для посещения в ближайшее время: Соединенных Штатов Америки (19–24 июня 2017 года), Франции (запрос направлен на 13–17 ноября 2017 года), Соединенного Королевства Великобритании и Северной Ирландии (запрос направлен на конец 2017 года, возможно, визит состоится 11–17 декабря), Германии (запрос направлен на 29 января – 2 февраля 2018 года) и Республики Кореи (запрос направлен на 3–15 июля 2018 года). Эти страны имеют прочные демократические традиции, и Специальный докладчик надеется на то, что они возьмут на себя ведущую роль в формулировании передовой практики и гарантий применительно к деятельности по ведению слежки и обеспечению уважения основных прав человека, особенно права на неприкосновенность частной жизни. Кроме того, в вопросах слежки эти страны в последние годы проявляли особую активность в плане как использования новых технологий слежения, так и разработки нового законодательства. При планировании каждого посещения Специальный докладчик запрашивает встречу с представителями разведывательных служб и органов

надзора, а также с министрами, отвечающими за работу правоохранительных органов и служб безопасности и разведки.

5. Кроме того, не желая вновь изобретать колесо и стремясь к максимальной синергии, Докладчик пристально следит за развитием и результатами параллельных инициатив, таких как проект по проработке альтернативных методов обеспечения неприкосновенности частной жизни, собственности и управления Интернетом (проект «МАППИНГ»), который осуществляется при поддержке Европейского союза и который направлен на формирование всесторонних общих взглядов на множество различных экономических, социальных, правовых и этических аспектов развития Интернета и их последствий для отдельных лиц и общества в целом. В рамках проекта «МАППИНГ», запущенного в 2014 году, более чем за год до утверждения Советом по правам человека мандата Специального докладчика и за 18 месяцев до его вступления на эту должность, между заинтересованными сторонами начались различные довольно хорошо подготовленные дискуссии, в том числе о необходимости разработки международного правового документа, регулирующего деятельность по ведению слежки. Эти дискуссии должны продлиться до конца февраля 2018 года. Специальный докладчик намерен следить за их результатами, а затем, в период с марта по июль 2018 года, определиться со своей позицией относительно желательности и целесообразности разработки такого международного правового документа. Есть вероятность, что свою позицию он выскажет в докладе Генеральной Ассамблеи в октябре 2018 года, в котором он, возможно, также сформулирует соответствующие рекомендации по поощрению и защите неприкосновенности частной жизни, в том числе в связи с вызовами, которые бросают новые технологии, как этого конкретно требует его мандат.

6. Специальный докладчик также взаимодействует и сотрудничает с другими органами и лицами, предпринимающими усилия для создания согласованной рамочной системы международной координации надзора за деятельностью по ведению слежки. За последние 18 месяцев интенсивной работы Специальному докладчику удалось установить и укрепить плодотворные отношения с властями стран по всему миру, которые готовы приступить к совместной работе над документом, закрепляющим общие стандарты ведения радиоэлектронной разведки. Хотя такое развитие событий не может не радовать, потребуются немало времени, чтобы достичь реальных результатов: в течение срока полномочий нынешнего мандатария этого, по всей вероятности, не произойдет. Тем не менее первые важные шаги были сделаны, и Специальный докладчик продолжит делать все от него зависящее для поощрения таких инициатив и содействия их успеху.

7. В настоящем докладе Специальный докладчик целенаправленно уделяет основное внимание деятельности по ведению слежки, осуществляемой государственными органами. Что касается других областей работы, то он ссылается на тематические направления деятельности, перечисленные и описанные в его первом докладе Генеральной Ассамблеи (A/71/368, пункты 7–17). Следует подчеркнуть, что проблемы безопасности и слежки были намеренно отделены от вопросов, связанных с личными данными, обрабатываемыми корпорациями, и других тем, таких как большие данные и открытые данные. В связи с этими последними темами возникают свои проблемы и вопросы, касающиеся обеспечения права на неприкосновенность частной жизни. Они рассматриваются отдельно, и до тех пор, пока они не будут сведены вместе в контексте «согласованного подхода», эти темы будут анализироваться в рамках различных параллельных инициатив Специального докладчика. По этим причинам в настоящем докладе речь в основном пойдет о ведении слежки государством, от его имени и по его распоряжению.

8. В то же время работа по другим тематическим направлениям деятельности продолжается, и ее результаты будут представлены в свое время, хотелось бы надеяться, в сроки, указанные в пункте 2 выше. В частности, целевая группа

по большим данным и открытым данным готовит свой первый доклад, который будет обсуждаться на консультативном совещании в июле 2017 года. Ожидается, что итоги консультаций составят основу ежегодного доклада, который Специальный докладчик представит Генеральной Ассамблее в 2017 году. Помимо этого, после успеха семинара по теме неприкосновенности частной жизни, правосубъектности и потокам информации, который прошел в Нью-Йорке в июле 2016 года, Специальный докладчик приступил к подготовке второго семинара, который будет посвящен Ближнему Востоку и Северной Африке. Специальный докладчик планирует провести его в Тунисе 22–23 мая 2017 года совместно с тунисским органом по защите данных в тесном сотрудничестве с организациями гражданского общества. Началась подготовка и третьего семинара, особый упор на котором будет сделан на Азию. Планируется, что он пройдет в Гонконге, Китай, 29–30 сентября 2017 года. Правительствам, организациям гражданского общества, корпорациям, органам по защите данных, учебным заведениям или отдельным лицам, желающим принять участие в этих мероприятиях или оказать им поддержку, следует как можно скорее связаться со Специальным докладчиком³.

9. Пользуясь случаем, Специальный докладчик хотел бы поблагодарить правительства Германии, Республики Корея, Соединенного Королевства, Соединенных Штатов и Франции за незамедлительный и положительный ответ на его просьбы об официальном посещении этих стран и выразить сожаление по поводу отсутствия ответа от некоторых других стран. Хотя для некоторых государств такое поведение, к сожалению, по всей видимости, является обычным, уместно и даже необходимо обратить внимание общественности на нежелание правительств выдавать разрешения на посещение своих стран. Специальный докладчик не хотел бы называть конкретные государства, но наличие или отсутствия ответа на его запросы помогает понять, какие государства готовы защищать права человека только на словах, а какие – искренне участвовать в деятельности по укреплению неприкосновенности частной жизни.

10. Прежде чем перейти к основной теме настоящего доклада, Специальный докладчик считает необходимым срочно обратить самое пристальное внимание на вызывающую обеспокоенность практику использования некоторыми государствами законодательства, гарантирующего неприкосновенность частной жизни, для воспрепятствования журналистским расследованиям. В качестве примера можно привести случаи, когда представители исполнительной власти и национальный независимый институт, по сообщениям, некорректно истолковывали права на неприкосновенность частной жизни и защиту личных данных в попытке подвергнуть цензуре исторические документы, с тем чтобы ограничить доступ к материалам 30-, 40- и даже 120-летней давности, очевидно нарушая право на свободное выражение мнений. Сообщается также о вызывающем обеспокоенность молчании со стороны компетентных органов, ответственных за защиту права на неприкосновенность частной жизни, перед лицом угрозы такой неприкосновенности и очевидных попыток властей подвергнуть цензуре представляющую общественный интерес информацию под предлогом защиты данных. Специальный докладчик установил конструктивные отношения с соответствующими органами власти и приступил к изучению этих сообщений, пока не сделав окончательных выводов относительно их достоверности. Следует отметить, что это не первое и не единственное известное ему утверждение о том, что правительство страны использует принцип неприкосновенности частной жизни в качестве предлога для изъятия представляющей общественный интерес информации из публичного доступа. Упомянув об этой проблеме, которая может стать темой для отдельного доклада, Специальный докладчик призывает всех, в особенности организации гражданского общества, сообщать ему о подобных случаях для их более досконального расследования.

³ Электронное сообщение можно направить по адресу srprivacy@ohchr.org или по другим адресам, указанным на веб-странице Специального докладчика, www.ohchr.org/EN/Issues/Privacy/SR/Pages/SRPrivacyIndex.aspx.

11. Специальный докладчик с удовлетворением отмечает вступление таких стран, как Бразилия, в ряды государств, принявших национальное законодательство для обеспечения неприкосновенности частной жизни и защиты данных, и призывает их соблюдать минимальные требования, установленные, например, в Конвенции о защите частных лиц в отношении автоматизированной обработки данных личного характера.

