Организация Объединенных Наций A/69/397

Генеральная Ассамблея

Distr.: General
23 September 2014
Russian
Original: English

Шестьдесят девятая сессия
Пункт 69(a) предварительной повестки дня
Поощрение и защита прав человека:
Осуществление документов по правам человека

Поощрение и защита прав человека и основных свобод в условиях борьбы с терроризмом*

Записка Генерального секретаря

Генеральный секретарь имеет честь препроводить Генеральной Ассамблее доклад Специального докладчика по вопросу о поощрении и защите прав человека и основных свобод в условиях борьбы с терроризмом Бена Эммерсона, представленный в соответствии с резолюцией 68/178 Генеральной Ассамблеи и резолюцией 15/15 Совета по правам человека.

* Позднее представление.

14-61490 X (R) 151014 151014

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

Резюме

Настоящий доклад является четвертым по счету ежегодным докладом, представленным Генеральной Ассамблее нынешним Специальным докладчиком по вопросу о поощрении и защите прав человека и основных свобод в условиях борьбы с терроризмом Беном Эммерсоном.

Основные мероприятия, осуществленные Специальным докладчиком в период с 17 декабря 2013 года по 31 июля 2014 года, перечислены в разделе II настоящего доклада. В разделе III Специальный докладчик оценивает применение массового цифрового слежения для целей борьбы с терроризмом и рассматривает последствия применения технологии широкомасштабного доступа для права на неприкосновенность личной жизни, предусмотренного Статьей 17 Международного пакта о гражданских и политических правах.

I. Введение

1. Настоящий доклад представляется Специальным докладчиком по вопросу о поощрении и защите прав человека и основных свобод в условиях борьбы с терроризмом Беном Эммерсоном в соответствии с резолюцией 66/178 Генеральной Ассамблеи и резолюциями 15/15, 19/19, 22/8 и 25/7 Совета по правам человека. В нем отражена деятельность Специального докладчика в период с 17 декабря 2013 года по 31 июля 2014 года. Далее в нем оценивается использование массового цифрового слежения для целей борьбы с терроризмом и рассматриваются последствия применения технологии широкомасштабного доступа для права на неприкосновенность личной жизни в соответствии со Статьей 17 Международного пакта о гражданских и политических правах (МПГПП).

II. Деятельность, связанная с мандатом

2. 13 февраля 2014 года Специальный докладчик принял участие в качестве выступающего в дискуссии «Дебаты Кади II: Омбудсмен Организации Объединенных Наций против судебного контроля в процессе принятия Советом Безопасности решений о санкциях» в Лондонской школе экономики (ЛШЭ), Соединенное Королевство.

3. С 23 по 25 февраля 2014 года Специальный докладчик принимал участие в семинаре экспертов на тему «Право на неприкосновенность личной жизни в цифровой век», организованном в Женеве, Швейцария, Постоянными представительствами Австрии, Бразилии, Германии, Лихтенштейна, Мексики, Норвегии и Швейцарии при содействии со стороны Женевской академии международного гуманитарного права и прав человека.

4. 11 марта 2014 года Специальный докладчик представил свой доклад по вопросу использования беспилотных летательных аппаратов, или дронов, в ходе экстерриториальных антитеррористических смертоносных операций, в том числе в рамках асимметричного вооруженного конфликта, и воздействия такого использования на гражданское население (A/HRC/25/59) двадцать пятой сессии Совета по правам человека. Он также имел интерактивный диалог с Советом относительно своих страновых миссий в Буркина-Фасо (A/HRC/25/59/Add.1) и Чили (A/HCR/25/59/Add.2).

5. 12 марта 2014 года Специальный докладчик принял участие в дискуссии на тему «Права человека и дроны» и провел пресс-конференцию на двадцать пятой сессии Совета по правам человека.

III. Борьба с терроризмом и массовое цифровое слежение

A. Введение и обзор

6. Наблюдающийся за последнее десятилетие бурный рост технологических возможностей государств повысил способность разведывательных и правоохранительных органов вести целевое слежение за находящимися под подозрением лицами и организациями. Перехват сообщений представляет собой цен-

ный источник информации, с помощью которой государства могут расследовать, предотвращать и подвергать преследованию террористические акты и другие серьезные преступления. Большинство государств в настоящее время имеют технические средства для перехвата и мониторинга телефонных разговоров, совершаемых по проводной и мобильной связи, что позволяет определять местоположение лиц, отслеживать их передвижения посредством анализа информации с узлов связи, а также читать и записывать их текстовые сообщения. Целевое слежение также дает возможность разведывательным и правоохранительным органам осуществлять мониторинг онлайновых действий конкретных лиц, проникать в базы данных и программы облака и получать хранящуюся там информацию. Все больше государств начинает пользоваться системами малвер, с помощью которых можно проникать в компьютер или смартфон конкретного лица, изменять их настройки и вести мониторинг осуществляемой на них деятельности. Сообща эти формы слежения обеспечивают получение разнообразных данных из различных источников, что позволяет сформировать ценные сведения о конкретных лицах или организациях.

7. Общей чертой этих методов слежения является то, что они зависят от наличия предварительных подозрений в отношении конкретного лица или организации. В таких случаях почти во всех государствах применяется практика получения какого-либо предварительного разрешения (судебного или исполнительного), а в некоторых государствах имеется еще и дополнительный независимый анализ *ex post facto*. Таким образом, в большинстве государств имеется, по крайней мере, одна возможность (а иногда и более чем одна) тщательно изучить ту информацию, которая предположительно должна вызвать подозрение, и оценить соразмерность применяемых мер слежения фактам по конкретному случаю. При целевом слежении имеется возможность объективно оценить необходимость и соразмерность предполагаемого слежения, взвесив масштабы предлагаемого вмешательства в личную жизнь в сравнении с предполагаемой пользой для конкретного расследования.

8. Однако динамичное развитие технологий позволило некоторым государствам получить широкомасштабный доступ к средствам коммуникации и передаваемым данным без необходимости наличия предварительных подозрений. Соответствующие органы в этих государствах теперь могут использовать алгоритмы автоматического «отбора данных» для прочесывания потенциально безграничного мирового трафика обмена информацией. Устанавливая считывающие устройства на оптоволоконные кабели, через которые передается основная масса цифровых данных, соответствующие государства могут осуществлять широкомасштабное слежение за передаваемой информацией и метатданными, обеспечивая разведывательным и правоохранительным органам возможность вести мониторинг и записывать сообщения не только своих собственных граждан, но и граждан, находящихся в других странах. Эта возможность обычно подкрепляется наличием законов об обязательном сохранении данных, согласно которым провайдеры услуг телекоммуникации и интернета обязаны сохранять передаваемые данные для последующей проверки и анализа. С помощью сканирующих программ, критериев профилирования и определенных сигнальных терминов соответствующие органы могут впоследствии отфильтровать огромные объемы хранящейся информации, чтобы выявить коммуникационные модели в общении отдельных лиц и организаций. Алгоритмы автоматического отбора данных связывают простые имена, места нахождения, номера и IP-

адреса и ищут совпадения, пересечения данных географического местоположения и схожие модели в социальных и других онлайновых средствах общения[1].

9. Таким образом, государства, обладающие большими возможностями проникновения в сети интернета, могут получать доступ к содержанию телефонных и электронных сообщений безграничного числа пользователей и осуществлять надзор за интернет-деятельностью по конкретным сайтам. Все это возможно делать без необходимости иметь какие-либо предварительные подозрения в отношении конкретных лиц или организаций. Сообщения буквально каждого пользователя интернета потенциально открыты для инспекции со стороны разведывательных и правоохранительных органов заинтересованных государств. Это означает систематическое вмешательство в осуществление права на неприкосновенность личной жизни в сфере коммуникаций и требует наличия соответствующего убедительного оправдания.

10. С правоохранительной точки зрения, ценность технологии массового слежения определяется самим фактом того, что она позволяет следить за сообщениями тех лиц и организаций, которые ранее не попадали в поле зрения соответствующих органов. Для общества ценность технологии широкомасштабного доступа заключается как раз в том, что она не требует наличия предварительных подозрений. Противодействовать круговому характеру этой логики можно, лишь подвергая практику государств в этой сфере тщательному анализу, в соответствии со Статьей 17 Международного пакта о гражданских и политических правах.

11. Статья 17 Пакта предусматривает, что любое вмешательство в неприкосновенность личной корреспонденции должно быть санкционировано законом и должно быть необходимым и соразмерным средством достижения законных целей государственной политики[2]. Предотвращение террористических актов в этом отношении, несомненно, может считаться законной целью[3], но деятельность разведывательных и правоохранительных органов в этой сфере все же не должна нарушать международное право в области прав человека[4]. Одно лишь заявление — без детализирования — о том, что технология массового слежения может помочь в подавлении и преследовании террористических актов, не является адекватным оправданием его применения, с точки зрения правовых норм в области прав человека. Тот факт, что что-либо является технически возможным и что оно может иногда обеспечить получение полезной информации, сам по себе не означает, что оно является обоснованным или законным (по нормам международного и национального права)[5].

12. Международное право в области прав человека требует, чтобы государства представляли четкие, обоснованные причины для любого вмешательства в

---

[1] http://blog.privacystrategy.eu/public/published/Submission_ISC_7.2.2014_-_Caspar_Bowden.pdf.

