Организация Объединенных Наций A/HRC/35/22

Генеральная Ассамблея

Distr.: General
30 March 2017
Russian
Original: English

Совет по правам человека
Тридцать пятая сессия
6–23 июня 2017 года
Пункт 3 повестки дня
Поощрение и защита всех прав человека, гражданских, политических, экономических, социальных и культурных прав, включая право на развитие

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

Записка секретариата

Секретариат имеет честь препроводить Совету по правам человека доклад Специального докладчика по вопросу о поощрении и защите права на свободу мнений и их свободное выражение Дэвида Кэя, подготовленный во исполнение резолюции 25/2 Совета. В своих двух предыдущих докладах Совету Специальный докладчик сосредоточил внимание на свободе мнений и их свободном выражении в эпоху цифровых технологий, подробно остановившись на том, как использование средств шифрования и анонимизации обеспечивают безопасность, необходимую для осуществления права на свободу выражения мнений (A/HRC/29/32), и наметив способы, с помощью которых в секторе информационно-коммуникационных технологий предполагается обеспечить свободу выражения мнений (A/HRC/32/38). В настоящем докладе он рассматривает роль частных субъектов, занимающихся предоставлением доступа к Интернету и телекоммуникационным ресурсам. Свое рассмотрение он начинает с изучения обязательств государства по защите и поощрению свободы выражения мнений в электронных сетях, затем дает оценку роли индустрии цифрового доступа и в заключение формулирует набор принципов, которые могли бы быть положены в основу мер по соблюдению прав человека, принимаемых в частном секторе.

GE.17-05047 (R) 210417 240417
1705047

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

Содержание

I. Введение

1. Государства все чаще используют индустрию цифрового доступа для контроля, ограничения или отслеживания мнений, выражаемых в электронных сетях. Когда власти хотят полностью отключить пользователей от веб-сайтов, социальных сетей или Интернета, им зачастую требуется помощь поставщиков услуг Интернета (ПУИ). Они вмешиваются в работу точек обмена интернет-трафиком (IXP), которые обеспечивают информационный поток на территорию страны или в ее пределах. Они получают доступ к частным сообщениям и другим личным данным, хранящимся у поставщиков телекоммуникационных услуг. Сегодня многие из этих субъектов находятся в частной собственности или под частным управлением. Они нередко играют существенную роль в установлении государственной цензуры и наблюдения, участвуя в этом либо против своей воли, либо молчаливо этому потворствуя или же активно проводя это в жизнь. То, чего правительства требуют от частных субъектов, и то, каким образом эти субъекты реагируют на эти требования, может подорвать обмен информацией; ограничить возможности журналистов безопасно вести расследования; препятствовать разоблачению злоупотреблений или деятельности правозащитников. Частные субъекты могут ограничивать свободу выражения мнений и по собственной инициативе. Они могут в обмен на вознаграждение или другие коммерческие выгоды отдать приоритет определенному интернет-контенту или интернет-приложениям, изменив тем самым способ взаимодействия пользователей с информацией в сетевом режиме. Компании, которые предлагают услуги в области фильтрации материалов, могут повлиять на доступность таких материалов для своих подписчиков.

2. Свобода выражения зависит как от государств, так и от частных субъектов. Обязательства государств по защите свободы выражения мнений ясны, но каковы при этом обязательства частных субъектов перед своими пользователями? Как они должны уважать свободу выражения мнений? Какие шаги они предпринимают, чтобы оценить и устранить те риски, которые их меры в ответ на действия и политику правительств могут порождать для свободы выражения мнений и неприкосновенности частной жизни? Каков объем информации о запросах и требованиях государства, который им следует довести до сведения своих клиентов? В каких случаях они непосредственно участвуют в злоупотреблениях или связаны с ними, какие средства правовой защиты должны быть доступны для отдельных лиц или широкой общественности, чьи интересы поставлены под угрозу?

3. Частные субъекты, обеспечивающие цифровой доступ, служат посредниками и дают возможность осуществлять свободу выражения мнений. Разумеется, в большинстве случаев инициаторами мер по цензуре и наблюдению являются государства. Но если государства часто, хотя и не всегда, полагаются на поставщиков для принятия мер, которые делают цензуру возможной, то мы как пользователи замечательных достижений цифровой эпохи вправе знать, как эти субъекты взаимодействуют друг с другом, как их взаимодействие и их самостоятельные меры сказываются на нас и каковы обязанности поставщиков в области уважения основных прав.

4. Настоящий доклад является результатом исследований и консультаций, которые проводились на протяжении более года и начались в 2016 году с описания сектора информационно-коммуникационных технологий (ИКТ) (см. A/HRC/32/38)[1]. На свою просьбу представить материалы[2] Специальный до-

[1] Я хотел бы поблагодарить Амоса Тоха, юрисконсульта мандатария и стипендиата Фонда Форда, являющегося сотрудником юридического факультета Калифорнийского университета в Ирвайне, за его качественные исследования и анализ, а также за координацию основательных и важных исследований, проведенных студентами

кладчик получил 25 ответов от государств; 3 – от компаний; 22 – от представителей гражданского общества, научных кругов и других субъектов; а также 1 ответ конфиденциального характера. Кроме того, Специальный докладчик провел под эгидой независимой правозащитной организации ARTICLE 19 совещание, посвященное совместному поиску творческих идей и организованное в Лондоне в июле 2016 года, совещание экспертов в Институте по правам человека Университета штата Коннектикут в Соединенных Штатах Америки, состоявшееся в октябре 2016 года, региональные консультации со Специальным докладчиком по вопросу о свободе выражения мнений Межамериканской комиссии по правам человека в Гвадалахаре, Мексика, в декабре 2016 года и региональные консультации в Бейруте в феврале 2017 года[3].

II. Обязательство государства по защите и поощрению свободы выражения мнений в электронных сетях

5. Международное право прав человека предусматривает право каждого человека беспрепятственно придерживаться своих убеждений и свободу искать, получать и распространять информацию и идеи любого рода, независимо от государственных границ, и через любые средства массовой информации по своему выбору (см. Всеобщая декларация прав человека, статья 19; и Международный пакт о гражданских и политических правах, статья 19). Совет по правам человека и Генеральная Ассамблея подтвердили, что свобода выражения мнений и другие права применяются в онлайновой среде (см. резолюции Совета 26/13 и 32/13; резолюцию 68/167 Генеральной Ассамблеи; и документ A/HRC/32/38). Комитет по правам человека, предыдущие мандатарии и Специальный докладчик изучили обязательства государств по статье 19 Пакта. Говоря коротко, государства не могут чинить препятствий способности придерживаться мнения или каким-либо образом ограничивать ее (см. пункт 1 статьи 19 Международного пакта о гражданских и политических правах; и A/HRC/29/32, пункт 19). В пункте 3 статьи 19 Пакта предусматривается, что государства могут ограничивать свободу выражения мнений лишь в тех случаях, когда это предусмотрено законом и является необходимым для уважения прав или репутации других лиц или для охраны государственной безопасности, общественного порядка, здоровья или нравственности населения (см. замечание общего порядка № 34 (2011) Комитета по правам человека; A/71/373; и A/HRC/29/32).

6. Государства также обязаны принимать меры для защиты лиц от ненадлежащего посягательства на права человека со стороны частных субъектов (см. пункт 2 статьи 2 Пакта, и замечание общего порядка № 31 (2004) Комитета по правам человека). Право прав человека защищает лиц от нарушений со стороны государства, а также нарушений, совершаемых физическими или юридическими лицами (см. замечание общего порядка № 31, пункт 8)[4]. В Руководящих принципах предпринимательской деятельности в аспекте прав человека: осуществление рамок Организации Объединенных Наций в отношении «защиты, соблюдения и средств правовой защиты», одобренных Советом по правам человека в 2011 году, содержится пояснение о том, что государства обязаны

лаборатории международного правосудия юридического факультета Калифорнийского университета в Ирвайне.

[2] См. https://freedex.org/new-call-for-submissions-freedom-of-expression-and-the-telecommunications-and-internet-access-sector/.

[3] С представленными материалами можно ознакомиться на веб-сайте мандатария. Обзор проведенных консультаций и материалов, полученных в ходе подготовки настоящего доклада, можно найти в дополнительном приложении, с которым также можно ознакомиться на веб-сайте мандатария.

[4] См. также African Commission on Human and Peoples' Rights, general comment No 3 (2015) on the right to life, para. 38; Inter-American Court of Human Rights, *Velásquez Rodríguez Case*, judgment of 29 July 1988, para. 172; и European Court of Human Rights, *Özel and others v. Turkey*, judgment of 17 November 2015, para. 170.

принимать надлежащие меры для предупреждения, расследования, наказания и компенсации за ущерб частных субъектов (см. A/HRC/17/31, приложение, принцип 1). Такие меры включают в себя принятие и осуществление законодательных, судебных, административных, просветительских и иных соответствующих мер, которые требуют или обеспечивают уважение свободы выражения мнений в деловых отношениях, а в случае злоупотреблений в частном секторе – доступ к эффективным средствам правовой защиты (см. замечание общего порядка № 31, пункт 7; и A/HRC/17/31, приложение, принципы 3 и 25).

7. Действия правительств, о которых говорится ниже, зачастую не соответствуют стандартам в области прав человека. Кроме того, характерной особенностью вмешательства правительства в сферу цифрового доступа является отсутствие транспарентности. Этому способствуют расплывчатые законы, предоставляющие властям чрезмерную свободу действий по своему усмотрению, юридические ограничения в отношении раскрытия третьей стороной сведений о доступе правительства к данным пользователей и конкретные запреты на разглашение информации. Отсутствие транспарентности подрывает верховенство права, а также понимание обществом того, что происходит в этом секторе[5].

A. Отключения Интернета и телекоммуникационных услуг

8. Отключения Интернета и телекоммуникационных услуг связаны с мерами по намеренному предотвращению или прекращению доступа или возможности распространения онлайновой информации в нарушение норм в области прав человека (см. A/HRC/32/13, пункт 10)[6]. Как правило, такие отключения осуществляются правительствами или по их распоряжению, зачастую при содействии частных субъектов, которые обслуживают работу сетей или обеспечивают сетевой трафик. К таким отключениям можно приравнять и последствия массированных атак на сетевую инфраструктуру, совершаемых частными сторонами, например распределенных сетевых атак (DDoS). Хотя отключения зачастую ассоциируются с полным выходом сети из строя, они также могут иметь место в случаях блокирования, закрытия или практического «вывода из строя» мобильной связи, веб-сайтов или социальных медиа и средств передачи сообщений[7]. Отключения могут затрагивать отдельные города или районы страны, всю страну или даже несколько стран и могут длиться от нескольких часов до нескольких месяцев.

