Организация Объединенных Наций A/HRC/27/37

Генеральная Ассамблея

Distr.: General
30 June 2014
Russian
Original: English

Совет по правам человека
Двадцать седьмая сессия
Пункты 2 и 3 повестки дня
Ежегодный доклад Верховного Комиссара Организации Объединенных Наций по правам человека и доклады Управления Верховного комиссара и Генерального секретаря

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

Право на неприкосновенность личной жизни в цифровой век

Доклад Управления Верховного комиссара Организации Объединенных Наций по правам человека

Резюме

В своей резолюции 68/167 Генеральная Ассамблея просила Верховного комиссара Организации Объединенных Наций по правам человека предоставить Совету по правам человека на его двадцать седьмой сессии и Генеральной Ассамблее на ее шестьдесят девятой сессии доклад о защите и поощрения 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, с мнениями и рекомендациями, которые будут рассмотрены государствами-членами. Настоящий доклад представляется во исполнение этой просьбы. Управление Верховного комиссара Организации Объединенных Наций по правам человека также представит доклад Генеральной Ассамблее на ее шестьдесят девятой сессии в ответ на ее просьбу.

GE.14-06873 (R) 260814 260814
1406873

Содержание

I. Введение

1. Цифровые коммуникационные технологии, такие как Интернет, мобильные смартфоны и устройства с поддержкой WiFi, стали частью повседневной жизни. Значительно усовершенствовав доступ к информации и обмену данными в режиме реального времени, новые средства связи расширяют свободу выражения мнений, упрощают глобальные дискуссии и поощряют демократические формы участия в жизни общества. Эти могущественные технологии, усиливающие голоса правозащитников и вооружающие их новыми способами доказательства и выявления нарушений, способны содействовать лучшему осуществлению прав человека. Сегодня, когда сетевое общение занимает как никогда важное место в жизни современного человека, Интернет становится повсеместным и все более личным пространством.

2. В цифровую эпоху коммуникационные технологии также расширили возможности правительств, компаний и отдельных лиц осуществлять слежение, перехват и сбор данных. Как отметил Специальный докладчик по вопросу о поощрении и защите права на свободу мнений и их свободное выражение, технологические достижения снимают ограничения с возможностей государства по осуществлению слежения с точки зрения охвата или продолжительности. Снижение стоимости технологий и хранения данных устраняет финансовые или практические препятствия к осуществлению слежения. В настоящее время государство обладает большими, чем когда-либо, возможностями осуществления одновременного, интрузивного, адресного или широкомасштабного слежения[1]. Другими словами, технологические платформы, от которых все больше зависит мировая политическая, экономическая и общественная жизнь, не только подвержены массовому электронному слежению, но и фактически могут его стимулировать.

3. Информация о систематическом использовании в разных странах такой подверженности цифровых коммуникационных технологий электронному слежению и перехвату вызывает большую тревогу. Как показывают многочисленные примеры открытого или тайного наблюдения с использованием цифровых технологий во всем мире, сплошное слежение со стороны государства из исключительной меры перерастает в опасную привычку. Сообщалось о случаях, когда правительства под угрозой закрытия телекоммуникационных и других компаний беспроводной связи требовали от них предоставления прямого доступа к коммуникационному трафику, возможности осуществлять прослушивание оптоволоконных сетей и систематически получать полную информацию о клиентах и сотрудниках. Поступают сообщения о том, что в некоторых странах наблюдение за телекоммуникационными системами используется для слежки за представителями политической оппозиции и/или диссидентами. Утверждается, что власти некоторых государств регулярно записывают все телефонные разговоры и сохраняют их для анализа и что правительства стран, принимающих глобальные мероприятия, отслеживают коммуникации во время таких событий. В одной из стран власти якобы требуют оснащать всех продаваемые в стране компьютеры фильтрующим программным обеспечением, которое может иметь и иное назначение как средство слежения. Согласно утверждениям, передовые средства цифрового слежения в настоящее время разрабатываются даже негосударственными субъектами. Технологии массового слежения сегодня выходят на

[1] A/HRC/23/40, пункт 33.

мировой рынок, повышая тем самым риск того, что цифровое наблюдение выйдет из-под правительственного контроля.

4. Дополнительную тревогу вызывает появление в 2013 и 2014 годах сообщений, о том, что Агентство национальной безопасности Соединенных Штатов Америки совместно с Центром правительственной связи Соединенного Королевства Великобритании и Северной Ирландии разработали технологии, позволяющие получить доступ практически ко всему мировому интернет-трафику, спискам телефонных звонков в США, электронным адресным книгам отдельных лиц и огромным объемам другой цифровой информации. Эти новые средства, как утверждается, были развернуты при помощи транснациональной сети с использованием стратегических партнерств разведслужб обоих государств, рычагов регулирования деятельности частных компаний и коммерческих контрактов.

5. Реагируя на обеспокоенность государств-членов и других заинтересованных сторон по поводу негативного влияния практики слежения на права человека, в декабре 2013 года Генеральная Ассамблея без голосования приняла резолюцию 68/167 о праве на неприкосновенность личной жизни в эпоху цифровых технологий. В этой резолюции, поддержанной 57 государствами-членами, Ассамблея подтверждает, что те же права, которые человек имеет в оффлайновой среде, должны также защищаться и в онлайновой среде, и призывает уважать и защищать право на неприкосновенность личной жизни в контексте цифровой коммуникации. Она также призывает 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.

6. Также в резолюции 68/167 Генеральная Ассамблея просит Верховного комиссара Организации Объединенных Наций по правам человека предоставить Совету по правам человека на его двадцать седьмой сессии и Генеральной Ассамблее на ее шестьдесят девятой сессии 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, с мнениями и рекомендациями, которые будут рассмотрены государствами-членами. Настоящий доклад представляется во исполнение этой просьбы. В соответствии с просьбой, содержащейся в резолюции 68/167, Управление Верховного комиссара Организации Объединенных Наций по правам человека (УВКПЧ) также представит доклад Генеральной Ассамблее на ее шестьдесят девятой сессии.

II. Основы и методология

7. В связи с резолюцией 68/167 УВКПЧ приняло участие в ряде мероприятий и осуществляло сбор информации из широкого круга источников. Верховный комиссар 24 февраля 2014 года выступила с основным докладом на семинаре экспертов по теме "Право на неприкосновенность частной жизни в эпоху цифровых технологий", который был совместно организован Австрией, Бразилией, Германией, Лихтенштейном, Мексикой, Норвегией и Швейцарией при содействии Женевской академии международного гуманитарного права и прав человека.

8. С ноября 2013 года по март 2014 года УВКПЧ совместно с Университетом Организации Объединенных Наций участвовало в осуществлении исследовательского проекта, касающегося применения международного права прав человека к национальным режимам регламентации практики цифрового слежения со стороны государственных органов. УВКПЧ благодарит Университет и высоко ценит его весомый вклад в подготовку настоящего доклада путем проведения исследовательского проекта.

