Организация Объединенных Наций A/HRC/29/32

Генеральная Ассамблея

Distr. General
22 May 2015
Russian
Original: English

Совет по правам человека
Двадцать девятая сессия
Пункт 3 повестки дня
Поощрение и защита всех прав человека, гражданских, политических, экономических, социальных и культурных прав, включая право на развитие

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

Резюме

В настоящем докладе, представляемом в соответствии с резолюцией 25/2 Совета по правам человека, Специальный докладчик рассматривает вопрос об использовании средств шифрования и анонимности при передаче цифровых сообщений. С учетом изученных международных и национальных норм и судебных решений, а также материалов, полученных от государств и гражданского общества, в докладе сделан тот вывод о том, что шифрование и анонимность позволяют людям осуществлять свои права на свободу мнений и их свободное выражение в цифровой век и ввиду этого должны заслуженно пользоваться надежной защитой.

* Представляется с опозданием.

GE.15-07497 (R) 170615 190615

Содержание

I. Введение

1. С появлением современных цифровых технологий у правительств, корпораций, преступников и мелких хулиганов появилась беспрецедентная возможность вмешиваться в осуществление прав на свободу мнений и их свободное выражение. Цензура в онлайновой среде, массовая и адресная слежка и сбор данных, кибератаки на гражданское общество и гонения на лиц, высказывающих свои мнения в Интернете, вынуждают жителей разных стран мира добиваться гарантий права беспрепятственно придерживаться своих мнений и искать, получать и распространять любого рода информацию и идеи. Многие в попытке обеспечить свою безопасность прибегают к шифрованию, т.е. кодированию данных, благодаря которым доступ к ним получают только обозначенные адресаты и которое может быть применено как к передаваемым данным (например, по электронной почте, системам направления сообщений, IP-телефонии), так и к хранимым данным (например, на жестких дисках, в удаленной среде так называемых "облачных" хранилищ). Другие пользователи прибегают к анонимности в качестве дополнительного элемента защиты, используя сложные технологии для сокрытия своей личности и следов присутствия в цифровом пространстве. Шифрование и анонимность, являющиеся на сегодняшний день основными средствами обеспечения онлайновой безопасности, открывают перед людьми возможность оградить свою частную жизнь от вмешательства и при этом беспрепятственно искать, читать, формировать и распространять мнения и информацию, а также позволяют журналистам, организациям гражданского общества, представителям этнических или религиозных групп, лицам, подвергающимся преследованиям по причине сексуальной ориентации или гендерной идентичности, общественным деятелям, ученым, деятелям искусства и всем прочим осуществлять свои права на свободу мнений и их свободное выражение.

2. Однако так же, как по телефону можно, с одной стороны, сообщить в полицию о совершении преступлении, а с другой, – вступить в заговор для его совершения, так и Интернет может быть неправомерно использован для нанесения ущерба правам других плюдей, национальной безопасности или общественному порядку. Представители правоохранительных и разведывательных служб нередко заявляют, что анонимные или зашифрованные сообщения затрудняют расследование финансовых преступлений или преступлений, связанных с незаконными наркотическими средствами, детской порнографией и терроризмом. Некоторые выражают обоснованные опасения в связи с тем, что с появлением новых технологий лицам, третирующим окружающих, и преступникам проще запугивать своих жертв. В некоторых государствах использование шифрования и анонимности ограничено или запрещено на этих и других основаниях, а в ряде других предлагаются или вводятся меры, позволяющие правоохранительных органам обойти такие элементы защиты и получить доступ к личным сообщениям.

3. В свете этих проблем в настоящем докладе рассматриваются два взаимно связанных вопроса. Во-первых, распространяются ли права на неприкосновенность частной жизни и свободу мнений и их свободное выражение на защищенную передачу сообщений в онлайновой среде, в частности при помощи шифрования или анонимности? И во-вторых, в случае утвердительного ответа, в какой мере правительства, руководствуясь нормами международного права по правам человека, могут вводить ограничения в отношении шифрования и анонимности? В настоящем докладе предпринимается попытка ответить на эти вопросы, рассмотреть примеры из практики государств и предложить рекомендации. В нем не ставится цель затронуть все технические или правовые вопросы, возникающие в связи с цифровыми технологиями, но при этом обозначаются наиболее важные из них для освещения их в последующих докладах.

4. При подготовке настоящего доклада Специальный докладчик направил государствам вопросник для сбора представляющей интерес информации об их законодательстве, нормативах, политике и практике. К 1 апреля 2015 года на его просьбу ответили 16 государств[1]. Специальный докладчик также обратился с просьбой о направлении соответствующих материалов к неправительственным заинтересованным сторонам и созвал совещание экспертов в Женеве в марте 2015 года. Размещенные на веб-странице мандатария ответы правительств и более 30 материалов, представленных организациями и отдельными представителями гражданского общества, послужили значительным подспорьем при составлении доклада.

5. С полным отчетом о деятельности, проведенной Специальным докладчиком с начала срока его полномочий в августе 2014 году, можно ознакомиться на веб-странице мандатария. Настоящий доклад, ставший первым для нынешнего мандатария, призван содействовать дальнейшему продвижению работы, посвященной препятствиям для свободы выражения мнений в цифровой век.

II. Защищенное и конфиденциальное общение в цифровой век

A. Современные виды шифрования и анонимность

6. Современные подходы к передаче конфиденциальных и защищенных сообщений продиктованы идеями, известными человечеству на протяжении тысячелетий. С распространением электронных носителей данных, Интернета и систем массового сбора и хранения информации стала очевидна потребность в передовых средствах защиты личных, корпоративных и государственных данных. С тех пор как электронная почта, системы мгновенной передачи сообщений, протоколы передачи голоса через Интернет, видео-конференц-связь и социальные сети перестали быть нишевыми услугами и превратились в доминирующие и легко отслеживаемые виды связи, у пользователей возникла потребность в онлайновой безопасности, в условиях которой они могли бы искать, получать и распространять информацию, не опасаясь негативных последствий, раскрытия данных, слежения или любых других форм ненадлежащего использования выраженных ими мнений.

7. Шифрование – это математический "процесс преобразования сообщений, информации или данных, в результате которого они не могут быть прочитаны никем, кроме обозначенного получателя"[2]; оно служит соблюдению конфиденциальности и сохранности содержимого и его защите от доступа или манипуляций третьих сторон. Криптостойкое шифрование, ранее бывшее прерогативой исключительно военных и разведслужб, стало общедоступным средством и зачастую свободно используется для защиты электронных писем, голосовых сообщений, изображений, информации на жестких дисках и веб-браузерах. При "шифровании в системе с открытым ключом", наиболее распространенной форме защиты при передаче данных между конечными пунктами, отправитель использует открытый ключ получателя для зашифровки сообщения и приложений к нему, а получатель использует свой личный ключ для их расшифровки. Шифрование может также применяться для создания цифровых подписей для засвидетельствования подлинности документа и личности отправителя, для идентификации и проверки

[1] Ответы были получены от следующих государств: Австрии, Болгарии, Гватемалы, Германии, Греции, Ирландии, Казахстана, Катара, Кубы, Ливана, Норвегии, Республики Молдова, Словакии, Соединенных Штатов Америки, Турции и Швеции.

[2] См. SANS Institute, "History of encryption" (2001).

сервера и для защиты содержания направляемых клиентам сообщений от компрометации или манипуляций процессом их передачи третьими сторонами (например, атаки с применением технологии "незаконный посредник"). Поскольку шифрование данных в процессе передачи не спасает от взлома нешифрованных данных на стадии их хранения в одной из конечных точек (и не обеспечивает защиту личного ключа), пользователь может также зашифровать данные, хранящиеся на переносных компьютерах, жестких дисках, серверах, электронных планшетах, мобильных телефонах и других устройствах. Кроме того, в складывающейся в онлайновой среде практике, возможно, наметился отказ от описанной здесь системы в пользу технологии "совершенной прямой секретности" или криптологического протокола "OTR", предусматривающих создание эфемерных ключей и особенно часто использующихся в системах мгновенной передачи сообщений.

8. Некоторые выступают за ослабление или компрометацию стандартов шифрования, чтобы доступ к зашифрованным сообщениям могли иметь только государства. Однако скомпрометированные алгоритмы шифрования вполне под силу раскрыть тем, кто овладел искусством находить и использовать слабые места, независимо от того, действуют ли они в государственных или негосударственных, законных или преступных целях. По всей видимости, все технические специалисты единодушны во мнении о том, что не существует особого доступа, который можно было бы открыть только для органов власти, даже для тех из них, кто в принципе руководствуется интересами населения. В существующей технологической среде намеренная компрометация ключей шифрования, даже в предположительно законных целях, подрывает онлайновую безопасность всех пользователей.