[2] См. пункты 28–31 ниже.

[3] См. пункты 33–34 ниже.

[4] См. Подборку оптимальных практических методов, применяемых в отношении законодательной и институциональной основы и мер, которые обеспечивают соблюдение прав человека специальными службами в условиях борьбы с терроризмом, в том числе касающихся надзора за их деятельностью, опубликованную бывшим Специальным докладчиком (A/HRC/14/46, пункты 9–50).

[5] A/HRC/27/37 пункт 24.

личную жизнь, будь то на индивидуальном или массовом уровне. Основная аксиома соразмерности заключается в том, что чем сильнее нарушение подлежащих защите прав человека, тем более убедительным должна быть оправданность, чтобы соответствовать требованиям Пакта. Суровая правда состоит в том, что применение технологии массового слежения практически сводит на нет право на неприкосновенность всякой корреспонденции по интернету. Позволяя широкомасштабный доступ ко всему трафику цифровых сообщений, такая технология уничтожает возможность любого анализа индивидуализированной соразмерности. Она позволяет осуществлять вмешательство в личную корреспонденцию без независимой (или какой-либо другой) предварительной санкции, основанной на подозрениях в отношении конкретного лица или организации. Таким образом, проверка *ex ante* возможна лишь в крайней степени обобщения.

13. Ввиду отсутствия поцелевого оправдания применения мер массового слежения, соответствующие государства должны дать объяснения общей практике стремления получить широкомасштабный доступ к средствам цифровой связи. Анализ соразмерности мер, таким образом, сдвигается от микроуровня (оценка оправданности вмешательства в личную жизнь конкретного лица или организации) до макроуровня (оценка оправданности применения системы, предусматривающей широкомасштабное вмешательство в осуществление индивидуальных и коллективных прав на личную жизнь всех пользователей интернета). Сам масштаб вмешательства в осуществление прав на личную жизнь требует соразмерного оправдания в плане государственной политики.

14. В качестве абсолютного минимума, Статья 17 требует от государств, использующих технологию массового слежения, предоставлять обществу значимые отчеты о существенных преимуществах, которые дает ее применение. Без такого оправдания просто нет никаких средств, чтобы определить, насколько эта распространяющаяся государственная практика соответствует требованиям Пакта. Оценка соразмерности мер в этом контексте требует достижения равновесия между интересами общества в плане защиты неприкосновенности личной жизни онлайн, с одной стороны, и несомненной необходимостью принятия эффективных мер борьбы с терроризмом и охраны правопорядка, с другой. Чтобы определить уровень такого равновесия, необходимо, чтобы внутри государств и между ними была организована соответствующая обоснованная дискуссия. Международное сообщество должно честно признать эту революцию в нашем коллективном понимании взаимоотношений между человеком и государством[6]. Для любой оценки законности этих мер необходимо, чтобы государства, использующие эту технологию, были прозрачны в отношении своих методов и их оправданности[7]. Иначе существует опасность того, что система-

[6] Как было отмечено американским Советом по наблюдению за гражданскими свободами и правами человека на частную жизнь: «Дозволение правительству в плановом порядке собирать информацию о звонках по всей стране кардинально меняет равновесие власти между государством и его гражданами»; *Доклад по Программе записи телефонных переговоров, осуществлявшейся в соответствии с Разделом 215 Закона «ПАТРИОТ США», и по операциям Суда по надзору за деятельностью иностранных спецслужб.*

[7] В ее докладе по Праву на неприкосновенность личной жизни в цифровой век (A/HRC/27/37, пункт 48) Верховный комиссар по правам человека отметила «вызывающую тревогу непрозрачность деятельности правительства, относящейся к политике, законодательному подкреплению и практике слежения, что сводит на нет любые усилия по

тическое нарушение безопасности цифровой связи продолжит нарастать без сколько-нибудь серьезного учета последствий масштабного отказа от неприкосновенности личной корреспонденции в интернете. Если использующие эту технологию государства будут сохранять монополию на информацию о ее воздействии, то будет превалировать некая форма концептуальной цензуры, не позволяющая вести обоснованную дискуссию.

15. Некоторые люди выдвигают аргумент, что, прежде всего, пользователи интернета не могут реально рассчитывать на неприкосновенность личной жизни и должны предполагать, что их сообщения доступны для контроля со стороны как отдельных учреждений, так и государства. Сторонники этого взгляда проводят классическую аналогию между отправкой незашифрованного электронного послания и отправкой почтовой открытки. Какими бы ни были преимущества такого сравнения, оно не дает ответа на ключевой вопрос о законности, необходимости и соразмерности. Сама цель содержащегося в Пакте требования о наличии исчерпывающего, открытого для общества законодательства, регулирующего вмешательство государства в сфере коммуникаций, состоит в том, чтобы позволить отдельным лицам знать об объеме тех прав неприкосновенности личной жизни, которые они в действительности имеют, и предвидеть те обстоятельства, при которых их сообщения могут проверяться[8]. Однако ценность этой технологии в качестве средства борьбы с терроризмом и охраны правопорядка обусловлена тем фактом, что пользователи интернета полагают, что их сообщения являются конфиденциальными (иначе не было бы смысла несанкционированно их отслеживать). Об этом свидетельствуют высказывания представителей спецслужб Соединенных Штатов и Соединенного Королевства, утверждающих, что раскрытие этой информации нанесло ущерб национальной безопасности, так как насторожило потенциальных террористов в отношении того факта, что их сообщения отслеживаются[9].

16. При любой оценке соразмерности также необходимо в полной мере учитывать тот факт, что интернет представляет собой повсеместное средство общения для миллионов людей во всем мире. Революция в сфере цифровых технологий привела к гигантским переменам в том, как мы общаемся друг с другом. Технологии цифровой связи, использующие интернет (включая переносные устройства и смартфоны), стали частью повседневной жизни[10]. Теперь любой, кто желает участвовать в обмене информацией и идеями в современном мире, вынужден использовать транснациональные технологии цифровой связи. Трафик интернета зачастую проходит через серверы, расположенные в иностранных юрисдикциях. Утверждение о том, что пользователи добровольно отказались от своего права на неприкосновенность личной жизни, абсолютно не обосновано[11]. Один из общих принципов международного права прав человека предусматривает, что человек может считаться отказавшимся от основополагающего права человека, только выразив четкое, однозначное желание сделать

оценке их соответствия международному праву прав человека и по обеспечению подотчетности».

[8] См. пункты 35–39 ниже.

[9] http://abcnews.go.com/Blotter/intel-heads-edward-snowden-profound-damage-us-security/story?id=22285388; http://www.itv.com/news/2013-10-09/the-damage-of-edward-snowdens-revelations/.

[10] A/HRC/27/37 пункт 1.

[11] A/HRC/27/37 пункт 18.

это, на добровольной основе и будучи в полной мере информированным. В нынешнем мире цифровых технологий одно лишь использование интернета в качестве средства личной связи не может логически считаться осознанным отказом от права на неприкосновенность личной жизни согласно Статье 17 Пакта.

17. Интернет не является чисто публичным пространством. Он состоит из многих слоев частных, а также социальных и публичных областей[12]. Те, кто осознанно используют социальные медиа-платформы, где сообщения помещаются в открытом публичном доступе, со всей очевидностью не могут ожидать сохранения неприкосновенности личной жизни. Аналогия с почтовыми открытками абсолютно противоположна распространению информации через публичные сети Твиттера и Фейсбука, например, или постингу на общественных интернет-сайтах. Однако чтение чужих почтовых открыток не является аналогией, противоположной перехвату частных сообщений по электронной почте, закодированных или нет.

18. Таким образом, если допустить, что законное право на неприкосновенность личной жизни в сфере цифровых коммуникаций сохраняется (а это невозможно оспаривать)[13], применение технологий массового слежения, несомненно, посягает на саму сущность этого права[14]. Это потенциально противоречит основополагающему принципу о том, что государства, посягая на защищаемые права человека, должны применять наименее интрузивные из существующих методов[15]; это исключает оценку какой-либо индивидуализированной соразмерности[16]; и оно обставлено различными заявлениями о секретности, что делает крайне сложным любой другой вид анализа соразмерности[17]. Государства, прибегающие к массовому слежению, пока не смогли представить подробных, основанных на реальных фактах оправданий для этого, и почти ни одно государство не приняло четких национальных законов, санкционирующих его применение[18]. С точки зрения Статьи 17 Пакта, это очень близко к полному отказу от права на неприкосновенность личной жизни в сфере цифровых коммуникаций. По всем этим причинам массовое отслеживание цифрового контента и коммуникационных данных представляет собой серьезный вызов для установленных норм международного права. По мнению Специального докладчика, само существование программ массового слежения является потенциально диспропорциональным нарушением права на неприкосновенность личной жизни[19]. Говоря коротко, для государств несовместимо с существующими концепциями неприкосновенности личной жизни постоянно и недискриминационно собирать всю передаваемую информацию и метаданные. Сама суть права на неприкосновенность личной жизни в сфере корреспонденции

---

[12] http://blog.privacystrategy.eu/public/published/Submission_ISC_7.2.2014_-_Caspar_Bowden.pdf.