9. В рамках открытого процесса консультаций 27 февраля 2014 года УВКПЧ направило вопросник в адрес государств-членов через их постоянные представительства в Женеве и Нью-Йорке, международных и региональных организаций, национальных правозащитных учреждений, неправительственных организаций и коммерческих предприятий. В вопроснике УВКПЧ предложило им высказаться по вопросам, поднятым в резолюции 68/167 Генеральной Ассамблеи. На сайте УВКПЧ был создан специальный раздел, где можно ознакомиться с вопросником и ответами на него и дополнительно выразить свои мнения. Материалы были получены от 29 государств-членов из всех регионов, пяти международных и/или региональных организаций, трех национальных правозащитных учреждений, 16 неправительственных организаций и двух инициатив частного сектора[2].

10. Во многих полученных материалах содержится подробный анализ действующих законодательных норм и других мер, призванных обеспечить уважение и защиту права на неприкосновенность личной жизни в эпоху цифровых технологий, а также инициатив, нацеленных на создание и осуществление процессуальных гарантий и эффективного надзора. В некоторых ответах отмечаются проблемы, возникающие в ходе осуществления права на неприкосновенность частной жизни в эпоху цифровых технологий, и предлагаются инициативы на международном уровне. В частности, Комитету по правам человека предлагается обновить соответствующие замечания общего порядка, в особенности по статье 17 Международного пакта о гражданских и политических правах; Совету по правам человека рекомендуется учредить мандат специальных процедур по вопросу о праве на неприкосновенность частной жизни и/или вовлечь уже действующих мандатариев в совместные или индивидуальные инициативы по решению вопросов, относящихся к праву на неприкосновенность частной жизни в контексте цифрового слежения и разработать руководство по надлежащей практике.

11. В соответствии с просьбой, изложенной в резолюции 68/167 Генеральной Ассамблеи, в настоящем докладе приводятся соображения и рекомендации на основе оценки информации, имевшейся на момент подготовки проекта, с привлечением большого объема сведений из различных полученных материалов.

III. Вопросы, касающиеся права на неприкосновенность частной жизни в цифровой век

12. Как было отмечено Генеральной Ассамблеей в резолюции 68/167, международное право прав человека предусматривает универсальную основу, в соответствии с которой должно оцениваться любое посягательство на право на неприкосновенность личной жизни. Согласно статье 12 Всеобщей декларации прав человека, "никто не может подвергаться произвольному вмешательству в

[2] Все материалы размещены на сайте www.ohchr.org/EN/Issues/DigitalAge/Pages/DigitalAgeIndex.aspx.

его личную и семейную жизнь, произвольным посягательствам на неприкосновенность его жилища, тайну его корреспонденции или на его честь и репутацию. Каждый человек имеет право на защиту закона от такого вмешательства или таких посягательств". Статья 17 Международного пакта о гражданских и политических правах, на сегодняшний день ратифицированного 167 странами, определяет, 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 сказано, что "каждый человек имеет право на защиту закона от такого вмешательства или таких посягательств".

13. Сходные положения содержатся в других международных договорах о правах человека. Право каждого человека на неприкосновенность частной и семейной жизни, жилища, тайну корреспонденции или право на признание и уважение достоинства, личной неприкосновенности или репутации также предусматривается законодательством на региональном и национальном уровнях. Поэтому можно говорить об универсальном признании де-юре и де-факто основополагающей важности и непреходящей ценности права на неприкосновенность частной жизни и необходимости гарантировать его соблюдение.

14. Хотя настоящий доклад посвящен праву на неприкосновенность частной жизни, необходимо сказать о том, что массовое слежение, перехват электронно-цифровых коммуникаций и сбор личных данных могут сказываться и на осуществлении других прав. К ним относятся право на свободу убеждений и их свободное выражение, право искать, получать и распространять информацию; право на свободу мирных собраний и свободу ассоциации; право на семейную жизнь, которые тесно связаны с правом на неприкосновенность частной жизни и все больше осуществляются посредством электронных средств информации. Практикой цифрового слежения также могут затрагиваться и другие права, например право на здоровье, скажем, если человек воздерживается от получения или сообщения деликатной информации, касающейся состояния здоровья, опасаясь, что из-за этого может быть утрачена ее анонимность. Есть веские основания полагать, что цифровые технологии уже использовались для сбора информации, которая впоследствии привела к актам пыток и других видов жестокого обращения. Имеются сообщения о том, что анализ метаданных, полученных посредством электронного наблюдения, использовался для установления местонахождения лиц и объектов, ставших мишенями смертоносных нападений с использованием беспилотных летательных аппаратов. Подобные нападения все так же вызывают серьезную обеспокоенность по поводу соблюдения международного права прав человека и гуманитарного права, а также ответственности за эти нарушения. Взаимосвязь между массовым слежением и такими другими видами воздействия на права человека, выходящими за рамки настоящего доклада, заслуживает дальнейшего рассмотрения.

A. Право на защиту от произвольного или незаконного вмешательства в личную и семейную жизнь, посягательства на неприкосновенность жилища или тайну корреспонденции

15. В некоторых материалах подчеркивается, что отслеживание данных, передаваемых по электронным каналам связи, может быть необходимой и эффективной мерой, принимаемой в законных интересах обеспечения правопорядка или национальной безопасности, когда оно осуществляется в соответствии с за-

коном, в том числе международным правом прав человека. Однако сообщения о массовом цифровом слежении порождают вопросы о том, насколько такие меры соответствуют международно-правовым стандартам и не требуется ли укрепить гарантии законности при отслеживании этой информации в целях защиты от нарушений прав человека. В частности, меры по слежению не должны приводить к произвольному или незаконному вмешательству в частную и семейную жизнь человека, нарушать неприкосновенность его жилища или раскрывать тайну его корреспонденции; правительства должны принять специальные меры по обеспечению защиты закона от такого вмешательства.

16. Как показал обзор различных ответов, решение этих вопросов требует оценки того, что представляет собой вмешательство в частную жизнь в контексте цифровых коммуникаций; определения значения терминов "произвольный и незаконный"; понимания того, чьи права защищаются международным правом прав человека и когда. В разделах ниже рассматриваются вопросы, которые были затронуты в различных ответах.

1. Вмешательство в частную жизнь

17. Международные и региональные органы по наблюдению за осуществлением договоров по правам человека, суды, комиссии и независимые эксперты предоставили соответствующие сведения относительно сферы охвата и содержания права на неприкосновенность частной жизни, в том числе значения понятия "вмешательство" в частную жизнь. В замечании общего порядка № 16 Комитета по правам человека подчеркивается, что соблюдение статьи 17 Международного пакта о гражданских и политических правах требует того, чтобы неприкосновенность и конфиденциальность корреспонденции были гарантированы де-юре и де-факто. "Корреспонденция должна доставляться адресату без перехвата, не вскрываться и не прочитываться так или иначе"[3].