9. Так, шифрование используется для защиты содержания сообщений, а не элементов идентификации, как то адресов сетевого протокола (IP-адреса), относящихся к категории метаданных. Третьи стороны могут почерпнуть важную информацию о личности того или иного человека с помощью анализа метаданных, в случае если пользователь не прибегает к средствам ононимизации. Анонимность является непременным фактором, позволяющим избежать идентификации. В условиях анонимности, как отражения присущего всем людям стремления скрыть сведения о себе от толпы, пользователь гораздо более свободен изучать и распространять идеи и мнения, чем если бы он использовал свое настоящее имя. В онлайновой среде частные лица могут взять псевдоним (или, например, использовать фиктивные адреса электронной почты или учетные записи в социальных сетях) в попытке скрыть свою личность, внешний вид, голос, местонахождение и так далее, однако степень конфиденциальности, обеспечиваемая использованием таких псевдонимов, невелика, и она легко нарушается государством или другими субъектами с соответствующими навыками; если не прибегать к сочетанию методов шифрования и анонимизации, то оставляемые пользователями цифровые следы помогают легко установить их личность. Пользователи, стремящиеся к полной анонимности или скрытию своих личных данных (например, пряча подлинный адрес сетевого протокола IP) от государства или преступных элементов, могут прибегнуть к таким техническим средствам, как виртуальные частные сети (VPN), сетевой сервис (прокси-сервис), сети и программное обеспечение для анонимизации трафика и одноранговые сети[3]. В сети "Tor", одном из обще-

[3] Сетевой сервис пересылает данные через сервер-посредник, или "прокси-сервер", который в свою очередь направляет эти данные конечному получателю от имени пользователя и при этом эффективно прячет адрес IP такого пользователя, подменяя его своим собственным. Одноранговые сети разбивают и перераспределяют данные между связанными друг с другом серверами, а затем зашифровывают сохраненные данные таким образом, чтобы доступа к

известных программных средств анонимизации задействовано более 6 000 децентрализованных компьютерных серверов по всему миру, которые получают и многократно ретранслируют данные, чтобы скрыть идентифицирующую информацию о конечных точках, благодаря чему пользователям обеспечивается высокий уровень анонимности.

10. Основной особенностью цифрового века является непрерывное обновление технологий для удовлетворения потребностей пользователей. Хотя в настоящем докладе и упоминаются современные технологии, используемые для шифрования и анонимизации, содержащиеся в нем анализ и выводы в целом относятся к концепциям, лежащим в основе существующих технологий, и должны сохранить свою актуальность в отношении новых технологий, приходящих на смену старым.

B. Использование технологий

11. Интернет исключительно ценен с точки зрения свободы мнений и их свободного выражения, поскольку он служит своего рода рупором для усиления сказанного, а информация в нем тиражируется и становится доступной для всех имеющих выход в сеть. За весьма короткое время Интернет превратился в основную публичную арену глобального уровня. В качестве таковой открытый и безопасный Интернет должен быть отнесен к числу обязательных в наше время предпосылок для осуществления свободы выражения мнений. Однако такая свобода постоянно находится под ударом: почти так же, как и в материальном мире, в пространстве Интернета есть место для преступной деятельности, целенаправленных преследований и массового сбора данных. Поэтому представляется крайне важным, чтобы люди нашли способы обезопасить себя в онлайновой среде, правительства гарантировали такую безопасность при разработке законов и проведении соответствующей политики, а корпоративные субъекты создавали, разрабатывали и выводили на рынок товары и услуги, имеющие конфигурацию безопасности по умолчанию. Все эти обязательные условия не новы. Уже на заре цифрового века правительства отдавали себе отчет в том, какую важную роль в обеспечении безопасности глобальной экономики играет шифрование, и использовали его или побуждали к его использованию для защиты личных идентификационных номеров, присваиваемых государством, кредитных карт и банковской информации, документов с коммерческими тайнами и для расследования самих случаев киберпреступности[4].

12. Шифрование и анонимность вместе и по отдельности создают некоторое конфиденциальное пространство, в котором мнения и убеждения защищены. Например, с их помощью сохраняется тайна переписки, а высказанное мнение ограждается от внешнего контроля, что особенно актуально во враждебной политической, социальной, религиозной и правовой среде. В случаях, когда государства принудительно вводят незаконную цензуру с помощью фильтрации и других технологий, использование шифрования и анонимизации открывает перед пользователями возможность обойти препятствия и получить доступ к информации и идеям без какого-либо вторжения со стороны властей. Журналисты, исследователи, адвокаты и представители гражданского общества обращаются к шифрованию и анонимности, с тем чтобы оградить себя (и свои источники, клиентов и партнеров) от наблюдения и преследований. Способность искать информацию в сети, развивать идеи и общаться в безопасном режиме для многих может быть

идентифицирующей информации не было ни у одного централизованного сервера. См., например, Freenet.

[4] См. OECD, *Guidelines for Cryptography Policy* (1997).

единственным способом соприкоснуться с основополагающими аспектами своей личности, как то половой, религиозной и этнической принадлежностью, национальным происхождением или сексуальностью. Творческие люди прибегают к шифрованию и анонимности в попытке отстоять и защитить свое право на свободное выражение мнений, в особенности в условиях, когда не только государство налагает ограничения, но и само общество не приемлет нетрадиционных мнений или форм их выражения.

13. "Темная" сторона шифрования и анонимности отражает тот факт, что правонарушения, совершаемые в реальной жизни, имеют место и в онлайновой среде. Сотрудники правоохранительных органов и органов по борьбе с терроризмом выражают обеспокоенность по поводу того, что террористы и обычные преступники используют средства шифрования и анонимность для сокрытия своей деятельности, в результате чего правительствам сложно предупреждать и расследовать преступления, связанные с терроризмом, незаконной торговлей наркотиками, организованной преступностью, детской порнографией и рядом других отслеживаемых на государственном уровне явлений. В случае травли и кибербуллинга анонимность может служить трусливым прикрытием дискриминации, в особенности членов уязвимых групп. В то же время представители правоохранительных органов сами часто прибегают к тем же самым инструментальным средствам для придания секретности скрытым операциям, а члены уязвимых групп могут использовать их для обеспечения неприкосновенности своей частной жизни в условиях притеснения. Кроме того, в арсенале правительств имеется множество альтернативных технологий, включая, например, электронное прослушивание, определение и отслеживание местонахождения, интеллектуальный анализ данных, традиционную физическую слежку и многие другие средства, благодаря которым в современных условиях укрепляется потенциал правоприменения и борьбы с терроризмом[5].

III. Шифрование, анонимность и права на свободу мнений и их свободное выражение и неприкосновенность частной жизни

14. В случае шифрования и анонимности международно-правовые нормы в области прав человека предполагают, во-первых, анализ сферы охвата соответствующих прав и их применимости к шифрованию и анонимности; а во-вторых, оценку того, можно или нет и, если да, то в какой степени на законных основаниях налагать ограничения на использование технологий, содействующих поощрению и защите права на неприкосновенность частной жизни и свободу мнений и их свободное выражение.

15. Права на неприкосновенность частной жизни[6] и свободу мнений и их свободное выражение[7] были регламентированы в универсальных и региональных документах в области прав человека, истолкованы договорными органами и ре-

[5] См. Center for Democracy and Technology, "Going Dark'Golden Age for Surveillance" (2011).

[6] Право на неприкосновенность частной жизни защищается в соответствии со статьей 12 Всеобщей декларации прав человека, статьей 17 of Международного пакта о гражданских и политических правах, статьей 16 Конвенции о правах ребенка, статьей 22 Конвенции о правах инвалидов, статьей 14 Конвенции о защите прав всех трудящихся-мигрантов и членов их семей, статьей 8 Европейской конвенции по правам человека и статьей 11 Американской конвенции о правах человека.

[7] Свобода выражения мнений защищается в соответствии со статьей 19 Всеобщей декларации Международного пакта о гражданских и политических правах, статьей 9 Африканской хартии прав человека и народов, статьей 13 Американской конвенции о правах человека и статьей 10 Европейской конвенции по правам человека.

гиональными судами, изучены специальными процедурами Совета по правам человека и проанализированы в ходе универсального периодического обзора. Универсальные нормы по защите неприкосновенности частной жизни, свободы мнений и их свободного выражения содержатся в Международном пакте о гражданских и политических правах, участниками которого являются 168 государств. Даже для оставшихся государств, не связанных его обязательствами, Пакт служит как минимум ориентиром и во многих случаях отражением нормы обычного права; государства же, подписавшие, но не ратифицировавшие Пакт, обязаны уважать его объект и цель согласно статье 18 Венской конвенции о праве международных договоров. Национальными правовыми системами также предусмотрена защита неприкосновенности частной жизни, свободы мнений и их свободного выражения, иногда на основе конституции или основного закона или толкований таковых. В рамках нескольких проектов глобального гражданского общества были также приведены убедительные примеры правовых норм, которые следует применять в условиях цифрового века, включая Международные принципы применения прав человека в отношении мониторинга средств связи и Глобальные принципы национальной безопасности и права на информацию. Хотя конкретные нормы могут различаться в случае того или иного права или того или иного документа, в системе права сложилось общее понимание того, что, поскольку права на неприкосновенность частной жизни и свободу выражения мнения сами по себе настолько первостепенны с точки зрения защиты человеческого достоинства и обеспечения демократического правления, ограничения в их отношении должны детально оговариваться, устанавливаться законом и применяться в строгом соответствии с ним и только в исключительных случаях. В эпоху цифровых технологий для защиты таких прав требуется исключительная бдительность.

A. Неприкосновенность частной жизни в качестве залога свободы мнений и их свободного выражения

16. Благодаря шифрованию и анонимности у отдельных пользователей и групп в онлайновой среде появляется конфиденциальное пространство, в условиях которого они могут придерживаться тех или иных мнений и пользоваться свободой их выражения, не опасаясь произвольного и незаконного вмешательства или посягательств. Предыдущий мандатарий указал, что права на "неприкосновенность личной жизни и свобода выражения мнений взаимосвязаны", и пришел к выводу о том, что шифрование и анонимность подлежат защите с учетом той решающей роли, которую они могут сыграть в обеспечении этих прав (A/HRC/23/40 и Corr.1). Статья 17 Международного пакта о гражданских и политических правах, практически совпадающая со статьей 12 Всеобщей декларации прав человека, прямо защищает каждого от "произвольного или незаконного вмешательства в его личную и семейную жизнь, произвольного или незаконного посягательства на неприкосновенность его жилища или тайну его корреспонденции" и "незаконных посягательств на его честь и репутацию", и предусматривает, что "каждый человек имеет право на защиту закона от такого вмешательства или таких посягательств". Генеральная Ассамблея, Верховный комиссар Организации Объединенных Наций по правам человека и мандатарии специальных процедур признали, что неприкосновенность частной жизни является залогом реализации других прав, в частности права на свободу мнений и их свободное выражение (см. резолюцию 68/167 Генеральной Ассамблеи, A/HRC/13/37 и резолюцию 20/8 Совета по правам человека).