[13] См. Резолюцию **68/167** Генеральной Ассамблеи.

[14] См. пункты 51–52 ниже.

[15] См. пункт 51 ниже.

[16] См. пункт 52 ниже.

[17] См. пункты 51–52 ниже.

[18] См. пункт 37 ниже.

[19] См. также мнение Верховного комиссара по правам человека, A/HRC/27/37, пункты 20 и 25.

подразумевает, что его нарушения должны носить исключительный характер и быть должным образом оправданы в каждом конкретном случае[20].

19. Для такого рода практики может требоваться оправданный борьбой с терроризмом радикальный пересмотр прав на неприкосновенность личной жизни в интернете. Однако заявления в пользу полной отмены права на неприкосновенность личной жизни в интернете пока не делались публично соответствующими государствами, и такие аргументы не подвергались тщательному рассмотрению и обсуждению. Угроза терроризма может быть оправданием для массового слежения лишь в том случае, если применяющее эту технологию государство способно детально продемонстрировать полученные в результате этого применения существенные преимущества в борьбе с терроризмом. Более того, меры, оправдываемые ссылкой на обязанность государства обеспечивать защиту от угрозы терроризма, не должны использоваться в качестве «троянского коня», чтобы оправдать более широкие полномочия слежения для не относящихся к этой сфере правительственных функций. Постоянно существует угроза «размывания целей», когда оправдываемые борьбой с терроризмом меры предоставляются в распоряжение государственным органам для куда менее весомых, с точки зрения общественного интереса, целей[21]. В настоящем докладе Специальный докладчик развивает то, что было сделано его предшественником[22], бывшим Специальным докладчиком по вопросу о поощрении и защите права на свободу мнений и их свободное выражение[23]. Он считает, что сейчас на государствах, использующих технологии широкомасштабного доступа для слежения, лежит обязанность объяснить незамедлительно, четко и во всеуслышание, почему это широкомасштабное вмешательство в неприкосновенность личной жизни граждан оправдано для целей предотвращения терроризма и других серьезных преступлений.

B. Недавно обнародованная информация о характере и масштабах возможностей государств в плане цифрового слежения

20. 5 июня 2013 года одна из национальных газет Соединенного Королевства опубликовала содержание секретного судебного распоряжения, санкционированного Судом Соединенных Штатов по надзору за деятельностью иностранных спецслужб согласно Разделу 215 Закона «ПАТРИОТ США». Данное распоряжение, как сообщалось, требовало от одного из крупнейших провайдеров телекоммуникационной связи в Соединенных Штатах ежедневно передавать Агентству национальной безопасности все «телефонные метаданные» в течение трех месяцев и запрещало этой компании разглашать наличие такой просьбы или самого распоряжения. 6 июня 2013 года в одной американской газете был опубликован отдельный репортаж, раскрывающий существование цифровой программы Агентства национальной безопасности под названием «Призма». Эта программа, по сообщениям санкционированная согласно разделу 702 Закона о наблюдении в сфере иностранной разведки, предположительно зани-

[20] См. пункт 51 ниже.
[21] См. пункт 55 ниже.
[22] A/HRC/13/37.
[23] A/HRC/23/40.

малась сбором данных контента из центральных серверов девяти ведущих технологических компаний Соединенных Штатов.

21. По сообщениям этих обеих газет, полученные через «Призму» данные предоставлялись другим разведывательным учреждениям, включая Центр правительственной связи Великобритании (GCHQ). В дальнейшем также сообщалось о существовании отдельной программы по сбору данных под названием «Апстрим», которая, предположительно, перехватывает как телефонные, так и интернет-сообщения, проходящие через оптоволоконные кабели и инфраструктуру провайдеров услуг в Соединенных Штатах. Значительная часть интернет-трафика в мире проходит через серверы, физически расположенные в Соединенных Штатах.

22. Затем средства массовой информации сообщили, что в Директорате разведывательных систем Агентства национальной безопасности имеется отдел уязвимости программ, который занимается сбором информации в различных системах связи по всему миру. Сообщается, что Агентство использует особый интернет-механизм, «Квантум», позволяющий ему проникать в компьютер третьей стороны. Предположительно, применяемый метод предполагает установление секретного контроля (или «владения») над серверами в ключевых точках «хребта» интернета. Имитируя выбранные сайты (включая такие популярные сайты, как поисковая система Google), Квантум способен внедрить несанкционированную программу дистанционного управления в компьютеры и работающие от wifi устройства тех, кто посещает такие клонированные сайты (и у кого, конечно же, не будет никаких причин сомневаться в аутентичности сайта-клона). По оценкам экспертов по технологиям, такой метод способен перманентно нарушить секретность работы компьютера пользователя, гарантируя, что он будет постоянно предоставлять информацию для Агентства национальной безопасности в Соединенных Штатах.

23. В ответ на эти разоблачения исполнительные и законодательные органы власти Соединенных Штатов предприняли ряд шагов. Один из вопросов, который возник в результате всего этого процесса, заключается в различии отношения к тем, кто является гражданами Соединенных Штатов, и теми, кто таковыми не являются (даже если они находятся под территориальной юрисдикцией Соединенных Штатов). Ключевые события можно суммировать следующим образом:

a) 9 августа 2013 года президент Обама объявил о том, что он просил Совет по наблюдению за гражданскими свободами и правами человека на частную жизнь (PCLOB)[24] пересмотреть предпринимаемые усилия в области борьбы с терроризмом[25]. В конце августа 2013 года Совет поручил Директору национальной разведки и Генеральному прокурору обновить методы разведывательных служб по сбору, хранению и распространению информации, касающейся граждан Соединенных Штатов[26];

[24] PCLOB является независимым учреждением исполнительной власти и имеет полномочия рассматривать и анализировать антитеррористические операции и обеспечивать, чтобы они были уравновешены с необходимостью защищать право на личную жизнь и гражданские свободы: http://www.pclob.gov/.

[25] http://www.whitehouse.gov/the-press-office/2013/08/09/remarks-president-press-conference.

[26] http://www.pclob.gov/newsroom.

b) 12 декабря 2013 года назначенная президентом Группа по обзору представила свой доклад «Свобода и безопасность в современном мире», в котором содержался ряд существенных рекомендаций в отношении проведения реформы. В ответ на этот доклад 17 января 2014 года президент огласил некоторые предлагаемые законодательные и административные изменения[27]. Одновременно президентской администрацией была выпущена новая Президентская директива по политике («PPD-28»), направленная на укрепление мер по обзору деятельности радиоэлектронной разведки разведывательных органов, как в Соединенных Штатах, так и за их пределами[28];

c) 23 января 2014 года Совет по наблюдению за гражданскими свободами и правами человека на частную жизнь представил первый из двух докладов, в котором было выражено мнение большинства о том, что программа по телефонным метаданным противоречит внутреннему законодательству, поскольку раздел 215 Закона «ПАТРИОТ США» не дает достаточно оснований для оправдания ее применения[29]. 27 марта президент огласил новый комплекс предложений, чтобы прекратить применение существующей программы[30]. 22 мая 2014 года Палата представителей приняла Закон Соединенных Штатов о свободе, куда вошли некоторые предложения президента;

d) 2 июля 2014 года Совет по наблюдению за личными и гражданскими свободами и правами человека на частную жизнь представил второй доклад, где детально описывалось, как на практике осуществляются операции слежения в соответствии с Разделом 702 Закона о наблюдении в сфере иностранной разведки[31]. Тогда как основной заботой этого доклада была совместимость этих программ с уставными и конституционными требованиями Соединенных Штатов, Совет признал, что они также вызвали «важные, но сложные правовые и политические вопросы» в связи с отношением к лицам, не являющимся гражданами Соединенных Штатов[32]. Совет пришел к выводу, что применение права на неприкосновенность личной жизни к слежению в интересах национальной безопасности, которое осуществляется в одной стране и может отрицательно сказаться на жителях другой страны, не до конца «урегулировано» между государствами-участниками Международного пакта о гражданских и политических правах — заключение, о котором, как было сказано, свидетельствовали «непрекращающиеся горячие споры»[33].

24. Параллельно осуществлялся процесс обзора в Соединенном Королевстве. 10 июня 2013 года, в ответ на заявления о том, что GCHQ обошел закон Соединенного Королевства, применив программу «Призма» Агентства национальной безопасности для доступа к содержанию сообщений, к которым, по национальному законодательству, доступа не было, министр иностранных дел сделал за-

[27] http://www.washingtonpost.com/politics/full-text-of-president-obamas-jan-17-speech-on-nsa-reforms/2014/01/17/fa33590a-7f8c-11e3-9556-4a4bf7bcbd84_story.html.

[28] http://www.whitehouse.gov/the-press-office/2014/01/17/remarks-president-review-signals-intelligence.

[29] *Доклад по Программе записи телефонных переговоров, осуществлявшейся в соответствии с Разделом 215 Закона «ПАТРИОТ США», и по операциям Суда по надзору за деятельностью иностранных спецслужб.*

[30] http://www.whitehouse.gov/the-press-office/2014/03/27/fact-sheet-administration-s-proposal-ending-section-215- bulk-telephony-m.

