

**Совет по правам человека**

Тридцать вторая сессия

Пункт 3 повестки дня

**Поощрение и защита всех прав человека,  
гражданских, политических, экономических,  
социальных и культурных прав,  
включая право на развитие****Доклад Специального докладчика по вопросу  
о поощрении и защите права на свободу мнений  
и их свободное выражение\*****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 в соответствии с резолюцией 25/2 Совета. Настоящий доклад является первым в серии исследований, посвященных вопросам взаимодействия государственного регулирования, частного сектора и свободы выражения мнений в эпоху цифровых технологий. В нем Специальный докладчик анализирует правовую базу, имеющую отношение к свободе выражения мнений, и принципы, применимые к частному сектору, определяет ключевых участников сектора информационно-коммуникационных технологий, так или иначе причастных к свободе выражения мнений, и предлагает вниманию правовые и политические аспекты, изучением которых он будет заниматься во время выполнения своего мандата.

\* Настоящий доклад был представлен позже установленного срока, с тем чтобы отразить самые последние события.

GE.16-07644 (R) 090616 100616



\* 1 6 0 7 6 4 4 \*

Просьба отправить на вторичную переработку



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

### Содержание

	<i>Стр.</i>
I. Введение .....	3
II. Свобода выражения мнений, государства и частный сектор в эпоху цифровых технологий.....	4
A. Международно-правовая основа .....	5
B. Рамки ответственности частного сектора.....	6
III. Функции частного сектора и государственное/частное регулирование .....	8
A. Влияние частных предприятий на свободу выражения мнений .....	8
B. Регулирование в эпоху цифровых технологий .....	10
IV. Правовые и политические вопросы .....	13
A. Регулирование контента.....	13
B. Слежение и цифровая безопасность .....	20
C. Транспарентность.....	22
D. Средства правовой защиты .....	24
V. Дальнейшая проработка тематики .....	25
VI. Выводы и рекомендации.....	27

## I. Введение

1. Роль частного сектора в эпоху цифровых технологий представляется повсеместной и неуклонно растущей, ибо он является локомотивом наиболее мощного за всю историю расширения доступа к информации. Колоссальные форумы в социальных сетях для публичного выражения мнений принадлежат частным компаниям. Крупнейшие платформы, агрегирующие и индексирующие глобальные знания, а также определяющие алгоритмы, которые оказывают воздействие на отображение информации в онлайн-режиме, представляют собой результат усилий частного сектора. Инфраструктура технологии мобильной связи, посредством которой миллиарды людей общаются друг с другом и получают доступ в Интернет, зависит от частных инвестиций, частного обслуживания и частной собственности. Инструменты для правоприменения и информационной поддержки часто создаются на базе продуктов частных предприятий по обеспечению наблюдения и обработки данных. Частные компании разрабатывают, производят и часто обслуживают устройства и сервисы, на которых хранятся наиболее важные персональные данные: от финансовой и медицинской информации до сообщений по электронной почте, текстовых посланий, истории поиска, фотографий и видеороликов.

2. Свобода мнений и их свободное выражение в современном мире в значительной мере обеспечиваются благодаря частной индустрии, которая обладает огромным влиянием над цифровым пространством, открывая доступ к информации и являясь посредником для выражения мнений. В эпоху цифрового пространства невозможно обойти такие важные вопросы, как применимое законодательство и рамки частных полномочий и государственного регулирования. Должны ли эти частные субъекты выполнять те же обязанности, что и государственные органы? Должны ли такие обязанности определяться нормами права прав человека, условиями предоставления услуг, договорными соглашениями или чем-либо иным? Каким образом должны выстраиваться отношения между корпоративными субъектами и государствами? Если в связи с осуществлением своей предпринимательской деятельности частные субъекты подвергаются давлению, нарушающему свободу выражения мнений, какие меры они должны принимать? Отказаться от выхода на рынок или покинуть рынок? Уведомить своих клиентов о таком давлении? По мере того, как мир все глубже погружается в цифровое пространство, а «Интернет вещей» становится вопросом ближайшего будущего, важнейшее значение приобретает руководство, обеспечивающее поощрение и защиту прав, а также пользование ими.