17. Шифрование и анонимность особенно актуальны для формирования и обмена мнениями, которые зачастую имеют место в онлайновой переписке в виде электронных писем, передачи текстовых сообщений и других форматов общения в онлайновой среде. Шифрование обеспечивает безопасность, благодаря чему частные лица имеют возможность "удостовериться, что их сообщение получают только обозначенные ими адресаты без вмешательства или изменений и что получаемые ими сообщения в равной степени защищены от вторжения" (см. A/HRC/23/40 и Corr.1, пункт 23). С учетом того, с какой точностью анализ метаданных позволяет получить представление "о поведении человека, его социальных отношениях, личных предпочтениях и личности" (см. A/HRC/27/37, пункт 19), решающую роль в обеспечении конфиденциальности переписки может сыграть анонимность. Согласно толкованию, принятому международными и региональными механизмами, неприкосновенность частной жизни охватывает не только переписку, но и ряд других обстоятельств[8].

18. Частные лица и гражданское общество сталкиваются с вмешательством и посягательствами со стороны государственных и негосударственных субъектов, при этом ключ к защите от таковых может скрываться в шифровании и анонимности. Согласно пункту 2 статьи 17 Международного пакта о гражданских и политических правах государства обязаны обеспечивать защиту частной жизни от незаконного и произвольного вмешательства или посягательств. Ввиду такого позитивного обязательства государствам следует обеспечить наличие в своем законодательстве положений, запрещающих незаконное и произвольное вмешательство в частную жизнь или любые посягательства, будь то со стороны государственных или негосударственных субъектов. Такая защита должна включать в себя право на доступ к средствам правовой защиты в связи с нарушением[9]. Для того чтобы право на средство правовой защиты приобрело действенный характер, частные лица должны сообщать о любых посягательствах на неприкосновенность их частной жизни, в частности о снижении уровня сложности шифрования или принудительном разглашении пользовательских данных.

B. Право беспрепятственно придерживаться своих мнений

19. В первой статье Всеобщей декларации прав человека признается, что все люди "наделены разумом и совестью", и этот принцип был развит в праве прав человека и стал включать в себя, среди прочего, защиту мнений, их свободного выражения, убеждений и мысли. В пункте 1 статьи 19 Международного пакта о гражданских и политических правах, также перекликающемся с положениями Всеобщей декларации, предусмотрено, что "каждый человек имеет право беспрепятственно придерживаться своих мнений". Мнения и возможность их выражения тесно связаны друг с другом, поскольку ограничения права получать информацию и идеи могут отразиться на способности придерживаться своих мнений, а препятствия, чинимые такой способности, неизбежно ограничивают и возможность выражения мнений. Тем не менее в праве прав человека между двумя понятиями проведено концептуальное различие. На переговорах по подготовке проекта Пакта "свобода формировать мнения и развивать их путем умозаключений была признана абсолютной и − в отличие от свободы выражения мне-

[8] Комитет по правам человека, замечание общего порядка № 16 (1988) о праве на личную и семейную жизнь, неприкосновенность жилища и тайну корреспонденции, и защиту чести и репутации. См. также Европейский суд по правам человека, информационные бюллетени по вопросу о защите данных и праве на защиту собственного изображения.

[9] См. Комитет по правам человека, замечание общего порядка № 16 и замечание общего порядка № 31 о характере общего юридического обязательства, налагаемого на государства-участники Пакта, и CCPR/C/106/D/1803/2008.

ний − не подлежащей ограничениям ни законом, ни другими формами власти"[10]. Способность свободно придерживаться мнений рассматривалась в качестве основополагающего элемента человеческого достоинства и демократического самоуправления и настолько важной гарантии, что в Пакте не допускалось никакого вмешательства, установления пределов или ограничений. Вследствие этого допустимые ограничения, предусматриваемые пунктом 3 статьи 19, явным образом распространяются только на право на свободное выражение своего мнения, закрепленное в пункте 2 статьи 19. Вмешательство же в осуществление права беспрепятственно придерживаться своих мнений, напротив, по определению будет нарушением пункта 1 статьи 19.

20. Составители комментариев и суды уделяют гораздо меньшее внимание праву придерживаться своих мнений, чем их выражению. При этом первое заслуживает большего внимания, поскольку в условиях цифрового века техническая сторона способности придерживаться мнений претерпела изменения и обнажила серьезные факторы уязвимости частных лиц. Способность частных лиц придерживаться своих мнений регулярно находит отражение в цифровой плоскости, где их мнения, история поисковых запросов и просмотров в браузере сохраняются, например, на жестких дисках, в "облачных" хранилищах и архивах сообщений электронной почты, которые в течение длительных, а, возможно, и неопределенных сроков остаются в распоряжении частных и государственных органов. Организации гражданского общества также составляют и хранят в цифровом формате меморандумы, документы и публикации, подготовка которых связана со способностью составлять мнения и придерживаться их. Другими словами, способность придерживаться своих мнений в цифровой век перестала быть абстрактным понятием, ограниченным тем, что находится у человека в голове. И при этом в наше время способность придерживаться мнений в цифровом пространстве находится под угрозой. В реальной жизни вмешательство в осуществление права на свое мнение предполагает физическое преследование, арест или менее явные формы наказания лиц за их мнения (см. CCPR/C/78/D/878/1999, приложение, пункты 2.5, 7.2 и 7.3). В других случаях вмешательство может также принимать такие формы, как адресная слежка, распределенная атака типа "отказ в обслуживании" (DDoS-атаки) и совершаемые как в онлайновой среде, так и реальной жизни акты запугивания, криминализации и преследования. Адресные цифровые атаки являются формой преследования частных лиц и организаций гражданского общества за мнения, которых они придерживаются в различных форматах. Шифрование и анонимность позволяют пользователям избежать такого преследования или снизить его степень.

21. Право беспрепятственно придерживаться своих мнений также включает в себя право формировать собственные мнения. Системы как индивидуального, так и массового слежения могут подрывать право формировать собственное мнение, поскольку страх неконтролируемого разглашения информации о следах интернет-активности, как то о запросах поиска или просматриваемых веб-страницах, удерживает лиц от попыток получить информацию, в особенности в условиях, когда такое слежение может привести к мерам репрессивного характера. Ввиду всего этого ограничения в отношении шифрования и анонимности должны подвергаться оценке на предмет того, могут ли они представлять собой недопустимое вмешательство в осуществление права придерживаться своих мнений.

[10] Manfred Nowak, *UN Covenant on Civil and Political Rights: CCPR Commentary* (1993), p. 441.

C. Право на свободное выражение мнений

22. Право на свободное выражение своего мнения по смыслу пункта 2 статьи 19 Международного пакта о гражданских и политических правах выходит за рамки включенной во Всеобщую декларацию и уже достаточно широкой гарантии и предусматривает защиту "свободы искать, получать и распространять всякого рода информацию и идеи, независимо от государственных границ, устно, письменно или посредством печати или художественных форм выражения, или иными способами по своему выбору". Как подчеркивалось в обширной правовой практике, докладах мандатариев специальных процедур и резолюциях, принимаемых в рамках как Организации Объединенных Наций, так и региональных систем защиты прав человека, свобода выражения мнений "имеет крайне важное значение для пользования другими правами человека и свободами и представляет собой одну из фундаментальных основ для построения демократического общества и укрепления демократии" (резолюция 25/2 Совета по правам человека). Совет по правам человека, Генеральная Ассамблея и отдельные государства регулярно подтверждают, что в онлайновой среде частные лица пользуются теми же правами, что и в офлайновой[11]. В настоящем докладе не будут повторяться все элементы этого консенсуса. В контексте шифрования и анонимности особого внимания заслуживают три аспекта текста (см. пункты 23–26 ниже).

23. **Свобода искать, получать и распространять информацию и идеи:** В условиях удушающей цензуры частные лица порою вынуждены прибегать к шифрованию и анонимности для обхода ограничений и осуществления права искать, получать и распространять информацию. В некоторых государствах доступ урезан с помощью целого ряда инструментальных средств. Так, в условиях государственной цензуры порою возводятся непреодолимые барьеры для пользования правом на доступ к информации. Некоторые государства устанавливают зависящие от содержания и зачастую дискриминационные ограничения или вводят уголовную ответственность за те или иные мнения, выражаемые в Интернете, тем самым запугивая политическую оппозицию и диссидентов и применяя законы о диффамации и оскорблении представителей власти, чтобы заставить замолчать журналистов, правозащитников и активистов. Единственным способом для частного лица получить доступ к информации и поделиться ею в таких условиях может стать соединение по VPN или же использование сети Tor или прокси-сервера в сочетании с шифрованием.

24. Следует подчеркнуть, что нормы права прав человека также предусматривают защиту права искать, получать и распространять научную информацию и идеи. В соответствии со Всеобщей декларацией и Международным пактом об экономических, социальных и культурных правах защищаются право на образование и право "участвовать в научном прогрессе и пользоваться его благами". Технологии шифрования и анонимизации позволяют частным лицам участвовать в обмене такой информацией в условиях, когда доступ к ней иначе запрещен, и сами по себе такие технологии являются примерами научного прогресса. Их использование дает частным лицам возможность получить доступ к результатам научного прогресса, в отношении которых государство, возможно, ввело ограничения. Специальный докладчик в области культурных прав отметила, что "как право на науку, так и право на культуру следует воспринимать как включающие право на доступ и использование информационно-коммуникационных и других

[11] См., например, резолюцию 68/167 Генеральной Ассамблеи, резолюцию 26/13 Совета по правам человека и принятую Советом Европы рекомендацию CM/Rec (2014) 6 Комитета министров государствам-членам о руководстве по правам человека для интернет-пользователей.