[31] Доклад о программе слежения, используемой в соответствии с Разделом 702 Закона о наблюдении в сфере иностранной разведки (FISA).

[32] Там же, пункт 98.

[33] Там же, пункт 100.

явление в парламенте, отметив, что к любым сведениям, полученным от Соединенных Штатов и касающимся граждан Соединенного Королевства, «применимы надлежащие, принятые в Соединенном Королевстве уставные средства контроля и гарантии», включая соответствующие положения Закона о разведывательных службах 1994 года, Закона о правах человека 1998 года и Закона о правовом регулировании следственных полномочий 2000 года[34].

25. 21 июня 2013 года в средствах массовой информации появилось сообщение о наличии у GCHQ отдельной программы («Темпора»), в соответствии с которой, как утверждалось, на оптоволоконные кабели, соединяющие Соединенное Королевство и Соединенные Штаты, устанавливались перехватывающие устройства, чтобы облегчить считывание как метаданных, так и передаваемой информации. И в стенах парламента Соединенного Королевства, и вне их, задавались вопросы о том, дает ли современное законодательство для GCHQ законные полномочия на осуществление подобных операций и соответствуют ли они праву на неприкосновенность личной жизни, гарантированному Статьей 8 Европейской конвенции о правах человека[35]. Последующие обнародованные данные в основном касались роли созданной в рамках GCHQ Объединенной группы по исследованию угроз. Сообщалось, что это учреждение распространило компьютерный вирус «Посольский прием» для онлайновых секретных операций. Как сообщается, этот вирус способен самокодироваться и выступать в качестве «хамелеона», имитируя сообщения от других пользователей интернета.

26. Проведя предварительное расследование вмешательства GCHQ в передачу сообщений и данных контента, Комитет по разведке и безопасности (парламентский комитет, осуществляющий надзор за разведывательными органами)[36], сделал 17 июля 2013 года заявление. Принимая во внимание правовые рамки, определяющие параметры обмена информацией между GCHQ и его зарубежными коллегами, Комитет пришел к заключению, что никакие законы Соединенного Королевства нарушены не были и что действия GCHQ соответствовали его уставным обязанностям, как предусмотрено Законом о разведывательных службах 1994 года. Тем не менее, Комитет далее сделал заключение, что следует провести дополнительное расследование, чтобы выяснить, насколько действующие правила, регламентирующие доступ к закрытым частным сообщениям, адекватны, учитывая «сложное взаимодействие» между Законом о разведывательных службах 1994 года, Законом о правах человека 1998 года и Законом о правовом регулировании следственных полномочий 2000 года. 17 октября 2013 года Комитет по разведке и безопасности объявил, что намерен расширить свое расследование в связи с той озабоченностью, которая высказывается по поводу расширения возможностей разведывательных служб и негативного влияния их операций на право неприкосновенности личной жизни[37].

27. 8 апреля 2014 года Суд Европейского Союза огласил свое решение по делу «*Права в сфере цифровой связи: Ирландия*», где он заявил, что Директива Европейского Союза об удержании информации несовместима с правом на

[34] https://www.gov.uk/government/speeches/foreign-secretary-statement-to-the-house-of-commons-gchq.
[35] http://www.theguardian.com/uk-news/2013/oct/14/conservative-peer-spying-gchq-surveillance; http://www.publications.parliament.uk/pa/cm201314/cmhansrd/cm131031/halltext/131031h0001.htm.
[36] http://isc.independent.gov.uk/.
[37] http://isc.independent.gov.uk/news-archive/17october2013.

неприкосновенность личной жизни и правом на защиту персональных данных, что гарантируется Хартией Европейского Союза об основных правах[38]. Согласно этой Директиве, от провайдеров услуг связи требуется удерживать данные информационного трафика, чтобы компетентные национальные органы имели к ним доступ с целью предотвращения, расследования, обнаружения и преследования серьезных преступлений, включая терроризм. Заявив, что удержание данных трафика и доступ к ним представляет собой «особенно серьезное нарушение» обоих этих прав, Суд Европейского Союза пришел к заключению о том, что данная Директива не соответствует принципу соразмерности. 10 июля 2014 года правительство Соединенного Королевства, в ответ на данное решение Суда, предложило Законопроект об удержании информации и следственных полномочиях. Правительство охарактеризовало этот Законопроект (теперь уже Закон) как меру для «разъяснения» характера и объема обязательств, которые могут налагаться на расположенных в Соединенном Королевстве провайдеров телекоммуникационных услуг и интернета[39].

C. Массовое слежение, борьба с терроризмом и право на неприкосновенность личной жизни

1. Право на личную жизнь в соответствии со Статьей 17 Международного пакта о гражданских и политических правах

28. Неприкосновенность личной жизни может быть определена как презумпция того, что частные лица должны иметь определенное поле для самостоятельного развития, взаимодействия и свободы, свободное от вмешательства государства и от чрезмерного инициативного вмешательства со стороны других незваных частных лиц[40]. Обязанность соблюдать неприкосновенность личной жизни и безопасность в сфере коммуникаций подразумевает, что отдельные лица имеют право делиться между собой информацией и идеями без вмешательства государства (или какого-либо частного субъекта), будучи уверенными, что их сообщения достигнут и будут прочитаны только лишь теми получателями, которым они предназначались[41]. Право на неприкосновенность личной жизни также представляет собой способность частных лиц определять, кто является держателем информации о них и каким образом используется эта информация[42].

29. Статья 17 Международного пакта о гражданских и политических правах является наиболее значимым, юридически обязывающим договорным положением глобального характера в отношении права человека на неприкосновенность личной жизни. Она предусматривает, 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 или незаконным посягательствам на его честь и репутацию». Далее в ней предусматривается, что «каждый чело-

[38] Court of Justice of the European Union, Judgment in Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland and Seitlinger and Others*, Judgment of 8 April 2014.
[39] https://www.gov.uk/government/speeches/communications-data-and-interception.
[40] A/HRC/23/40 пункт 22; A/HRC/13/37 пункт 11.
[41] Замечание общего порядка № 16 Комитета по правам человека, пункт 8.
[42] Замечание общего порядка № 16 Комитета по правам человека, пункт 10; A/HRC/23/40 пункт 22.

век имеет право на защиту закона от такого вмешательства или таких посягательств». В других международных документах по правам человека содержатся аналогичные положения; право каждого человека на неприкосновенность личной и семейной жизни, жилища и на тайну корреспонденции также предусматривается законодательством на региональном и национальном уровнях.

30. Однако право на неприкосновенность личной жизни не является абсолютным. Если в отношении какого-либо лица возникают подозрения или ведется официальное расследование разведывательным или правоохранительным органом, за ним может быть установлена слежка на абсолютно законных основаниях борьбы с терроризмом и охраны правопорядка[43]. Хотя в Статье 17 Пакта и нет конкретного ограничительного положения с описанием условий, при которых посягательство на право неприкосновенности личной жизни может не противоречить Пакту, общепризнанно, что такие меры допустимы, при условии, что a) они санкционированы национальным законодательством, которое является доступным, четким и которое соответствует требованиям Пакта,[44] b) они преследуют законную цель и c) они отвечают требованиям необходимости и соразмерности[45].

31. Осознавая, что значительная доля мирового интернет-трафика на какой-то стадии проходит через Соединенные Штаты, ряд государств высказали свою обеспокоенность по поводу того, не нарушает ли программа «Призма» прав их граждан на неприкосновенность личной жизни. В декабре 2013 года Генеральная Ассамблея приняла резолюцию 68/167 «О праве на неприкосновенность личной жизни в цифровой век» (которая была поддержана 57 государствами-членами и была принята без голосования). Эта резолюция подтвердила, что право на неприкосновенность личной жизни должно защищаться и в онлайновой среде, и призвала все государства провести обзор своих процедур, практики и законодательства, касающихся слежения за сообщениями, их перехвата и сбора личных данных, в целях защиты права на неприкосновенность личной жизни путем обеспечения полного и эффективного выполнения всех их обязательств по международному праву прав человека.

32. В резолюции 68/167 также содержалось поручение Верховному комиссару Организации Объединенных Наций по правам человека представить Совету по правам человека и Генеральной Ассамблее доклад о защите и поощрении права на неприкосновенность личной жизни в контексте национального и экстерриториального слежения за цифровыми сообщениями и/или их перехвата и сбора личных данных, в том числе в массовом масштабе. В своем докладе, опубликованном 30 июня 2014 года, Верховный комиссар сделала вывод о том, что Международное право прав человека обеспечивает четкую и универсальную основу для поощрения и защиты права на неприкосновенность личной жизни, в том числе в контексте внутреннего и экстерриториального слежения за ин-

[43] A/HRC/13/37 пункт 13.

[44] Замечание общего порядка № 16 Комитета по правам человека, пункт 3.

[45] A/HRC/27/37 пункты 22-25 и указанные там источники; A/HRC/23/40 пункты 28–29; A/HRC/13/37 пункты 13–17; Сиракузские принципы о положениях, касающихся ограничения и умаления прав, в Международном пакте о гражданских и политических правах, E/CN.4/1985/4, приложение; Замечания общего порядка №№ 16, 27, 29, 34 и 31 Комитета по правам человека; Комитет по правам человека, *Van Hulst v Netherlands*, Communication No. 903/2999, 2004; *Madafferi v Australia*, Communication No. 1011/2001, 2004; *Toonen v Australia*, Communication No. 488/1992, пункт 8.3; *MG v Germany*, Communication No. 1482/2006, 2008; CCPR/C/USA/CO/4.