9. Отключения, осуществленные по тайному приказу или без явных законных оснований, являются нарушением требования пункта 3 статьи 19 Пакта о том, что ограничения должны быть «установлены законом». В Чаде факт непредставления властями какого-либо вразумительного разъяснения причин ряда отключений Интернета и социальных сетей в период с февраля по октябрь 2016 года дал основания предполагать, что они были незаконными[8]. По сообщениям, в Габоне в период выборов 2016 года каждый вечер в течение почти двух недель наблюдался полный выход сети из строя, вопреки заверениям правительства в том, что обслуживание прерываться не будет[9].

10. Отключения в соответствии с распоряжением, выданным на основании нечетко сформулированных законов и нормативных актов, также не удовлетворяют требованию законности. В Таджикистане измененный закон «О правовом режиме чрезвычайного положения» разрешает органам государственной власти

[5] Freedom Online Coalition, Report of Working Group 3: Privacy and Transparency Online, November 2015.

[6] Организацией «Access Now» зарегистрировано 15 отключений в 2015 году и 56 отключений в 2016 году. Как сообщается, первое зарегистрированное отключение произошло в Непале в феврале 2005 года.

[7] Материал, представленный организацией «Access Now», part I, p. 1.

[8] Материал, представленный организацией «Internet Sans Frontières», p. 2, TCD 3/2016.

[9] Ibid., GAB 1/2016.

блокировать услуги мобильной связи и доступ в Интернет без постановления суда после объявления чрезвычайного положения[10]. В законе не сказано, когда и с какими целями может вводиться чрезвычайное положение. Такое отсутствие определенности позволяет властям свободно прибегать к отключениям по своему усмотрению. В некоторых странах для оправдания отключений власти опираются на устаревшие законы[11]. Критерий законности нарушают также законы и правила, которые принимаются или осуществляются под завесой секретности. В Соединенных Штатах Америки Национальный координационный центр по телекоммуникации значительно сократил опубликованный в публичном доступе вариант стандартной операционной процедуры 303, в которой определяется «подробный порядок действий на случай нарушения услуг сотовой связи»[12]. Хотя эти процедуры и не применялись на практике, сама возможность властей уклоняться от юридической экспертизы и подотчетности обществу противоречит статье 19 Пакта.

11. Ограничения на выражение мнений должны быть необходимыми для достижения целей, указанных в пункте 3 статьи 19 Пакта, и ни при каких условиях не могут служить оправданием для подавления тех, кто защищает демократические права (см. замечание общего порядка № 34 Комитета по правам человека, пункт 23; и A/71/373, пункт 26). Однако правительства зачастую устраивают отключения в ходе демонстраций, выборов и других событий, которые вызывают особый общественный интерес, практически без каких-либо объяснений[13]. В Бахрейне сбои мобильной связи и доступа в Интернет в Диразе, по утверждениям, совпали по времени с сидячими демонстрациями у дома известного религиозного лидера, которого правительство лишило гражданства[14]. Интернет-пользователи в Боливарианской Республике Венесуэла, по сообщениям, были лишены доступа к Интернету во время массовых антиправительственных протестов в 2014 году[15]. Нарушения работы сети были зафиксированы в ходе или в периоды выборов или протестов в Камеруне[16], Гамбии[17], Индии[18], Мьянме[19], Исламской Республике Иран[20], Уганде[21] и Черногории[22].

12. Отсутствие объяснений или признания отключений наводит на мысль о том, что они предназначены для недопущения информирования и подавления критики или инакомыслия. Сообщения о репрессиях и санкционированном государством насилии вслед за нарушениями работы сети дают основания предполагать, что некоторые государства используют обстановку неведения для совершения и сокрытия злоупотреблений. Например, в сентябре 2013 года в Судане доступ в Интернет был закрыт в течение нескольких часов во время же-

[10] OHCHR, “Preliminary observations by the United Nations Special Rapporteur on the right to freedom of opinion and expression, Mr. David Kaye, at the end of his visit to Tajikistan, press release (9 March 2015).

[11] India, Code of Criminal Procedure, sect. 144; а также Apar Gupta and Raman Jit Singh Chima, “The cost of internet shutdowns”, *The Indian Express* (26 October 2016).

[12] United States of America, NCC Standard Operating Procedure (SOP) 303.

[13] Материал, представленный организацией «Access Now», part I, pp. 5-7.

[14] Bahrain Center for Human Rights, *Digital Rights Derailed in Bahrain* (2016), pp. 13-14.

[15] Danny O’Brien, “Venezuela’s Internet crackdown escalates into regional blackout”, Electronic Frontier Foundation (20 February 2014).

[16] OHCHR, “UN expert urges Cameroon to restore Internet services cut off in rights violation”, press release (10 February 2017).

[17] Deji Olukotun, “Gambia shuts down Internet on eve of elections”, Access Now (30 November 2016).

[18] Software Freedom Law Center, “Internet shutdowns in India, 2013-2016”.

[19] Freedom House, “Freedom on the Net: Myanmar” (2011).

[20] Center for Democracy and Technology, “Iran’s Internet throttling: unacceptable now, unacceptable then” (3 July 2013).

[21] Article 19, “Uganda: Blanket ban on social media on election day is disproportionate” press release (18 February 2016).

[22] Global Voices, “WhatsApp and Viber blocked on election day in Montenegro” (17 October 2016).

стокого разгона демонстрантов, протестующих против повышения цен на топливо[23].

13. Наблюдатели также отмечают все более широкое использование отключений для предотвращения мошенничества учащихся в ходе национальных экзаменов. Узбекистан, возможно, был первой страной, которая прибегла к такому обоснованию во время университетских вступительных экзаменов в 2014 году[24]. В 2016 году предположительно по распоряжению властей были совершены отключения в ходе экзаменов в Алжире, Индии, Ираке и Эфиопии[25].

14. Отключения сети неизменно не отвечают требованию необходимости. С точки зрения необходимости необходимо продемонстрировать, что отключения способствовали бы достижению заявленной цели, которую они, по сути дела, нередко ставят под угрозу. По мнению некоторых правительств, важно запретить распространение новостей о террористических нападениях, даже точных сообщений, с тем чтобы не допустить паники и избежать повторения аналогичных действий[26]. Вместе с тем было установлено, что сохранение возможности сетевого подключения может способствовать ослаблению обеспокоенности в отношении общественной безопасности и восстановлению общественного порядка. Например, в ходе общественных беспорядков в Лондоне в 2011 году власти использовали социальные сети для выявления виновных лиц, распространения точной информации и проведения операций по зачистке. В Кашмире полицейские сообщили о позитивной роли, которую сыграли мобильные телефоны в розыске людей, оказавшихся в ловушке в ходе террористических нападений[27].

15. Продолжительность отключений и их географический охват могут варьироваться, однако, как правило, эти отключения являются несоразмерными. Пользователи, которых это затрагивает, оказываются отрезанными от услуг в области чрезвычайной помощи и от медико-санитарной информации, доступа к мобильным банковским операциям и электронной торговле, транспорта, школьных классов, голосования и наблюдения за выборами, сообщений об основных кризисах и событиях и проведения расследований в области прав человека[28]. С учетом количества важных видов деятельности и услуг, затрагиваемых отключениями, это ограничивает возможности выражения мнений и препятствует осуществлению других основополагающих прав.

16. Кроме того, отключения затрагивают и другие районы помимо тех, в которых они непосредственно происходят[29]. В 2015 году в преддверии парада по случаю национального праздника в Пакистане сети мобильной связи, по сообщениям, прекратили работу не только в том месте, где должен был состояться парад, но и в прилегающих районах, где не ожидалась какой-либо потенциальной угрозы безопасности[30]. В ходе визита Папы на Филиппины в 2015 году отключение мобильных сетей по соображениям безопасности сказалось на районах, расположенных далеко от его маршрута следования[31]. При отключении

[23] Human Rights Watch, “Sudan: Dozens killed during protests” (27 September 2013).

[24] Материал, представленный организацией «Access Now», part I; а также Freedom House, “Freedom on the Net: Uzbekistan” (2016).

[25] Материал, представленный организацией «Access Now», part I.

[26] См., например, OHCHR, “Preliminary conclusions and observations by the UN Special Rapporteur on the right to freedom of opinion and expression to his visit to Turkey, 14-18 November 2016”, press release (18 November 2016).

[27] Institute for Human Rights and Business (IHRB), “Security v. Access: The impact of mobile network shutdowns”, case study: Telenor Pakistan (September 2015), pp. 31-32.

[28] Материал, представленный организацией «Access Now», part I, pp. 11-14; а также материалы, представленные организацией «Global Network Initiative».

[29] IHRB, “Security v. Access: The impact of mobile network shutdowns”, case study: Telenor Pakistan (September 2015), p. 20.

[30] Ibid., pp. 27-28.

[31] Deniz Duru Aydin, “Five excuses governments (ab)use to justify Internet shutdowns” Access Now (6 October 2016).

конкретных услуг или платформ правительства, как правило, выбирают наиболее эффективные, надежные и широко используемые[32].

B. Доступ правительства к данным пользователей

17. Современная система государственного наблюдения опирается на доступ к средствам связи и связанным с ними данным, принадлежащим пользователям частных сетей. Хотя для такого доступа зачастую требуется помощь частных субъектов, этого также можно достичь и без их ведома или участия. Как и в случаях с другими формами наблюдения, доступ правительства к данным пользователей может привести к такому вмешательству в личную жизнь, что это может как напрямую, так и косвенно ограничить свободное развитие идей и свободный обмен ими (см. A/HRC/23/40, пункт 24). Неправомерный доступ к личным данным служит для пользователей своего рода предупреждением, побуждающим их тщательно взвешивать свои действия и, по возможности, избегать высказывания спорных мнений, обмена конфиденциальной информацией и других проявлений свободы выражения мнений, которые могут находиться под пристальным вниманием правительства (см. A/HRC/27/37, пункт 20).

Запросы о предоставлении данных пользователей

18. Расплывчатые законы и нормативные положения нарушают требование законности (см. A/HRC/23/40, пункт 50). В Малайзии, например, в соответствии с законом о средствах связи и мультимедийных средствах властям разрешено выдавать распоряжения о раскрытии «любого сообщения или группы сообщений» в случае «возникновения в обществе чрезвычайной ситуации или в интересах общественной безопасности». В законе не определены условия, которые вызывают чрезвычайную ситуацию в обществе, и факт, засвидетельствованный королем, считается «убедительным доказательством в этом вопросе»[33]. В Катаре правоохранительные органы пользуются широким правом требовать доступа к сообщениям клиентов поставщиков сетевых услуг в случаях, когда вопрос касается национальной безопасности или чрезвычайной ситуации[34]. Эти положения дают властям возможность требовать предоставления данных пользователей на основании лишь упоминания о национальной безопасности. Таким образом, пользователи не в состоянии предсказать с разумной степенью уверенности, при каких обстоятельствах их сообщения и связанные с ними данные могут быть предоставлены властям.