технологий таким образом, который обеспечивает самостоятельный выбор и расширение возможностей" (см. A/HRC/20/26, пункт 19).

25. **Независимо от границ:** В основных правовых актах, гарантирующих свободу выражения мнений, прямо признается трансграничный характер сферы охвата этого права. Частные лица пользуются правом получать и передавать всякого рода информацию и идеи из мест и в места за пределами их границ[12]. Тем не менее некоторые государства фильтруют или блокируют содержимое сайтов по ключевым словам, лишая пользователей доступа к данным с помощью технологий контентного доступа к тексту. Шифрование позволяет частному лицу обойти такие фильтры и обеспечивает передачу информации через границы. Кроме того, частные лица не могут контролировать, а во многих случаях не знают, передаются ли их сообщения через границы и каким образом. С помощью шифрования и анонимизации можно защитить информацию всех пользователей во время ее передачи через серверы, находящиеся в третьих странах, которые применяют контентное фильтрование.

26. **Любыми средствами:** Статья 19 Всеобщей декларации и статья 19 Международного пакта о гражданских и политических правах были предусмотрительно составлены с расчетом на будущие технологические достижения (A/HRC/17/27). Государства − участники Пакта решили остановиться на общей формулировке "любыми средствами" вместо того, чтобы перечислять еще не существовавшие тогда средства связи. Исходя отчасти из этого понимания, международные механизмы неоднократно признавали, что гарантии защиты свободы выражения мнений распространяются и на деятельность в Интернете. Региональные суды также признали, что гарантии защиты применимы в онлайновой среде[13]. Европейский суд по правам человека в ходе рассмотрения вопроса об аналогичном принципе защиты свободного выражения мнений, предусмотренном в Европейской конвенции о защите прав человека и основных свобод, указал, что способы и средства передачи и получения информации сами по себе защищены, поскольку любые ограничения, вводимые в отношении таких средств, неизбежно представляют собой препятствие для осуществления права получать и распространять информацию[14]. С этой точки зрения технологии шифрования и анонимизации являются конкретными средствами, с помощью которых частные лица пользуются своей свободой выражения мнений.

D. Роль корпораций

27. В ряде секторов корпорации имеют отношение к поощрению или вмешательству в личную жизнь и созданию препятствий для свободы мнений и их выражения, в том числе для шифрования и анонимности. Большая часть (а в некоторых странах практически 100%) онлайновой коммуникации происходит в сетях, принадлежащих частными корпорациями и поддерживаемых ими, в то время как другие корпорации владеют и управляют веб-сайтами, на которых значительная

[12] Этот принцип был признан Европейским судом по правам человека. См. *Ahmet Yildirim* v. *Turkey*,(2012); *Cox* v. *Turkey*, (2010); *Case of Groppera Radio AG and Others* v. *Switzerland* (1990).

[13] European Commission of Human Rights, *Neij and Sunde Kolmisoppi* v. *Sweden*, (2013); European Court of Human Rights, *Perrin* v. *United Kingdom*, (2005); African Court on Human and Peoples' Rights, *Zimbabwe Lawyers for Human Rights and Institute for Human Rights and Development (on behalf of Meldrum)* v. *Zimbabwe* (2009); *Case of Herrera Ulloa* v. *Costa Rica*, *Herrera Ulloa* v. *Costa Rica*, Preliminary Objections, Merits, Reparations and Costs, Series C No. 107, IHRL 1490 (IACHR 2004).

[14] См. *Autronic AG* v. *Switzerland* (1990); *De Haes and Gijsels* v. *Belgium* (1997), para. 48; *News Verlags GmbH and Co.KG v. Austria* (2000).

часть материалов создается пользователями. Некоторые корпорации занимают прочные позиции на рынке средств слежения и программ-шпионов, поставляя правительствам оборудование и программное обеспечение для снижения защиты выходящих в онлайновую среду частных лиц. Ряд других разрабатывают и предоставляют услуги в области безопасного и конфиденциального оперативного хранения данных. Телекоммуникационные структуры, провайдеры Интернет-услуг, серверы-поисковики, операторы "облачных" услуг и многие другие корпоративные субъекты, зачастую характеризуемые в качестве посредников, поощряют, контролируют или нарушают конфиденциальность и свободу выражения мнений в онлайновой среде. Посредники могут хранить огромные объемы данных пользователей, к которым правительства зачастую требуют предоставить доступ. Каждый из таких корпоративных субъектов может поощрять шифрование и анонимность или ослаблять их действенность.

28. Полновесный анализ роли корпораций в обеспечении безопасности их пользователей в онлайновой среде выходит за рамки настоящего доклада, который в первую очередь посвящен вопросу об обязательствах государств. Все же представляется важным подчеркнуть, что "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" (см. A/HRC/27/37, пункт 43). Корпорациям следует, как минимум, применять такие принципы, как Руководящие принципы предпринимательской деятельности в аспекте прав человека, выработанные Глобальной сетевой инициативой Руководящие принципы свободы выражения мнений и неприкосновенности частной жизни, Руководство Европейской комиссии для сектора ИКТ по вопросу о применении утвержденных Организацией Объединенных Наций Руководящих принципов предпринимательской деятельности в аспекте прав человека и Диалог телекоммуникационной индустрии: Руководство по принципам; в них к корпорациям обращен призыв взять обязательство по защите прав человека, проявлять добросовестность для обеспечения положительных результатов их деятельности с точки зрения прав человека и устранения вызванных ею отрицательных последствий. В будущем Специальный докладчик отдельно рассмотрит вопрос о том, какую роль должны играть корпорации в обеспечении личной безопасности в интересах осуществления свободы мнений и их свободного выражения.

IV. Анализ ограничений, действующих в отношении шифрования и анонимности

A. Правовая основа

29. Допустимые ограничения права на неприкосновенность частной жизни должны толковаться строго, в особенности в условиях вездесущего онлайнового слежения, будь то пассивного или агрессивного, массового или индивидуального, и независимо от того, определяются ли применимые стандарты как "произвольные или незаконные" по смыслу статьи 17 Международного пакта о гражданских и политических правах, "произвольные" по смыслу статьи 12 Всеобщей декларации, "произвольные и оскорбительные" по смыслу статьи 11 Американской конвенции о правах человека или "необходимые в демократическом обществе" по смыслу статьи 8 Европейской конвенции о защите прав человека и основных свобод (см. A/HRC/13/37, пункты 14–19). Вмешательства в частную жизнь, чреватые ограничением свободы мнений и их свободного выражения, как это описывается в настоящем докладе, не должны ни в коем случае распространяться на право придерживаться своих мнений, а ограничения в отношении свободы выра-

жения мнений должны быть предусмотрены законом и необходимы и соразмерны одной из небольшого числа законных целей.

30. В отношении права беспрепятственно придерживаться своих мнений не могут вводиться никакие ограничения; предусмотренные пунктом 3 статьи 19 Пакта ограничения применяются исключительно к праву на свободное выражение своего мнения по смыслу пункта 2 статьи 19. В условиях, когда наличие мнений у того или иного лица, пусть даже в онлайновой среде, чревато слежением или преследованием, шифрование и анонимность могут послужить необходимой гарантией неприкосновенности частной жизни. Ограничения в отношении использования таких средств обеспечения безопасности могут сказаться на способности частных лиц придерживаться мнений.

31. Ограничения в отношении использования средств шифрования и анонимизации, как факторов обеспечения права на свободное выражение мнений, должны удовлетворять хорошо известному тройному критерию: любые ограничения должны предусматриваться законом, могут налагаться только на законных основаниях (как это предусмотрено пунктом 3 статьи 19 Пакта) и должны строго отвечать требованиям необходимости и соразмерности.

32. Во-первых, чтобы ограничение в отношении использования средств шифрования и анонимизации было "предусмотрено законом", такой закон должен быть четко сформулирован, носить публичный и транспаретный характер и не допускать наделения государственных властей неограниченными дискреционными полномочиями устанавливать ограничения (см. Комитет по правам человека, замечание общего порядка № 34 (2011)). Предложения о введении ограничений в отношении использования средств шифрования или анонимизации следует выносить на общественное обсуждение и, если и утверждать, то только по итогам обычной законодательной процедуры. Кроме того, следует предусматривать надежные процедурные и судебные гарантии для обеспечения прав на надлежащее судопроизводство любого лица, использующего подлежащие ограничению средства шифрования или анонимизации. В частности, применение такого ограничения должно контролироваться судом, трибуналом или иным независимым судебным органом[15].

33. Во-вторых, ограничения могут оправдываться только соображениями защиты конкретных интересов: уважения прав или репутации других лиц, охраны национальной безопасности, общественного порядка, охраны здоровья и нравственности населения. Даже в случаях, когда государство в законодательном порядке запрещает "выступления в пользу национальной, расовой или религиозной ненависти, представляющее собой подстрекательство к дискриминации, вражде или насилию", как это предусмотрено статьей 20 Пакта, любые ограничения свободы выражения мнений должны соответствовать положениям пункта 3 статьи 19 (A/67/357). Для оправдания ограничений свободы выражения мнений не могут приводиться никакие другие основания. Кроме того, поскольку под предлогом достижения законных целей часто скрываются незаконные, применение самих ограничений должно носить узкий характер[16].