II. Последние события и тревожные тенденции в области деятельности государственных органов по ведению слежки

A. Деятельность государственных органов по ведению слежки и неприкосновенность частной жизни в эпоху цифровых технологий: статус-кво

12. Начало нынешнему обсуждению деятельности государственных органов по ведению слежки положили такие лица, как Эдвард Сноуден и его сторонники. Несмотря на то, что этот вопрос представляется достаточно неоднозначным с национальной точки зрения, следует признать, что информация о реальной практике некоторых служб национальной безопасности, приданная г-ном Сноуденом широкой огласке, дала толчок необходимой дискуссии по вопросу о том, что значит и должна значить неприкосновенность частной жизни в эпоху цифровых технологий. Известная цитата из интервью Сноудена газете «Гардиан» – «Я не хочу жить в мире, где все, что я делаю и говорю, записывается»⁴ – породила множество важных инициатив и действий.

13. Организация Объединенных Наций вносит свой вклад в обсуждение деятельности государственных органов по ведению слежки. В своей резолюции 69/166 Генеральная Ассамблея призвала государства учредить новые или продолжать использовать уже имеющиеся независимые, эффективные, обеспеченные надлежащими ресурсами и беспристрастные внутренние механизмы судебного, административного и/или парламентского надзора, способные обеспечивать в соответствующих случаях прозрачность и подотчетность в отношении слежения государств за сообщениями, их перехвата и сбора личных данных. Региональные суды по правам человека, такие как Европейский суд по правам человека, вынесли решения, устанавливающие конкретные обязательные требования, которые правительства должны соблюдать при разработке и использовании средств ведения слежки⁵.

14. Специальный докладчик следит за развитием событий в области ведения слежки государственными органами самыми разными путями, в том числе посредством регулярных контактов с рядом национальных и международных организаций гражданского общества. Многие из них делают отличную работу, доводя различные вызывающие озабоченность вопросы до сведения Специального докладчика, национальных правительств и мирового сообщества в целом. Ни в коей мере не умаляя значения работы других организаций, Специальный докладчик хотел бы особо выделить важность усилий Американского союза защиты гражданских свобод⁶, организации «Экسس нау»⁷, организации «Между-

⁴ См. по адресу www.theguardian.com/world/2013/jun/09/nsa-whistleblower-edward-snowden-why; информация получена 08.12.2016.

⁵ См., например, European Court of Human Rights, *Zakharov v. Russia*, judgment of 4 December 2015, по адресу hudoc.echr.coe.int/eng?i=001-159324.

⁶ См. www.aclu.org/issues/national-security/privacy-and-surveillance.

⁷ См. www.accessnow.org/issue/privacy/.

народная амнистия»⁸, Ассоциации прогрессивных коммуникационных технологий⁹, организации «Статья 19»¹⁰, организации «Хьюман райтс уотч»¹¹, Международной сети организаций за гражданские свободы¹² и организации «Прайвеси интернэшнл»¹³, с которыми он сотрудничает в рамках своего мандата по ряду направлений. Актуальные доклады этих и других организаций гражданского общества имеют огромное значение, поскольку в рамках ограничений на размер официальных докладов Специального докладчика, установленных Организацией Объединенных Наций, невозможно рассказать, например, о тех эпизодах слежки, сведения о которых содержатся в информационной записке, представленной организацией «Прайвеси интернэшнл» Специальному докладчику в ноябре 2016 года и впоследствии опубликованной на веб-сайте «Прайвеси интернэшнл»¹⁴. Важно отметить, что Специальный докладчик разделяет обеспокоенность «Прайвеси интернэшнл» последними событиями, связанными с ведением слежки в Венесуэле (Боливарианской Республике), Зимбабве, Колумбии, Марокко, Мексике, Новой Зеландии, Польше, бывшей югославской Республике Македония, Российской Федерации, Руанде, Соединенном Королевстве, Соединенных Штатах Америки, Уганде, Франции, Швеции, Эстонии и Южно-Африканской Республике, и сам следит за их развитием. Специальный докладчик призывает правительства этих государств обратить внимание на обеспокоенность, высказанную «Прайвеси интернэшнл» в своих материалах, и предлагает им публично отреагировать на нее и/или при необходимости связаться с ним напрямую.

15. Тем не менее серьезную обеспокоенность вызывает тот факт, что с момента принятия резолюции 69/166 и несмотря на судебные решения, упомянутые в пункте 13 выше, ситуация с уважением права на неприкосновенность частной жизни в ходе ведения слежки со времени представления предыдущего доклада Специального докладчика не изменилась в лучшую сторону. Отреагировавшие на критику государства приступили к работе и принимают новые законы по данному вопросу, но они в лучшем случае содержат лишь незначительные улучшения в отдельных областях. В целом такие законы разрабатываются и принимаются в спешке, с тем чтобы легитимизовать практику, которая не должна применяться вообще.

16. 21 декабря 2016 года Суд Европейского союза вынес очень важное и полезное решение, в котором он напомнил государствам – членам Европейского союза об их обязанности уважать, поощрять и защищать право человека на неприкосновенность частной жизни и другие права в эпоху цифровых технологий. Относительно законодательного требования к поставщикам телекоммуникационных услуг хранить большие объемы данных суд постановил: «Нарушение основных прав, к которому привело такое законодательство... имеет далеко идущие последствия и должно расцениваться как особо серьезное. Тот факт, что данные хранятся без уведомления подписчика или зарегистрированного пользователя, может вызвать у затронутых лиц ощущение, что их частная жизнь находится под постоянным наблюдением»¹⁵. Суд также упомянул о возможных негативных последствиях для осуществления свободы выражения мнений.

⁸ См. www.amnestyusa.org/our-work/issues/security-and-human-rights/mass-surveillance и www.amnesty.org.uk/issues/Mass-surveillance.

⁹ См. www.apc.org/en/pubs/research.

¹⁰ См. www.article19.org/cgi-bin/search.cgi?q=privacy.

¹¹ См. www.hrw.org/sitesearch/surveillance.

¹² См. www.inclo.net/.

¹³ См. www.privacyinternational.org/reports.

¹⁴ Privacy International, «Monitoring and oversight of communications surveillance», November 2016, документ доступен по ссылке www.documentcloud.org/documents/3454560-UN-Briefing-Monitoring-and-Oversight-of.html.

¹⁵ См. European Court of Justice, *Tele 2 Sverige AB v. Swedish Post and Telecom Authority*, judgment of 21 December 2016.

17. Кроме того, суд признал, что, «хотя эффективность борьбы с серьезными преступлениями, в частности с организованной преступностью и терроризмом, может в значительной степени зависеть от использования современных методов расследования, такая представляющая общий интерес цель, какое бы основополагающее значение она не имела, не может сама по себе служить оправданием принятия для ведения этой борьбы национального законодательства, предусматривающего полное и неизбирательное хранение данных о трафике и местоположении»¹⁶. Помимо этого, Суд дал ясно понять, что хранение данных трафика должно осуществляться в качестве исключения, а не общего правила. При наличии конкретных оснований для хранения таких данных в целях борьбы с терроризмом и серьезными преступлениями необходимо устанавливать ограничивающие критерии, например, точные географические ограничения. Суд также напомнил, что затронутые лица нуждаются в гарантиях и средствах правовой защиты и что необходимо внедрять эффективные механизмы надзора, основанные на системе сдержек и противовесов¹⁷.

18. В то время как сторонники защиты неприкосновенности частной жизни по вполне понятным причинам положительно отнеслись к судебному решению, другие его аспекты, судя по всему, наиболее успешно обобщил независимый эксперт по законодательству о терроризме Соединенного Королевства, королевский адвокат Дэвид Андерсон, который отметил, что: «Решение Суда Европейского союза, таким образом, является поистине радикальным. С учетом доказанной полезности существующих полномочий на хранение данных и ограничений, которые теперь на них наложены, данное решение, по всей вероятности, создаст серьезные трудности для правоприменения как в Соединенном Королевстве, так и в других государствах-членах. С другой стороны, не все согласятся с Судом в том, что эти полномочия представляют собой «особо серьезное» нарушение права на неприкосновенность частной жизни или что они «могут вызвать у затронутых лиц ощущение, что их частная жизнь находится под постоянным наблюдением» (пункт 100). Следовало бы провести более тщательный анализ соразмерности, оценив реальный ущерб, нанесенный за годы применения этих полезных полномочий, и попытаться избежать утверждений, основанных на теориях или непроверенных предположениях о настроении общественности»¹⁸.