3. Настоящий доклад преследует несколько целей<sup>1</sup>. Во-первых, в нем принята попытка определить категории частных субъектов, оказывающих глубокое влияние на свободу выражения мнений в эпоху цифровых технологий. Во-вторых, в нем определяются вопросы, касающиеся как защиты свободы мнений и их свободного выражения со стороны частного сектора, так и обязанностей государственного сектора по обеспечению защиты пространства для выражения мнений. В-третьих, в нем очерчен ряд областей, в которых нормативное руководство представляется наиболее необходимым. Эти области будут рассмотрены и систематизированы посредством подготовки тематических докладов, посещений стран и компаний, а также контактов и консультаций с пра-

<sup>1</sup> Специальный докладчик хотел бы поблагодарить своего консультанта по правовым вопросам Амоса Тоха и его студентов с Ирвинского юридического факультета Калифорнийского университета за оказанное содействие в подготовке настоящего доклада.

вительствами, ценовым сектором и гражданским обществом. Иными словами, настоящий доклад является первым из целого ряда докладов, которые будут представлены Специальным докладчиком в целях обеспечения руководящих ориентиров в вопросе о том, каким образом частным субъектам следует защищать и поощрять свободу выражения мнений в эпоху цифровых технологий.

4. Подготовке настоящего доклада способствовал открытый процесс представления материалов и проведения консультаций. 3 декабря 2015 года Специальный докладчик обратился с призывом представить материалы для доклада. На дату опубликования доклада Специальный докладчик получил 15 представлений от государств<sup>2</sup> и 15 представлений от организаций<sup>3</sup>; со всеми этими материалами можно ознакомиться на веб-сайте Специального докладчика<sup>4</sup>. Большую пользу Специальный докладчик извлек также из консультаций. 25 и 26 января 2016 года он провел встречу с 25 представителями гражданского общества на Ирвинском юридическом факультете Калифорнийского университета, а 29 февраля 2016 года – еще одну встречу с 20 представителями частного сектора и гражданского общества в Управлении Верховного комиссара Организации Объединенных Наций по правам человека в Женеве. С краткими отчетами об этих встречах также можно ознакомиться на веб-сайте Специального докладчика.

## II. Свобода выражения мнений, государства и частный сектор в эпоху цифровых технологий

5. Настоящий вводный доклад посвящен одному из основополагающих вопросов: в какой мере сектор информационно-коммуникационных технологий должен нести ответственность за поощрение и защиту свободы мнений и их свободного выражения? Для ответа на этот вопрос необходимо начать с краткого изложения норм международного права прав человека, в соответствии с которыми государства обязуются поощрять и защищать свободу выражения мнений, а также с принципов, регулирующих обязанности частного сектора в области прав человека.

<sup>2</sup> Армения, Греция, Иордания, Кувейт, Маврикий, Мексика, Нидерланды, Перу, Республика Молдова, Румыния, Сальвадор, Словакия, Соединенные Штаты Америки, Турция и Эстония.

<sup>3</sup> Организация «Статья 19»; Ассоциация за прогрессивные коммуникации; Центр по вопросам демократии и технологий; Центр по вопросам технологий и общества; Центр по вопросам коммуникационного управления Национального университета права, Нью-Дели; Датский институт по правам человека; организация «Цифровые права»; европейская организация «Цифровые права»; Рабочая группа по вопросам защиты персональных данных и транспарентности в сетевом пространстве Коалиции «Фридом онлайн»; Глобальная сетевая инициатива; Институт по исследованиям в области прав человека и предпринимательской деятельности; Международный центр некоммерческого права; Общество Интернета; Корейская прогрессивная сеть «Jinbonet»; организация «Прайваси интернэшнл»; организация «Классификация цифровых прав»; и «Новая Америка».

<sup>4</sup> Размещены по адресу <http://www.ohchr.org/EN/Issues/FreedomOpinion/Pages/Annual.aspx>.

## A. Международно-правовая основа

6. Как статья 19 Международного пакта о гражданских и политических правах, так и статья 19 Всеобщей декларации прав человека защищают право каждого человека беспрепятственно придерживаться своих мнений, а также искать, получать и распространять всякого рода информацию и идеи, независимо от государственных границ и любыми средствами. Широкое распространение получило мнение о том, что люди пользуются теми же правами как в виртуальном пространстве, так и в реальной жизни. Предыдущий мандатарий высветил проблему растущего числа и множественных форм ограничений права на информацию в Интернете (см. A/HRC/17/27) и продемонстрировал воздействие расширения слежения в цифровом пространстве на свободу выражения мнений (см. A/HRC/23/40). В 2015 году Специальный докладчик особо отметил важную роль использования средств шифрования и анонимности для защиты и укрепления свободы выражения мнений (см. A/HRC/29/32). В совместных заявлениях Специальный докладчик и региональные партнеры уделяли особое внимание вопросам ответственности посредников, доступа, ограничений контента и другим ключевым темам, касающимся свободы выражения мнений в онлайн-режиме.