34. В-третьих, государство должно продемонстрировать, что любое ограничение в отношении использования средств шифрования и анонимизации "необхо-

[15] См. Международный пакт о гражданских и политических правах, подпункт b) пункта 3 статьи 2; CCPR/C/79/Add.110, пункт 22; Йоханнесбургские принципы национальной безопасности, свободы выражения мнений и доступа к информации.

[16] См. Комитет по правам человека, пункт 30 замечания общего порядка № 34 о свободе мнений и их выражения и замечание общего порядка № 31.

димо" для достижения законной цели[17]. Европейский суд по правам человека, соответственно, пришел к выводу, что под словом "необходимы" в статье 10 Европейской конвенции о защите прав человека и основных свобод понимается, что ограничение должно быть не просто "целесообразным", "разумным" или "желательным"[18]. Как только законная цель достигается, ограничение более применяться не может. С учетом того, что речь идет об основополагающих правах, ограничения должны вводиться по решению независимого и беспристрастного судебного органа, в особенности в целях соблюдения прав лиц на надлежащую законную процедуру.

35. Критерий необходимости также предполагает оценку соразмерности мер, ограничивающих использование средств онлайновой безопасности или доступ к ним[19]. Оценка соразмерности призвана обеспечить, что ограничение "представля[ет] собой наименее ограничительное средство из числа тех, с помощью которых может быть достигнут желаемый результат"[20]. Ограничение должно быть направлено на конкретную цель и не быть чревато неоправданным ущемлением других прав попавших под него лиц, а вмешательство в осуществление прав третьих сторон должно быть ограничено и оправдано в свете интереса, отстаиваемого с помощью такого посягательства на права. Кроме того, ограничение должно "являться соразмерным защищаемому интересу"[21]. Высокая вероятность ущемления насущного законного государственного интереса может оправдать ограниченное вмешательство в свободу выражения мнений. Напротив, если ограничение ведет к значительным последствиям для лиц, не представляющих собой какой-либо угрозы для законного интереса правительства, ложащаяся на государство ответственность оправдать ограничение будет очень высока[22]. Кроме того, при анализе критерия соразмерности необходимо учитывать большую вероятность того, что посягательства на шифрование и анонимность будут использованы в собственных интересах как раз теми преступными и террористическими сетями, для сдерживания которых вводились ограничения. В любом случае "подробные, основанные на реальных фактах оправдания" крайне важны для возможности проведения на транспарентной основе публичного обсуждения ограничений, затрагивающих и возможно подрывающих свободу выражения мнений (см. A/69/397, пункт 12).

B. Практика государств: примеры и поводы для обеспокоенности

36. Тенденции, связанные с онлайновой безопасность и конфиденциальностью, вызывают серьезную тревогу. Государства во многих случаях не предоставляют публичных объяснений и обоснования ограничений. Зашифрованные и анонимные сообщения могут вызывать раздражение у сотрудников правоохранительных и органов по борьбе с терроризмом и затрудняют слежение, но государственные власти в целом не определили ситуаций (пусть даже в общих чертах с учетом возможных соображений конфиденциальности), в которых ограничение было бы необходимо для достижения законной цели. Государства преуменьшают значение традиционных нецифровых средств правоприменения и борьбы с терроризмом,

[17] См. Комитет по правам человека, замечание общего порядка № 34, пункт 2, и сообщение № 2156/2012, Соображения, принятые 10 октября 2014 года.

[18] См. *Case of The Sunday Times* v. *United Kingdom*, judgement of 26 April 1979, para. 59.

[19] См. African Court Human and Peoples' Rights, *Lohe Issa Konate* v. *Burkina Faso*, application No. 004/2013, paras. 148 and 149 (2014); European Court of Human Rights, *Case of The Sunday Times*, para. 62.

[20] См. Комитет по правам человека, замечание общего порядка № 27 (1999) о свободе передвижения, пункт 14.

[21] См. там же, пункт 14.

[22] См. Inter-American Commission on Human Rights, OEA /Serv.L/V/II.149, para. 134.

включая международное сотрудничество[23]. В результате этого население лишено возможности определить, когда ограничения, налагаемые на их онлайновую безопасность, действительно оправданы реальными выгодами в плане национальной безопасности и предотвращения преступности. Помимо этого, попытки ограничить использование средств шифрования и анонимизации, как правило, являются первой реакцией на терроризм, даже если сами террористы предположительно не прибегали к шифрованию или анонимности при планировании и совершении нападения. Кроме того, даже в тех случаях, когда ограничение, возможно, служит законным интересам, многие законы и меры политики систематически не удовлетворяют критериям необходимости и соразмерности и ощутимым образом пагубно сказываются на способности всех лиц беспрепятственно осуществлять свои права на неприкосновенность частной жизни и свободу мнений и их свободное выражение.

37. Также следует отметить, что сама Организация Объединенных Наций не обеспечила ни собственных сотрудников, ни лиц, посещающих ее веб-сайты, надежными средствами защиты связи, ввиду чего лицам, находящимся под угрозой, довольно непросто в безопасном режиме связаться с правозащитными механизмами Организации по Интернету[24].

1. Шифрование

38. Некоторые правительства стремятся защищать и поощрять шифрование в качестве средства сохранения тайны корреспонденции. Например[25], в соответствии с принятым в Бразилии в 2014 году законом о принципах защиты гражданских прав в Интернете гарантируются неприкосновенность и конфиденциальность онлайновой переписки пользователей, при этом исключения допускаются только по решению суда. Действующие в Австрии законы об электронной торговле и о телекоммуникационной связи не ограничивают использование средств шифрования, и правительство провело разъяснительные кампании для обучения населения навыкам цифровой безопасности. Законы и подзаконные акты, принятые в Греции, направлены на поощрение эффективного использования средств как шифрования, так и анонимизации. Германия, Ирландия и Норвегия разрешают и поощряют использование технологий шифрования и пресекают любые попытки снизить эффективность протоколов шифрования. В шведском и словацком законодательстве также не предусмотрено ограничений использования средств шифрования в онлайновой среде. Соединенные Штаты Америки приветствуют использование средств шифрования, а конгрессу Соединенных Штатов следует продолжить рассмотрение внесенного проекта закона о защите данных, в соответствии с которым правительству будет запрещено требовать от компаний снижения степени защищенности программных продуктов или включения мер скрытого удаленного администрирования. В ряде стран, включая Канаду, Нидерланды, Соединенное Королевство Великобритании и Северной Ирландии и Швецию, правительства финансируют деятельность по обмену опытом или подготовке специалистов в области использования технологий шифрования и анонимизации, чтобы помочь пользователям избежать цензуры и повысить свою онлайновую безопасность. Кроме того, экспортные правила должны, насколько это возможно,

[23] Однако см. Centre for International Governance Innovation and Chatham House, *Toward a Social Compact for Digital Privacy and Security: Statement by the Global Commission on Internet Governance* (2015).

[24] Например, сотрудники Управления Верховного комиссара Организации Объединенных Наций по правам человека (УВКПЧ) в Женеве не имеют доступа к сквозному шифрованию сообщений электронной почты, а содержание сайта УВКПЧ не зашифровано.

[25] Многие примеры, приводимые в данном пункте, взяты из соответствующих материалов, представленных правительствами.

содействовать передаче технологий шифрования. Хотя в настоящем докладе не приводится общей правовой оценки всего спектра национальных подходов к шифрованию, упомянутые элементы, а именно отказ от ограничений или всесторонняя защита, обязательное наличие судебного разрешения в случае каждого конкретного ограничения и информирование общественности, заслуживают более широкого распространения в качестве средств защиты и поощрения права на свободу мнений и их свободное выражение.

39. Вместе с тем попытки регламентировать шифрование часто не соответствуют стандартам свободы выражения мнений в двух основных аспектах. Во-первых, как правило, не удается доказать, что ограничения необходимы для защиты какого-то конкретного законного интереса. Это тем более верно, если учесть охват и эффективность других средств, включая традиционную деятельность сил полиции и служб разведки и транснациональное сотрудничество, которые сами по себе могут предоставить достаточную информацию для конкретных правоохранительных мер или других законных целей. Во-вторых, ограничения несоразмерно сказываются на правах на свободу мнений и их свободное выражение, имеющихся у попавших под ограничения лиц или у населения в целом.

Запрет на индивидуальное использование технологий шифрования

40. Прямые запреты на индивидуальное использование технологии шифрования несоразмерно ограничивают свободу выражения мнений, поскольку они лишают всех пользователей сети в пределах той или иной юрисдикции права создавать для себя некое личное пространство для мнений и их свободного выражения, при этом какие-либо конкретные основания заявлять об использовании шифрования в незаконных целях отсутствуют.

41. Государственные нормы, регламентирующие шифрование, могут быть тождественны запрету, как, например, в случае правил, которые a) предусматривают обязательное получение лицензии для использования технологий шифрования, b) вводят низкие технические стандарты шифрования, и c) устанавливают контроль над импортом и экспортом инструментальных средств шифрования. Привязывая порог качества средств шифрования к государственным стандартам и контролируя импорт и экспорт технологий шифрования, государства добиваются низкого уровня эффективности шифровательного программного обеспечения, при котором правительства имеют доступ к содержанию сообщений. Так, хотя соответствующее законодательство может быть изменено, правительство Индии запретило поставщикам услуг использовать "массовое шифрование" в своих сетях, при этом по закону частным лицам без предварительного разрешения нельзя использовать алгоритмы шифрования, превышающие легко поддающуюся взлому 40-битную ключевую последовательность, а лица использующие более криптостойкие ключи шифрования обязаны предоставить правительству их копию[26]. По некоторым сообщениям, в Китае к устройствам и программам шифрования может быть предъявлено требование о соответствии установленным правительством алгоритмам шифрования, которые не проходили независимой экспертной проверки на предмет устойчивости[27]. По правилам Телекоммуникационного управления Пакистана для использования ВЧС и шифрования требуется предварительно получить разрешение[28]. На Кубе лицам, использующим шифрование,

[26] Министерство коммуникационных и информационных технологий Индии, Лицензионное соглашение о предоставлении интернет-услуг (2007). Размещено по адресу http://dot.gov.in/sites/default/files/internet-licence-dated%2016-10-2007_0.pdf. См. особенно раздел 2.2 (vii).