формационными потоками, перехвата цифровых сообщений и сбора личных данных[46]. Однако она отметила, что практика многих государств свидетельствует об отсутствии адекватного национального законодательства и/или правоприменения, о слабости процессуальных гарантий и неэффективности надзора, что в совокупности приводит к отсутствию ответственности за произвольное или незаконное вмешательство в личную жизнь[47]. Верховный комиссар подчеркнула, что информация о характере и объемах операций цифрового слежения продолжает поступать, но она выразила обеспокоенность «вызывающим тревогу отсутствием прозрачности в деятельности правительства, относящейся к политике, законодательному подкреплению и практике слежения, что сводит на нет любые усилия по оценке их соответствия международному праву прав человека и по обеспечению подотчетности»[48]. Она призвала государства пересмотреть свое собственное внутреннее законодательство, политику и практику, чтобы обеспечить их полное соответствие международному праву прав человека, внося, где необходимо, соответствующие поправки. Она также призвала международное сообщество продолжить детальное изучение этих вопросов[49].

2. Борьба с терроризмом в качестве законной цели

33. В отличие от ряда ограниченных прав, которые защищаются Пактом, в Статье 17 не приводится исчерпывающий перечень законных целей государственной политики, которые могли бы стать основой для оправдания вмешательства в личную жизнь. Тем не менее, по смыслу Статьи 17, предотвращение, подавление и расследование террористических актов, несомненно, являются законной целью. Терроризм способен дестабилизировать общины, создавать угрозу социально-экономическому развитию, нарушать территориальную целостность государств и подрывать международный мир и безопасность. В соответствии со Статьей 6 Пакта, государства несут несомненную обязанность защищать граждан и всех, кто находится в их юрисдикции, от актов терроризма[50]. Одним из аспектов этой обязанности является создание эффективных механизмов для выявления потенциальных будущих угроз террористических актов до того, как они будут осуществлены. Государства выполняют эту обязанность посредством сбора и анализа соответствующей информации через свои разведывательные и правоохранительные органы[51].

34. Утверждается, что расширение возможностей государств отслеживать весь интернет-трафик имеет особенную значимость в контексте борьбы с терроризмом, поскольку связь по интернету всегда играла важную роль в финансировании и осуществлении международных террористических актов; поскольку интернет использовался для целей вербовки в террористические организации; и поскольку ограничение разведывательной деятельности может помешать своевременному выявлению лиц, участвующих в планировании или подстрекающих к совершению террористических актов. Ввиду того, что терроризм имеет международный размах, розыск тех, кто в нем участвует, должен

[46] A/HRC/27/37 пункт 47.
[47] Там же, пункт 47.
[48] Там же, пункт 48.
[49] Там же, пункт 49 и 51.
[50] Там же, пункт21.
[51] A/HRC/20/14 пункт 21.

вестись за пределами национальных границ. Таким образом, предотвращение и подавление терроризма представляет собой важнейшую задачу государственной важности и, в принципе, может быть причиной возможного оправдания для применения массового слежения в интернете.

3. Массовое слежение и качество правовых требований

35. Статья 17 Пакта предусматривает, что каждый человек имеет право на защиту закона от незаконного или произвольного вмешательства в его личную жизнь. В связи с этим возникает требование «качества законодательства», предусматривающее три условия: a) мера должна в какой-то степени основываться на национальном законодательстве; b) само национальное законодательство не должно противоречить верховенству права и требованиям Пакта; и c) соответствующие положения национального законодательства должны быть доступными, ясными и четкими. Тем не менее, санкционированное национальным законодательством вмешательство может быть «незаконным» и/или «произвольным» по смыслу Статьи 17, если соответствующее национальное законодательство не отвечает основным требованиям доступности, конкретности и предсказуемости[52], или если национальное законодательство в чем-либо ином не соответствует нормам необходимости и соразмерности[53]. Соответственно, в национальном законодательстве должны содержаться положения, обеспечивающие, чтобы полномочия применять интрузивные методы слежения соответствовали конкретным законным целям[54], и предусматриваться эффективные гарантии против злоупотреблений[55]. Кроме того, свобода в применении таких мер должна быть с разумной четкостью ограничена применимыми законами или опубликованными правилами, имеющими обязательную силу[56].

36. Доступность требует не только, чтобы национальные законы были опубликованы, но и чтобы они отвечали требованиям ясности и четкости, которые позволяли бы тем, кого они затрагивают, регулировать свое поведение, предусматривая такие обстоятельства, когда могут быть применены интрузивные методы слежения. В своем Замечании общего порядка № 16 о праве на личную жизнь Комитет по правам человека подчеркнул, что законодательство, санкционирующее вмешательство в неприкосновенность частных сообщений, «должно подробно определять условия, при которых такое вмешательство допускается»[57]. До внедрения программ массового слежения, описанных в данном докладе, это положение всегда понималось как требующее от национального законодательства ясно излагать те условия, при которых может быть санкционировано любое вмешательство, как и процедуры такого санкционирования; определять категории лиц, чьи сообщения могут перехватываться; устанавливать ограничения по времени на осуществление слежения; и определять про-

[52] Замечание общего порядка № 16 Комитета по правам человека, пункт 3.
[53] Там же, пункт 8.
[54] A/HRC/13/37 пункт 60; A/HRC/27/37 пункт 28.
[55] CCPR/C/USA/CO/2 пункт 22; *Malone v United Kingdom*, Application No. 8691/79, Judgment 2 August 1984, пункты 67–68; *Weber and Saravia v Germany*, Application No. 54934/00, Judgment 29 June 2006.
[56] A/HRC/27/37 пункт 29; Сиракузские принципы о положениях, касающихся ограничения и умаления прав, в Международном пакте о гражданских и политических правах, E/CN.4/1985/4, приложение, пункты 16 и 18.
[57] Замечание общего порядка № 16 Комитета по правам человека, пункт 8.

цедуры использования и хранения собранных данных[58]. Европейский суд по правам человека также подчеркнул необходимость разработки четких, детальных правил по этому вопросу[59].

37. Программы массового слежения представляют собой существенный вызов требованиям законности, предусмотренным в Статье 17 Пакта. Там, где применяются программы широкомасштабного доступа, нет никаких ограничений в отношении того, какие лица могут подвергаться слежению и в течение какого периода времени. Поэтому такие условия не могут быть детально прописаны в законодательстве. Подробная информация о правовых и административных рамках массового слежения зачастую остается засекреченной, и до сих пор очень немногое известно о том, как применяются собранные таким образом данные. Очень немногие государства до настоящего времени приняли первичные законы, однозначно санкционирующие применение таких программ. Вместо этого к новым цифровым технологиям применяются устаревшие национальные законы, когда-то разработанные в отношении рудиментарных форм слежения, без внесения в них каких-либо поправок, которые отражали бы значительно увеличившиеся возможности, используемые некоторыми государствами. И действительно, высказывались предположения, что определенные государства «преднамеренно стремились к применению устаревших и малодейственных режимов гарантий в отношении все более конфиденциальной информации»[60].

38. Специальный докладчик считает, что существует острая необходимость в том, чтобы государства пересмотрели национальные законы, регулирующие современные формы слежения, чтобы обеспечить соответствие этой практики международному праву прав человека. Необходимо обновить национальные законы, регулирующие перехват сообщений, чтобы они учитывали современные формы цифрового слежения, намного более широкие по своим возможностям и связанные с намного более глубоким вмешательством в сферу личной жизни, чем те формы, которые предусматривались, когда принималась основная часть действующих национальных законов. Отсутствие четко сформулированного современного законодательства создает условия, при которых может осуществляться произвольное нарушение права неприкосновенности личной жизни без каких-либо соизмеримых гарантий. Для обеспечения законности и соразмерности действий в этом контексте необходимо иметь четко сформулированные, детализированные законы. Они также являются абсолютно необходимым средством для того, чтобы частные лица могли предполагать, могут ли их сообщения стать объектом слежения и при каких обстоятельствах.

39. Государственный законодательный процесс предоставляет правительствам возможность оправдать принятие мер массового слежения перед обществом. Открытая дискуссия позволяет обществу понять баланс между неприкосновенностью личной жизни и соображениями безопасности[61]. Транспарентный законотворческий процесс также должен выявить уязвимые места, прису-

[58] CCPR/C/USA/CO/2, пункт 22; *Malone v United Kingdom*, Application No. 8691/79, Judgment 2 August 1984, пункты 67–68; *Weber and Saravia v Germany*, Application No. 54934/00, Judgment 29 June 2006.

[59] *Weber and Saravia v Germany*, Application No. 54934/00, Judgment 29 June 2006; *Uzun v Germany* (2012) 54 EHRR 121 пункт 35.

[60] A/HRC/13/37 пункт 57.

[61] Там же, пункт 56.