19. Поскольку Специальный докладчик является убежденным сторонником традиции принимать важные решения, опираясь на факты, он разделяет настроения независимого эксперта, выступающего за более тщательный анализ соразмерности. На сегодняшний день Специальный докладчик еще не получил доступа (по крайней мере, в Соединенном Королевстве) к некоторым (в некоторых случаях засекреченным) данным, которые могли бы стать подтверждением того, что неизбирательный сбор данных необходим и соразмерен риску. Более того, Специальный докладчик поддерживает решение Суда именно потому, что он до сих пор не имеет убедительных доказательств соразмерности и необходимости законов, регулирующих ведение слежки, которые разрешали бы осуществлять неизбирательный сбор всех типов данных, включая метаданные и контент.

20. В данном контексте важно обратить внимание на культурные аспекты, которые также отметил независимый эксперт:

«Тем не менее следует признать, что на территории Европы отношение к таким мерам является разным, по крайней мере, в определенной степени. Так:

- комментарии Суда Европейского союза относительно серьезности нарушения права на неприкосновенность частной жизни не нашли реального отклика ни в трех парламентских докладах и экспертных заключениях, на

¹⁶ Там же.

¹⁷ Там же.

¹⁸ См. www.terrorismlegislationreviewer.independent.gov.uk/cjeu-judgment-in-watson/.

основании которых был принят Закон о полномочиях на ведение досудебного расследования, ни в докладах, регулярно представляемых Уполномоченным по перехвату сообщений, ранее занимавшим пост старшего судьи, который осуществляет тщательный надзор за этой деятельностью в Соединенном Королевстве;

- в то же время в странах восточной части Европы и в Германии, которые имеют особый исторический опыт и которым доводилось сталкиваться с проявлениями терроризма сравнительно нечасто (до последнего времени), такие меры вызвали большую настороженность. В Болгарии, Румынии, Германии, Чешской Республике и на Кипре национальные правила хранения данных вызвали противоречивую реакцию и были отменены еще до появления организации «Цифровые права – Ирландия».

Это может служить подтверждением того, что я ранее описал как «замечные и последовательные различия в точках зрения европейских судов и британских судей... которые, по меньшей мере частично, связаны с различным восприятием роли полиции и сил безопасности и разными (но в равной мере оправданными) выводами, сделанными из истории XX века в разных частях Европы» (A Question of Trust, 2.24)¹⁹.

В. Вызовы и тревожные тенденции

21. В ходе различных исследований, имеющих отношение к мандату Специального докладчика, и других смежных исследовательских проектов был сделан вывод о том, что деятельность правоохранительных органов и служб безопасности и разведки по ведению слежки становится все менее различимой. В то время как деятельность первых, как правило, связана с ведением слежки на национальной территории, а внимание двух других распространяется на зарубежные территории, в эпоху цифровых технологий характер трансграничных потоков данных и технических средств слежения за ними зачастую требует использования одинакового или очень похожего оборудования.

22. Все чаще личные данные оказываются в общей корзине, где они могут использоваться и повторно использоваться во всевозможных известных и неизвестных целях. В этой связи крайне важные вопросы встают в отношении требований к сбору, хранению, анализу и последующему уничтожению данных. В качестве конкретного примера можно привести недавнее исследование, проведенное центром по вопросам неприкосновенности частной жизни и технологий Центра права Джорджтаунского университета в Вашингтоне, в ходе которого было установлено, что в системах распознавания лиц правоохранительных органов имеются данные каждого второго совершеннолетнего американца. Авторы исследования заявили следующее: «Мы почти ничего не знаем об этих системах. Мы не знаем, какое влияние они оказывают на неприкосновенность частной жизни и гражданские свободы. Мы не знаем, каким образом в них решаются проблемы с точностью. И мы не знаем, как эти системы – на местном уровне, уровне штата или федеральном уровне – затрагивают расовые и этнические меньшинства»²⁰.

23. Эти и аналогичные выводы наводят на ряд соображений. Во-первых, характер трансграничных потоков данных и современных информационных технологий требует формирования глобального подхода к защите и поощрению прав человека, в частности права на неприкосновенность частной жизни. Для того чтобы обмен информацией продолжал носить глобальный характер со всеми теми серьезными выгодами, которые он принес и продолжает приносить че-

¹⁹ Там же.

²⁰ Clare Garvie, Alvaro Bedoya and Jonathan Frankle, «The perpetual line-up: unregulated police face recognition in America», October 2016, см. по адресу www.perpetuallineup.org.

ловечеству, он должен происходить в согласованной и надежной среде. В такой среде люди не могут дискриминироваться по признаку национальной принадлежности, происхождения, расы, пола, возраста, способностей, вероисповедания и т.д. Необходимо определить ключевой набор прав и ценностей, которые международное сообщество будет неукоснительно уважать, защищать и поощрять.

24. Во-вторых, растущее значение обмена информацией в виртуальном пространстве требует защищенных, надежных и безопасных методов. Специальный докладчик уже уделил значительное внимание таким технологиям, как шифрование, в частности в своем первом докладе Генеральной Ассамблее (см. A/71/368, пункты 19–40). Кроме того, внушительную и полезную работу в этой области уже проделали и другие мандатарии, например Специальный докладчик по вопросу о поощрении и защите права на свободу мнений и их свободное выражение (см. A/HRC/29/32).

25. Когда правоохранительные органы и службы безопасности и разведки высказывают обеспокоенность по поводу невозможности перехватывать и читать все сообщения, отправляемые и получаемые всеми пользователями современных информационных технологий, им не следует забывать, что мы живем в эпоху, когда обмен информацией осуществляется через тысячи каналов. Люди стали так много обмениваться информацией через цифровые каналы, что, даже если некоторые из них недоступны государству, это не значит, что не существует других способов отследить людей с дурными намерениями. В частности, существует множество возможностей анализировать поведение людей с помощью огромных объемов метаданных, создаваемых смартфонами и подключенными друг к другу устройствами – метаданных, которые зачастую говорят о намерениях не меньше, чем само содержание сообщений²¹. С другой стороны, если государства будут способны вторгаться в любой информационный поток, даже ретроактивно, благодаря неизбежному накоплению огромных объемов данных и применению таких технологий, как «быстрая заморозка», право на неприкосновенность частной жизни попросту не совершит полноценный переход в эпоху цифровых технологий.

26. Следует поприветствовать тот факт, что некоторые страны и организации уже приступили к активной работе над решением этих вопросов. В частности, значительным вкладом в эту работу стала инициатива Совета Европы в контексте правоприменения в облачной вычислительной среде. Она связана с Конвенцией о киберпреступности и направлена на разработку нового правового инструмента²².

27. Тем не менее вызывает обеспокоенность тот факт, что в современных законах о слежке все чаще допускается возможность создания личных данных, получения к ним доступа и их анализа без соответствующего разрешения и надлежащего надзора. Требование получения соответствующего разрешения и надлежащего надзора должно действовать «в момент выдачи распоряжения о принятии такой меры, а также в ходе и по окончании ее применения»²³. В то время как для использования «традиционных» методов, например, для перехвата телефонных звонков и сообщений в целом, зачастую требуется предварительное разрешение суда, применение других методов, таких как сбор и анализ метаданных, относящихся к протоколам истории посещений в Интернете, или данных, возникающих при использовании смартфонов (данных о местоположении, телефонных звонков, данных использованных приложений и т.д.), обстав-

²¹ См., например, доклад Беркмановского центра по изучению Интернета и общества Гарвардского университета «Don't panic. Making progress on the 'going dark' debate», 2016 год, по адресу cyber.harvard.edu/pubrelease/dont-panic/Dont_Panic_Making_Progress_on_Going_Dark_Debate.pdf.

²² См. www.coe.int/en/web/portal/-/cybercrime-towards-a-new-legal-tool-on-electronic-evidence.

²³ European Court of Human Rights, *Zakharov v. Russia*.