[27] См. например, закон о борьбе с терроризмом, статья 15 (первоначальный проект от 8 ноября 2014 года). Размещен по адресу http://chinalawtranslate.com/en/ctldraft/.

[28] См. www.ispak.pk/Downloads/PTA_VPN_Policy.pdf.

требуется получить разрешение регулирующих органов[29]. В Эфиопии правительство уполномочено устанавливать технические стандарты шифрования, а согласно недавно принятому постановлению вводится уголовная ответственность за изготовление, сборку или импорт любого телекоммуникационного оборудования без соответствующей лицензии[30]. Такие нормативные положения чреваты непозволительным вмешательством в индивидуальную практику использования шифрования в переписке.

Намеренное понижение степени эффективности шифрования

42. Ряд государств предусмотрели или планируют ввести так называемый элемент скрытого удаленного администрирования в имеющиеся в продаже товары и программы, вынуждая разработчиков оставлять в них слабые места, с помощью которых государственные органы могут получить доступ к зашифрованным сообщениям. Некоторые правительства разработали или закупили программы, обеспечивающие такой доступ для целей внутригосударственного слежения[31]. Высокопоставленные должностные лица Соединенного Королевства и Соединенных Штатов Америки, по всей видимости, выступают за обязательный характер такого скрытого удаленного администрирования[32]. Государства, поддерживающие такие меры, зачастую утверждают, что требование о возможности скрытого удаленного администрирования необходимо для перехвата содержания зашифрованных сообщений. Вместе с тем правительства, выступающие за меры скрытого удаленного администрирования, не продемонстрировали, что использование средств шифрования преступниками или террористами становится непреодолимым препятствием на пути обеспечения правопорядка. Кроме того, с учетом характеристик существующих технологий включение заведомых изъянов неизбежно подрывает безопасность всех пользователей сети, поскольку такой удаленный "обходной" доступ, хоть и предназначен исключительно для правительства, может быть несанкционированно использован другими субъектами, как государственными, так и негосударственными. С учетом его широкого и неизбирательного воздействия от удаленного администрирования рискуют несоразмерно пострадать все пользователи сети.

43. В спорах по этому вопросу прослеживается один важный момент: требование о предоставлении такого удаленного доступа для обхода шифрования, пусть даже для достижения законных целей, ставит под угрозу конфиденциальность, необходимую для беспрепятственного осуществления права на свободное выражение мнений. У удаленного администрирования есть и практические недостатки: из-за злоупотребления наличием заведомо слабых сторон зашифрованное содержание сайтов может подвергнуться взлому, даже если доступ предоставляется исключительно в интересах правительственного или судебного контроля. Перед правительствами, безусловно, встает дилемма: их обязательство защищать свободу выражения мнений вступает в противоречие с их обязательствами предотвращать нарушения права на жизнь или физическую неприкосновенность, которым угрожают терроризм и иная преступная деятельность. Однако государства могут иным способом добиться разглашения зашифрованной информации, например на основании судебного ордера. В таких случаях государства должны

[29] Материалы, представленные Кубой.

[30] См. Ethiopia Telecom Fraud Offence Proclamation 761/2012, sects. 3–10.

[31] См. Morgan Maquis-Boire and others, *For Your Eyes Only* (2013, Citizen Lab).

[32] См. заявление, сделанное премьером-министром Дэвидом Кэмероном 12 января 2015 года на конференции по вопросу об обязательствах, которые берет на себя консервативная партия в преддверии всеобщих выборов 2015 года, а также речь директора Федерального бюро расследований Джеймса Коми, с которой он выступил 16 октября 2014 года в Брукингском институте, Вашингтон, округ Колумбия ("Going dark: are technology, privacy and public safety on a collision course?").

доказать, что общие ограничения защиты, обеспечиваемой шифрованием, представляются необходимыми и соразмерными. Государства должны, действуя на началах гласности и транспарентности, продемонстрировать, что другие, менее радикальные меры отсутствуют или оказались неэффективными и что законная цель может быть достигнута только с помощью широких радикальных мер, таких как удаленное скрытое администрирование. Как бы то ни было, меры, предусматривающие введение широко применимых ограничений в отношении огромного числа людей и не предполагающие оценку каждой ситуации в отдельности, практически наверняка не удовлетворят критерию соразмерности.

Депонирование ключей

44. Система депонирования ключа дает частным лицам доступ к шифрованию, но при этом пользователи обязаны сдавать свои индивидуальные ключи на хранение правительству или "доверенной третьей стороне". Вместе с тем у системы депонирования ключей есть значительные недостатки. Например, эффективность системы зависит от добросовестности того или иного лица, ведомства или системы, которым поручено хранить индивидуальные ключи, а сама база данных ключей может подвергнуться взлому, что ставит под угрозу безопасность и конфиденциальность сообщений любого пользователя. После острой полемики, развернувшейся в Соединенных Штатах во время "Криптовойн" 1990-х годов, было решено отказаться от системы депонирования ключей (наряду с удаленным скрытым администрированием), при этом в ряде стран эти системы действуют и в настоящее время, а в некоторых других внесены предложения об их применении. В соответствии с правилами, утвержденными Турцией в 2011 году, поставщики криптографических услуг, обязаны предоставлять копии ключей шифрования государственным регулирующим органам до вывода своих средств шифрования на рынок пользователей[33]. Из-за недостатков, присущих депонированию ключей, эти системы представляют собой серьезную угрозу с точки зрения и безопасного пользования свободой выражения мнений.

Обязательное раскрытие ключа по сравнению с адресными распоряжениями о расшифровке данных

45. В ситуациях, когда правоохранительные органы или службы национальной безопасности могут обосновать необходимость потребовать доступ к сообщениям, перед властями открываются два варианта действий: либо распорядиться о расшифровке конкретных сообщений, либо в случае, когда есть основания опасаться, что соответствующая сторона не выполнит распоряжение о расшифровке, потребовать сдать ключ, необходимый для расшифровки. Адресные распоряжения о расшифровке данных представляются несколько более сдержанными мерами, при использовании которых с меньшей вероятностью встает вопрос о соразмерности, поскольку они направлены на конкретные сообщения, а не на всю историю переписки того или иного частного лица, зашифрованной с помощью конкретного ключа. Раскрытие ключа, напротив, может привести к разглашению частных данных в объемах, многократно превышающих уровень, требуемый в конкретной ситуации[34]. Кроме того, в свете распоряжений о раскрытии ключа или расшифровки данных корпорации зачастую вынуждены сотрудничать с правительствами, что ведет к серьезным проблемам, затрагивающим индивидуаль-

[33] Закон № 5651 о регламентировании вещания в сети Интернет и борьбе с преступлениями, совершаемыми с помощью Интернет-вещания.

[34] Координатор по вопросам борьбы с терроризмом в составе Европейской комиссии настоятельно призвал к рассмотрению возможности обязательного раскрытия ключей. См. Совет Европейского союза, Генеральный секретариат, документ совещания D1035/15 (2015 год).

ных пользователей сети. Раскрытие ключа предусматривается по закону в ряде европейских стран[35]. Как бы то ни было, в обоих случаях такие распоряжения должны быть основаны на доступных для всеобщего ознакомления законах, сфера их охвата должна быть четко ограничена конкретной целью, применение – контролироваться независимым и беспристрастным судебным органом, в частности в целях соблюдения прав затрагиваемых лиц на надлежащее судопроизводство, а сами они должны приниматься только в случае необходимости и отсутствия возможности прибегнуть к менее радикальным методам расследования. Такие меры могут быть оправданы только в случае адресного применения в отношении конкретного пользователя или пользователей и при условии судебного контроля.

Правовая презумпция

46. В некоторых государствах само по себе использование технологий шифрования может быть отнесено к числу противоправных действий. Так, в тексте обвинений, предъявленных в Эфиопии коллективу авторов блога "Зона 9", высказывались предположения о том, что одно лишь обучение навыкам засекречивания связи является признаком преступной деятельности[36]. Подобные презумпции не отвечают критериям допустимых ограничений. Аналогичным образом государства, подвергающие наказанию производителей и продавцов инструментальных средств, способствующих доступу активистов к Интернету, ущемляют права на неприкосновенность частной жизни и свободу выражения мнений.

2. Анонимность

47. Анонимность, по общему признанию, играет важную роль в защите и поощрении частной жизни, свободного выражения мнений, политической подотчетности, участия общественности и публичных обсуждений[37]. Ни во Всеобщей декларации прав человека, ни в Международном пакте о гражданских и политических правах анонимность не упоминается. В ходе переговоров по подготовке Пакта было предложено включить в пункт 1 статьи 19 фразу "анонимность не допускается". Однако это предложение было отклонено "среди прочего, на том основании, что анонимность может в некоторых случаях оказываться необходимой для защиты автора" и "такая оговорка может стать препятствием для использования псевдонимов"[38]. Специальный докладчик по вопросу о свободе выражения мнений Межамериканской комиссии по правам человека пришел к выводу о том, что "право на свободу мнений и слова и право на неприкосновенность частной жизни гарантируют защиту анонимных высказываний от ограничений со стороны правительства"[39]. В политической культуре некоторых государств издавна сложились традиции уважения анонимности, но лишь в очень небольшом числе государств в законодательном порядке введен общий режим защиты ано-

[35] См., например, Соединенное Королевство, закон о регламентации следственных полномочий 2000 года (обязательное раскрытие ключа); Франция, Закон № 2001-1062 (раскрытие ключей шифрования по постановлению судьи); Испания, закон о телекоммуникациях № 25/2007 (раскрытие ключа).