18. Некоторые полагают, что пересылка личной информации и обмен ею по электронным средствам связи являются частью сознательного компромисса, посредством которого люди добровольно сообщают информацию о себе и своих отношениях в обмен на цифровой доступ к товарам, услугам и информации. Однако возникают серьезные вопросы по поводу того, насколько потребители действительно осознают то, какими данными они делятся, как и с кем, и для чего эти данные будут использованы. Как сказано в одном из докладов, "специфика больших объемов информации состоит в том, что, когда данные собраны, сохранять их анонимность становится очень сложно. Несмотря на многообещающие исследования способов сохранения в тайне идентифицирующей личность информации при работе с большими массивами данных, используемые сегодня методы повторной идентификации якобы "анонимных" данных представляются намного более совершенными. Совокупные инвестиции в методики соединения данных в разы больше вложений в технологии по обеспечению лучшей защиты неприкосновенности частной жизни". Далее авторы доклада отмечают, что "концентрация на контроле за сбором и сохранением личных данных при всей своей важности может оказаться недостаточной для защиты неприкосновенности частной жизни" отчасти потому, что "большие объемы данных позволяют

[3] *Официальные отчеты Генеральной Ассамблеи, сорок третья сессия, Дополнение № 40* (A/43/40), том I, приложение VI, пункт 8.

применять новые и неочевидные способы использования данных, которые способны оказывать неожиданно мощное воздействие"[4].

19. Аналогичным образом высказываются идеи о том, что перехват или сбор данных о каком-либо коммуникационном сообщении, в отличие от непосредственного содержания этого сообщения, сами по себе не являются вмешательством в частную жизнь. С точки зрения права на неприкосновенность частной жизни это различие не является убедительным. Сбор информации, относящейся к так называемым "метаданным", может дать даже еще более полное представление о поведении человека, его социальных отношениях, личных предпочтениях и личности, чем то, что можно было бы узнать из самого содержания частного общения. Как недавно отметил Суд Европейского союза, метаданные коммуникации, "взятые в целом, могут позволить прийти к очень точным выводам в отношении частной жизни людей, которых эти данные касаются"[5]. Признание этого нового обстоятельства стало причиной призывов к преобразованию существующей политики и практики для обеспечения лучшей защиту личных данных.

20. Из этого следует, что любая регистрация данных коммуникации является потенциальным вмешательством в частную жизнь и что сбор и сохранение данных коммуникации является вмешательством в частную жизнь вне зависимости от того, принимаются ли во внимание или используются ли эти данные в дальнейшем. Даже сама возможность того, что информация о коммуникации может быть зарегистрирована, представляет собой вмешательство в личную жизнь[6], потенциально сдерживая осуществление прав, в том числе права на свободу выражения и ассоциации. Таким образом, вмешательством в личную жизнь становится само существование программы массового слежения. Причем именно государству требовалось бы доказать, что подобное вмешательство не является ни произвольным, ни незаконным.

2. Что подразумевается под "произвольным" или "незаконным" вмешательством?

21. Согласно международному праву прав человека, ограничение права на неприкосновенность частной жизни допустимо единственно в том случае, когда таковое не является ни произвольным, ни незаконным. В своем замечании общего порядка №16 Комитет по правам человека разъяснил, что термин "незаконное" означает, что вмешательство вообще не может иметь места "за исключением случаев, предусмотренных законом. Вмешательство, разрешаемое государствами, может совершаться только на основании закона, который должен в свою очередь соответствовать положениям, целям и задачам Пакта"[7]. Иными словами, вмешательство, допустимое по национальным законам, может в то же время быть "незаконным", если национальное право вступает в противоречие с положениями Международного пакта о гражданских и политических правах.

[4] Executive Office of the President of the United States, “Big Data: Seizing Opportunities, Preserving Values”, May 2014 (размещено по адресу www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf), p. 54.

[5] 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, paras. 26-27, and 37. See also Executive Office of the President, “Big Data and Privacy: A Technological Perspective” (размещено по адресу www.whitehouse.gov/sites/default/files/microsites/ostp/PCAST/pcast_big_data_and_privacy_-_may_2014.pdf), p. 19.

[6] См. European Court of Human Rights, *Weber and Saravia v. Germany*, para. 78; *Malone v. UK*, para. 64.

[7] Официальные отчеты Генеральной Ассамблеи (см. сноску 3), пункт 3.

Понятие "произвольное вмешательство" также может распространяться на вмешательства, осуществляемые в соответствии с законом. Комитет пояснил, что введение этого понятия "призвано обеспечить, чтобы даже допускаемое законом вмешательство соответствовало положениям, целям и задачам Пакта и в любом случае являлось обоснованным в конкретных обстоятельствах"[8]. Концепцию обоснованности Комитет трактует как указание на то, что "любое вмешательство в личную жизнь должно быть пропорционально конечной цели и продиктовано обстоятельствами в каждом конкретном случае"[9].

22. В отличие от некоторых других положений Пакта, статья 17 четкой ограничительной клаузулы не содержит. Тем не менее, о сущности определений "произвольное или незаконное" можно судить на основе Сиракузских принципов толкования ограничений и отступлений от положений Международного пакта о гражданских и политических правах[10]; практики Комитета по правам человека, отраженной в его замечаниях общего порядка, включая № 16, 27, 29, 34 и 31; выводов по индивидуальным сообщениям[11] и заключительных замечаний[12]; положений регионального и национального прецедентного права[13]; а также мнений независимых экспертов[14]. В своем замечании общего порядка № 31 о характере общего юридического обязательства, налагаемого на государства − участники Пакта, Комитет по правам человека, например, отмечает, что вышеупомянутые должны воздержаться от нарушения прав, признаваемых данным Пактом, и что "любое ограничение любого из этих прав должно быть допустимым соответствующими положениями Пакта. Когда такие ограничения имеют место, государства обязаны доказывать их необходимость и принимать только такие меры, которые требуются для достижения законных целей с точки зрения обеспечения непрерывной и эффективной защиты прав по Пакту"[15]. Комитет в очередной раз подчеркнул, что "ни при каких обстоятельствах ограничения не могут применяться или осуществляться таким образом, чтобы это нарушало существо признанного в Пакте права".