лено гораздо менее жесткими требованиями. Такое положение дел нельзя назвать оправданным, поскольку последние виды данных дают не меньшее представление об индивидуальной деятельности отдельных лиц, чем реальное содержание разговоров. Таким образом, применение таких мер также должно быть увязано с надлежащими гарантиями.

28. Хотя необходимость получения разрешения суда на осуществление интрузивных мер, как правило, повышает степень защиты неприкосновенности частной жизни, необходимо также гарантировать, чтобы при принятии решений по конкретным делам судьи действовали независимо и беспристрастно. Более того, они должны располагать необходимой информацией и фактами, с тем чтобы тщательно рассматривать запросы на осуществление таких мер и понимать возможные последствия своих решений, в частности в отношении выбора технологий и последствий их использования. Таким образом, государства должны проводить соответствующую подготовку судей и предоставлять им необходимые ресурсы для выполнения этой сложной задачи.

29. В целом то же самое касается и надзора за ведением слежки со стороны специализированных парламентских органов. Они должны не только обладать соответствующей информацией для понимания деятельности правоохранительных органов и служб безопасности и разведки, но и иметь доступ к надлежащим ресурсам для ее анализа и изучения.

30. В большинстве стран решить эту задачу будет непросто по причине большого объема данных. Осуществляющие слежку органы должны принимать меры, позволяющие непрерывно и тщательно анализировать и контролировать надзорную практику. Надзор, в особенности если он осуществляется на политическом уровне, должен затрагивать структурные вопросы и касаться общей направленности операций.

31. Еще одна сфера, вызывающая пристальное внимание, – это международный характер деятельности по надзору. Особое внимание следует уделить двум конкретным аспектам данного вопроса. Во-первых, очень важно, чтобы государства на глобальном уровне уважали право на неприкосновенность частной жизни, в основе которого лежит человеческое достоинство. Слежка, вне зависимости от того, ведется ли она против иностранцев или собственных граждан, должна осуществляться исключительно при условии соблюдения основных прав человека, таких как право на неприкосновенность частной жизни. Все национальные законы или международные соглашения, не признающие этого факта, должны быть признаны устаревшими и не соответствующими универсальному характеру права на неприкосновенность частной жизни и основных прав в эпоху цифровых технологий.

III. Первые подходы к надзору за деятельностью государственных органов по ведению слежки, призванному обеспечить большую неприкосновенность частной жизни

A. Комплексный обзор подходов и тем

32. По итогам исследовательской работы и обмена мнениями с официальными представителями ряда государств, а также с представителями гражданского общества и корпораций, функционирующих в различных регионах мира, в частности в ходе состоявшегося в 2016 году Международного форума по надзору за деятельностью по ведению слежки, был назван ряд новых тем, касающихся деятельности государственных органов по ведению слежки. К числу таких тем относятся:

- a) необходимость интернационализации и стандартизации используемых терминов и лексики;
- b) необходимость проведения конфиденциального и открытого диалога для лучшего понимания национальных систем, их сходных черт и различий;
- c) поощрение и защита основных прав человека при использовании конкретных методов слежения;
- d) гарантии и средства защиты, предпочтительно международного характера;
- e) подотчетность и прозрачность;
- f) сбор и обсуждение информации о хороших и плохих видах практики;
- g) более обстоятельная дискуссия на тему того, как лучше организовать надзор за деятельностью по ведению слежки, осуществляемой государственными органами;
- h) поиск ответов на вопрос о том, как следует взаимодействовать по данной тематике с общественностью;
- i) необходимость более открыто и активно разъяснять смысл работы, которую выполняют спецслужбы и органы правопорядка при осуществлении слежки;
- j) потребность в новых форумах для достижения прогресса на данном направлении.

В. Обсуждение

33. Целью интернационализации и стандартизации используемых терминов и лексики является выработка определения таких понятий, как «слежка», «массовая слежка», «массовый сбор», «массовый перехват», «масштабные хакерские атаки», «вмешательство в работу оборудования» и т.д. Власти Великобритании опубликовали полезный, хотя и несколько спорный, документ, озаглавленный «Operational case for bulk powers» (Оперативные основания для массовой слежки), в котором предлагаются варианты определений ряда из указанных терминов²⁴. Очень важно, чтобы органы государственной власти, осуществляющие слежение, представители гражданского общества и другие заинтересованные субъекты четко представляли себе, что они фактически имеют в виду, используя соответствующие термины применительно к слежке. Некоторые из этих терминов, такие как «массовая слежка», имеют особую коннотацию и являются весьма неоднозначными. Необходимо добиться более системного и гармонизированного использования терминов и общего понимания их содержания в контактах между государственными органами, отвечающими за ведение слежки. При этом надзорные органы судебной и политической ветвей власти, представители гражданского общества, исследователи, занимающиеся проблемами безопасности, и корпорации также должны правильно понимать и употреблять эти термины.

34. Поскольку тема слежки имеет и международное измерение, необходимо обсуждать ее на международном уровне, в атмосфере конфиденциальности и доверия. Важно расширять диалог между национальными органами, отвечающими за ведение слежки. Кроме того, необходимо, чтобы в дискуссиях такого рода могли принимать участие и высказывать свои мнения и озабоченности эксперты гражданского общества.

²⁴ См. веб-сайт www.gov.uk/government/uploads/system/uploads/attachment_data/file/504187/Operational_Case_for_Bulk_Powers.pdf.

35. Исключительно важно, чтобы соблюдение основных прав человека, и в частности права на неприкосновенность частной жизни, права на свободу выражения мнений и права на доступ к информации, оставалось основным критерием при оценке любых типов и видов деятельности государственных органов по ведению слежки. Хотя защита прав на жизнь и на физическую неприкосновенность является одним из важнейших условий самого существования человека, следует иметь в виду, что строгой иерархии прав человека не существует. Они, как правило, взаимно усиливают друг друга. Иными словами, необходимо поощрять весь спектр прав человека, не заикливаясь на одном-двух правах.

36. Ценность того или иного права определяется тем, насколько четко оно прописано и как оно обеспечивается правоприменительными механизмами. Это имеет самое непосредственное отношение к деятельности государственных органов по ведению слежки, поскольку гарантии должны выходить за пределы национальных границ, а средства защиты носить трансграничный характер. Как отмечалось выше, необходимо расширить масштабы и повысить качество взаимной правовой помощи. Если глобальный подход выработать не удастся, хотя исключать такую возможность пока нельзя, необходимо активизировать работу на региональном и межрегиональном уровнях.

37. Необходимо обеспечить ясность структуры подотчетности и прозрачность деятельности государственных учреждений, отвечающих за ведение слежки. Должно быть хорошо понятно, почему осуществляется сбор тех или иных конкретных данных, в каких целях проводится конкретный анализ и какие цели не являются законными. Эти функции должны в первую очередь лежать на тех

государственных органах, которым поручено ведение слежки, и после того, как будут определены правовые рамки соответствующей деятельности, необходимо четко определить, кто именно несет ответственность за соблюдение правовых требований.

38. Полезно собирать информацию о примерах хорошей и плохой практики. Например в некоторых учреждениях, осуществляющих надзор за деятельностью спецслужб, созданы экспертные органы консультативного характера, в состав которых вошли пользующиеся доверием внешние эксперты, формулирующие свои рекомендации по конкретным вопросам. Помимо этого, исключительно важно проводить оценку оперативной работы и анализировать ее последствия для поощрения и защиты основных прав человека. Наконец, сотрудников государственных органов, отвечающих за ведение слежки, следует учить не слишком полагаться на технические устройства и понимать, что технологии должны помогать людям принимать решения, а не управлять этим процессом.

39. На случай сбоев в работе внутренних механизмов подотчетности и обеспечения прозрачности необходимо иметь другие действенные механизмы сдержек и противовесов. Государства должны быть в состоянии выявлять и оценивать структурные проблемы в учреждениях, уполномоченных на ведение слежки.

В некоторых государствах эту функцию выполняют парламентские комитеты. Однако нередко надзорные органы не располагают необходимыми знаниями в этой области, достаточными ресурсами и/или доступом к соответствующей информации. То же самое можно сказать и о механизмах судебного контроля, когда они существуют.