[36] См. http://trialtrackerblog.org/2014/07/19/contextual-translation-of-the-charges-of-the-zone9-bloggers/.

[37] См., например, Inter-American Commission on Human Rights, OEA /Serv.L/V/II.149, para. 134; United States, *McIntyre* v. *Ohio Elections Commission* (1995); Lord Neuberger, speech to RB Conference on the Internet, entitled, "What's a name? Privacy and Anonymous Speech on the Internet" (2014).

[38] Marc J. Bossuyt, *Guide to the "Travaux Préparatoires" of the International Covenant on Civil and Political Rights* (1987), pp. 379-80.

[39] См. Organization of American States, press release 17/15.

нимного выражения мнений. Ряд государств активно противостоят анонимности как в реальной жизни, так и в онлайновой среде. Между тем, поскольку в онлайновой среде анонимность во многом служит благодатной почвой для формирования мнений и свободы их выражения, государствам следует защищать ее и в целом не ограничивать обеспечивающие анонимность технологии. Судебные власти ряда государств предусмотрели защиту анонимности, по крайней мере в отдельных редких случаях. Например, Верховный суд Канады недавно признал незаконным факт получения данных о личности анонимного пользователя без соответствующего ордера[40]. Конституционный суд Республики Корея аннулировал законы о запрете анонимности, объявив их неконституционными[41]. Верховный суд Соединенных Штатов неоднократно выступал на стороне права на анонимное выражение мнений[42]. Европейский суд по правам человека признает анонимность в качестве важного фактора свободы выражения мнений, но при этом допускает ограничения в тех случаях, когда потребность в них продиктована законными целями.

48. Многие государства признают законность сохранения анонимности журналистских источников. В соответствии с решениями Верховного суда Мексики и положениями мексиканского Уголовно-процессуального кодекса признается право журналистов сохранять анонимность своих источников, однако на деле на журналистов оказывается колоссальное давление[43]. Конституции Аргентины, Бразилии, Парагвая и Эквадора содержат положения, прямо защищающие анонимность источников; в Венесуэле (Боливарианской Республике), Панаме, Перу, Сальвадоре, Уругвае и Чили источники данных охраняются законом[44]. В Мозамбике источники охраняются на основании Конституции, а в Анголе такая защита подразумевается по закону[45]. В правовой практике Австралии, Канады, Новой Зеландии и Японии применяются дифференцированные судебные критерии для сбалансированного сопоставления факторов и анализа вопросов защиты источника, однако давление, оказываемое на журналистов, рискует со временем подорвать такие гарантии защиты[46]. На практике государства зачастую нарушают анонимность источников, даже если таковая предусмотрена законом.

Запрет анонимности

49. Запрет анонимности в онлайновой среде препятствует осуществлению права на свободное выражение мнений. Во многих государствах запрет вводится безотносительно каких-либо конкретных государственных интересов. Согласно Конституции Бразилии (статья 5) запрещены анонимные выступления. Анонимность также запрещена положениями Конституции Боливарианской Республики Венесуэла (статья 57). В 2013 году во Вьетнаме было запрещено использование псевдонимов, ввиду чего всем частным лицам, ведущим персональные блоги,

[40] *R.* v. *Spencer* (2014).

[41] Decision 2010 Hun-Ma 47, 252 (consolidated) announced 28 August 2012.

[42] *McIntyre* v. *Ohio Elections Commission* (1995), pp. 342 and 343.

[43] См. новый Федеральный уголовно-процессуальный кодекс, статья 244.

[44] См. Конституция Аргентины, статья 43; Конституция Бразилии, раздел II, глава I, статья 5, XIV; Конституция Эквадора, статья 20; Конституция Парагвая, статья 29 (1). См. также принятый в Чили закон № 19733; Уголовно-процессуальный кодекс Сальвадора; панамский закон № 67, статья 21; Уголовно-процессуальный кодекс Перу; уругвайский закон № 16099; принятый в Боливарианской Республике Венесуэла закон о журнализме № 4819, статья 8.

[45] См. Конституция Мозамбика, статья 48 (3); ангольский закон о печати № 7/06, статья 20 (1).

[46] Australia Evidence Amendment (Journalistsà Privilege) Act 2007; Canada, Court of Queen's Bench of Alberta, *Wasylyshen* v. *Canadian Broadcasting Corporation* (2005); Japan, Case 2006 (Kyo) No. 19 (2006); New Zealand Evidence Act, sect. 68 (2006).

пришлось официально сообщить свое настоящее имя и адрес[47]. В 2012 году в Исламской Республике Иран было введено требование о регистрации всех адресов IP, используемых в стране, а посетителей Интернет-кафе обязали регистрироваться под своим настоящим именем до начала пользования компьютером[48]. В соответствии с законами, действующими в Эквадоре, лица, оставляющие комментарии на веб-сайтах, и владельцы мобильных телефонов обязаны регистрироваться под своим настоящим именем[49].

50. Некоторые государства приняли законы, требующие регистрации под настоящим именем, независимо от видов сетевой активности, что по сути является запретом анонимности. В Российской Федерации авторы блогов с ежедневной аудиторией более 3 000 читателей должны зарегистрироваться в органе, регулирующем деятельность СМИ, и официально удостоверить свою личность, а посетители Интернет-кафе должны, по сообщениям, предъявлять удостоверение личности для получения доступа к общественным беспроводным сетям[50]. По сообщениям, в Китае объявлено о введении правил, требующих от пользователей Интернета регистрировать свои подлинные имена для доступа к определенным веб-сайтам и избегать распространения материалов, содержание которых задевает национальные интересы[51]. В Южной Африке пользователи Интернета и сотовой связи также обязаны регистрировать свои настоящие имена[52].

51. Кроме того, правительства часто требуют регистрации сим-карты; так, почти в 50 странах Африки действуют или принимаются законы, требующие при активации сим-карты вводить персональные данные, удостоверяющие личность[53]. В Колумбии с 2011 года введен порядок обязательной регистрации номеров мобильной связи, а в Перу начиная с 2010 года все сим-карты привязываются к национальному идентификационному номеру[54]. Возможность введения таких правил рассматривается и в других странах. Такие правила нарушают анонимность, в особенности в случае лиц, выходящих в Интернет только с помощью мобильных технологий. Обязательная регистрация сим-карт дает правительствам возможность следить за частными лицами и журналистами в гораздо большей степени, чем того требуют их законные интересы.

52. Государства также пытаются бороться со средствами и программами анонимизации, такими как сеть "Tor", прокси-серверы и VPN, запрещая к ним доступ. В Китае давно заблокирован доступ к сетям "Tor"[55], а лица из российского правительства, по сообщениям, предложили более 100 000 долл. за разработку

---

[47] Human Rights Watch, "Vietnam: new decree punishes press", 23 February, 2011; Freedom House, "Vietnam: freedom of the press", 2012; Article 19, Comment Decree No. 02 of 2011 on Administrative Responsibility for Press and Publication Activities of the Prime Minister of the Socialist Republic of Vietnam (June 2011).

[48] Законопроект № 106 Исламской Республики Иран об органе регулирования вещания.

[49] См. эквадорский Органический закон о коммуникациях (2013 год).

[50] Законопроект № 428884-6 о внесении изменений в Федеральный закон "Об информации, информационных технологиях и о защите информации" и отдельные законодательные акты Российской Федерации по вопросам упорядочения обмена информацией с использованием информационно-телекоммуникационных сетей; Reuters, "Russia Demands Internet Users Show ID to Access Public Wifi," 8 August 2014.

[51] Статья 5 китайского постановления об авторском праве, средствах массовой информации и порядке регистрации учетных имен пользователей Интернета (2015 год).

[52] Действующий в Южной Африке с 2003 года закон № 70 о порядке перехвата сообщений и предоставлении коммуникационной информации; см. также закон 2002 года об электронных сообщениях и сделках (требование регистрации подлинных имен поставщиков услуг).

[53] Kevin P. Donovan and Aaron K. Martin, "The Rise of African SIM Registration", 3 February 2014.

[54] См. Колумбия, декрет № 1630 (2011 год); Perú 21, *Los celulares de prepago en la mira*, 27 May 2010.

[55] MIT Technology Review, *How China Blocks the Tor Anonymity Network*, 4 April 2012.

методов установления личности анонимных пользователей сети "Tor"[56]. Кроме того, по сообщениям, попытки заблокировать передаваемые через сеть "Tor" данные предпринимались правительствами Ирана (Исламской Республики)[57], Казахстана[58] и Эфиопии[59]. Поскольку такие средства и программы могут быть единственным механизмами для безбоязненного пользования свободой мнений и их свободного выражение, доступ к ним следует защищать и поощрять.

Ограничения в условиях общественных беспорядков

53. Необходимость в анонимных выступлениях возникает у активистов и демонстрантов, при этом государства раз за разом пытаются запретить или перехватить анонимные сообщения в период протестов. Такие попытки подавить свободу выражения мнений неправомерны и преследуют незаконную цель, заключающуюся в ущемлении права на мирные протесты, предусмотренного Всеобщей декларацией и Международным пактом о гражданских и политических правах.