19. Поставщики сетевых услуг должны раскрывать данные пользователей только в тех случаях, когда соответствующее распоряжение было выдано судебными органами, удостоверившими необходимость и соразмерность этого для достижения законной цели. В Уголовном кодексе Канады содержится требование к правоохранительным органам представлять судье на утверждение просьбы о раскрытии записей телефонных разговоров в ходе уголовных расследований[35]. В Португалии для раскрытия данных сообщений власти должны получить судебный приказ[36]. Однако национальное законодательство часто не распространяет требование об обязательном получении санкции судебного органа на предоставление данных пользователей. В Бангладеш властям для доступа к данным сообщений подписчиков телекоммуникационных услуг по соображениям национальной безопасности и общественного порядка требуется только разрешение органов исполнительной власти[37].

[32] Материал, представленный организацией «Article 19», p. 2.
[33] Malaysia, Communications and Multimedia Act (1998), sect. 266.
[34] Qatar, Decree Law No. (34) of 2006.
[35] См. материал, представленный Канадой, p. 6.
[36] Portugal, Criminal Proceedings Code, arts. 187-190.
[37] Bangladesh, Telecommunication Regulatory Act (2001), sect. 97 (Ka).

20. Обеспокоенность в плане необходимости и соразмерности вызывают законы, требующие от частных субъектов создания доступных для правительства крупных баз данных, содержащих информацию пользователей. В Казахстане номера телефонов, адреса электронной почты и интернет-протокола (IP) и информация о выставлении счетов должны храниться поставщиком сетевых услуг в течение двух лет[38]. В Российской Федерации от частных субъектов требуется хранить содержание всех телефонных разговоров и текстовых сообщений клиентов в течение шести месяцев, а метаданные о соответствующих сообщениях – в течение трех лет[39]. В обеих странах также требуется хранить такие данные на местном уровне[40]. В странах, где основным средством связи являются мобильные телефоны, законы об обязательной регистрации СИМ-карт действительно требуют от большинства населения раскрывать информацию, позволяющую установить личность (см. A/HRC/29/32, пункт 51). Требование сохранять большой объем данных пользователей противоречит установленным процессуальным нормам, таким как необходимость индивидуализированного подозрения в совершении правонарушения.

Противодействие шифрованию

21. Со времени публикации доклада Специального докладчика об использовании средств шифрования и обеспечении анонимности (A/HRC/29/32) во всем мире все более широко стали применяться неоправданные и несоразмерные меры по противодействию шифрованию, которые угрожают подорвать как свободу выражения мнений, так и безопасность пользователей в цифровой среде. В Соединенном Королевстве Великобритании и Северной Ирландии, например, законом о следственных полномочиях 2016 года государственному секретарю разрешается рассылка «уведомлений о технических возможностях», в которых от поставщиков сетевых услуг требуют снятия «электронной защиты» с сообщений, что является мерой, которая вынуждает обходными путями или иным образом ограничивать или ослаблять систему шифрования[41]. Государства не представили достаточных доказательств того, что столь чувствительное вмешательство является наименее интрузивным способом защиты национальной безопасности и общественного порядка, особенно с учетом изобилия и изощренности других имеющихся в их распоряжении следственных инструментов (там же, пункт 39).

Прямой доступ

22. Прямой доступ в Интернет и телекоммуникационные сети позволяет властям перехватывать и отслеживать сообщения в условиях ограниченной юридической проверки или подотчетности. Технические достижения расширили возможности правоохранительных и разведывательных ведомств получать прямую связь с сетями, без участия или знания сетевого оператора[42]. В ходе всеобщих выборов в бывшей югославской Республике Македония в 2014 году руководство разведывательных органов, как представляется, получило прямой доступ к основным телекоммуникационным сетям страны для перехвата сообщений свыше 20 000 человек, в том числе политиков, активистов, государственных должностных лиц и журналистов. Многим лицам, на которых были нацелены эти действия, были также направлены записи их телефонных разговоров[43]. Как представляется, в Индии власти занимаются разработкой программы по созда-

[38] Казахстан, постановление правительства № 1593 (23 декабря 2011 года).

[39] OHCHR, letter to the Government of the Russian Federation, 28 July 2016 (OL RUS 7/2016).

[40] Материал, представленный организацией «Article 19», p. 5.

[41] United Kingdom of Great Britain and Northern Ireland, Investigatory Powers Act (2016), art. 253; а также OHCHR, letter to the Government of the United Kingdom, 22 December 2015 (AL GBR 4/2015).

[42] Материалы, представленные организациями «Privacy International»; а также «Telecommunications Industry Dialogue», p. 3.

[43] Privacy International, “Macedonia: Society On Tap” (23 March 2016).

нию центральной системы мониторинга, которая позволит «государственному учреждению через защищенную сеть с помощью электронных средств обеспечивать выявление искомых номеров без какого-либо оперативного вмешательства со стороны поставщиков телекоммуникационных услуг»[44]. Эта деятельность, как представляется, не предусмотрена законом, не санкционирована судебным органом и не является предметом внешнего надзора. Кроме того, риски, которые она создает для безопасности и неприкосновенности сетевой инфраструктуры, вызывают вопросы относительно ее соразмерности.

C. Сетевая нейтральность

23. Сетевая нейтральность – принцип, согласно которому со всеми содержащимися в Интернете данными следует обращаться одинаково и без неоправданного вмешательства, – способствует наиболее широкому доступу к информации[45]. В эпоху цифровых технологий свобода выбора между источниками информации имеет смысл лишь в том случае, когда интернет-контент и всякого рода приложения передаются без неправомерной дискриминации или вмешательства со стороны негосударственных субъектов, в том числе поставщиков сетевых услуг. Для выполнения государством обязанностей по поощрению свободы выражения мнений решительно требуется сетевая нейтральность, с тем чтобы содействовать как можно более широкому недискриминационному доступу к информации.

Платная приоритизация

24. В рамках платной приоритизации поставщики сетевых услуг устанавливают преференциальный режим для определенных видов интернет-трафика по сравнению с другими видами – за плату или в обмен на иные коммерческие выгоды. Эти механизмы приводят к созданию в Интернете быстрых полос трафика для тех поставщиков контента, которые могут позволить себе дополнительную плату, и медленных полос для всех остальных[46]. Такая иерархия данных негативно влияет на выбор пользователей. Пользователи несут более высокие расходы или получают услуги более низкого качества при доступе к интернет-контенту и приложениям в медленных полосах трафика. В то же время они могут быть вынуждены взаимодействовать с контентом, который был отнесен к числу приоритетных без их ведома или участия.

25. В некоторых государствах запрещена платная приоритизация. Например, в Нидерландах, которые одними из первых признали принцип сетевой нейтральности, поставщикам сетевых услуг запрещено устанавливать «расценки на услуги по обеспечению доступа в Интернет в зависимости от услуг и приложений, которые предлагаются или используются посредством оказания этих услуг»[47]. Постановлением Федеральной комиссии по связи Соединенных Штатов об открытом Интернете 2015 года запрещается «органам управления, осуществляющим оперативное руководство сетью поставщиков услуг в широкополосном доступе, прямо или косвенно отдавать предпочтение некоторым видам трафика по сравнению с другими видами... за вознаграждение (денежное

[44] Материал, представленный организацией «Access Now», part II, p. 4.

[45] Материал, представленный Лукой Белли; а также материал, представленный организацией «Article 19», pp. 7-8.

[46] Dawn C. Nunziato and Arturo J. Carrillo, “The price of paid prioritization: The international and domestic consequences of the failure to protect Net neutrality in the United States”, Georgetown Journal of International Affairs: International Engagement on Cyber V: Securing Critical Infrastructure (2 October 2015), p. 103.

[47] Netherlands, Telecommunications Act, art. 7.4a (3).

или иное) от третьей стороны, или в интересах аффилированной организации»[48].

Нулевая ставка

26. Применение нулевой ставки представляет собой практику невзимания платы за использование интернет-данных, связанных с конкретным приложением или услугой; в то же время другие услуги или приложения подлежат оплате по тарифам. Применение нулевой ставки варьирует от тарифных планов, в которых использование подписчиками некоторых интернет-услуг в счетчике пользователей не учитывается, до предоставления неограниченного доступа к некоторым услугам без приобретения плана[49]. Несмотря на различия, при применении нулевой ставки предпочтение отдается доступу, а не контенту, что может привести к повышению стоимости тарифицируемых данных. Пользователи, которые пытаются позволить себе доступ к тарифицируемым данным, могут в конечном итоге быть вынуждены пользоваться услугами по нулевым ставкам, в результате чего ограничится доступ к информации для общин, которые возможно и без того значительно вытеснены из процесса получения информации и участия в общественной жизни.

27. Применение нулевой ставки может предоставить пользователям ограниченный доступ в Интернет в тех областях, где в ином случае доступ был бы полностью невозможен[50]. Тем не менее более широкий доступ в Интернет может по-прежнему оставаться недоступным для пользователей, которые оказываются в ловушке постоянно огражденного онлайнового пространства[51]. Предположение о том, что ограниченный доступ постепенно дозреет до состояния полноценного подключения, требует дальнейшего изучения. Возможно, это будет зависеть от таких факторов, как поведение пользователей, состояние рынка, общая ситуация в области прав человека и нормативно-правовая среда[52].

28. Эти конкурирующие соображения привели к изменениям в подходах регулированию. В Индии в результате выражавшейся обеспокоенности общественности по поводу «Facebook's Free Basics» в конечном итоге был введен запрет на любую договоренность, которая «имеет силу дискриминационных тарифов на информационное обслуживание, предоставляемое или начисляемое к оплате потребителям на основе контента»[53]. Ограничения в отношении нулевой ставки действуют в Чили, Норвегии, Нидерландах, Финляндии, Исландии, Эстонии, Латвии, Литве, Мальте и Японии[54]. С другой стороны, в Соединенных Штатах, к которым позднее присоединилась Ассоциация европейских регуляторов в сфере электронных коммуникаций (BEREC), были приняты руководящие принципы, основанные на индивидуальном подходе[55]. Государствам, берущим

[48] United States of America, Federal Communications Commission, Protecting and Promoting the Open Internet, FCC 15-24 (12 March 2015), para. 18. Это постановление, которому на момент подготовки настоящего доклада, возможно, грозит отмена, по-прежнему является полезным образцом нормативного положения по вопросу о сетевой нейтральности.