23. Упомянутые авторитетные источники указывают на главнейшие принципы законности, необходимости и соразмерности, важность которых также отмечалась во многих из полученных материалов. Прежде всего, любые ограничения права на неприкосновенность частной жизни, предусмотренного в статье 17, должны быть подкреплены законом, а этот закон, в свою очередь, должен быть достаточно доступным, четким и однозначным, чтобы человек мог ознакомиться с текстом закона и удостоверится, кто и при каких обстоятельствах уполномочен заниматься сбором личной информации. Такое ограничение должно быть необходимым для достижения законной цели, адекватным ей, равно как и минимальным по масштабу вмешательства[16]. Более того, необходимо

[8] Там же, пункт 4.

[9] Сообщение № 488/1992, *Тунан против Австралии*, пункт 8.3; см. также № 903/1999, пункт 7.3, и 1482/2006, пункты 10.1 и 10.2.

[10] См. E/CN.4/1985/4, приложение.

[11] Например, сообщение № 903/1999, 2004, *Ван Хюлст против Нидерландов*.

[12] CCPR/C/USA/CO/4.

[13] Например, European Court of Human Rights, *Uzun v. Germany*, 2 September 2010, and *Weber and Soravia v. Germany*, para. 4; and Inter-American Court of Human Rights, *Escher v. Brazil*, Judgment, 20 November 2009.

[14] См. A/HRC/13/37 и A/HRC/23/40. Также см. Международные принципы применения прав человека в отношении мониторинга средств связи, доступно по ссылке https://ru.necessaryandproportionate.org/text.

[15] CCPR/C/21/Rev.1/Add. 13, пункт 6.

[16] CCPR/C/21/Rev.1/Add.9, пункты 11–16. См. также A/HRC/14/46, приложение, метод 20.

иметь возможность продемонстрировать, что ограничение, наложенное на осуществление конкретного права (вмешательство в частную жизнь, например, в целях защиты национальной безопасности или права на жизнь других людей) может потенциально способствовать достижению такой цели. Бремя доказывания того, что ограничение отвечает законной цели, ложится на власти, намеревающиеся ввести такое ограничение. Кроме того, никакое ограничение права на неприкосновенность частной жизни не должно подрывать существо соответствующего права, и любое ограничение должно соответствовать другим правам человека, включая запрет дискриминации. Любое ограничение, не отвечающее этим требованиям, является незаконным, и/или соответствующее вмешательство в осуществление права на неприкосновенность частной жизни − произвольным.

24. Правительства часто объясняют необходимость программ по слежению и сбору цифровых данных со ссылкой на интересы национальной безопасности, включая противодействие угрозе терроризма. В нескольких ответах утверждается, что, поскольку цифровые технологии могут использоваться и уже были использованы отдельными лицами в преступных целях (включая вербовку террористов, а также финансирование и совершение террористических актов), законное адресное отслеживание цифровых сообщений может стать необходимой и действенной мерой со стороны разведывательных и/или правоохранительных органов, при условии что оно осуществляется в соответствии с международным и национальным правом. Слежение в интересах национальной безопасности или в целях предотвращения проявлений терроризма или иных преступлений согласно статье 17 Пакта может рассматриваться как "законная цель". Степень вмешательства, однако, должна соизмеряться со степенью необходимости и практической пользой конкретной меры для достижения цели.

25. Говоря о степени необходимости той или иной меры, Комитет по правам человека в своем замечании общего порядка № 27 по статье 12 Международного пакта о гражданских и политических правах подчеркнул, что "ограничения не должны ущемлять существа рассматриваемого права […]; соотношение между правом и ограничением, между нормой и исключением, не должно видоизменяться"[17]. Далее Комитет разъяснил, что "недостаточно лишь того, чтобы ограничения служили достижению разрешенных целей; они также должны являться необходимыми для их защиты". Более того, такие меры должны быть соразмерными: "наименее ограничительное средство из числа тех, с помощью которых может быть достигнут желаемый результат"[18]. При наличии законной цели и надлежащих процессуальных гарантий государству позволяется осуществлять достаточно интрузивное слежение; однако государство по-прежнему обязано доказать, что такое вмешательство одновременно является необходимым и соразмерным конкретному риску. Массовые или "сплошные" программы слежения, таким образом, могут быть сочтены "произвольными", даже если они служат законной цели и были утверждены на основании общедоступного правового режима. Другими словами, 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.

26. Наряду с опасениями относительно того, что доступ к данным и их использование могут не всегда быть ориентированы исключительно на достиже-

[17] CCPR/C/21/Rev.1/Add.9, пункты 11–16. См. также Европейский суд по правам человека, *Handyside v. the United Kingdom*, пункт 48; и *Klass v. Germany*, пункт 42.

[18] CCPR/C/21/Rev.1/Add.9, пункты 11–16.

ние узконаправленных законных целей, также возникает вопрос, связанный с набирающей силу тенденцией правительств опираться на субъектов частного сектора для сохранения данных "на всякий пожарный случай", если они вдруг понадобятся для правительственных целей. Не может считаться необходимой или соразмерной практика обязательного сохранения данных третьей стороны − стандартная практика слежения во многих странах, где правительства обязывают телефонные компании и компании, поставляющие интернет-услуги, хранить метаданные о контактах и местоположении клиентов для последующего использования в рамках правоохранительной деятельности, равно как и для предоставления разведывательным агентствам[19].

27. Помимо прочих факторов при определении соразмерности следует учитывать, какие именно действия производятся с единожды собранными сплошными данными, и кто имеет к ним доступ. В законодательстве многих стран отсутствует концепция "ограниченного использования" данных, вследствие чего допускается не только сбор данных с конкретной законной целью, но и их последующее использование для любой иной цели. Отсутствие эффективных ограничительных мер стало еще острее ощущаться после 11 сентября 2001 года с размыванием границ между уголовным правосудием и охраной национальной безопасности. Установившаяся в результате этого практика обмена данными между правоохранителями, разведкой и другими государственными органами ставит под угрозу положения статьи 17 Пакта, поскольку меры слежения, являющиеся необходимыми и соразмерными для одной законной цели, могут не быть таковыми для другой цели. Обзор национальной практики по доступу правительства к данным третьих сторон показал, что, "прежде всего, в сочетании со все большей легкостью доступа к данным частного сектора для агентств и ведомств по национальной безопасности и охране правопорядка нарастающая свобода обмена информацией между ними, равно как и свобода использования этой информации в целях, отличных от изначальной, свидетельствует о значительном ослаблении традиционной системы защиты данных"[20]. Именно по этой причине суды нескольких стран приняли решения, отменяющие действие такого режима обмена данными. Другие высказали предположение, что упомянутые ограничительные меры являются надежным гарантом добросовестного исполнения государством своих обязательств, предусмотренных статьей 17 Пакта[21], при наличии действенных санкций за нарушение предусмотренных ими ограничений.