щие цифровым коммуникационным системам, что позволит пользователям делать осознанный выбор. Это не только важный элемент требования правовой ясности в соответствии со Статьей 17 Пакта, но также и важное средство обеспечения участия общества в дискуссии по вопросу, представляющему национальный и международный общественный интерес[62]. По мнению Специального докладчика, когда права неприкосновенности личной жизни в сфере цифровых технологий в целом подвергаются систематическим нарушениям, для соблюдения принципа законности достаточно иметь ни что иное, как детальное и исчерпывающее обоснование в первичных законодательных актах.

40. В отличие от этого, применение делегированного законодательства (законодательных актов, принятых исполнительными органами в рамках их полномочий) уже позволило принять секретные правовые основы для осуществления массового слежения, что подрывает возможности осуществления контроля за реализацией этих новых полномочий государства со стороны законодательных органов, судебных органов и общественности[63]. Такие положения не соответствуют содержащимся в Статье 17 Пакта требованиям по качеству законодательства, поскольку они недостаточно открыты для всеобщего ознакомления[64]. Хотя и могут иметься законные, обусловленные государственными интересами причины для сохранения в секрете технических и оперативных характеристик, они не могут оправдать сокрытие от общества базовой информации о характере и размерах вмешательства государства в интернет. Без такой информации невозможно оценить законность, необходимость и соразмерность этих мер. Поэтому государства должны демонстрировать полную транспарентность в отношении применения и охвата методов массового слежения в сфере коммуникаций[65].

4. Экстерриториальные программы массового слежения

41. Определенные государства обладают техническими возможностями для массового слежения за сообщениями между лицами, не находящимися в рамках их юрисдикции, и поэтому осуществляют слежение, которое имеет экстерриториальный эффект. Некоторые из таких действий физически осуществляются на территории соответствующего государства и поэтому затрагивают принципы территориальной юрисдикции по определению Международного пакта о гражданских и политических правах (МПГПП). Это относится не только к тем случаям, когда государственные субъекты устанавливают перехватывающие устройства на оптоволоконные кабели, проходящие через их юрисдикцию, но и когда государство осуществляет регулятивные полномочия в отношении провайдеров телекоммуникационных или интернет-услуг, физически контролирующих передаваемые данные[66]. В любом случае, необходимо распространить сферу защиты прав человека на тех, чья личная жизнь подвергается вмешательству, независимо от того, находятся ли они физически в той стране, где была учреждена компания-провайдер этих услуг. То же самое относится и к тем случаям, когда законы об обязательном удержании информации накладывают обязательства на провайдеров услуг, расположенных в рамках

[62] A/HRC/27/37 пункт 29; A/HRC/14/46.
[63] A/HRC/13/37 пункт 54.
[64] CCPR/C/USA/CO/4.
[65] A/HRC/23/40 пункт 91.
[66] A/HRC/27/37 пункт 34.

территориальной или правовой юрисдикции государства. Даже в тех случаях, когда государства проникают в инфраструктуры, целиком располагающиеся за пределами их территориальной юрисдикции, соответствующие органы, тем не менее, по-прежнему обязаны выполнять обязательства, предусмотренные Пактом[67].

42. Операции экстерриториального слежения представляют собой исключительный вызов для применения требований «качества законодательства», предусмотренных в Статье 17 Пакта. Национальное законодательство, регулирующее перехват внешних (международных) сообщений, зачастую предусматривает меньше защитных мер, чем аналогичные положения, защищающие сообщения исключительно внутри страны[68]. Еще большую обеспокоенность вызывает то, что некоторые государства (включая Соединенные Штаты) продолжают разрешать обеспечение асимметричной защиты своим гражданам в отличие от тех, кто их гражданами не является. Эти различия в отношении отрицательно сказываются на всей сфере цифровых коммуникаций, поскольку послания зачастую направляются через серверы, расположенные в других юрисдикциях. Однако особенно серьезные последствия это имеет для «облачных» компьютерных технологий[69].

43. Любая форма дифференциального отношения несовместима с принципом недискриминации, закрепленным в Статье 26 МПГПП, а также воплощенным в самом понятии соразмерности[70]. Кроме того, использование программ массового слежения для перехвата сообщений тех, кто находится в других юрисдикциях, поднимает серьезные вопросы о доступности и предсказуемости последствий законов, регулирующих вмешательство в осуществление прав на неприкосновенность личной жизни, и о невозможности для частных лиц выяснить, что они могут подвергаться иностранному слежению или что их сообщения могут перехватываться в иностранных юрисдикциях. Специальный докладчик считает, что на государствах лежит юридическая ответственность за предоставление равной правовой защиты как своим гражданам, так и не имеющим гражданства, а также тем, кто находится внутри их юрисдикции и за ее пределами.

5. Международное сотрудничество между разведывательными учреждениями

44. Аналогичная обеспокоенность возникает в отношении международных договоренностей об обмене разведывательной информацией. В отсутствие законов, регулирующих межгосударственные договоренности об обмене разве-

---

[67] Там же, пункты 32–35 и упомянутые там источники.

[68] В ее докладе по Праву на неприкосновенность личной жизни в цифровой век Верховный комиссар по правам человека отметила ряд таких положений: в the United States, the Foreign Intelligence Surveillance Act s.1881(a); в the United Kingdom, the Regulation of Investigatory Powers Act 2000, s.8(4); в New Zealand the Government Security Bureau Act 2003 s.15A; в Australia the Intelligence Services Act s.9; и в Canada the National Defence Act, s.273.64(1), см. A/HRC/27/37 пункт 35, ссылка 30.

[69] European Parliament Directorate General for Internal Policies, The US Surveillance Programmes and Their Impact on EU Citizens' Fundamental Rights, 2013, Caspar Bowden.

[70] Комитет по правам человека также подчеркивал важность принятия «мер к обеспечению того, чтобы любое вмешательство в осуществление права лица на неприкосновенность личной жизни отвечало принципам законности, пропорциональности и необходимости независимо от гражданства или местонахождения лиц, сообщения которых становятся объектом непосредственного отслеживания», CCPR/C/USA/4 пункт 22.

дывательной информацией разведывательные учреждения имеют возможность заключать секретные двусторонние и многосторонние соглашения, не подпадающие под контроль какого-либо независимого органа[71]. Информацией о телекоммуникационных сообщениях частного лица могут делиться с иностранными разведывательными учреждениями без всякой защиты со стороны государственной правовой структуры и без адекватных (или вообще каких бы то ни было) гарантий. После проведения продолжительных консультаций, Верховный комиссар по правам человека недавно получил достоверные доказательства того, что правительства некоторых государств систематически перепоручали функции по сбору и анализу органам, действующим в странах с более слабыми гарантиями неприкосновенности личной жизни[72]. Подобная практика делает непредсказуемыми последствия применения режима слежения для тех, кого это затрагивает, и потому противоречит Статье 17 Пакта.

6. Гарантии и надзор

45. Одна из основных форм защиты, предусмотренных Статьей 17, состоит в том, что к системам скрытого слежения должны применяться соответствующие процедурные гарантии для защиты от злоупотреблений[73]. Эти гарантии могут быть различного вида, но, как правило, включают применение независимого предварительного санкционирования и/или последующего независимого анализа. Оптимальный вариант предусматривает участие исполнительных, законодательных и судебных органов, а также независимый общественный контроль[74]. Отсутствие адекватных гарантий может привести к практике непривлечения к ответственности за произвольные или незаконные посягательства на право на неприкосновенность личной жизни в сфере интернета[75].

46. Многие государства, применяющие целевые программы слежения, предусматривают необходимость получения для этого предварительных санкций судебных органов. Соответствующее международным нормам участие судебных органов является важной гарантией, хотя и существуют свидетельства того, что в некоторых юрисдикциях эффективность такого контроля была ограничена ввиду почтительного отношения к исполнительной власти[76]. В других государствах, таких как Соединенное Королевство, разрешения на перехват сообщений по конкретным лицам выдаются министрами правительства без каких-либо предварительных санкций со стороны судебных органов. Как заявлено, это оправдывается тем, что министры отчитываются на демократической основе перед своим электоратом. Случаи применения исполнительным лицом таких полномочий затем рассматриваются независимым Комиссаром по перехвату сообщений, а пострадавшие лица также могут подать жалобу в судебный орган, Трибунал по следственным полномочиям, который может рассматривать секретные вопросы на закрытых заседаниях.

---

[71] A/HRC/13/37.
[72] A/HRC/27/37 пункт 30.
[73] CCPR/C/USA/CO/2, пункт 22; *Malone v United Kingdom*, Application No. 8691/79, Judgment 2 August 1984, пункты 67–68; *Weber and Saravia v Germany*, Application No. 54934/00, Judgment 29 June 2006.
[74] A/HRC/27/37.
[75] Там же.
[76] Там же, пункт 38.

47. В контексте целевого слежения, какой бы метод предварительного санкционирования ни был принят (судебный или исполнительный), при нем, по крайней мере, существует, возможность оценки *ex ante* необходимости и пропорциональности интрузивных мер слежения посредством рассмотрения конкретных обстоятельств дела, а также того частного лица или организации, чьи сообщения должны перехватываться. В случае же программ массового слежения ни одной из таких возможностей нет, поскольку их применение не зависит от наличия подозрения в отношении конкретных лиц. Таким образом, оценка *ex ante* здесь ограничивается лишь тем, чтобы санкционировать продолжение применения программы слежения в целом, а не чтобы использовать ее в отношении какого-то конкретного лица. Специальный докладчик считает, что государства, использующие технологии массового слежения, должны создать влиятельные независимые контрольные органы, с адекватными ресурсами и полномочиями, для проведения оценки *ex ante* применения интрузивных методов слежения в соответствии с требованиями законности, необходимости и соразмерности, изложенными в Статье 17 Пакта[77].