[49] Erik Stallman and R. Stanley Adams, IV, "Zero Rating: A framework for assessing benefits and harms", Center for Democracy and Technology (January 2016).

[50] Ibid., pp. 4 and 11.

[51] Barbara van Schewick, "Network neutrality and zero-rating", submission to the United States Federal Communications Commission (19 February 2014), p. 7.

[52] Erik Stallman and R. Stanley Adams, IV, "Zero Rating: A framework for assessing benefits and harms" (January 2016), p. 15.

[53] India, Telecom Regulatory Authority, "TRAI releases the Prohibition of Discriminatory Tariffs for Data Services Regulations, 2016", press release (8 February 2016).

[54] Emily Hong, "A zero sum game? What you should know about zero-rating", *New America Weekly*, Edition 109 (4 February 2016).

[55] United States, Federal Communications Commission, Protecting and Promoting the Open Internet, FCC 15-24 (12 March 2015), para. 21; и BEREC, Guidelines on the Implementation by National Regulators of European Net Neutrality Rules (August 2016) (BoR (16) 127).

за основу индивидуальный подход, следует тщательно проанализировать его и, в случае необходимости, отвергнуть договоренности, которые, среди прочего, распространяют применение нулевой ставки на аффилированный контент, обусловливают применение нулевой ставки фактом оплаты или содействуют доступу к определенным приложениям из категории аналогичных приложений (например, применение нулевой ставки для определенных услуг по передаче музыки в потоковом режиме, а не всей потоковой передачи музыки). Кроме того, государства должны требовать полноценного раскрытия корпорациями информации о практике управления сетевым трафиком. В Чили, например, от ПУИ требуют раскрывать имеющиеся скорости доступа в Интернет, цены или разницу скоростей между национальным и международным подключением и связанные с этим гарантии[56].

III. Поставщики услуг цифрового доступа и свобода выражения мнений

29. Несмотря на общепризнанную обязанность государств уважать и защищать свободу выражения мнений, важную роль в этом также играют частные субъекты, которые устанавливают, обслуживают и поддерживают цифровой доступ.

A. Поставщики телекоммуникационных и интернет-услуг

30. Поставщики услуг связи (Telcos) и ПУИ (вместе называемые в настоящем докладе «поставщиками») предлагают широкий спектр услуг. Хотя в основном они управляют доступом и продают доступ к целому ряду сетей, в число которых входит и Интернет, они также обеспечивают пользователям возможность общаться друг с другом и обмениваться информацией с помощью мобильных услуг и традиционных наземных линий связи (см. A/HRC/32/38, пункт 16). Хотя во многих регионах поставщики по-прежнему принадлежат государству, все большее их число в настоящее время создается и управляется частными структурами. Эта отрасль также становится все более многонациональной: некоторые крупнейшие в мире поставщики управляют сетями во многих странах и регионах, часто на основе долевого участия в отечественных компаниях или их дочерних предприятиях.

31. Следя за работой обширных информационных сетей, поставщики сталкиваются с серьезным давлением со стороны правительств в плане выполнения требований, связанных с цензурой и наблюдением. Для управления сетью в какой-либо стране от них требуется направление существенных инвестиций в физическую и деловую инфраструктуру, включая сетевое оборудование и персонал. Они, как правило, подчиняются местным законам и другим лицензионным требованиям, изложенным в соглашениях с государством. В дополнение к правовому давлению поставщики также сталкиваются с угрозами вне правового поля, такими как угрозы безопасности своих сотрудников и объектов инфраструктуры в случае неисполнения требований[57].

32. Хотя некоторые поставщики пытаются сопротивляться требованиям в отношении цензуры и наблюдения, многие содействуют усилиям правительства без какого-либо противодействия. В Соединенных Штатах один из крупнейших в стране поставщиков якобы создал «суперпоисковую программу» для облегчения доступа правоохранительных органов к телефонам клиентов, даже несмот-

[56] Chile, Ley No. 20.453, art. 24 H (D).

[57] Материал, представленный организацией «Telecommunications Industry Dialogue», p. 10.

ря на то, что по закону не был обязан этого делать[58]. В Соединенном Королевстве в жалобе, поступившей в Организацию экономического сотрудничества и развития, утверждалось, что основные поставщики предоставили разведывательной службе страны доступ к своим сетям и данным клиентов, хотя на тот момент этого вовсе не требовалось по закону[59].

33. Все большее число поставщиков заключают со средствами массовой информации и другими компаниями по производству контента соглашения, которые угрожают сетевой нейтральности, и активно лоббируют уступки в отношении стандартов сетевой нейтральности. Например, при разработке европейскими регулирующими органами руководящих принципов сетевой нейтральности 17 основных поставщиков этого региона издали «Манифест 5G», в котором предупреждали о том, что «чрезмерно предписывающий характер» руководящих принципов замедлит их инвестиции в 5G, следующее поколение мобильной интернет-связи[60].

B. Точки обмена интернет-трафиком (IXP)

34. IXP обеспечивают возможность обмена интернет-трафиком между двумя и более сетями, которыми управляют различные поставщики сетевых услуг в пределах той или иной страны или региона[61]. Эта форма взаимодействия позволяет избежать длительных и обходных международных маршрутов местного или регионального интернет-трафика, тем самым способствуя повышению скорости и эффективности подключения к Интернету. IXP могут создаваться инфраструктурными интернет-компаниями как часть более широкого комплекса услуг, проданных поставщикам или управляемых в качестве некоммерческих организаций или организаций волонтеров[62].

35. IXP обрабатывают огромный объем интернет-трафика, который может фильтроваться или перехватываться по запросу правительства. Растущее число случаев применения цензуры и наблюдения с участием IXP свидетельствует о том, что они являются основными пунктами контроля доступа, даже если их конкретная роль неясна. Например, способ, с помощью которого в Пакистане в 2013 году был заблокирован доступ к «YouTube», указывает на то, что платформа была подвергнута фильтрации IXP, а не ПУИ, методом, известным как «пакетная инъекция»[63]. Согласно ставшему достоянием гласности внутреннему меморандуму работающего в Эквадоре многонационального ПУИ, пользователи не могли получить доступ к «Гугл» и «YouTube» в марте 2014 года, поскольку частная ассоциация интернет-провайдеров Эквадора, которая управляет двумя крупнейшими IXP в стране, «блокировала доступ к некоторым веб-сайтам в Интернете по просьбе национального правительства»[64]. Выявление фактов массового наблюдения, осуществляемого Агентством национальной безопасности Соединенных Штатов, породили среди технических специалистов обеспокоенность тем, что Агентство перехватывает значительную долю отечественного и зарубежного интернет-трафика через IXP Соединенных Штатов[65]. В сентябре

[58] Dave Maass and Aaron Mackey, “Law enforcement’s secret ‘super search engine’ amasses trillions of phone records for decades”, Electronic Frontier Foundation (29 November 2016).

[59] Privacy International, “OECD complaint against BT, Verizon Enterprise, Vodafone Cable, Viatel, Level 3, and Interoute”.

[60] Материал, представленный организацией «Article 19», p. 9.

[61] См. www.bgp4.as/internet-exchanges/.

[62] Jason Gerson and Patrick Ryan, “A primer on Internet exchange points for policymakers and non-engineers” *Social Science Research Network* (12 August 2012), p. 10.

[63] Zubair Nabi, “The anatomy of web censorship in Pakistan” (2013), p. 4.

[64] Katitza Rodriguez, “Leaked documents confirm Ecuador’s Internet censorship machine”, Electronic Frontier Foundation (14 April 2016).

[65] Andrew Clement and Jonathan Obar, “Canadian Internet ‘boomerang’ traffic and mass NSA surveillance: Responding to privacy and network sovereignty challenges”, in *Law, Privacy*

2016 года расположенная в Германии крупнейшая в мире точка обмена интернет-трафиком опротестовала постановления разведывательной службы страны об отслеживании международных сообщений, проходящих через ее центр связи[66].

C. Сети доставки контента

36. Сеть доставки контента (CDN) представляет собой сеть серверов, стратегически распределенных по всему миру с целью обеспечения возможности эффективной доставки веб-страниц и других материалов в Интернете. Для того чтобы связаться с наибольшим числом пользователей в кратчайшие сроки, крупные производители контента всецело полагаются на сети доставки контента[67]. В сети доставки контента хранятся копии контента, размещенного на этих платформах, и сеть переадресует запрос пользователя на такой контент с серверов платформы на сервера, входящие в сеть и расположенные ближе всего к пользователю[68]. Этот процесс повышает скорость доставки контента, особенно для пользователей, которые находятся далеко от серверов платформы. Сети доставки контента считаются эффективной мерой защиты от блокировки веб-сайта; меры цензуры, направленные против серверов, на которых размещены конкретные веб-сайты или платформы, не сказываются на доставке пользователям через сети доставки контента копий того же контента[69]. Сети доставки контента также стали важнейшей защитой от сетевых сбоев. Требования быстрого доступа создали для них стимулы для инвестирования значительных средств в инфраструктуру и услуги, которые могут выдерживать распределенный отказ в обслуживании и иные злонамеренные атаки[70].

37. Устойчивость сетей доставки контента к мерам цензуры также сделала их объектами несоразмерных ограничений на свободу выражения мнений. В Египте блокировка веб-сайта «The New Arab» в августе 2016 года также привела к сбою доступа к контенту других сайтов, которые, не будучи связаны друг с другом, входили в одну и ту же сеть доставки контента, что навело исследователей на мысль о том, что против этой сети и были направлены действия властей[71]. В Китае, согласно сообщениям, с помощью национального фильтра была заблокирована сеть доставки контента EdgeCast, которая обеспечивает доставку контента для ряда крупных веб-сайтов страны[72].

38. Поскольку сети доставки контента обрабатывают большие объемы заявок пользователей на интернет-контент с многочисленных веб-сайтов и платформ, они также уязвимы для наблюдения со стороны правительства. Например, в 2016 году Amazon Web Services, где расположена одна из крупнейших сетей доставки контента[73], сообщила о том, что число просьб правительства о предоставлении доступа к данным возросло более чем вдвое по сравнению с преды-

and Surveillance in Canada in the Post-Snowden Era, Michael Geist, ed. (University of Ottawa Press, 2015).

[66] De Cix, “Information on the lawsuit against the Federal Republic of Germany” (16 September 2016).

[67] Geoff Huston, “The death of transit?”, Asia Pacific Network Information Centre (27 October 2016).

[68] Vangie Beal, “CDN – Content Delivery Network”, *Webopedia*.

[69] John Holowczak and Amir Houmansadr, “CacheBrowser: bypassing Chinese censorship without proxies using cached content” (2015).

[70] Geoff Huston, “The death of transit?”, Asia Pacific Network Information Centre (27 October 2016).