7. Пункт 3 статьи 19 Международного пакта о гражданских и политических правах допускает ограничения свободы выражения мнений (однако не затрагивает свободу мнений, предусмотренную в пункте 1 статьи 19). Согласно пункту 3 статьи 19, любое ограничение, для того чтобы быть легитимным, должно быть установлено законом и являться необходимым для уважения прав и репутации других лиц или для охраны государственной безопасности, общественного порядка, здоровья или нравственности населения. Любое ограничение должно быть достаточно конкретным и доступным для общественности, для того чтобы ограничивать дискреционные полномочия властей и предоставлять людям надлежащие ориентиры (см. замечание общего порядка № 34 (2011) Комитета по правам человека по статье 19: свобода мнений и их выражения). Для того чтобы ограничение являлось необходимым, оно должно быть не просто полезным, разумным или желательным<sup>5</sup>. Признается также, что необходимость нуждается в оценке соразмерности (см. A/HRC/29/32). Для соблюдения принципа соразмерности следует показать, что ограничительные меры являются наименее интрузивными из числа тех, с помощью которых может быть достигнут желаемый результат, и они должны являться соразмерными защищаемому интересу (см. Замечание общего порядка № 34). Если ограничения не соответствуют стандарту пункта 3 статьи 19, лица пользуются правом на эффективное средство правовой защиты согласно пункту 3 статьи 2 Пакта.

8. В онлайн-режиме все лица также пользуются полной совокупностью других прав, связанных, например, с неприкосновенностью частной жизни, религиозными убеждениями, ассоциацией и мирными собраниями, образованием, культурой и свободой от дискриминации. На государства возлагаются как негативное обязательство воздерживаться от нарушения прав, так и позитивное обязательство обеспечивать пользование этими правами. Такие позитивные обязательства могут потребовать от государственных органов принятия мер по защите отдельных лиц от действий частных сторон<sup>6</sup>.

<sup>5</sup> European Court of Human Rights, Application No. 6538/74, *The Sunday Times v. The United Kingdom* (26 April 1979), para. 59.

<sup>6</sup> См. замечание общего порядка № 31 (2004) о характере общего юридического обязательства, налагаемого на государства – участники Международного пакта

## **В. Рамки ответственности частного сектора**

9. В целом право прав человека непосредственно не регулируют деятельность и ответственность частного сектора. Существуют различные инициативы, которые обеспечивают руководство для предприятий в сфере соблюдения основных прав. Совет по правам человека одобрил Руководящие принципы предпринимательской деятельности в аспекте прав человека: осуществление рамок Организации Объединенных Наций, касающихся «защиты, соблюдения и средств правовой защиты» (см. A/HRC/17/4 и A/HRC/17/31). Опираясь на существующие нормы права прав человека, Руководящие принципы подтверждают, что государства должны обеспечивать, чтобы не только государственные органы, но и предприятия, находящиеся под их юрисдикцией, соблюдали права человека<sup>7</sup>.

10. Руководящие принципы обеспечивают рамки для определения ответственности частного предпринимательства в секторе информационно-коммуникационных технологий по всему миру независимо от обязательств государства или соблюдения этих обязательств. Так, Руководящие принципы обосновывают глобальную обязанность предприятий избегать оказания или содействия оказанию неблагоприятного воздействия на права человека в рамках своей деятельности и устранять последствия такого воздействия в случае, когда оно имело место, а также стремиться предотвращать или смягчать неблагоприятное воздействие на права человека, которое непосредственно связано с их деятельностью, продукцией или услугами вследствие их деловых отношений, даже если они непосредственно не способствовали оказанию такого воздействия<sup>8</sup>.

11. Согласно Руководящим принципам, должная забота позволяет предприятиям обеспечивать выявление, предотвращение, смягчение последствий и представлять отчетность о том, как они устраняют свое неблагоприятное воздействие на права человека<sup>9</sup>. В цифровой среде последствия для прав человека могут возникнуть в связи с принятием внутренних решений о том, как реагировать на требование правительства ограничить содержание материалов или доступ к информации о клиентах, установить условия предоставления услуг, разработать конструктивные и технические решения, влияющие на безопасность и неприкосновенность частной жизни, а также решения о предоставлении или прекращении оказания услуг на конкретном рынке.