48. Еще одним процедурным аспектом Статьи 17 является требование проведения оценки *ex post facto* интрузивных мер слежения. В некоторых государствах предусмотрено, чтобы независимый оценщик осуществлял контроль над законностью операций слежения, анализируя способы такого слежения, масштабы и оправданность этих операций. Такие обзоры всегда должны содержать анализ соответствия осуществляемой государством практики требованиям Пакта.

49. Помимо проведения такого рода общих обзоров, на государстве лежит конкретная обязанность предоставлять средства правовой защиты тем лицам, у которых, предположительно, были нарушены права, предусмотренные Пактом. В пункте 3(b) Статьи 2 Пакта предусматривается, что государства-участники должны обеспечить, чтобы любое лицо, требующее правовой защиты, имело осуществимое право на то, чтобы его заявление решалось компетентным национальным судебным, административным или законодательным органом. Чтобы обеспечить эффективность этого права, в национальном законодательстве должен быть независимый механизм, который способен провести тщательную, беспристрастную проверку, при доступе ко всем соответствующим материалам и при гарантиях адекватных правовых процедур, и который имеет полномочия предоставить необходимое средство защиты, имеющее обязательную силу (включая, где необходимо, распоряжение о прекращении слежения или об уничтожении полученных данных)[78].

50. Для того чтобы сослаться на право прибегнуть к эффективному средству правовой защиты, частному лицу, как правило, необходимо установить, что оно стало жертвой нарушения. В плане мер секретного слежения такие требования сложно или невозможно выполнить. Очень немногие государства имеют действующие нормы, требующие *ex post* уведомления подозреваемого. Европейский суд по правам человека соответственно смягчил требование к отдельным лицам относительно доказательства того, что они стали объектом секретного слежения. Он разграничил жалобы относительно существования режима, который, предположительно, не соответствует требованиям Европейской конвен-

[77] Там же, пункт. 62.
[78] A/HRC/14/46; A/HRC/27/37.

ции о правах человека, и жалобы по конкретным случаям незаконных действий со стороны государства. В первом случае Суд готов рассматривать оспариваемые положения в том виде, как они представлены[79], тогда как во втором случае он обычно требует, чтобы заявители продемонстрировали «разумное подтверждение» того, что они стали объектом незаконной слежки[80]. В контексте режимов массового слежения Специальный докладчик считает, что любой пользователь интернета должен быть в состоянии поставить под вопрос законность, необходимость и соразмерность таких мер.

7. Необходимость и соразмерность программ массового слежения

51. На государствах лежит обязанность продемонстрировать, что любое вмешательство в осуществление права на неприкосновенность личной жизни, как оно предусмотрено Статьей 17 Пакта, является необходимым средством достижения законной цели. Это требует наличия рациональной связи между применяемым средством и той целью, которую оно должно достичь. Для этого также необходимо, чтобы избранное средство было «наименее ограничительным из числа тех, с помощью которых может быть достигнут желаемый результат» [81]. Связанный с этим принцип соразмерности подразумевает сбалансирование объема нарушения прав на неприкосновенность личной жизни в сфере интернета и конкретных преимуществ для расследования, осуществляемого государственным органом в интересах общества. Тем не менее, существует определенный предел для дозволенного нарушения права, предусмотренного Пактом. Как подчеркнул Комитет по правам человека, «ни при каких обстоятельствах ограничения не могут применяться или осуществляться таким образом, чтобы это нарушало существо признанного в Пакте права»[82]. Поэтому, в том, что касается секретного слежения, Комитет подчеркнул, что любое решение о санкционировании перехвата сообщений должно приниматься только конкретным органом, предусмотренным законом, и «строго индивидуально»[83]. Таким образом, соразмерность любого вмешательства в осуществление права на неприкосновенность личной жизни должна определяться конкретными обстоятельствами каждого отдельного случая[84].

52. Ни один из этих принципов идеально не согласуется с применением государствами технологий массового слежения. Наличие технических возможностей для осуществления программ широкомасштабного сбора и анализа данных, несомненно, предлагает дополнительные средства в борьбе с терроризмом и в ведении расследований. Однако при оценке соразмерности этих программ необходимо также принимать во внимание сопутствующий ущерб, который наносится коллективному праву на неприкосновенность личной жизни. Программы массового сбора данных, как представляется, нарушают требование о том, что разведывательные органы должны применять наименее интрузивные из существующих методов в отношении прав человека (если только соответствующие государства не смогут продемонстрировать, что только полный до-

---

[79] *Klass v Germany*, (1979-80) 2 EHRR 214.
[80] *Halford v United Kingdom* (1997) 24 EHRR 523.
[81] CCPR/C/21/Rev.1/Add.9; A/HRC/13/37 пункт 60.
[82] Замечания общего порядка №№ 27 и 31 Комитета по правам человека.
[83] Замечание общего порядка № 16 Комитета по правам человека, пункт 8.
[84] Замечание общего порядка № 16 Комитета по правам человека, пункт 4, *Van Hulst v. The Netherlands*, Communication No. 903/1999, 2004, пункт 7.3; *Toonen v. Australia*, Communication No. 488/1992, пункт 8.3.

ступ ко всем передаваемым через интернет посланиям сможет защитить от угрозы терроризма и других серьезных преступлений). Ввиду отсутствия возможности провести какую-либо индивидуализированную оценку соразмерности таких мер до их принятия, представляется, что такие программы подрывают саму суть права на неприкосновенность личной жизни. Они абсолютно исключают применение «строго индивидуального» анализа, который Комитет по правам человека счел крайне важным, и таким образом, могут быть сочтены произвольными, даже если они служат законной цели и были утверждены на основании общедоступного правового режима[85]. Соответственно Специальный докладчик приходит к выводу, что такие программы могут не противоречить Статье 17 Пакта только в том случае, если соответствующие государства способны оправдать как соразмерное систематическое вмешательство в осуществление прав на личную жизнь в сфере интернета потенциально неограниченного числа невиновных людей в любой части света[86].

8. Законы об обязательном удержании информации и автоматическое извлечение данных из сообщений, сохраняемых провайдерами телекоммуникационных услуг и интернета

53. Программы массового слежения не ограничиваются лишь перехватом контента сообщений. Цифровая связь генерирует большие объемы транзакционных данных. Эти коммуникационные данные (или метаданные) включают личную информацию о пользователях, их местоположении и их онлайновой активности. Многие государства приняли законодательные акты, обязывающие провайдеров телекоммуникационных и интернет-услуг собирать и сохранять коммуникационные данные, чтобы их можно было впоследствии проанализировать. Как правило, эти законы требуют, чтобы провайдеры услуг предоставляли государственным органам информацию о распределении IP-адресов, чтобы они могли в любое время идентифицировать пользователя конкретного IP-адреса. Перехват передаваемых данных становится все более важной технологией слежения для государств. Коммуникационные данные легко хранятся и анализируются и могут быть использованы для составления файлов на частных лиц, столь же уязвимых в плане неприкосновенности личной жизни, как и контент их сообщений[87]. Составляя и накапливая информацию, полученную из сообщений, можно определить местоположение конкретного лица, его связи и активность[88]. В отсутствие специальных гарантий, практически не существует никакого секретного аспекта личной жизни человека, который не мог бы подвергнуться тщательному анализу метаданных[89]. Таким образом, автоматическое извлечение информации имеет особенно разрушительное воздействие на неприкосновенность личной жизни.

54. Во многих государствах весьма различные государственные органы имеют доступ к коммуникационным данным, по совершенно различным причинам,

---

[85] A/HRC/27/37 at para. 25.

[86] См. A/HRC/27/37 пункт 25, где Верховный комиссар по правам человека отметил: «одного того, что меры нацелены на поиск конкретных иголок в стоге сена, недостаточно; должная мера определяется через анализ совокупного воздействия конкретных мер на «стог сена» с учетом потенциальной угрозы; т.е. тем, является ли мера необходимой и соразмерной».

[87] A/HRC/27/37 пункт 19.

[88] A/HRC/23/40 пункт 15.

[89] http://blog.privacystrategy.eu/public/published/Submission_ISC_7.2.2014_-_Caspar_Bowden.pdf.

зачастую без судебных санкций или сколько-нибудь существенного независимого контроля. Например, в Соединенном Королевстве более 200 различных учреждений имеют полномочия доступа к коммуникационным данным в соответствии с Законом о правовом регулировании следственных полномочий 2000 года[90], и только лишь в 2013 году от государственных органов было получено 514 608 запросов на получение таких данных[91]. Суды уже в течение некоторого времени признают, что предоставление метаданных государственным органам является вмешательством в осуществление права на личную жизнь, а Суд Европейского Союза недавно подтвердил, что удержание метаданных, относящихся к личной жизни человека и коммуникационным сообщениям, само по себе является вмешательством в осуществление этого права[92], (а предоставление доступа к сохраненным метаданным также представляет собой несомненное вмешательство)[93]. Придя к такому заключению, Суд Европейского Союза подчеркнул, что коммуникационные метаданные позволяют «прийти к очень точным выводам в отношении частной жизни людей, которых эти данные касаются»[94].