40. Кроме того, разоблачения Сноудена и последовавшие за этим события отчетливо показали, что государственным органам просто необходимо разъяснять свою работу. Одна из возможностей видится в том, чтобы постфактум уведомлять о слежке тех, кто ей подвергся. После появления такой возможности эти люди должны быть поставлены в известность о слежке, и им должны быть разъяснены последствия проделанной работы. Они должны также иметь возможность изменить или удалить неактуальную личную информацию, при условии, что такая информация больше не требуется для целей текущего или запла-

нированного расследования, в связи с которым было в надлежащем порядке получено разрешение на ее сбор и использование.

41. Наконец, необходимо восстановить доверие населения к деятельности занимающихся слежкой учреждений. Несомненно, что вопросы безопасности волнуют каждого человека. Поэтому, хотя широкой публике нет необходимости знать детали и тонкости каждой операции слежения, население должно получать информацию, которая позволяла бы ему понимать общие параметры работы, направленной на защиту его интересов. Действительно, чтобы полететь на пассажирском самолете, пассажиру нет необходимости уметь пилотировать его, однако он не станет покупать билет на самолет, не доверяя общим возможностям и безопасности системы воздушных перевозок.

IV. Деятельность Специального докладчика

42. Специальный докладчик по вопросу о праве на неприкосновенность частной жизни представляет доклады об основных мероприятиях публичного или полупубличного характера, осуществляемых им в рамках своего мандата. Данный доклад охватывает деятельность за период с июля 2016 года до начала февраля 2017 года. К числу проведенных в этот период мероприятий относятся:

- a) Европейский семинар по вопросам инновационных методов защиты права на неприкосновенность частной жизни, Научно-исследовательский центр компании «Хуавэй» в Германии, Мюнхен, Германия, 3 августа 2016 года;
- b) участие в качестве основного докладчика в организованной Советом Европы конференции на тему «Свобода Интернета: постоянный фактор демократической безопасности в Европе», Страсбург, Франция, 9 сентября 2016 года;
- c) участие в качестве председателя рабочей группы по биометрике и праву на неприкосновенность частной жизни в отраслевой конференции Европейской биометрической ассоциации научно-исследовательских учреждений, Дармштадт, Германия, 19–20 сентября 2016 года;
- d) участие в организованном Генеральным директором по вопросам миграции и внутренних дел Европейской комиссии совещании Консультативной группы по вопросам защиты и безопасности программы ЕС «Горизонт 2020», Брюссель, 27 сентября 2016 года;
- e) участие в качестве Специального докладчика на Международном форуме по надзору за деятельностью по ведению слежки Бухарест, 11–12 октября 2016 года;
- f) участие в качестве основного докладчика и председателя дискуссионной группы на конференции на тему «Программы слежения в обществе, основанном на знаниях», Бухарест, 13–14 октября 2016 года;
- g) участие в качестве основного докладчика в 38-й Международной конференции представителей национальных органов, обеспечивающих защиту данных, по вопросам соотношения между защитой данных и правом на неприкосновенность частной жизни, Марракеш, Марокко, 18–22 октября 2016 года;
- h) участие во второй ежегодной генеральной ассамблее проекта «Управление альтернативами воздействия Интернета на частную жизнь и ответственность» (проект МАППИНГ), Прага, 31 октября – 2 ноября 2016 года;
- i) участие в качестве основного докладчика в конференции на тему «Киберпространство 2016», Брно, Чехия, 25–26 ноября 2016 года;
- j) участие в качестве основного докладчика в конференции «Азиатско-Тихоокеанский форум представителей государственных органов, занимающихся вопросами неприкосновенности частной жизни», проходившей в городе Мансанильо, Мексика, с 30 ноября по 2 декабря 2016 года;

к) участие в качестве основного докладчика и участника дискуссионной группы в симпозиуме по вопросам слежения, организованном Ирландским советом за гражданские свободы, Дублин, 7 декабря 2016 года;

л) участие в качестве основного докладчика в заседании, посвященном представлению ежегодного заявления Комиссии по правам человека Северной Ирландии, Белфаст, Соединенное Королевство, 8 декабря 2016 года;

м) участие в подготовительных совещаниях ко второй сессии Рабочей группы по вопросам обеспечения неприкосновенности частной жизни, безопасности личных данных и свободного движения информации, Тунис, 12–14 декабря 2016 года;

н) участие в качестве члена дискуссионной группы по вопросам искусственного интеллекта и обеспечения неприкосновенности частной жизни в десятой международной конференции на тему «Компьютеры, неприкосновенность частной жизни и защита данных», Брюссель, 25–27 января 2017 года;

о) участие в качестве основного докладчика по вопросам неприкосновенности частной жизни и безопасности на девятой сессии Форума по вопросам систем управления информационной безопасностью (ИСМС), Мадрид, 1–2 февраля 2017 года.

V. Выводы и рекомендации

43. На данном этапе на основе своих предварительных выводов Специальный докладчик хотел бы предложить пять конкретных рекомендаций. Эти рекомендации касаются следующих вопросов:

а) почему популизм в вопросах обеспечения неприкосновенности частной жизни наносит вред безопасности;

б) каким образом государства могут улучшить защиту неприкосновенности частной жизни, организовав более эффективный надзор за программами слежения;

в) кто заслуживает того, чтобы пользоваться правом на неприкосновенность частной жизни, т.е. идет ли речь обо всех лицах и во всех ли обстоятельствах, – в этом контексте универсальность права на неприкосновенность частной жизни приобретает особый смысл;

г) каким образом можно улучшить защиту права на неприкосновенность частной жизни инструментами национального и международного права;

д) когда степень проработки некоторых мер в области международного права, касающихся, в частности, правовых инструментов, регулирующих деятельность по ведению слежки, может выйти на тот уровень, когда их было бы полезно вынести на обсуждение в более широком формате.

Почему популизм в вопросах обеспечения неприкосновенности частной жизни наносит вред безопасности

44. Этот раздел доклада, возможно, было бы точнее назвать «Безопасность, популизм и неприкосновенность частной жизни». В период с 2015 по 2017 год в первую очередь в Европе, но не только в ней, отмечалось все большее стремление к проведению «политики жестов». Иными словами, в течение последних 18 месяцев можно было видеть, как политические деятели желали показать, что они готовы пользоваться своими законодательными полномочиями в интересах безопасности в нарушение неприкосновенности частной жизни или легитимизировать существующую практику, не приводя никаких доказательств того, что такая практика соразмерна угрозе терроризма или позволяет эффективно бороться с ней.

45. В основе новых законодательных мер лежит психология страха – непропорционально сильного, хотя вполне объяснимого, страха, который могут испытывать избиратели перед лицом угрозы терроризма. Испытываемый избирателями высокий уровень страха не позволяет им объективно оценивать эффективность предлагаемых мер.

46. По мнению Специального докладчика, невозможно найти практически никаких доказательств эффективности или пропорциональности некоторых мер, исключительно сильно ущемляющих право на неприкосновенность частной жизни, которые предусмотрены в новых законодательных актах, регулирующих ведение слежки во Франции, Германии, Соединенном Королевстве и Соединенных Штатах Америки. Как и судья в недавно рассматривавшемся деле о запрете иммиграции в Соединенные Штаты Америки, Специальный докладчик обязан требовать доказательств того, что меры, предусмотренные в упомянутых законодательных актах, соразмерны существующим угрозам²⁵. Так же, как упомянутый судья просил представить точную информацию о том, сколько террористических актов было совершено за период с 2001 года гражданами государств, которых должен был коснуться запрет на въезд в США, Специальный докладчик должен спросить, не было ли бы более соразмерным и, безусловно, более экономически целесообразным и в меньшей степени ущемляющим право на неприкосновенность частной жизни потратить дополнительные средства на людские ресурсы, необходимые для целенаправленного сбора разведывательной информации и внедрения осведомителей, чем на ведение электронного слежения, тем более что происходит это в то время, когда подавляющее большинство террористических актов совершают лица, уже известные властям.

47. Кроме того, появляется все больше доказательств того, что имеющаяся в распоряжении государств информация, в том числе информация, полученная путем массового сбора данных и массовой слежки, становится все более уязвимой для взлома государственными службами враждебно настроенных государств или представителями организованных преступных групп. Никто не продемонстрировал, что риски, создаваемые сбором упомянутых данных, соразмерны снижению рисков в результате массового сбора данных.