B. Защита закона

28. В пункте 2 статьи 17 Международного пакта о гражданских и политических правах четко прописано, что каждый человек имеет право на защиту закона от незаконного или произвольного вмешательства в личную жизнь. Подразумевается, что все программы по наблюдению за коммуникацией должны про-

[19] См. мнение главного адвоката Круза Вильялона при рассмотрении Судом Европейского союза объединенных дел C-293/12 и C-594/12, где сказано, что директива 2006/24/EU (по сохранению данных, касающихся общедоступных услуг электронного обмена данных) "в целом" является нарушением Хартии Европейского союза об основных правах, поскольку она не налагает строгих ограничений на такое сохранение данных. См. также CCPR/C/USA/CO/4, пункт 22.

[20] Fred H. Cate, James X. Dempsey and Ira S. Rubinstein, “Systematic government access to private-sector data”, International Data Privacy Law, vol. 2, No. 4, 2012, p. 198.

[21] См. A/HRC/14/46, приложение, метод 23.

водиться на основании доступных для всеобщего ознакомления законодательных норм, которые, в свою очередь, должны соответствовать конституционному режиму государства и международному праву прав человека[22]. "Доступность" предусматривает не только обнародование закона, но и то, что он будет достаточно четким, чтобы затронутое лицо могло регулировать свое поведение, зная о возможных последствиях того или иного действия. Государство должно обеспечить, чтобы любое вмешательство в осуществление права на неприкосновенность личной жизни, семейной жизни, жилища или тайны переписки санкционировалось законом, который: a) доступен для всеобщего ознакомления; b) обеспечивает соответствие сбора, доступа или использования содержащихся в сообщениях данных конкретным предусмотренным в законе целям; c) достаточно четким, подробно определяя условия, при которых такое вмешательство допускается, порядок получения разрешения, категории лиц, в отношении которых может вестись слежение, предельные сроки слежения; порядок использования и хранения полученных данных; и d) предусматривает эффективные гарантии против злоупотребления[23].

29. Следовательно, тайные правила и тайные толкования, и даже тайные судебные толкования законов не обладают необходимыми качествами "закона"[24]. Не обладают ими ни законы и правила, которые предоставляют органам исполнительной власти, например службам безопасности и разведки, чрезмерную свободу действий; объем и порядок осуществления таких дискреционных полномочий должны оговариваться с достаточной четкостью (в самом законе или в обязательных опубликованных правилах). Не может быть адекватным открытый для всеобщего ознакомления закон, если невозможно заранее предугадать, как именно он будет действовать. Тайный характер особых полномочий на проведение наблюдения влечет за собой еще больший риск произвольного осуществления дискреционных полномочий, что, в свою очередь, требует дополнительного надзора и большей четкости норм, регулирующих осуществление дискреционных полномочий. Некоторые страны требуют наличия нормативной регламентации на уровне первичного законодательства, которое обсуждается в парламенте, а не на уровне обычных подзаконных актов, вводимых органами исполнительной власти, – это требование позволяет гарантировать доступность нормативно-правовой основы для заинтересованных лиц не только после принятия, но и в ходе ее разработки в соответствии со статьей 25 Международного пакта о гражданских и политических правах[25].

30. Требование о доступности закона также важно в процессе оценки новой практики государств по привлечению внешних субъектов к ведению наблюдения. Существует достоверная информация, которая позволяет предположить, что правительства некоторых государств систематически перепоручали функции по сбору и анализу органам, действующим в странах с более слабыми гарантиями неприкосновенности частной жизни. По имеющимся сведениям, некоторые государства пользовались услугами транснациональной сети разведывательных агентств, совмещая и преумножая лазейки в законодательстве для координации наблюдения таким образом, чтобы обойти гарантии, предоставляемые национальными правовыми режимами. Есть веские основания утвер-

[22] See ibid., annex.

[23] CCPR/C/USA/CO/4, пункт 22. См. также European Court of Human Rights, *Malone v. the United Kingdom*, No. 8691/79, 2 August 1984, paras. 67 and 68; and *Weber and Saravia v. Germany*, application no. 54934/00, 29 June 2006, где суд перечисляет минимальные гарантии, которые должны быть отражены в статутном праве.

[24] См. CCPR/C/USA/CO/4, пункт 22.

[25] См. также A/HRC/14/46.

ждать, что подобная практика является незаконной, потому что, как было отмечено в некоторых материалах, предоставленных для данного доклада, действие режима по наблюдению становится непредсказуемым для тех, на кого он распространяется. Она может поставить под угрозу сам принцип права, закрепленного в статье 17 Международного пакта о гражданских и политических правах, и поэтому запрещается статьей 5 этого документа. Государствам также не принимают эффективных мер для защиты отдельных лиц, находящихся под их юрисдикцией, от незаконного наблюдения, практикуемого другими государствами или компаниями, что противоречит их собственным обязательствам по защите правам человека.

C. Кто и где находится под защитой?

31. Проблема экстерриториального применения Международного пакта о гражданских и политических правах к цифровому наблюдению и слежению рассматривалась в нескольких полученных ответах. При всех очевидности того, что определенные аспекты программ, о которых стало известно недавно, непосредственно затрагивают территориальные обязательства государств, проводящих наблюдение, была выражена дополнительная обеспокоенность по поводу экстерриториального слежения и перехвата сообщений.

32. Статья 2 Международного пакта о гражданских и политических правах предписывает каждому государству-участнику уважать и обеспечивать всем находящимся в пределах его территории и под его юрисдикцией лицам права, признаваемые в Пакте, без какого бы то ни было различия, как-то в отношении расы, цвета кожи, пола, языка, религии, политических и иных убеждений, национального или социального происхождения, имущественного положения, рождения или иного обстоятельства. Комитет по правам человека в замечании общего порядка № 31 подтвердил, что согласно пункту 1 статьи 2 от государств-участников требуется уважать и обеспечивать признаваемые в Пакте права всем лицам, находящимся в пределах их территории, и всем лицам, находящимся под их юрисдикцией. Это означает, что государство-участник обязано уважать и обеспечивать любому лицу, находящемуся в пределах компетенции или эффективного контроля этого государства-участника, права, признаваемые в Пакте, даже если лицо не находится на территории государства-участника[26]. Это относится к лицам, на которых распространяются полномочия государств[27].

33. Совет по правам человека исходит из принципа, отмеченного еще в ранней практике Совета, согласно которому государство не может уклониться от выполнения своих международных обязательств в области прав человека, совершая вне своих территорий такие действия какие ему запрещено совершать "в пределах границ"[28]. Данная позиция согласуется с взглядами Международного Суда, который подтвердил, что Международный пакт о гражданских и политических правах применяется в отношение деяний, совершенных государством "при осуществлении своей юрисдикции за пределами своей собственной терри-

[26] CCPR/C/21/Rev.1/Add.13, пункт 10.