55. Исходя из подхода, примененного Судом Европейского Союза, можно утверждать, что сбор и удержание коммуникационных данных является вмешательством в осуществление права на личную жизнь, независимо от того, осуществлялся ли впоследствии доступ к этим данным и анализировались ли они каким-либо государственным органом[95]. Ни для перехвата коммуникационных данных по закону об обязательном удержании информации, ни для их последующего раскрытия для государственных органов (и анализа ими) не требуется наличия предварительных подозрений в отношении конкретного лица или организации. Поэтому Специальный докладчик присоединяется к высказанным Верховным комиссаром оговоркам относительно необходимости и соразмерности законов об обязательном удержании данных[96].

9. Указание цели

56. У многих государств отсутствуют положения по «указанию цели», ограничивающие использование информации, собранной для одной цели, для других правительственных целей, не связанных с первоначальной. В результате данные, якобы собранные для целей национальной безопасности, могут предоставляться другим разведывательным учреждениям, правоохранительным и другим государственным органам, включая налоговые службы, местным советам и лицензирующим органам[97]. Органы национальной безопасности и правоохранительные органы обычно исключаются из положений законов о защите данных, которые ограничивают обмен данными на частных лиц. В результате

[90] Перечень учреждений, имеющих право запрашивать коммуникационные данные, включает налоговые органы и местные административные органы и может быть расширен посредством делегированного законодательства (административный указ).

[91] http://www.intelligencecommissioners.com/.

[92] Court of Justice of the European Union, Judgment in Joined Cases C-293/12 and C-594/12, Digital Rights Ireland and Seitlinger and Others, Judgment of 8 April 2014, para. 34.

[93] Там же, пункт 35.

[94] Там же, Судебное решение, пункты 26–27 и 37.

[95] A/HRC/27/37 пункт 26.

[96] Там же, пункт 26.

[97] Анализ случаев такого размывания целей, имевших место в Соединенном Королевстве см. вhttps://www.whatdotheyknow.com/request/127491/response/315758/attach/html/2/Summay%20of%20Counsels%20advice.pdf.html.

частным лицам сложно предвидеть, когда и какой государственный орган может осуществлять за ними слежение. «Размывание целей» рискует нарушить Статью 17 Пакта, не только потому, что у соответствующих законов нет предсказуемости последствий их применения, но и поскольку меры слежения, являющиеся необходимыми и соразмерными для одной законной цели, могут не быть таковыми для другой цели[98]. Поэтому Специальный докладчик поддерживает рекомендацию своего предшественника о том, что государства в обязательном порядке должны предоставлять правовые основания для использования личной информации в других целях в соответствии с принципами в области прав человека[99]. Это имеет особую важность в ситуации, когда обмен информацией носит трансграничный или межгосударственный характер.

10. Частный сектор

57. Чтобы облегчить цифровой слежение, государства все больше полагаются на частный сектор. Это не обусловлено лишь законами об обязательном удержании данных. Корпорации также принимают участие во внедрении технологий широкомасштабного доступа, разрабатывая коммуникационную инфраструктуру, которая облегчает осуществление массового слежения. Провайдеров телекоммуникационных услуг и интернета просили внести в свои технологии определенные уязвимые элементы, чтобы обеспечить их готовность для возможного считывания данных. Верховный комиссар по правам человека охарактеризовал такую практику как «делегирование правоприменительных и квазиюридических полномочий интернет-посредникам под предлогом саморегулирования и сотрудничества»[100]. Специальный докладчик согласен с этим утверждением. Чтобы не стать соучастником в нарушении прав человека, провайдеры услуг должны обеспечить соответствие своей деятельности Руководящим принципам предпринимательской деятельности в аспекте прав человека, утвержденным Советом по правам человека в 2011 году[101].

IV. Выводы и рекомендации

58. **Обязательства государств согласно Статье 17 Международного пакта о гражданских и политических правах включают обязательство соблюдать неприкосновенность личной жизни и безопасность в сфере цифровых коммуникаций. В принципе это подразумевает, что люди имеют право делиться друг с другом информацией и идеями без вмешательства государства, будучи абсолютно уверенными, что их сообщение достигнет только предполагаемого получателя и будет прочитано им одним. Посягающие на это право меры должны санкционироваться таким национальным законодательством, которое является доступным и четким и которое не противоречит требованиям Пакта. Оно также должно преследовать законную цель и отвечать требованиям необходимости и соразмерности.**

59. **Предотвращение и подавление терроризма является важнейшей задачей государства и, в принципе, может быть причиной возможного оправ-**

[98] A/HRC/27/37 пункт 27.
[99] A/HRC/13/37 пункты 50 и 66.
[100] A/HRC/27/37 пункт 42.
[101] A/HRC/27/37 пункты 43-46.

дания для применения массового слежения в интернете. Однако, технические возможности используемых в настоящее время программ настолько высоки, что они могут не противоречить требованиям Статьи 17 Пакта только в том случае, если соответствующие государства способны оправдать как соразмерное систематическое вмешательство в осуществление прав на личную жизнь в сфере интернета потенциально неограниченного числа невиновных людей в любой части света. Технология широкомасштабного доступа к информации имеет неизбирательно разрушительный эффект для неприкосновенности личной жизни онлайн и посягает на саму сущность права, гарантированного Статьей 17. В отсутствие официального отказа со стороны государств от своих обязательств согласно Пакту эти программы представляют собой непосредственный и актуальный вызов установленным нормам международного права.

60. **Специальный докладчик согласен с Верховным комиссаром по правам человека в том, государства, применяющие подобные технологии, срочно должны пересмотреть и обновить соответствующие национальные законы, чтобы обеспечить их соответствие международному праву прав человека. И дело не только в том, что это требование Статьи 17, но и в том, что это предоставляет важную возможность провести осознанную дискуссию, которая может повысить информированность общества и позволить частным лицам делать осознанный выбор. Когда на кону стоят права на неприкосновенность личной жизни всего цифрового сообщества, необходимо ни что иное, как принятие детальных и исчерпывающих первичных законодательных актов. Должны быть наложены надлежащие ограничения на использование перехваченных данных с требованием к соответствующим государственным органам предоставлять правовые основания для использования личной информации в других целях.**

61. **Государства должны создать влиятельные независимые контрольные органы, с адекватными ресурсами и полномочиями, для проведения оценки *ex ante* не только в отношении требований национального законодательства, но в отношении соответствия требованиям необходимости и соразмерности, предусмотренным Пактом. Кроме того, частные лица должны иметь право обращаться за эффективным средством защиты против возможного нарушения их права на неприкосновенность личной жизни в сфере интернета. Для этого нужно такое средство, с помощью которого пострадавшее частное лицо могло бы подать жалобу в независимый орган, способный провести тщательную, беспристрастную проверку, при доступе ко всем соответствующим материалам и при гарантиях адекватных правовых процедур. Механизмы подотчетности могут иметь различные формы, но должны иметь полномочия давать распоряжения, имеющие обязательную силу. Государства не должны навязывать постоянно действующие требования, которые подрывают осуществление права на эффективное средство защиты.**

62. **Специальный докладчик согласен с Верховным комиссаром по правам человека в том, что в тех случаях, когда государства проникают в инфраструктуры, располагающиеся за пределами их территориальной юрисдикции, они по-прежнему обязаны выполнять свои обязательства, предусмотренные Пактом. Кроме того, в Статье 26 Пакта запрещается дискриминация по признаку национальности и гражданства. Таким образом,**

Специальный докладчик считает, что на государствах лежит юридическая ответственность за предоставление равной защиты прав на неприкосновенность личной жизни как своим гражданам, так и не имеющим гражданства, а также тем, кто находится внутри их юрисдикции и за ее пределами. Режимы асимметричной защиты прав на неприкосновенность личной жизни являются прямым нарушением требований Пакта.

63. **Специальный докладчик призывает все государства, применяющие в настоящее время технологии массового цифрового слежения, предоставить детальное, подтвержденное фактами обоснование систематического вмешательства в осуществление прав на неприкосновенность личной жизни пользователями интернета, со ссылкой на требования Статьи 17 Пакта. Государства должны быть прозрачны в отношении характера и глубины своего проникновения в интернет, своих методов и их оправданности, а также должны предоставить общественности подробный отчет о тех реальных преимуществах, которые удалось получить в результате применения таких методов.**

64. **Специальный докладчик согласен со своим предшественником[102] и бывшим Специальным докладчиком по вопросу о поощрении и защите права на свободу убеждений и их свободное выражение[103] в том, что Комитету по правам человека следует составить и утвердить новое Замечание общего порядка в отношении права неприкосновенности личной жизни в онлайновой сфере, где были бы отражены последние перемены в плане отслеживания цифровых коммуникаций, которые произошли со времени принятия Замечания общего порядка № 16 в 1988 году.**

---

[102] A/HRC/13/37 пункт 19.
[103] A/HRC/23/40 пункт 98.