[71] Leonid Evdokimov and Vasilis Ververis, “Egypt: Media censorship, Tor interference, HTTPS throttling and ads injections?”, Open Observatory of Network Interference (27 October 2016).

[72] Joss Wright, “A quick investigation of EdgeCast CDN blocking in China”, blog, Oxford Internet Institute (18 November 2014).

[73] На момент подготовки настоящего доклада Amazon Cloudfront обслуживал наибольшее число доменов веб-сайтов во всем мире.

дущим годом[74]. Исследователи также считают, что массовое наблюдение стратегически направлено на сети доставки контента с целью максимального сбора информации, однако остается неясным, как конкретно это происходит и, если таковое имеет место, какова степень участия в этом процессе сетей доставки контента[75].

D. Поставщики сетевого оборудования

39. Поставщики поставляют аппаратные средства и программное обеспечение, которые формируют основу Интернета и телекоммуникационных сетей. Сетевое оборудование, как правило, включает в себя маршрутизаторы, коммутаторы и точки доступа, которые позволяют нескольким устройствам и сетям подключаться друг к другу (см. A/HRC/32/38, пункт 18). Поставщики также диверсифицировали свои предприятия, обеспечив оборудование для передачи голоса по IP-протоколу (VoIP), которое позволяет делать беспроводные звонки и создает условия для технологий «Интернета вещей» (IoT), обеспечивающих взаимодействие между «умными» устройствами[76]. Поставщики редко ориентированы на прямое взаимодействие с потребителями: их основными клиентами являются сетевые операторы, такие как правительства, ПУИ или сети доставки контента. В результате от них требуется сконфигурировать сети по техническим стандартам, указанным этими операторами, включая стандарты установленные местными законами (например, требования в области охраны правопорядка и национальной безопасности). Однако поставщики могут также разрабатывать или модифицировать оборудование и технологию для обеспечения соответствия частным или государственным требованиям.

40. С учетом своей бизнес-модели поставщики обязаны находить решения правозащитных проблем, с которыми сталкиваются или которые создают их клиенты. В области наблюдения поставщики зачастую вынуждены учитывать меры «законного перехвата», для которых требуется такая конфигурация сетей, чтобы у правительства имелась возможность доступа к данным пользователей[77]. Кроме того, с поставщиками могут заключаться соглашения о создании «систем управления и посредничества», которые облегчают обмен перехваченными данными между сетевым оператором и государственным органом, а также государственными системами, которые занимаются обработкой этих перехваченных данных[78]. В условиях, когда поставщики также управляют созданными ими сетями, они могут также нести ответственность за удовлетворение запросов правительства о предоставлении данных пользователей от имени оператора[79].

41. Разработка сетевого оборудования и технологий многоцелевого использования порождает обеспокоенность в отношении свободы выражения мнений и неприкосновенности частной жизни. Например, устройства для углубленной проверки пакетов используются в обычных технических целях, например, для устранения сетевых перегрузок, но могут применяться и для фильтрации интернет-контента, перехвата сообщений и регулирования потоков данных. Мобильные сети сконфигурированы так, чтобы отслеживать местонахождение сотовых телефонов в режиме реального времени и обеспечивать доступность со-

[74] Amazon Information Request Report (June 2016).

[75] См. например, Harrison Weber, “How the NSA & FBI made Facebook the perfect mass surveillance tool”, *Venture Beat* (15 May 2014).

[76] Michael E. Raynor and Phil Wilson, “Beyond the dumb pipe: The IoT and the new role for network service providers”, Deloitte University Press (2 September 2015).

[77] См., например, резолюцию Совета Европейского союза от 17 января 1995 года о законном перехвате телекоммуникационных сообщений, Official Journal C 329; и материалы, представленные организацией «Privacy International», pp. 2-3.

[78] IHRB, “Human rights challenges of telecommunications vendors: addressing the possible misuse of telecommunications systems: case study: Ericsson” (November 2014), p. 16.

[79] Ibid., p. 17.

товой связи из любого места, однако такое отслеживание может также быть нацелено на самих пользователей[80].

42. Отдельные факты свидетельствуют о том, что поставщики могут оказывать правительству поддержку в осуществлении цензуры и наблюдения. На рассмотрении в судах Соединенных Штатов Америки находится дело, в котором компанию «Сиско» обвиняют в разработке, применении и содействии в обслуживании китайской сети наблюдения и обеспечения внутренней безопасности, известной под названием «Золотой щит»[81]. («Сиско» отвергает эти обвинения.)[82] В Эфиопии группы правозащитников обнаружили, что ZTE Corporation разработала и установила для Ethio Telecom базу данных управления работой с клиентами, которая позволяет вести интрузивное наблюдение[83].

E. Другие частные субъекты

43. Выводы и рекомендации, содержащиеся в настоящем докладе, применимы к любой организации, занимающейся предоставлением цифрового доступа, как указано выше. Все большее число интернет-компаний формируют свои портфели с включением в списки услуг неограниченного цифрового доступа и необходимого инфраструктурного обслуживания. Например, две крупнейшие китайские интернет-компании Alibaba и Tencent в настоящее время предлагают также услуги сетей доставки контента[84]. Компания «Гугл» на экспериментальной основе осваивает методы обеспечения беспроводного доступа в обход традиционных поставщиков сетевых услуг; в 2010 году она начала оказывать услуги по высокоскоростному подключению к Интернету из домов и предприятий в отдельных городах Соединенных Штатов[85]. Она также сотрудничает с «Фейсбук» и «Майкрософт» в деле создания подводных кабельных сетей, которые позволят им связать пользователей без применения оборудования или систем третьей стороны[86].

44. Организации-разработчики стандартов (ОРС), не являясь, строго говоря, «промышленными субъектами», тем не менее, создают технические протоколы и стандарты, обеспечивающие совместимость инфраструктуры в сфере телекоммуникаций и Интернета. Разработка стандартов без учета правозащитных соображений может негативно сказаться на свободе выражения мнений. Например, отсутствие требования защиты транспортного уровня (TLS) в качестве одного из обязательных элементов протокола передачи гипертекста (HTTP) делает сетевой трафик уязвимым к цензуре и наблюдению. Таким образом, усилия технического сообщества по обеспечению должной заботы о правах человека в процессе разработки стандартов являются шагом в правильном направлении[87].

[80] Ibid., p. 13.

[81] United States District Court for the Northern District of California, San Jose Division, *Doe et al. v. Cisco Systems, Inc. et al.*, Case No. 5:11-cv-02449-EJD-PSGx (18 September 2013).

[82] John Earnhardt, “Cisco Q&A on China and censorship” Cisco blogs (2 March 2006).

[83] Human Rights Watch, “They know everything we do: telecom and Internet surveillance in Ethiopia” (25 March 2014).

[84] Tencent Cloud CDN and Alibaba Cloud CDN.

[85] Klint Finley, “Google eyes blazing-fast wireless as a way into your home”, *Wired* (12 August 2016).

[86] Joon Ian Wong, “Google and Facebook are doubling down on Internet infrastructure with a new Pacific cable”, *Quartz* (17 October 2016).

[87] Internet Research Task Force, “Research into human rights protocol considerations” (25 February 2017). Имеется по адресу https://datatracker.ietf.org/doc/draft-irtf-hrpc-research/?include text 1. В дополнительном приложении содержится более подробный анализ функций и обязанностей организаций-разработчиков стандартов.

IV. Правозащитные обязанности поставщиков услуг цифрового доступа

45. В Руководящих принципах предпринимательской деятельности в аспекте прав человека признается обязанность предприятий уважать права человека независимо от обязательств государства или от выполнения этих обязательств (см. A/HRC/17/31, приложение; и A/HRC/32/38, пункты 9–10). В них предусмотрен минимальный базовый уровень корпоративной подотчетности в области прав человека и содержится настоятельный призыв к компаниям сделать заявление программного характера об обязательстве соблюдать права человека, утверждаемое на самом высоком уровне руководящего звена предприятия; обеспечивать должную заботу в целях реального «выявления, предотвращения, смягчения последствий и представления отчетности» о фактическом и потенциальном воздействии на права человека в ходе всей деятельности компании; и обеспечить возмещение ущерба или сотрудничать в деле такого возмещения в случаях неблагоприятного воздействия на права человека (см. A/HRC/17/31, приложение, принципы 16–24).

A. Учет сложившихся условий

46. В Руководящих принципах подчеркивается необходимость того, чтобы компании учитывали особенности условий, в которых они осуществляют свою деятельность, при исполнении ими своих обязанностей в области прав человека (там же). В сфере индустрии цифрового доступа необходимо учитывать несколько аспектов условий.

Поставщики услуг доступа предоставляют общественное благо

47. Индустрия цифрового доступа относится к области выражения мнений в цифровой среде; ее коммерческая жизнеспособность зависит от пользователей, которые ищут, получают и передают информацию и идеи через сети, которые она создает и которыми управляет. Поскольку находящиеся в частном владении сети необходимы для осуществления в наши дни права на свободу выражения мнений, те, кто ими управляет, также берут на себя важнейшие социальные и общественные функции. Принимаемые в этой отрасли решения − будь то в ответ на требования правительства или исходя из коммерческих интересов − могут непосредственно оказывать как благоприятное, так и крайне негативное воздействие на свободу выражения мнений и связанные с этим права человека.

Ограничения на доступ в Интернет сказываются на свободе выражения мнений в глобальном масштабе

48. Воздействие этой отрасли на права человека часто носит глобальный характер, затрагивая даже пользователей на рынках, которые соответствующая компания не обслуживает. Например, наблюдение за одной из точек обмена интернет-трафиком в Соединенных Штатах может охватывать крупные потоки сообщений между гражданами США и иностранцами и даже исключительно между иностранцами. Аналогичным образом уязвимость системы безопасности в структуре сети сказывается на всех пользователях, которые получают цифровой доступ через эту дефектную сеть, включая пользователей, находящихся вдали от этой сети. Соответственно, компаниям следует выявлять и устранять более масштабные последствия их деятельности для свободы выражения мнений, в целом, помимо последствий для клиентов или правообладателей на тех рынках, где они осуществляют свою деятельность. Разумеется, способы, которыми они объясняют свое воздействие, могут различаться в зависимости от их размера, ресурсов, принадлежности, структуры и условий, в которых они осуществляют свою деятельность (там же, принцип 14). Например, все поставщики должны проверять запросы, касающиеся данных пользователей, на соответствие минимальному набору формальных требований независимо от того, отку-

да исходит этот запрос и кем является соответствующий пользователь. Однако, если у многонационального поставщика может иметься специализированная группа по проверке запросов, малый или средний поставщик для выполнения этой же функции может поручить выполнение этой задачи своей юридической группе или группе по связям с общественностью.