[27] См. *Официальные отчеты Генеральной Ассамблеи, тридцать шестая сессия, Дополнение № 40* (A/36/40), приложение XIX, пункт 12.2; см. также приложение XX. См. также CCPR/CO/78/ISR, пункт 11; CCPR/CO/72/NET, пункт 8; CCPR/CO/81/BEL, пункт 6 и Inter-American Commission of Human Rights, *Coard et al. v. the United States*, дело № 10.951, отчет № 109/99, 29 сентября 1999 года, пункты 37, 39, 41 и 43.

[28] См. *Официальные отчеты Генеральной Ассамблеи, тридцать шестая сессия* (см. сноску 27), приложение XIX, пункты 12.2−12.3 и приложение XX, пункт 10.3.

тории"[29], а также со статьями 31 и 32 Венской конвенции о праве международных договоров. Понятия "властных полномочий" и "эффективного контроля" являются показателями того, осуществляет ли государство "юрисдикцию" или властные полномочия, злоупотребление которыми должно предполагаемо сдерживаться гарантиями прав человека. Государство не может уклониться от выполнения своих обязательств в области прав человека, попросту воздержавшись от регламентации этих полномочий на основе закона. В противном случае это не только подрывало бы универсальность и существо прав, которые находятся под защитой международного права прав человека, но и могло бы создавать структурные стимулы, побуждающие государства передавать друг другу функции по проведению слежения.

34. Соответственно цифровое слежение может задействовать обязательства государства в области прав человека, если такое слежение сопровождается осуществлением властных полномочий или эффективным контролем государства в отношении инфраструктуры цифровой связи, где бы она ни находилась, посредством прямого перехвата информации или проникновения в данную инфраструктуру. Аналогичным образом, если государство осуществляет нормативную юрисдикцию в отношении третьей стороны, которая физически контролирует информацию, данное государство также обязано следовать требованиям Пакта. Если государство претендует на установление юрисдикции в отношении информации частных компаний в результате регистрации данных компаний в стране, то необходимо распространить сферу защиты прав человека на тех, чья личная жизнь подвергается вмешательству как в стране, где компания осуществляет деятельность, так и за ее пределами. Это утверждение справедливо вне зависимости от того, осуществляется ли юрисдикция законным образом или фактически нарушает суверенитет другого государства.

35. Данный вывод в равной степени важен в свете текущих обсуждений того, должны ли "иностранцы" и "граждане" иметь равный доступ к средствам защиты конфиденциальной информации в рамках режимов контроля за деятельностью спецслужб. В некоторых правовых режимах проводятся различия между обязательствами перед гражданами или лицами, находящимися на территории государства, и негражданами и лицами, находящимися вне территории государства[30], либо иным образом предусматривается более низкая защищенность зарубежной или внешней коммуникации. При наличии каких-либо сомнений по поводу того, являются ли данные внутренними или внешними, спецслужбы всегда рассматривают данные как внешние (а цифровая информация регулярно в какой-то момент пересекает границу) и на этом основании дают разрешение на их сбор и хранение. Как следствие, защита частной жизни иностранцев и неграждан, по сравнению с гражданами страны, становится очень слабой (или вообще отсутствует).

36. Международное право прав человека недвусмысленно определяет принцип недискриминации. Согласно статье 26 Международного пакта о граждан-

[29] Консультативное заключение Международного Суда относительно правовых последствий строительства стены на оккупированной палестинской территории, от 9 июля 2004 года (A/ES-10/273 и Corr.1), пункты 107−111. См. также Международный Суд, дело о вооруженной деятельности на территории Конго (*Демократическая Республика Конго против Уганды*), решение суда, 2005 год, стр. 168.

[30] См., например, в the United States, the Foreign Intelligence Surveillance Act S1881(a); в the United Kingdom, the Regulation of Investigatory Powers Act 2000, s8(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).

ских и политических правах, "все люди равны перед законом и имеют право на равную защиту закона без всякой дискриминации", далее говорится, что "в этом отношении всякого рода дискриминация должна быть запрещена законом, и закон должен гарантировать всем лицам равную и эффективную защиту против дискриминации по какому бы то ни было признаку, как-то расы, цвета кожи, пола, языка, религии, политических или иных убеждений, национального или социального происхождения, имущественного положения, рождения или иного обстоятельства". Эти положения следует рассматривать вместе со статьей 17, из которой следует, что "никто не может подвергаться произвольному вмешательству в его личную жизнь" и что "каждый человек имеет право на защиту закона от такого вмешательства или таких посягательств", а также пунктом 1 статьи 2. В этой связи Комитет по правам человека подчеркивает важность "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"[31].

D. Процессуальные гарантии и эффективный надзор

37. Пункт 2 статьи 17 Международного пакта о гражданских и политических правах гласит, что каждый человек имеет право на защиту закона от незаконного или произвольного вмешательства или посягательства. "Защита закона" должна быть обеспечена посредством надежных процессуальных гарантий, включая эффективные институциональные механизмы с необходимыми ресурсами. Однако очевидно, что отсутствие эффективного надзора стимулировало практику непривлечения к ответственности за произвольные или незаконные посягательства на право на неприкосновенность частной жизни в цифровой среде. Внутренние гарантии, особенно без независимого внешнего контроля, оказались неэффективны в борьбе с незаконными или произвольными методами слежения. Хотя эти гарантии могут принимать различные формы, участие всех ветвей власти, а также независимого гражданского агентства в надзоре за программами слежения за электронными коммуникациями очень важно для обеспечения эффективной защиты закона.

38. Вовлеченность судебной власти, которая отвечает международным стандартам в отношении независимости, беспристрастности и прозрачности, может увеличить шансы того, что общий правовой режим будет соответствовать минимальным стандартам, требуемым международным правом прав человека. В то же время не следует полагать, что участие судебной власти в осуществлении надзора станет панацеей; в некоторых государствах судебное разрешение на цифровое слежение разведывательных и правоохранительных служб или надзор за его осуществлением стали пустой формальностью. Вследствие этого все больше внимания уделяется смешанным моделям административного, судебного и парламентского надзора, что подчеркивалось в некоторых материалах, представленных при подготовке настоящего доклада. Особый интерес представляет создание должностей "защитников интересов общественности" при процедурах выдачи разрешений на слежение. С учетом растущей значимости третьих сторон, например провайдеров интернет-услуг, возможно, также следует рассмотреть вопрос о том, чтобы позволить им участвовать в выдаче разрешения на методы наблюдения, влияющие на их интересы, или позволить

[31] CCPR/C/USA/CO/4, пункт 22.