Ответственность посредников

54. Некоторые государства и региональные суды предпринимают шаги для установления ответственности провайдеров Интернет-услуг и создателей электронных форумов за проверку онлайновых комментариев, оставляемых анонимными пользователями. Так, в соответствии с действующим в Эквадоре органическим законом о коммуникациях посредники обязаны использовать механизмы записи личных данных для целей удостоверения личности пользователей, оставляющих комментарии. В решении по делу "*Дельфи*" *против Эстонии* (заявление № 64569/09) Европейский суд по правам человека подтвердил конституционность эстонского закона, в соответствии с которым на владельцев электронных форумов ложится ответственность за размещаемые на них анонимные диффамационные заявления. Такие положения об ответственности посредников скорее всего приведут либо к введению норм регистрации настоящего имени, что нарушит анонимность, либо к полному прекращению деятельности теми веб-сайтами, владельцы которых не могут позволить себе обзавестись фильтрами для проверки, в результате чего пострадают небольшие независимые новостные компании. В недавно принятые Манильские принципы ответственности посредников, разработанные коалицией организаций гражданского общества, вошел тщательно проработанный набор руководящих принципов в области свободы выражения мнений в онлайновой среде, предназначенных для государств и международных и региональных механизмов.

Сохранение данных

55. В условиях широких стратегий обязательного сохранения данных ограничивается способность лица сохранять свою анонимность. Наличие у государств возможности потребовать от провайдеров Интернет- и телекоммуникационных услуг собирать и хранить архивы записей, фиксирующих деятельность всех пользователей в онлайновой среде, неизбежно привело к тому, что государства могут найти цифровой след любого пользоваться. Наличие у государства возможности собирать и хранить личные данные расширяет его возможности ве-

[56] Заказ был первоначально размещен по адресу http://zakupki.gov.ru/epz/order/notice/zkk44/view/common-info.html?regNumber= 0373100088714000008.

[57] "Phobos", "Iran partially blocks encrypted network traffic", The Tor Blog (10 February 2012).

[58] "Phobos", "Kazakhstan upgrades censorship to deep packet inspection", The Tor Blog (16 February 2012).

[59] Runa Sandvik, Ethiopia Introduces Deep Packet Inspection, The Tor Blog (31 May 2012); см. также Article 19, 12 January 2015.

сти наблюдение и увеличивает вероятность кражи и разглашения личной информации.

V. Выводы и рекомендации

56. **Шифрование и анонимность, а также лежащая в их основе концепция обеспечения безопасности являются залогом конфиденциальности и безопасности, необходимых для осуществления права на свободу мнений и их свободное выражение в цифровой век. В условиях отсутствия такой безопасности порою невозможно осуществлять другие права, включая экономические права, права на неприкосновенность частной жизни, надлежащую законную процедуру, свободу мирных собраний и ассоциации и право на жизнь и физическую неприкосновенность. С учетом важного значения шифрования и анонимности с точки зрения осуществления права на свободу мнений и их свободное выражение ограничения, вводимые в их отношении, должны строго подчиняться принципам законности, необходимости, соразмерности и правомерности их цели. В связи с этим Специальный докладчик рекомендует следующее.**

A. Государства

57. **Государствам следует пересмотреть или, в случае необходимости, принять законы и подзаконные акты для поощрения и защиты прав на неприкосновенность частной жизни и свободу мнений и их свободное выражение. Что касается шифрования и анонимности, то государствам следует проводить политику неограничения или всесторонней защиты, применять ограничения исключительно на индивидуальной основе и в соответствии с требованиями законности, необходимости, соразмерности и правомерности их цели, в обязательном порядке получать распоряжения суда для введения каждого конкретного ограничения и поощрять безопасность и конфиденциальность в онлайновой среде путем информирования общественности.**

58. **При обсуждении вопросов шифрования и анонимности основное внимание слишком часто уделяется возможности их использования в преступных целях в контексте террористической деятельности. Однако даже в условиях чрезвычайных ситуаций государства не освобождаются от обязательства обеспечивать соблюдение норм международного права прав человека. Законодательные предложения о пересмотре или принятии ограничений в отношении личной безопасности в онлайновой среде подлежат публичному обсуждению и утверждаются только на основе обычного, публичного, обоснованного и транспарентного законодательного процесса. Государства обязаны поощрять действенное участие широкого круга представителей гражданского общества и групп меньшинств в таких обсуждениях и процессах и избегать принятия такого законодательства на основании ускоренных законодательных процедур. В рамках общих обсуждений акцент следует делать на защите, обеспечиваемой шифрованием и анонимностью, в особенности в случае групп, наиболее подверженных опасности незаконного вмешательства. При любых обсуждениях следует также учитывать, что ограничения должны соответствовать строгим критериям: если они чреваты нарушениям права придерживаться своих мнений, вводить их нельзя. Ограничения права на неприкосновенность частной жизни, ведущие к ущемлению свободы выражения мнений, – или для целей настоящего доклада ограничения в отношении применения средств шифрования и аноними-**

зации – должны быть предусмотрены законом и необходимы и соразмерны одной из небольшого числа законных целей.

59. **Государствам следует поощрять применение надежных средств шифрования и анонимизации. В их законах за частными лицами должно признаваться право соблюдать конфиденциальность своих цифровых сообщений с помощью технологий и средств шифрования, позволяющих им сохранить анонимность в онлайновой среде. В законы и подзаконные акты, направленные на защиту правозащитников и журналистов, следует, среди прочего, включить положения, предусматривающие доступ к технологиям по обеспечению безопасности сообщений и меры по содействию их применению.**

60. **Государствам не следует ограничивать те виды шифрования и анонимности, с помощью которых облегчается и зачастую обеспечивается осуществление права на свободу мнений и их свободное выражение. Запреты, носящие абсолютный характер, не отвечают требованиям необходимости и соразмерности. Государствам следует отказаться от любых мер, снижающих степень безопасности частных лиц в онлайновой среде, в том числе от удаленного скрытого администрирования, низких стандартов шифрования и систем депонирования ключа. Кроме того, государствам следует воздержаться от введения требований, при которых обязательным условием для доступа к электронным сообщениям или онлайновым услугам являлась бы идентификация пользователей или которые предусматривали бы регистрацию сим-карты владельцев мобильных телефонов. Корпоративным субъектам также следует пересмотреть свою политику в области ограничения шифрования и анонимности (в том числе с использованием псевдонимов). К расшифровке, назначаемой судом в соответствии с нормами внутреннего законодательства и международного права, можно прибегать только в тех случаях, когда соответствующие меры опираются на транспарентые и доступные для всеобщего ознакомления законы и применяются исключительно на адресной и индивидуальной основе в отношении отдельных лиц (а не совокупности пользователей) с санкции судебных органов и при условии защиты прав лиц на надлежащее судопроизводство.**

B. Международные организации, частный сектор и гражданское общество

61. **Государствам, международным организациям, корпорациям и группам гражданского общества следует поощрять безопасность в онлайновой среде. С учетом актуального значения новых коммуникационных технологий с точки зрения поощрения прав человека и развития всем сторонам, имеющим отношение к этой проблематике, следует на систематической основе поощрять доступ к шифрованию и анонимности без какой бы то ни было дискриминации. Специальный докладчик настоятельно призывает все учреждения системы Организации Объединенных Наций, в особенности те из них, которые связаны с правами человека и гуманитарной защитой, содействовать использованию средств защиты связи для обеспечения возможности связаться с ними в безопасном режиме. Учреждения Организации Объединенных Наций должны пересмотреть свои методы и средства связи и выделить ресурсы в целях повышения степени безопасности и конфиденциальности в интересах широкого круга заинтересованных сторон, общающихся с Организацией в формате цифровых сообщений. Механизмы по защите прав человека должны проявлять особую осмотрительность при направлении просьб о предоставлении информации и работе с информацией,**

поступающей от гражданского общества или свидетелей и жертв нарушения прав человека.

62. **Хотя в настоящем докладе не делается выводов об ответственности корпораций за обеспечение безопасности связи, тем не менее с учетом угроз свободе выражения мнений в онлайновой среде совершенно очевидно, что корпоративным субъектам следует пересмотреть свою практику на предмет ее соответствия правозащитным нормам. Компаниям следует как минимум придерживаться принципов, изложенных в Руководящих принципах предпринимательской деятельности в аспекте прав человека, выработанных Глобальной сетевой инициативой Руководящих принципах свободы выражения мнений и неприкосновенности частной жизни, Руководстве Европейской комиссии для сектора ИКТ по вопросу о применении утвержденных Организацией Объединенных Наций Руководящих принципов предпринимательской деятельности в аспекте прав человека и документе, озаглавленном "Диалог телекоммуникационной индустрии: Руководство по принципам". Как и государствам, компаниям следует воздерживаться от блокирования или ограничения передачи зашифрованных сообщений и разрешать анонимные виды общения. Следует уделять внимание усилиям по расширению доступности ссылок на центры обработки зашифрованных данных, содействию использованию в веб-сайтах надежных технологий и повсеместному введению устанавливаемого по умолчанию сквозного шифрования. Корпоративным субъектам, поставляющим технологии, предназначенные для ослабления шифрования и анонимности, следует практиковать повышенную транспарентность в отношении своих товаров и клиентов.**

63. **Следует поощрять использование средств шифрования и анонимизации, а также повышать уровень "цифровой грамотности". Специальный докладчик, отдавая себе отчет в том, что ценность средств шифрования и анонимизации возрастает по мере их повсеместного распространения, призывает государства, организации гражданского общества и корпорации принять участие в кампании, направленной на обеспечение пользователям во всем мире доступа к встроенным и устанавливаемым по умолчанию средствам шифрования, и, при необходимости, предоставить наиболее уязвимым пользователям надлежащие средства для безопасного осуществления ими своего права на свободу мнений и их свободное выражение.**