Отрасль подвержена давлению со стороны государства в ущерб свободе выражения мнений…

49. Руководящие принципы направлены на устранение пробелов в корпоративной подотчетности, возникших в результате отсутствия национального законодательства или его неисполнения[88]. Однако ревностное приведение в исполнение национального законодательства также создает правозащитные проблемы в сфере индустрии цифрового доступа. Например, государства могут возлагать на поставщиков ответственность за интернет-контент или иным образом оказывать на них давление с целью ограничения интернет-контента, размещенного пользователями в своих сетях, в соответствии с законами об ответственности за самые различные деяния, включая ненавистнические высказывания, диффамацию, киберпреступность и государственную измену. Однако такая промежуточная ответственность порождает мощные стимулы к цензуре: поставщики могут счесть более безопасным не оспаривать такое регулирование, а вместо этого чрезмерно регулировать контент, в связи с чем законное и правомерное выражение мнений также в конечном итоге ограничивается. Давление с целью содействия осуществлению государственной цензуры и наблюдения также возрастает, когда власти преследуют, угрожают или арестовывают служащих компании или пытаются вмешиваться в работу сетей или оборудования компании[89].

…но в то же время ее положение уникально для обеспечения уважения прав пользователей

50. Двойная роль этой отрасли в качестве средства обеспечения цифрового доступа и естественного этапа для введения налагаемых государством ограничений повышает ее важность в качестве средства защиты от государства и частного произвола. Например, поставщики, как правило, располагают наибольшими возможностями противодействовать отключению или запросу на предоставление данных пользователей. Сети доставки контента стратегически расположены в инфраструктуре Интернета, позволяя противодействовать злонамеренным атакам, подрывающим доступ. Только поставщики в состоянии оценить, будут ли использованы или используются ли их продукты в ущерб правам человека, особенно когда они применяют меры должной осмотрительности в отношении продаж или оказывают текущие услуги.

B. Обязанность уважать свободу выражения мнений пользователей

51. Для практического выполнения своих правозащитных обязательств индустрии цифрового доступа следует выделять надлежащие ресурсы, по крайней мере для тех видов своей деятельности, которые описаны ниже. Хотя эти принципы оцениваются в контексте цифрового доступа, они также имеют отношение к другим секторам цифровой экономики, таким как социальные сети, торговля, наблюдение и поиск.

[88] Yael Ronen, “Big Brother’s little helpers: the right to privacy and the responsibility of Internet service providers”, *Utrecht Journal of International and European Law*, vol. 31, No. 80 (February 2015), p. 76.

[89] В 2014 году запрос об отключении сети, полученный компанией Orange, многонациональным поставщиком телекоммуникационных услуг, от властей Центральноафриканской Республики, как сообщалось, «сопровождался угрозой применения персональных санкций в случае неподчинения». См. материалы, представленные организацией «Telecommunications Industry Dialogue», p. 11.

1. Должная осмотрительность

52. Процессы, связанные с должной осмотрительностью, позволяют поставщику услуг цифрового доступа выявлять, предотвращать и смягчать неблагоприятное воздействие своей деятельности на права человека (см. A/HRC/17/31, приложение, принцип 19). В то время как единообразные подходы в обеспечении должной осмотрительности невозможны и нежелательны, оценки воздействия на права человека позволяют выявлять степень рисков для свободы выражения мнений и неприкосновенности частной жизни и служить средством для их устранения[90]. Должная осмотрительность предполагает по крайней мере следующее.

Стратегии, регулирующие применение мер должной осмотрительности

53. Компаниям следует разработать четкие и конкретные критерии для выявления тех видов деятельности, которые связаны со свободой выражения мнений и осуществлением процессов обеспечения должной осмотрительности[91]. Полезными показателями в этой связи являются правозащитные последствия прошлой и нынешней деятельности компании, а также принятая в отрасли практика. В индустрии обеспечения цифрового доступа такая деятельность может включать в себя слияния и приобретения компаний; вхождение на рынок или уход с рынка; правительственные или неправительственные запросы об ограничении контента или о предоставлении данных о пользователях; дальнейшее развитие или изменения политики, касающейся ограничения контента и неприкосновенности частной жизни; изменения продукта в части регулирования контента или шифрования сообщений; механизмы, облегчающие приоритетный доступ к интернет-контенту и приложениям; конструктивное исполнение, продажа и приобретение сетевого оборудования и технологий перехвата и фильтрации, а также связанные с этим услуги по обучению и консультированию[92]. Этот перечень является далеко не полным, «требует постоянного внимания и обновления» с учетом новых сфер ведения предпринимательской деятельности, развития технологий и других изменений условий оперативной деятельности[93].

Вопросы для изучения

54. В ходе процессов обеспечения должной осмотрительности следует критически проанализировать по крайней мере применимые местные и международные нормы и стандарты, в том числе возможные противоречия между местными законами и правами человека; риски для свободы выражения мнений и неприкосновенности частной жизни, связанные с приобретением продуктов и услуг компании; стратегии смягчения и предотвращения таких рисков; пределы эффективности этих стратегий с учетом юридических, нормативных и оперативных условий, в которых работает компания; и возможности поощрения прав человека в рамках всей деятельности компании[94].

---

[90] К основным поставщикам телекоммуникационных услуг, которые разработали критерии оценки воздействия на права человека, относятся компании «Telia Company» и «Telefonica». Ibid., pp. 7-8.

[91] Nokia встроила в свой модуль для продаж автоматизированную функцию, которая указывает на риски для прав человека, сопряженные с возможной продажей. Ibid., p. 7.

[92] European Commission, *ICT Sector Guide on Implementing the UN Guiding Principles on Business and Human Rights* (2013), pp. 32-36.

[93] Michael A. Samway, “Business, human rights and the Internet: a framework for implementation”, in *Human Dignity and the Future of Global Institutions*, Mark P. Lagon and Anthony Clark Arend, eds. (Washington, D.C., Georgetown University Press, 2014), p. 308.

[94] Ibid., pp. 310-312, для более всеобъемлющего обзора соответствующих тематических областей, которые должен охватывать процесс обеспечения должной осмотрительности.

Внутренний процесс и профессиональная подготовка

55. Хотя наличие в составе компании специалистов по вопросам бизнеса и прав человека и имеет важное значение, обеспечение должной осмотрительности не должно быть исключительно их обязанностью, а должно охватывать и другие соответствующие функциональные группы, вовлеченные в предпринимательскую деятельность. Для этого требуется диалог и сотрудничество между различными оперативными подразделениями (по таким вопросам, как конфиденциальность, правоприменение, отношения с государством, обеспечение соблюдения требований, управление рисками, разработка продукции и ведение оперативной деятельности) и специалистами (такими, как инженеры, исследователи сферы взаимодействия с пользователями, группы сбыта и руководители предприятий)[95]. В контексте неприкосновенности частной жизни исследователи пришли к выводу о том, что меры, связанные «с участием старших руководителей оперативных подразделений и возложением на них ответственности» за управление конфиденциальными делами, а также с «включением сотрудников, имеющих опыт обеспечения защиты неприкосновенности частной жизни и лично ответственных за соблюдение конфиденциальности …в состав оперативных подразделений», создают условия, благоприятные для защиты неприкосновенности частной жизни[96]. Аналогичные методы управления могут также обеспечить уважение свободы выражения мнений со стороны деловых кругов. Исходя из этих соображений, для участия в деятельности по обеспечению должной осмотрительности малым и средним предприятиям может потребоваться целая операция[97].

Опыт внешних экспертов

56. Учитывая необходимость широкой базы знаний, процесс обеспечения должной осмотрительности должен опираться на внешний опыт неправительственных экспертов, в том числе местного гражданского общества, международных правозащитных организаций, правозащитных механизмов международных и региональных организаций, научных кругов и технического сообщества. Возможности для совместного обучения и взаимной подотчетности также предоставляют многосторонние форумы. Например, исследователи пришли к выводу о том, что участие в правозащитных инициативах в конкретных секторах или отраслях, таких как Глобальная сетевая инициатива и Диалог телекоммуникационной индустрии, отражаются на показателях правозащитной деятельности компаний[98].

Консультации с пользователями и затрагиваемыми правообладателями

57. Все поставщики услуг цифрового доступа в той или иной форме оказывают влияние на свободу выражения мнений конечными пользователями. Таким образом, даже те компании, которые напрямую не взаимодействуют с потребителями, должны консультироваться с конечными пользователями в рамках процесса оценки рисков. Такие консультации отличаются от более широких многосторонних усилий заинтересованных участников, о которых говорилось выше, и предусматривают «двусторонний диалог» с целью «сбора конкретных мнений или сообщений от затрагиваемых заинтересованных сторон (или их представителей), которые затем учитываются в ходе внутренних процессов принятия и осуществления решений компании»[99]. Например, в ходе переговоров о лицензи-

[95] European Commission, *ICT Sector Guide on Implementing the UN Guiding Principles on Business and Human Rights* (2013), p. 36.

[96] Kenneth A. Bamberger and Deirdre K. Mulligan, *Privacy on the Ground: Driving Corporate Behavior in the United States and Europe* (Cambridge, Massachusetts, MIT Press, 2015), p. 177.

[97] European Commission, *ICT Sector Guide on Implementing the UN Guiding Principles on Business and Human Rights* (2013), p. 37.

[98] Материал, представленный организацией «Ranking Digital Rights», p. 5.

[99] European Commission, *ICT Sector Guide on Implementing the UN Guiding Principles on Business and Human Rights* (2013), pp. 37-38.

ровании в условиях работы с высокой степенью риска или в ходе разработки, проверки и внедрения политики нулевой ставки могут проводиться консультации с уязвимыми или маргинализованными лицами и группами. Конструктивные консультации должны также включать в себя регулярное привлечение к сотрудничеству организаций гражданского общества, которые могут представлять потребности и интересы конечных пользователей в конкретных общинах и могут сами подвергаться еще большему риску давления в связи со своей пропагандистской деятельностью.

Текущие оценки изменения положения

58. Компаниям следует принимать оперативные меры по адаптации процессов обеспечения должной осмотрительности к изменениям обстоятельств или оперативных условий. Например, оценка рисков должна продолжаться и после этапа проектирования и через регулярные промежутки времени в течение всего жизненного цикла продукта или услуги с учетом таких факторов, как технологические и инфраструктурные изменения и связанные с ними факторы уязвимости в сфере безопасности, перемены в поведении потребителей и изменение правовых, политических и социальных условий, в которых действуют компании[100].