им обжаловать существующие методы. В судебной практике по этому вопросу с одобрением отмечалась польза независимого заключения, мониторинга и/или процедур пересмотра для обеспечения строгого контроля над мерами, принимаемыми на основе предусмотренного законом режима электронного слежения. Парламентские комитеты также могут сыграть важную роль, однако и у них могут отсутствовать необходимая степень независимости, ресурсы или желание распознать нарушение, или же они могут попасть в так называемую "регулятивную ловушку". В судебной практике на региональном уровне подчеркивается польза абсолютно независимого надзорного органа, в частности, в целях контроля над исполнением утвержденных мер наблюдения[32]. В этой связи в 2009 году Специальный докладчик по вопросу о поощрении и защите прав человека и основных свобод в условиях борьбы с терроризмом заявил, что "не должно быть места для секретной системы наблюдения, на которую не распространяется контроль со стороны эффективного надзорного органа, а на все виды вмешательства должно выдаваться разрешение независимого органа"[33].

E. Право на эффективное средство правовой защиты

39. Согласно Международному пакту о гражданских и политических правах, государства-участники должны гарантировать, что жертвы нарушений Пакта обладают эффективным средством правовой защиты. В пункте 3 b) статьи 2 далее определяется, что государства-участники Пакта берут на себя обязательство "обеспечить, чтобы право на правовую защиту для любого лица, требующего такой защиты, устанавливалось компетентными судебными, административными или законодательными властями или любым другим компетентным органом, предусмотренным правовой системой государства, и развивать возможности судебной защиты". Государства также должны гарантировать, что компетентные органы обеспечат соблюдение таких средств правовой защиты. Как подчеркивает Комитет по правам человека в своей общей рекомендации № 31, непринятие государством-участником мер для проведения расследования утверждений об имевших место нарушениях само по себе может стать отдельным нарушением Пакта[34]. Кроме того, одной из важнейших составляющих права на эффективное средство правовой защиты является пресечение длящихся нарушений.

40. Таким образом, эффективные средства правовой защиты жертв нарушений права на неприкосновенность личной жизни посредством отслеживания цифровых данных могут принимать разные судебные, законодательные и административные формы. Эффективные средства правовой защиты, как правило, имеют некоторые общие характерные особенности. Во-первых, такие средства правовой защиты должны быть известны и доступны всем, кто утверждает, что их права были нарушены. Так, уведомление (о том, что применяются специальные меры наблюдения или общий режим наблюдения) и право на обращение в суд (для обжалования таких мер) становятся решающими в определении доступа к эффективному средству правовой защиты. Государства по-разному подходят к вопросу об уведомлениях: в то время как некоторые требуют уведомления об объектах наблюдения постфактум, сразу после окончания расследования, многие режимы не предусматривают процедуру уведомления. Некоторые также могут формально требовать подобное уведомление в уголовных делах, однако

[32] См., например, European Court of Human Rights, *Ekimdzhiev v. Bulgaria*, application No. 62540/00, 28 June 2007.

[33] A/HRC/13/37, пункт 62.

[34] CCPR/C/21/Rev.1/Add. 13, пункт 15.

на деле эту процедуру обычно игнорируют. Существуют и различные подходы на национальном уровне, касающиеся права физического лица на обращение в суд для обжалования. Европейский суд по правам человека вынес решение, согласно которому, хотя существование режима наблюдения, возможно, является вмешательством в личную жизнь, заявление о том, что это приводит к нарушению прав, может рассматриваться только в тех случаях, когда есть "разумная вероятность" того, что человек на самом деле подвергся незаконной слежке[35].

41. Во-вторых, эффективные средства правовой защиты будут включать в себя тщательное оперативное и беспристрастное расследование предполагаемых нарушений. Оно может проводиться "независимым надзорным органом […], при наличии надлежащих процессуальных гарантий и судебного надзора в рамках ограничений, допустимых в демократическом обществе"[36]. В-третьих, чтобы средства правовой защиты были эффективными, они должны быть способны остановить длящиеся нарушения, например путем удаления данных или других средств восстановления нарушенных прав[37]. Такие органы правовой защиты должны иметь "полный и беспрепятственный доступ ко всей соответствующей информации, необходимым ресурсам и опыту экспертов для проведения расследований, а также иметь полномочия издавать обязательные распоряжения"[38]. В-четвертых, в случаях, когда нарушения прав человека переходят на уровень грубых нарушений, несудебных средств правовой защиты будет недостаточно, так как потребуется уголовное преследование[39].

IV. Какая роль отведена бизнесу?

42. Существуют убедительные доказательства того, правительства все шире полагаются на услуги частного сектора для отслеживания или содействия отслеживанию электронных данных. На каждом континенте для того, чтобы получить доступ к содержанию электронных сообщений и метаданным, правительства применяли как официальные правовые механизмы, так и негласные методы. Этот процесс становится все более и более формализованным: по мере передачи функций по предоставлению телекоммуникационных услуг от государственного сектора частному происходит "делегирование правоприменительных и квазиюридических полномочий интернет-посредникам под предлогом

[35] См. *Esbester v. the United Kingdom*, application No. 18601/91, Commission decision of 2 April 1993; *Redgrave v. the United Kingdom*, application No. 202711/92, Commission decision of 1 September 1993; and *Matthews v. the United Kingdom*, application No. 28576/95, Commission decision of 16 October 1996.

[36] "Joint declaration on surveillance programs and their impact on freedom of expression", issued by the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression and the Special Rapporteur for Freedom of Expression of the Inter-American Commission on Human Rights, June 2013 (размещено по адресу www.oas.org/en/iachr/expression/showarticle.asp?artID=927&lID=1), para. 9.

[37] См., например, European Court of Human Rights, *Segersted-Wiber and others v. Sweden*, application No. 62332/00, 6 June 2006. См. также CCPR/C/21/Rev.1/Add. 13, пункты 15−17.

[38] A/HRC/14/46.

[39] Основные принципы и руководящие положения, касающиеся права на правовую защиту и возмещение ущерба для жертв грубых нарушений международных норм в области прав человека и серьезных нарушений международного гуманитарного права (приложение к резолюции 60/147 Генеральной Ассамблеи).

"саморегулирования" и "сотрудничества"[40]. Введение законодательных требований, согласно которым компании обязаны конфигурировать свои сети таким образом, чтобы сделать возможным перехвату электронных сообщений вызывает особое беспокойство в значительной степени потому, что таким образом создается среда, которая упрощает применение масштабных мер по слежению.

43. Государство может иметь законные основания запросить данные о пользователях у компании, работающей в области информационных и коммуникационных технологий; однако если компания предоставляет данные или информацию о пользователях государству в ответ на запрос, который нарушает право на неприкосновенность частной жизни, предусмотренное международным правом, передает государству технологии или оборудование для массового слежения без надлежащих гарантий или если информация иным образом используется в нарушение прав человека, то такая компания рискует стать соучастником или быть иным образом замешанной в нарушении прав человека. В Руководящих принципах предпринимательской деятельности в аспекте прав человека, одобренных Советом по правам человека в 2011 году, содержится общепринятая норма, направленная на предупреждение и устранение неблагоприятного воздействия предпринимательской деятельности на права человека. Обязательство уважать права человека распространяется на отделения компании по всему миру вне зависимости от места нахождения ее пользователей и существует независимо от того, выполняет государство свои обязательства в области прав человека или нет.