48. Следует также иметь в виду, что проблема злоупотребления информацией, получаемой в результате массового сбора данных, по-прежнему стоит очень остро. Ни в коей мере не пытаясь бросить тень на новую администрацию Соединенных Штатов, представляется уместным воспроизвести озабоченность, высказанную в этом контексте одним из старших научно-исследовательских работников неправительственной организации «Хьюман Райтс Уотч»: «Несмотря на скромную реформу, предпринятую в 2015 году, в США Национальное агентство безопасности через свою сеть перехвата данных продолжает каждый день собирать информацию о миллионах людей. Сегодня ключи от самого совершенного в мире аппарата слежения оказались в руках... кандидата, который угрожал арестовать своего политического оппонента, организовать регистрацию и поставить мусульман вне закона, депортировать миллионы иммигрантов и запретить свободную прессу»²⁶. Хотя можно надеяться, что существующая в Соединенных Штатах система сдержек и противовесов или даже этические стандарты самого главы администрации США отодвинут угрозу реализации упомянутых рисков, Специальный докладчик хотел бы попросту сказать, что, когда имеются массивы данных, полученных в результате массовой слежки или массового

²⁵ См. www.npr.org/2017/02/04/513446463/who-is-judge-james-l-robart-and-why-did-he-block-trumps-immigration-order.

²⁶ Cynthia M. Wong, «Surveillance in the age of populism», Human Rights Watch, February 2017, см. www.hrw.org/news/2017/02/07/surveillance-age-populism.

сбора, а к власти в той или иной части мира приходит новая неразборчивая в средствах администрация, угроза злоупотребления соответствующей информацией может оказаться настолько серьезной, что следует задуматься об изначальной оправданности сбора таких данных.

49. В этой связи Специальный докладчик рекомендует государствам не спекулировать на чувстве страха и повышать безопасность своих стран путем принятия эффективных и пропорциональных мер, а не неоправданно жестких законодательных актов, ущемляющих право на неприкосновенность частной жизни. Как сказал в этой связи архиепископ Вестминстерский кардинал Винсент Николс: «Я не верю в то, что лидерство лучше всего строить на страхе. Подлинные политические лидеры не разыгрывают карту страха»²⁷.

Каким образом государства могут улучшить защиту неприкосновенности частной жизни, организовав более эффективный надзор за программами слежения

50. Состоявшийся в 2016 году International Intelligence Oversight Forum (ИОФ) продемонстрировал, что обсуждение того, каким образом следует осуществлять надзор за программами слежения так, чтобы при этом укреплять гарантии неприкосновенности частной жизни, представляет собой сложный и длительный процесс, требующий значительных ресурсов, некоторых изменений в культурных подходах, политической воли и укрепления доверия. Более коротких путей выявления и дальнейшего развития передовой практики просто не существует.

51. Специальный докладчик предлагает простую, но очень важную рекомендацию: всем государствам – членам Организации Объединенных Наций следует начать кропотливую дискуссию по вопросам надзора за программами слежения, которая была инициирована Специальным докладчиком на Международном форуме по надзору за деятельностью по ведению слежки

в 2016 году и будет продолжена на следующих мероприятиях этого форума в 2017 году. Правительствам следует поощрять органы, отвечающие за ведение слежки, и спецслужбы принимать активное участие в работе упомянутых форумов и всячески содействовать этому.

Кто заслуживает того, чтобы пользоваться правом на неприкосновенность частной жизни

52. Специальный докладчик рекомендует государствам принимать меры к тому, чтобы обеспечивать соблюдение права на неприкосновенность частной жизни как в их собственных странах, так и в международных масштабах, и чтобы это право рассматривалось как подлинно универсальное, особенно в ситуациях, когда речь идет о слежке в Интернете, и не зависело от национальной принадлежности гражданина.

53. Эта рекомендация требует некоторых разъяснений и будет проиллюстрирована на примерах, ограничивающихся (исключительно в силу требований к объему документа) прецедентным правом и изменениями в законодательстве Соединенных Штатов. С самого начала необходимо иметь в виду, что все рекомендации, адресованные Соединенным Штатам, в аналогичных ситуациях применимы также ко всем государствам – членам Организации Объединенных Наций.

54. 6 февраля 2017 года Палата представителей Соединенных Штатов сделала весьма похвальный шаг, которого Специальный докладчик долго ожидал от этого органа. Был единогласно принят проект закона о непри-

²⁷ Кардинал Винсент Николс, выступление в программе BBC Radio 4, the Westminster Hour, 5 февраля 2017 года.

косновенности сообщений, отправляемых по электронной почте, который восполнил пробел, существовавший до того момента в законодательстве Соединенных Штатов. Законопроект устанавливает, что получение доступа к электронным сообщениям более чем шестимесячной давности, хранящимся в облачных или иных хранилищах данных, возможно лишь с санкции суда. Специальный докладчик искренне приветствует этот законопроект и надеется, что он окажется приемлемым и для Сената, который в апреле 2016 года заблокировал аналогичную попытку принять закон по указанному вопросу. Более того, Специальный докладчик призывает Сенат воспользоваться представившейся исторической возможностью и сделать шаг вперед, тем самым демонстрируя приверженность Соединенных Штатов соблюдению прав человека во всем мире и одновременно отмечая одно из ксенофобских заблуждений, которые сознательно или не сознавая того поощряют некоторые правительства. Это заблуждение сводится к тому, что только «отвратительные иностранцы» стремятся «вредить нам», и поэтому они не заслуживают того, чтобы их основные права были защищены законом.

55. Вина за недостатки законотворчества лежит не на одних Соединенных Штатах. Так недавно по неверному пути пошло и правительство Германии, принявшее закон, в котором проводится различие между гражданами Германии и стран Европейского союза, с одной стороны, и гражданами всех остальных стран мира – с другой (см. документ A/71/368, пункты 35–36). Естественно, что такие законы не выдерживают критики с позиции простой логики: известно, что исполнителями подавляющего большинства террористических актов в Европе были не иностранные граждане, а граждане Европейского союза, имеющие удостоверения личности и паспорта Европейского союза. То же самое, по всей видимости, можно сказать и о большинстве террористических актов, произошедших в последнее время в Соединенных Штатах. Так зачем же потворствовать заблуждению и считать логичной и разумной дискриминацию людей, гражданство которых отличается от гражданства законодателей? Логика подсказывает, что, если правительства искренне стремятся предупреждать проявления терроризма и бороться с ними, они должны искоренять коренные причины этой проблемы, такие как радикализация. Представляется, что, направляя гораздо большие ресурсы на противодействие радикализации и на долгосрочные адресные меры слежения и внедрение осведомителей в террористические ячейки, можно добиться гораздо большего, чем политикой жестов. Демонстрировать бескомпромиссность по вопросам безопасности, легитимизируя зачастую бесполезные, очень дорогостоящие и совершенно несоразмерные меры, ущемляющие право на неприкосновенность частной жизни – и не только это право – огромного числа людей, это совсем не то, что следует делать правительствам.

56. Специальный докладчик со всей ответственностью заявляет, что было бы гораздо более целесообразным и эффективным и послужило бы примером для остального мира, если законодательство Соединенных Штатов было бы приведено в соответствие с принципами, недавно сформулированными в Европе Европейским судом по правам человека в решении по делу *Захаров против России* и Европейским судом в решении по делу *«Теле 2 Сверддж АБ» против Шведского почтового и телекоммуникационного агентства*, которые сводятся к тому, что основным аргументом в пользу проведения целенаправленной слежки является наличие разумных подозрений, а не гражданство человека. Если спецслужбы и разведывательные или правоохранительные органы могут продемонстрировать обоснованное подозрение, то судебный ордер, разрешающий слежку, должен выдаваться независимо от того, паспорт какой страны имеет подозреваемое лицо. Ключевым фактором является фактор риска, и действовать нужно так, чтобы управлять соответствующим риском. Если какое-либо лицо явно представляет определенный риск, то за ним должна быть орга-

низована полномасштабная слежка, независимо от того, какой у него паспорт. Гарантии против неоправданных обысков и задержаний – в данном случае такой гарантией является судебный ордер – также целесообразно применять, независимо от того, какой паспорт имеет подозреваемое лицо. Во Всеобщей декларации прав человека совершенно справедливо не говорится о том, что правом на неприкосновенность частной жизни обладают одни только граждане Соединенных Штатов. Напротив, в Декларации говорится, что право на защиту закона от такого вмешательства или таких посягательств имеет каждый человек (см. статью 12); по мнению Специального докладчика, речь идет в том числе и о законе Соединенных Штатов. Таким образом, у законодателей Соединенных Штатов имеется возможность показать пример всему миру, следуя букве и духу Всеобщей декларации прав человека, и принять конкретные меры к тому, чтобы законодательство Соединенных Штатов действительно уважало универсальный характер права на неприкосновенность частной жизни, внося для этого в Закон о неприкосновенности сообщений, отправляемых по электронной почте, надлежащие поправки, смысл некоторых из которых излагается в общем виде ниже.