2. Включение правозащитных гарантий путем проектных решений

59. Как и в случае всех крупных технических разработок, выработка проектных и инженерных решений происходит с учетом государственной политики и при их принятии необходимо руководствоваться правозащитными принципами. Например, ключевая технология сетевого сегментирования 5G может позволить поставщикам мобильных услуг более эффективно управлять сетевым трафиком и способствовать удовлетворению постоянно растущих запросов потребителей в эпоху «Интернета вещей» (IoT). В то же время сети также можно сегментировать на быстрые и медленные полосы, что обеспечит приоритетный доступ к некоторым интернет-приложениям по сравнению с другими и, возможно, нарушит сетевую нейтральность. Соответственно, компаниям следует обеспечить, чтобы инновационное сетевое оборудование и технологии – особенно многоцелевого использования – разрабатывались и внедрялись таким образом, чтобы соответствовать стандартам свободы выражения мнений и неприкосновенности частной жизни[101].

60. Компании должны играть активную и конструктивную роль в разработке мер, способствующих выражению мнений и неприкосновенности частной жизни. Например, меры по обеспечению цифровой безопасности, выявлению и предотвращению распределенных сетевых атак и хакерской деятельности должны быть направлены на злонамеренный трафик и не затрагивать законное взаимодействие между отдельными лицами, организациями и общинами. Соответствующая конфигурация сетевого оборудования для сведения к минимуму необязательного сбора информации о пользователях – с учетом местных требований закона и маршрутизации – фактически предвосхищает чрезмерные запросы о предоставлении данных, поскольку компании не могут передать информацию, которой у них нет[102]. Даже если информация пользователя зарегистрирована, разумные сроки, ограничивающие необходимость сообщать о том, имеются ли данные и как долго они хранятся, также ограничивают сферу личных и конфиденциальных данных, к которым третья сторона может получить доступ.

[100] Business and Social Responsibility, “Applying the Guiding Principles on Business and Human Rights to the ICT industry”, Version 2.0: Ten lessons learned, A briefing paper (September 2012), p. 9.

[101] ARTICLE 19, “Our 5G future: Light at the end of the tunnel or Internet fast-lane for the elite?” (15 September 2016).

[102] Electronic Frontier Foundation, “User privacy for ISPs and accidental ISPs”.

3. Взаимодействие заинтересованных сторон

61. Взаимодействие с правительствами, корпоративными партнерами и другими заинтересованными сторонами в вопросах прав человека в итоге может предотвращать или смягчать нарушения прав человека. Компаниям, которые непосредственно ведут дела с правительствами, следует в лицензионных соглашениях и договорах купли-продажи добиваться правозащитных гарантий, таких как заверения в том, что без ведома компании не будут совершаться подключения к сетевому оборудованию и оно не будет подвергаться модификации (что может происходить для облегчения нарушений прав человека). Правовой защите свободы выражения мнений и неприкосновенности частной жизни также могут способствовать своевременное вмешательство в ходе судебных разбирательств (например, приобщение консультативных заключений к материалам по делам, возбужденным группами гражданского общества или партнерскими компаниями в отношении законов о цензуре или наблюдении) и правозащитное лоббирование в законодательных и политических процессах.

62. Достигнутые договоренности с корпоративными партнерами должны позволить всем сторонам выполнять свои правозащитные обязанности. В частности, такие договоренности должны быть направлены на обеспечение того, чтобы филиалы, партнеры по совместным предприятиям, поставщики и дистрибьюторы твердо придерживались той политики в отношении свободы выражения мнений и неприкосновенности частной жизни, которую проводит компания. Например, в тех случаях, когда на местах получают нестандартные запросы, касающиеся цензуры или наблюдения, политика компании должна обеспечивать, чтобы эти запросы рассматривались на уровне глобального управления компанией. Механизмы информирования о нарушениях должны быть доступны как для сотрудников, так и для подрядчиков[103]. С учетом того, что компании уже работают в сфере, связанной с правозащитной проблематикой, они должны стремиться к созданию со временем механизма, направленного на предотвращение или уменьшение ущерба[104].

63. Компании также могут способствовать соблюдению прав человека на основе совместных действий. Такое сотрудничество включает в себя совместные усилия и правозащитную деятельность с партнерскими компаниями; взаимодействие с региональными и международными органами, включая правозащитные механизмы и экономические учреждения; и членство в отраслевых ассоциациях и участие в многосторонних инициативах[105]. Мобилизации общественной поддержки усилий компании по противодействию произволу правительства может также способствовать проведение регулярных консультаций с пользователями, гражданским обществом и затрагиваемыми правообладателями. Межсекторальное сотрудничество способствует укреплению нормативного значения передовой практики и стандартов в области прав человека и усиливает давление на правительства и партнерские компании, побуждая к их соблюдению.

4. Стратегии смягчения последствий[106]

64. С учетом того, что компании занимаются регулированием контента и запросами на данные пользователей, могут быть приняты конкретные стратегии и

[103] Материал, представленный организацией «Telecommunications Industry Dialogue», pp. 13 and 16.

[104] SHIFT, “Using leverage in business relationships to reduce human rights risks” (New York, November 2013).

[105] Материал, представленный организацией «Telecommunications Industry Dialogue», p. 12; а также материалы, представленные организацией «Global Network Initiative», p. 7.

[106] В рекомендациях, представленных в настоящем разделе, в значительной мере использованы материалы, представленные организацией «Telecommunications Industry Dialogue», и «Руководство по осуществлению принципов свободы выражения мнений и неприкосновенности частной жизни» Глобальной сетевой инициативы.

практические меры в целях смягчения негативного воздействия ограничений, налагаемых правительством.

Обеспечение строгого соответствия закону запросов на ограничение контента и предоставление данных клиентов

65. Компаниям следует обеспечивать, чтобы все запросы на ограничение контента и предоставление данных клиентов соответствовали не только процедурным и правовым требованиям, конкретно указанным в местном законодательстве, но и международно признанным стандартам надлежащей правовой процедуры[107]. Учитывая вмешательство в права человека, такие запросы должны быть санкционированы независимым и беспристрастным судом или судебным органом. Кроме того, компаниям следует требовать, чтобы запросы направлялись в письменном виде и содержали четкое разъяснение законных оснований, а также имя, должность и подпись санкционирующего должностного лица. Компаниям также следует стремиться убедиться в том, что соответствующее должностное лицо или государственный орган уполномочены подавать этот запрос[108]. Следует добиваться соблюдения этих формальных требований, даже если это конкретно не предусмотрено законом. Кроме того, компаниям следует сохранять в письменном виде все записи о сообщениях между ними и запрашивающей инстанцией по каждому запросу и регистрационные записи доступа к данным пользователей при выполнении запроса, при условии, что такие записи не создают неоправданных рисков для неприкосновенности частной жизни[109].

Трактовка сферы охвата запросов правительства и законов

66. Расплывчатый и открытый характер запросов правительств и правовых рамок создает для компаний трудности при определении того, соответствуют ли они местному законодательству. Компании могут, однако, сгладить эту неопределенность приняв общесистемную политику, которой руководствовались бы все их оперативные подразделения, в том числе местные филиалы, и согласно которой любая правовая двусмысленность разрешалась бы в пользу соблюдения свободы выражения мнений, неприкосновенности частной жизни и других прав человека. В основу такой политики положены не только правозащитные обязанности поставщика, но и обязательство государства выполнять применимые законы о правах человека и обеспечивать соответствующие средства защиты прав в соответствии с местным законодательством (например, конституционные, уголовные процедуры и законы о защите данных).

67. На практике компании должны в максимальной степени трактовать запросы таким образом, чтобы обеспечить наименьшее ограничение контента и наименьший доступ к данным клиентов. Например, в тех случаях, когда запрос представляется чрезмерным, Глобальная сетевая инициатива рекомендует компаниям добиваться разъяснений относительно сферы его применения и требовать внесения соответствующих изменений[110].

Оспаривание запросов и базовых законов

68. Компании заинтересованы в том, чтобы действовать в правовых условиях, отвечающих правозащитным требованиям и обеспечивающих надлежащее

[107] См., например, Манильские принципы, касающиеся ответственности посредников, и Международные принципы применения прав человека в отношении мониторинга средств связи, соавторами которых стали несколько неправительственных организаций.

[108] Глобальная сетевая инициатива, «Implementation guidelines», pp. 5-6; а также материалы, представленные организацией «Telecommunications Industry Dialogue», pp. 8-10.

[109] Материал, представленный организацией «Telecommunications Industry Dialogue», pp. 8-9.

[110] Ibid.

соблюдение процессуальных норм и верховенство права. Компаниям следует использовать все правовые возможности для оспаривания чрезмерно интрузивных запросов, таких как требования об отключении целого ряда услуг или платформ, об удалении веб-сайтов, выбранных явно за критику или несогласие, или о предоставлении данных клиентов в широком смысле без указания конкретных пользователей[111].

69. Как и при принятии любого решения о начале судебного разбирательства, компании могут учитывать целый ряд соображений, таких как «возможные благоприятные последствия [для прав человека], вероятность успеха, серьезность дела, стоимость, репрезентативность дела и может ли данное дело быть частью более широкого направления»[112]. Тем не менее в процессе принятия решений компаниям следует уделять существенное внимание правозащитным соображениям и тщательно оценивать потенциальные выгоды и риски для прав человека. Например, компании должны быть готовы оспаривать чрезмерные запросы в тех случаях, когда существует разумная вероятность успеха, даже если для решения этих задач могут потребоваться значительные ресурсы; с другой стороны, компании могут использовать альтернативные варианты, если есть вероятность того, что проблема приведет к созданию нежелательного прецедента или вызовет негативную реакцию и отрицательно скажется на выражении мнений и неприкосновенности частной жизни.

5. Транспарентность

70. Транспарентность является одним из ключевых элементов, который должна обеспечивать индустрия услуг цифрового доступа. Информация о тех видах деятельности правительства, для которых требуется помощь или участие корпораций, должна раскрываться в максимальной степени, разрешенной законом. Компаниям следует иметь в виду, что такая информация используется главным образом гражданским обществом для обжалования в суде нарушений прав человека, регистрации жалоб от имени пользователей в национальных или международных механизмах или поиска альтернативных способов обеспечения подотчетности. Соответственно, раскрытие такой информации должно носить регулярный и постоянный характер и осуществляться в доступном формате, который обеспечивает надлежащий контекст.

71. Даже если местное законодательство не допускает полной транспарентности, компании должны, тем не менее, раскрывать всю соответствующую информацию, которая может быть опубликована. Например, если компаниям запрещено сообщать, откуда и на каком основании выдан запрос об отключении, они, тем не менее, должны стремиться на регулярной основе представлять обновленную информацию об услугах, которые были затронуты или восстановлены, и о мерах, которые они принимают для решения этого вопроса, и давать разъяснения после случившегося. Новаторские меры транспарентности, такие как публикация сводных данных и выборочный отказ в предоставлении информации[113], также смягчают последствия постановлений о запрещении раскрытия информации и других законов о неразглашении. Компаниям следует открыто указывать все местные законы, в соответствии с которыми они действуют, и, когда это возможно, оспаривать любой закон или постановление, которые не дают им возможности или препятствуют им быть транспарентными для пользователей и широкой общественности[114].