44. Многие стороны предприняли важные усилия для того, чтобы уточнить сферу применения Руководящих принципов в коммуникационном секторе и секторе информационных технологий. Предприятия, которые предоставляют информацию и услуги по доступу в интернет или поставляют технологии и оборудование, обеспечивающее цифровую связь, должны, например, выступить с конкретными программными заявлениями о своей приверженности соблюдению прав человека во всех аспектах своей деятельности. Они должны также придерживаться соответствующей политики должной осмотрительности, с тем чтобы определить, оценить, предупредить и смягчить любое неблагоприятное воздействие. Компаниям следует оценивать вероятность и степень возможного воздействия их услуг или политики сбора и передачи информации о пользователях на права человека.

45. В ситуациях, когда компании сталкиваются с требованиями правительства обеспечить доступ к информации, которая не соответствует международным правозащитным стандартам, они должны стремиться как можно более полно уважать принципы защиты прав человека и быть готовым продемонстрировать свои постоянные усилия, предпринимаемые в этом направлении. Например, это может предполагать наиболее узкую трактовку запросов государственных органов о доступе к информации, направление просьб о предоставлении разъяснений по поводу охвата и правовых оснований таких запросов, обращение за решением суда перед выполнением требования о предоставлении данных, а также непосредственное обсуждение с пользователями рисков и порядка соблюдения требований правительства. Существуют положительные примеры действий, предпринятых отраслью в этом направлении, как на уровне отдельных компаний, так и на совместных началах.

[40] См. European Digital Rights, “The Slide from ’Self-Regulation’ to Corporate Censorship”, Брюссель, январь 2011 года, доступно по адресу www.edri.org/files/EDRI_selfreg_final_20110124.pdf.

46. Важнейшим аспектом проявления должной заботы о правах человека, как она определена Руководящих принципах, является проведение конструктивных консультаций с затрагиваемыми сторонами. В контексте компаний, работающих в области информационных и коммуникационных технологий, сюда также входит обеспечение пользователей необходимыми сведениями о порядке сбора, хранения, использования и потенциального распространения информации о них, чтобы они могли выражать обеспокоенность и принимать взвешенные решения. В Руководящих принципах разъясняется, что там, где предприятия определили, что они оказали или способствовали оказанию неблагоприятного воздействия на права человека, они обязаны загладить ущерб, либо непосредственно предоставив возмещение, либо сотрудничая с предусмотренными законом процедурами правовой защиты. Для исправления положения на возможно более ранней стадии компании должны создать механизмы рассмотрения жалоб на оперативном уровне. Такие механизмы на уровне компаний могут быть особенно важными в странах, где права не защищены надлежащим образом или где нет доступа к судебным и внесудебным средствам правовой защиты. В дополнение к таким элементам, как компенсация и реституция, правовая защита должна предполагать получение информации о том, какие именно сведения были переданы в распоряжение государственных органов и каким образом.

V. Выводы и рекомендации

47. **Международное право прав человека обеспечивает четкую и универсальную основу для поощрения и защиты права на неприкосновенность частной жизни, в том числе в контексте внутреннего и экстерриториального слежения за информационными потоками, перехвата цифровых сообщений и сбора личных данных. Однако практика многих государств свидетельствует об отсутствии адекватного национального законодательства и/или правоприменения, слабости процессуальных гарантий и неэффективности надзора, что в совокупности приводит к отсутствию ответственности за произвольное или незаконное вмешательство в личную жизнь.**

48. **При восполнении существенных пробелов в осуществлении права на неприкосновенность частной жизни необходимо принять во внимание два обстоятельства. Первое заключается в том, что вскрываются все новые и новые сведения о политике и практике внутринационального и экстерриториального слежения. Продолжаются расследования с целью получения информации об электронном слежении и сборе и хранении персональных данных, а также с целью оценки воздействия слежения на осуществление прав человека. Суды на национальном и региональном уровнях изучают вопросы законности политики электронного слежения и мер, связанных с его проведением. При любой оценке соответствия политики и практики слежения международному праву прав человека необходимо учитывать меняющийся характер самой этой проблемы. Вторым связанным с этим обстоятельством, которое вызывает тревогу, является непрозрачность 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.**

49. **Эффективное реагирование на вызовы, связанные с правом на неприкосновенность личной жизни в контексте современных коммуникационных технологий, потребует последовательной и слаженной работы мно-**

гих заинтересованных сторон. Этот процесс должен включать в себя диалог с привлечением всех заинтересованных сторон, в том числе государств-членов, гражданского общества, научных и технических сообществ, предпринимателей, ученых и специалистов по правам человека. На фоне дальнейшего развития коммуникационных технологий лидерство призвано сыграть решающую роль в обеспечении того, чтобы потенциал этих технологий использовался для лучшего осуществления прав человека, закрепленных в международно-правовых актах.

50. **С учетом вышеупомянутых обстоятельств существует явная и насущная потребность в строгом контроле за соответствием любой политики или практики слежения международному праву прав человека, в том числе праву на неприкосновенность частной жизни, посредством создания эффективных гарантий от любых посягательств. В качестве безотлагательной меры государствам следует пересмотреть свое собственное внутреннее законодательство, политику и практику, чтобы обеспечить их полное соответствие международному праву прав человека. При выявлении любых упущений государства должны принять меры по их устранению, в том числе посредством создания четкой, конкретной, доступной, всеобъемлющей и недискриминационной нормативно-правовой базы. Необходимо принять меры по введению режима и практики независимого надзора, уделив особое внимание праву потерпевших на эффективное возмещение.**

51. **На пути поощрения и защиты права на неприкосновенность частной жизни в цифровую эпоху потребуется решить целый ряд важных практических проблем. Опираясь на первоначальное исследование в настоящем докладе некоторых из них, необходимо продолжить обсуждение и изучение вопросов, связанных с эффективной защитой закона, процессуальными гарантиями, эффективным надзором и средствами правовой защиты. Углубленный анализ этих проблем поможет выработать дальнейшие практические рекомендации, основанные на международном праве прав человека, принципах необходимости, соразмерности и правомерности в отношении практики слежения; на мерах эффективного, независимого и непредвзятого надзора; и на мерах по возмещению. Дальнейший анализ также поможет компаниям выполнять свои обязательства по соблюдению прав человека, включая должную заботу и гарантии по управления рисками, а также выполнять свою роль по обеспечению эффективных средств правовой защиты.**