57. Право на неприкосновенность частной жизни, так же как право на свободу от пыток и многие другие права, является одним из основных прав человека, а также универсальным правом. Это означает, что право на неприкосновенность частной жизни имеет каждый человек, независимо от того, где он находится, какой у него паспорт и каковы цвет его кожи, вероисповедание, этническое происхождение, политические взгляды или сексуальная ориентация. Это именно то, что Специальный докладчик призывает подтвердить Сенат Соединенных Штатов. Довольно часто правительства Соединенных Штатов стремились наказать нарушителей прав человека в других странах, зачастую выступая инициаторами «красных линий» и санкций, призванных повысить шансы на соблюдение таких прав. Устранив различия между гражданами Соединенных Штатов и других стран и распространив гарантии права на неприкосновенность частной жизни на граждан всех стран мира, Сенат внес бы ощутимый вклад в укрепление универсальности основного права человека на неприкосновенность частной жизни и одновременно нанес бы чувствительный удар по ксенофобским тенденциям в законодательской деятельности. Кроме того, такая позиция Сената полностью соответствовала бы законодательству Европейского союза и Совета Европы по вопросам защиты данных и права на неприкосновенность частной жизни, в котором не проводится никаких различий между правами на неприкосновенность частной жизни граждан и неграждан.

Каким образом можно улучшить защиту права на неприкосновенность частной жизни инструментами национального и международного права

58. Если в предыдущих рекомендациях речь шла в основном о возможностях защиты универсальности права на неприкосновенность частной жизни в национальном праве, то в нескольких следующих пунктах речь пойдет о том, как дополнить национальные меры инструментами международного права.

59. В связи с Законом Соединенных Штатов о неприкосновенности сообщений, отправляемых по электронной почте, в его нынешней редакции возникает еще один серьезный вопрос, поскольку неясно, относятся ли гарантии, усиливаемые этим законом, также и к электронным данным, где бы они ни хранились – в Соединенных Штатах или в любом другом месте. Эту проблему можно проиллюстрировать на примере судебного дела, в котором компания «Майкрософт» оспаривала законность выдачи американскими властями ордера на проверку данных, хранящихся за пределами Со-

единенных Штатов²⁸. Легко понять, почему «Майкрософт» не хотел разрешать доступ к данным, которые хранятся за пределами Соединенных Штатов. Это не только угрожало конкурентоспособности продукции «Майкрософт» во всем мире, но и создавало чрезвычайно опасную проблему, – как реагировать на всевозможные запросы самых разных правительств, требующих предоставления данных. Проблема касается не только компании «Майкрософт». Большинству других технологических гигантов этой отрасли, преимущественно с американскими корнями, таким как «Гугл», «Фейсбук», «Эппл» и «Твиттер» (и многим другим), ежегодно приходится получать от правительств самых разных стран мира тысячи запросов с требованиями предоставить доступ к данным.

60. Если Конгресс Соединенных Штатов желает добиться разумного прогресса на этом направлении и принять решение, полностью соответствующее основополагающим принципам прав человека и не ставящее американские фирмы в коммерчески невыгодное положение, он должен осознать, что в данной ситуации невозможно найти решение исключительно в рамках национального права. Он также должен отдавать себе отчет в том, что в данной конкретной области права такие инструменты, как соглашения взаимной правовой помощи, которые существуют уже много десятилетий, не отличаются особой эффективностью. Конгресс должен признать, что, хотя с заключением Конвенции о киберпреступности в некоторых областях удалось добиться серьезного прогресса, достигнутые договоренности пока не сделали трансграничную передачу данных и доступ к данным, необходимым для проведения следственных действий, столь быстрым и беспроblemным, как хотелось бы некоторым. Одна из основных причин этого относительного провала заключается в том, что в основу Конвенции во многом лег менталитет суверенных национальных государств XIX, а не реалии безграничного Интернета XXI века. Хотя Конвенция, вероятно, может служить хорошим примером того, какие результаты могут быть достигнуты «детскими шажками», и с ее заключением, безусловно, были достигнуты некоторые успехи, в том числе в отношении идентификации и кодификации преступлений, совершаемых с использованием компьютерных технологий и Интернета, она не оправдала ожиданий в том, что касается своевременной трансграничной передачи личных данных, пригодных для выявления, расследования и предупреждения преступлений в век Интернета. Одна из возможных причин этого заключается в том, что не был сделан еще один шаг – шаг к созданию такого механизма, как международный орган, который был бы наделен функцией и необходимыми полномочиями выдавать разрешения на международный доступ к электронным данным.

61. Аналогично тому, как в других областях международного права были приняты решения о создании агентств, в задачи которых входит укрепление доверия и осуществление конкретных гарантий в самых разных областях, таких как морское право, космическое право, ядерное оружие, химическое оружие и т.д., Конвенция о киберпреступности в tandem с другими многосторонними договорами, в том числе с теми, которые преследуют схожие цели, может быть дополнена с целью создания международного органа, наделенного полномочиями выдавать эквиваленты международных ордеров на проведение слежки или на доступ к данным, которые подлежали бы обязательному исполнению в киберпространстве. Страны, подписывающие такой новый договор или дополнительный протокол, могли бы предоставить своих собственных независимых судей для работы в составе

судейской коллегии, которая, действуя по принципу «одного окна», выдавала бы соответствующие судебные ордера, снабженные правовой санкцией на меж-

²⁸ См. blogs.microsoft.com/on-the-issues/2016/07/14/search-warrant-case-important-decision-people-everywhere/#sm.0019d8sjw1492dnr7k1yawh09b46.

дународном уровне – в странах – участницах соответствующего договора. Возвращаясь к ранее упомянутому примеру решения, принятого в июле 2016 года по делу «Майкрософт», следует отметить, что в новой ситуации таким компаниям, как «Майкрософт», «Гугл», «Фейсбук», «Амазон», «Эппл», и другим технологическим гигантам, располагающим центрами обработки данных в разных странах, не пришлось бы беспокоиться по поводу того, что какое-либо государство выйдет за пределы своих границ, а пришлось бы иметь дело с международным ордером на доступ к данным, выданным на основании разумных подозрений в соответствии с понятной нормой международного права. При этом граждане самых разных стран мира могли бы быть уверенными в том, что их право на неприкосновенность частной жизни, равно как и другие права, такие как право на свободу выражения мнений и на свободу ассоциаций, защищены надлежащими гарантиями в равной степени и повсеместно. Если серьезно стремиться к универсальности права на неприкосновенность частной жизни, то следует исходить из того, что прогресс на этом направлении может быть достигнут при наличии механизмов, которые были бы одновременно международными и универсальными, применяющими одни и те же стандарты и гарантии по всему миру.

62. Это не утопия. Это подход, основанный на холодном расчете и учете реалий нашей жизни, отличающий истинные демократии от государств, которые стремятся использовать Интернет главным образом как средство социального контроля и удержания властных полномочий в пределах своей собственной юрисдикции. Этот подход может быть также увязан с другими инициативами, направленными на защиту киберпространства, с которыми недавно выступили президент и главный юрист компании «Майкрософт»²⁹.

63. Имеющаяся на сегодняшний день в распоряжении Специального докладчика информация свидетельствует о том, что ряд государств, в том числе даже некоторые ведущие демократии, к сожалению, относятся к Интернету с позиций собственной выгоды, рассматривая его как сферу, в которой их национальные правоохранительные органы, и в первую очередь их органы безопасности и разведывательные службы, могут оперировать относительно беспрепятственно, перехватывая данные и взламывая миллионы устройств (смартфонов, планшетов, ноутбуков и серверов) по всему миру. При этом 15–25 государств рассматривают Интернет как свою собственную игровую площадку, на которой они могут бороться за добычу, всегда стремясь выйти победителями, идет ли речь о кибервойне, о шпионаже и контрразведке или о промышленном шпионаже. Перечень мотивов, которыми они руководствуются, является очень длинным; в то же время остальные примерно 175 стран мира взирают на происходящее беспомощно, будучи не в состоянии как-то повлиять на происходящее. Им лишь остается надеяться, что в киберпространстве так или иначе воцарится мир.