---

[111] Yael Ronen, “Big Brother’s little helpers” (February 2015), p. 81.

[112] Глобальная сетевая инициатива, «Implementation guidelines».

[113] Например, когда ««Telia Company» получила запрос о приостановке обслуживания, компания не заявила, что это случилось в результате технических проблем», материал, представленный организацией «Telecommunications Industry Dialogue», p. 14.

[114] Telecommunications Industry Dialogue, “Information on country legal frameworks pertaining to freedom of expression and privacy in telecommunications” (2016).

72. Компаниям следует раскрывать свою политику и действия, имеющие последствия для свободы выражения мнений. Соответствующее раскрытие информации включает сведения о хранении данных и принципах их использования, практике управления сетью и купле-продаже сетевых технологий фильтрации и перехвата[115]. Компаниям следует также раскрывать информацию о периодичности проведения, сфере охвата и тематике процессов обеспечения должной осмотрительности и резюме выводов, сделанных на высоком уровне. В целом компаниям следует консультироваться с растущим числом источников, которые изучают ценные показатели транспарентности и другие передовые методы обеспечения транспарентности. В консультациях по вопросам разработки и осуществления мер транспарентности также должны участвовать пользователи, гражданское общество и компании-партнеры.

6. Эффективные средства правовой защиты

73. Хотя в последние годы и наблюдается развитие определенных аспектов корпоративной ответственности, часто возникает впечатление, что меры по устранению допущенных нарушений исключены из повестки дня частного сектора. Между тем средства правовой защиты являются ключевым элементом корпоративной ответственности и должны обеспечиваться в тех случаях, когда предприятия «оказали неблагоприятное воздействие или способствовали ему» (см. A/HRC/17/31, приложение, принцип 22). Основная обязанность по устранению связанных с предпринимательской деятельностью нарушений прав человека, особенно совершаемых по инициативе государств, таких как чрезмерное ограничение контента, незаконные запросы о доступе к данным пользователей и несоразмерное наблюдение, лежит на самих государствах. Вместе с тем компании, которые не принимают соответствующих мер по обеспечению должной осмотрительности и не применяют других гарантий, могут также вызывать такие нарушения или способствовать им. В этих ситуациях компании должны «в рамках законных процессов возмещать причиненный ущерб или сотрудничать с целью его возмещения» (там же).

74. Средства правовой защиты могут включать в себя как финансовые, так и нефинансовые средства (там же, принцип 27). В тех случаях, когда ограничивается свобода выражения мнений, надлежащие средства правовой защиты могут включать в себя доступ к механизмам подачи и рассмотрения жалоб и информации о нарушении и гарантии неповторения[116]. Пользователи, счета которых были необоснованно заблокированы, возможно, пожелают удовлетвориться тем, что их выслушают и предоставят им разъяснения и гарантии неповторения[117].

75. Уже существующие стратегии и механизмы также можно реформировать и укрепить в целях пресечения нарушений свободы выражения мнений. Например, поставщик может улучшить свою политику ограничения контента и подготовку групп регулирования контента, с тем чтобы уменьшить вероятность несправедливого удаления веб-сайта или таких чрезмерных ограничений контента, как фильтрация. Также можно было бы обновить механизмы рассмотрения жалоб потребителей, с тем чтобы дать пользователям возможность обозначить те виды практического управления сетевым трафиком, классификации коммерческой фильтрации и другие ограничения контента, которые они считают чрезмерными или несправедливыми.

[115] Ranking Digital Rights submission.

[116] Материал, представленный организацией «Telecommunications Industry Dialogue», p. 17.

[117] Peter Micek and Jeff Landale, “Forgotten pillar: the Telco remedy plan”, Access Now (May 2013), p. 6.

V. Выводы и рекомендации

76. **Физические лица зависят от цифрового доступа для осуществления основных прав, включая право на свободу мнений и их свободное выражение, право на жизнь и целый ряд экономических, социальных и культурных прав. Они также регулярно сталкиваются с препятствиями в доступе: от отключений сетей до наблюдения. В настоящем докладе в основном рассматриваются препятствия, которые приводят к лишению, сдерживанию или исключению возможности выражения мнения в результате применения сетевой цензуры. В настоящем докладе не рассматриваются другие серьезные препятствия, такие как отсутствие надлежащей инфраструктуры подключения к Интернету, введенная правительством высокая стоимость доступа, гендерное неравенство и языковые барьеры, которые также могут представлять собой определенные формы цензуры[118]. Поэтому основное внимание уделяется роли и обязанностям государств. Однако государства все чаще применяют цензуру, используя частный сектор. Цель доклада состоит в том, чтобы обратить внимание не только на необходимость ограничения действий государства в соответствии с правом прав человека, но и на принципы, которые частные субъекты должны соблюдать при уважении прав человека. Ниже изложены основные рекомендации, уже отмеченные в ходе анализа выше.**

Государства и Совет по правам человека

77. **Совет по правам человека в своей резолюции 32/13 недвусмысленно осудил меры по умышленному недопущению или нарушению доступа к информации или ее распространения в режиме онлайн в нарушение норм международного права прав человека и призвал все государства воздерживаться от таких мер и прекратить их использование. Это осуждение, которое имеет исключительно важное значение для поощрения Советом прав человека в режиме онлайн, следует дополнить и уточнить. Умышленное недопущение или нарушение доступа включает в себя любые действия, которые приводят к отключению доступа к телекоммуникационным сетям, услугам мобильной связи, платформам социальных сетей и т.д., либо делают доступ неэффективным. В будущем работа Совета по разъяснению правил, которые применяются к цифровому доступу, как указано в настоящем докладе, будет направлена на продвижение права на свободу мнений и их свободное выражение в режиме онлайн.**

78. **Также крайне важно, чтобы Совет и государства обращали внимание на связь между вмешательством в частную жизнь и свободой выражения мнений. Разумеется, вмешательство в частную жизнь должно оцениваться исходя из конкретных обстоятельств в соответствии со статьей 17 Международного пакта о гражданских и политических правах и другими нормами в области прав человека. Однако некоторые виды вмешательства – например, чрезмерные запросы о предоставлении данных о пользователях и хранение таких данных третьей стороной – могут оказывать сдерживающее воздействие на выражение мнений как в краткосрочной, так и в долгосрочной перспективе, и этого следует избегать как с правовой, так и с политической точек зрения. Как минимум, государствам следует обеспечивать, чтобы наблюдение было санкционировано независимым, беспристрастным и компетентным судебным органом, удостоверяющим, что запрос необходим и соразмерен законной цели защиты.**

[118] Материал, представленный Глобальной комиссией по вопросам управления Интернетом; Arco Iris Libre de Cuba, Centro de Información Hablemos Press, Centro de Información Legal CubaLex, Mesa de Diálogo de la Juventud Cubana Plataforma Femenina Nuevo País, “Situación del derecho a la libertad de opinion y expression en Cuba” (Situation of the right to freedom of opinion and expression in Cuba) (July 2016), p. 20.

79. **Специальный докладчик выражает особую обеспокоенность по поводу сообщений об угрозах и запугивании, направленных против компаний, их сотрудников, а также их оборудования и инфраструктуры. Кроме того, заслуживает рассмотрения то особое внимание, которое Совет уделяет важной роли – и необходимости защиты – частного сектора. Государствам следует провести обзор всех мероприятий по получению сетевого доступа, с тем чтобы убедиться, что они являются законными, необходимыми и соразмерными, обращая особое внимание на то, являются ли эти мероприятия наименее интрузивными средствами для достижения законной цели.**

80. **Защитная роль, которую государства могут осуществлять в отношении частного сектора, может распространяться лишь до определенных пределов. Им не следует поощрять достижение экономической выгоды частными юридическими лицами в ущерб праву пользователей на свободу мнений и их свободное выражение. Таким образом, государства должны запретить попытки приоритизации определенных видов интернет-контента или приложений, по сравнению с другими, за плату или в обмен на иные коммерческие выгоды.**

81. **Пересечение поведения государств с корпоративными функциями в эпоху цифровых технологий по-прежнему является новым явлением для многих государств. Одним из многообещающих направлений как на международном, так и на национальном уровнях могла бы быть разработка национальных планов действий по вопросам предпринимательской деятельности и прав человека с целью создания реальных возможностей для всех категорий индустрии цифрового доступа выявлять и устранять последствия их воздействия на права человека.**

Частные субъекты

82. **На протяжении уже многих лет отдельные лица и компании в секторе цифрового доступа осознают, что играют важную роль в процессе значительного расширения доступа к информационно-коммуникационным услугам. Они работают в той сфере бизнеса, где модель успеха должна заключаться в расширении доступа, повышении эффективности, разнообразия и транспарентности. Они должны отнестись к принципам, определенным в настоящем докладе, как к инструментам для укрепления собственной роли в продвижении прав пользователей на свободу выражения мнений. В связи с этим в дополнение к подтвержденной на высоком политическом уровне приверженности правам человека отрасли следует выделять надлежащие ресурсы для выполнения этих обязательств, включая обеспечение должной осмотрительности, принятие ориентированных на соблюдение прав проектных и инженерных решений, вовлечение заинтересованных сторон, стратегии предотвращения или смягчения рисков для прав человека, транспарентность и эффективные средства правовой защиты. При этом в ходе разработки и осуществления мер по обеспечению подотчетности корпораций в области прав человека следует опираться на опыт как внутренних, так и внешних экспертов и обеспечивать конструктивный вклад со стороны клиентов и других затрагиваемых правообладателей, гражданского общества и правозащитных организаций.**

83. **Это не означает, что частные компании не подвергаются давлению. Они ему подвергаются. Однако в тех случаях, когда государства требуют участия корпораций в применении цензуры или наблюдения, компании должны в максимально возможной и допускаемой законом степени стремиться к предотвращению или смягчению негативных последствий их участия для прав человека. В любом случае компании должны принимать все необходимые и законные меры к тому, чтобы не вызывать нарушения прав человека, не становиться их соучастниками и не способствовать им. Договоренности, достигнутые с корпоративными партнерами, должны быть выстроены так, чтобы обеспечить всем сторонам возможность вы-**

полнять свои правозащитные обязанности. Компаниям также следует стремиться к укреплению уже существующих деловых отношений в целях предотвращения или смягчения негативных последствий для прав человека.