64. Если говорить начистоту, представители ничтожного меньшинства стран активно пытались неофициально повлиять на Специального докладчика, с тем чтобы он отказался от поиска возможных решений в этой области, но он считает своим долгом сообщить, что, похоже, это были единственные люди, не желающие иметь гарантии и средства защиты в Интернете, обеспеченные международной правовой санкцией. Мне еще не приходилось встречать ни одной организации гражданского общества, ни одной корпорации, и даже ни одного здравомыслящего правоохранительного агентства или органа безопасности и разведки, которые не хотели бы видеть гарантии и средства защиты в Интернете более четкими и примени-

²⁹ См. www.itpro.co.uk/security/28134/how-can-nation-states-win-the-unfolding-cyberwar?_mout=1&utm_campaign=newsletter&utm_medium=email&utm_source=newsletter&tpid=109380765640.

мыми на универсальной основе; при этом они могут не верить в то, что этого можно достичь в недалекой перспективе.

65. Единственным возможным способом добиться упомянутой четкости и внедрения гарантий и средств защиты таким образом, чтобы обеспечить их своевременное, беспристрастное и надлежащее применение, является заключение многосторонних соглашений на принципах международного права. Миру нужны не новые налеты на Интернет, спонсорами которых выступают государства, а рациональное цивилизованное соглашение относительно надлежащего поведения государств в киберпространстве, что возвращает нас к вопросу о слежке.

66. Некоторые из упомянутых выше усовершенствованных международных механизмов весьма пригодились бы для правоприменительной работы в киберпространстве, которая в настоящее время регулируется Конвенцией о киберпреступности. Однако, как это следует из самого ее названия, Конвенция, к которой к настоящему времени присоединились примерно 25% государств – членов Организации Объединенных Наций, регулирует только вопросы, относящиеся к сектору уголовного правосудия. Конвенция не касается вопросов национальной безопасности или слежки, осуществляемой по соображениям национальной безопасности. Иными словами, те виды деятельности, о которых сообщил Эдвард Сноуден, лежат за пределами сферы действия Конвенции, и для того, чтобы обеспечить их удовлетворительное регулирование, пришлось бы значительно расширить охват Конвенции или заключить отдельный, но дополняющий Конвенцию договор, адекватно охватывающий вопросы слежки в киберпространстве. Такое решение было бы гораздо предпочтительнее ситуации, при которой ряд демократий, таких как Франция, Германия, Соединенное Королевство и Соединенные Штаты, наперегонки торопятся принять новые законы, регулирующие программы слежки, не изжив из своего менталитета унаследованные из XIX века концепции суверенного национального государства.

67. Хотя национализм и шовинизм, не говоря уже о популизме, как представляется, сегодня вновь оказались востребованными в рамках циклической поступи истории, их полезность для целей избирательных кампаний не следует путать с их эффективностью инструмента обеспечения подлинной безопасности как в национальных, так и в международных масштабах. Следует признать – даже политическим деятелям, обращающимся к национальной аудитории, – что подавляющее большинство государств-членов не заинтересовано в поощрении организованной преступной или террористической деятельности, независимо от того, где такая деятельность имеет место и кто является ее автором. Иными словами, если представить, что следователю из Бельгии приходится обращаться к международной коллегии, в состав которой входят судьи, например, из таких случайно пришедших на ум стран, как Бразилия, Гана, Германия, Индия, Соединенное Королевство, Соединенные Штаты и Франция, едва ли можно опасаться, что эта или аналогичная коллегия, составленная для соответствующих целей, не выдаст ордер на доступ к данным о лице, в отношении которого были представлены обоснованные подозрения. Если в результате этого процесса будет выдан международный ордер на доступ к данным, это значительно упростит жизнь правительствам и корпорациям, находящимся под юрисдикцией государств, согласившихся на создание такого механизма в рамках международного договора.

68. Правовой инструмент такого рода не следует путать со всеохватывающим договором о регулировании Интернета, который некоторые окрестили «Женевской конвенцией об Интернете». Существует много других аспектов управления Интернетом, которых не коснулись бы положения правового документа, регулирующего слежку в киберпространстве, в том числе очень важная, но зачастую упускаемая из виду вторая часть статьи 12 Всеобщей декларации прав человека и статья 17 Международного пакта

о правах человека. Эти положения касаются права на защиту репутации, которое представляет собой самостоятельное право, хотя и близкое по смыслу к праву на неприкосновенность частной жизни.

Когда степень проработки некоторых мер в области международного права, касающихся, в частности, правовых инструментов, регулирующих деятельность по ведению слежки, может выйти на тот уровень, когда их было бы полезно вынести на обсуждение в более широком формате

69. Обобщая вышесказанное, можно сказать, что правовой инструмент, регулирующий слежку в киберпространстве, дополнил бы другие элементы существующего законодательства, регулирующего киберпространство, в частности Конвенцию о киберпреступности, и сыграл бы важную роль в обеспечении конкретных гарантий права на неприкосновенность частной жизни в Интернете. К счастью для мандата Специального докладчика, при поддержке Европейского союза уже осуществляется проект по проработке альтернативных методов обеспечения неприкосновенности частной жизни, собственности и управления Интернетом (проект МАППИНГ), в рамках которого в настоящее время рассматриваются возможные варианты документа, который регулировал бы слежку в киберпространстве. Уже существует проект текста соответствующего договора, который находится на обсуждении экспертов гражданского общества и ряда крупных международных корпораций; ожидается, что документ будет обнародован в течение 2017 года и, несомненно, до весны 2018 года. На данном начальном этапе рассмотрения возможных вариантов текста было бы преждевременным, в том числе и Специальному докладчику, высказывать свою позицию по этому или по аналогичному документу. В то же время для правительств этот текст может стать в конечном счете полезной отправной точкой для дискуссий в рамках межправительственных организаций, в том числе и, возможно, в первую очередь в Организации Объединенных Наций.

70. По аналогии с подготовкой Специального докладчика к дискуссиям по этому вопросу, в частности в период между мартом и июлем 2018 года, было бы разумным, чтобы национальные парламенты – и электорат стран, в которых в 2017 и 2018 годах запланировано проведение выборов, – дали поручения соответствующим подразделениям исполнительной власти активно изучать варианты надлежащего регулирования слежки в киберпространстве, а также гарантий и средств защиты, обеспечивающих неприкосновенность частной жизни. Это не только имело бы прямую ценность для граждан всего мира, но и послужило бы четким сигналом для тех государств, демократий, псевдо-демократий и недемократических государств, которые ошибочно считают, что с киберпространством лучше всего иметь дело, заявив о суверенитете над отдельными сегментами Интернета или над той информацией, которую граждане получают в нем. Права человека носят универсальный характер, и законодательство, регулирующее киберпространство, должно быть таким, чтобы обеспечивать защиту не только права на неприкосновенность частной жизни, но и других основных прав человека.

71. Какими бы трудными не были эти задачи, они имеют решение; действительно, реально и разумно предположить, что значительное число государств в конечном счете объединится вокруг правового документа, который будет регулировать программы слежки и защищать неприкосновенность частной жизни в киберпространстве. Это было бы благом для граждан, для правительств, для частной жизни и для бизнеса. Число государств, объединяющихся вокруг новых принципов и новых механизмов, может постепенно расти и достичь критической массы. Именно этот урок мы усвоили, наблюдая за развитием международного права в течение нескольких последних столетий. Нет никаких оснований игнорировать этот урок, когда речь идет о частной жизни, слежке и киберпространстве. Вполне вероятно, что в течение срока своего мандата действующий Специальный докладчик

не дождется конкретных результатов, но, по крайней мере, этот путь, возможно, является самым многообещающим. Все, что узнал Специальный докладчик за время осуществления своего мандата, убеждает его в том, что, когда для этого созреют необходимые условия, лучше всего пойти именно этим путем. Такое время может наступить раньше, чем думают многие.