12. В отношении прозрачности Руководящие принципы предусматривают, что предприятия должны быть готовы распространять за пределами предприятия информацию о том, как они устраняют свое воздействие на права человека, особенно в тех случаях, когда озабоченности высказываются затрагиваемыми сторонами или от их имени<sup>10</sup>. Верховный комиссар Организации Объединенных Наций по правам человека также настоятельно призвал компании, работающие в области информационно-коммуникационных технологий, проводить транспортное обсуждение с пользователями рисков и требований прави-

---

о гражданских и политических правах. К деятельности частных субъектов могут иметь прямое отношение другие нормы международного права, такие как уголовная ответственность за преступления против человечности, военные преступления и акты геноцида в соответствии с международным гуманитарным правом.

<sup>7</sup> Руководящие принципы предпринимательской деятельности в аспекте прав человека, глава I (A) (1).

<sup>8</sup> Там же, глава II (A) (11)–(13).

<sup>9</sup> Там же, глава II (A) (17).

<sup>10</sup> Там же, глава II (B) (21).

тельства (см. A/HRC/27/37). Конструктивное раскрытие информации проливает свет, в числе прочего, на объем и контекст запросов правительства, касающихся удаления контента и данных клиента, процессы обработки таких запросов и толкование соответствующих законов, политики и нормативных положений. Корпоративные обязательства по обеспечению прозрачности могут также включать в себя обязанность раскрывать информацию о процессах и сообщениях, касающихся выполнения условий предоставления услуг, а также о частных запросах, касающихся регулирования контента и пользовательских данных.

13. И наконец, ответственность за соблюдение предусматривает необходимость уделять внимание наличию средств правовой защиты – от возмещения морального вреда до компенсации и гарантий неповторения – в тех случаях, когда частный субъект оказал неблагоприятное воздействие или способствовал ему<sup>11</sup>.

14. Руководящие принципы являются полезной отправной точкой для определения ответственности частного сектора в сфере информационно-коммуникационных технологий, однако в рамках ряда других проектов также предлагаются определенные принципы для данного сектора. В разработанных Глобальной сетевой инициативой Принципах свободы выражения мнений и неприкосновенности частной жизни учтены опыт и экспертные знания инвесторов, гражданского общества и академических кругов. Европейская комиссия опубликовала *Руководство для сектора ИКТ по вопросу о применении утвержденных Организацией Объединенных Наций принципов предпринимательской деятельности в аспекте прав человека*. В число соответствующих инициатив гражданского общества входят Манильские принципы ответственности посредников, устанавливающие базовую защиту посредников в соответствии со стандартами свободы выражения мнений; Африканская декларация прав и свобод в Интернете, поощряющая соблюдение на континенте стандартов прав человека и принципов открытости при разработке и осуществлении политики в отношении Интернета; и разработанный в рамках проекта «Классификация цифровых прав» Индекс корпоративной подотчетности оценивающий совокупность основных частных субъектов в цифровом пространстве на основе их приверженности нормам свободы выражения мнений и неприкосновенности частной жизни. Гражданское общество также действует в качестве сдерживающей и уравновешивающей силы в отношении других субъектов, участвующих в управлении Интернетом: так, например, Кодекс надлежащей практики в области информации, участия и прозрачности в руководстве функционированием Интернета призван обеспечивать эффективное информирование общественности о соответствующих процессах, устанавливает подотчетность всем заинтересованным сторонам и подчеркивает необходимость демократического участия.

---

<sup>11</sup> Там же, глава II (B) (22).

### III. Функции частного сектора и государственное/частное регулирование

#### A. Влияние частных предприятий на свободу выражения мнений

15. Диапазон функций частного сектора в сферах организации, обеспечения доступа, насыщения и регулирования Интернета колоссален и зачастую охватывает пересекающиеся категории<sup>12</sup>.

##### 1. Обеспечение подсоединения к Интернету

16. Если интернет-провайдеры обеспечивают конкретное подключение своих абонентов к Интернету, то поставщики телекоммуникационных услуг предлагают более широкий набор услуг, включая доступ к радио, телевидению, телефонной и мобильной связи. Крупные транснациональные корпорации предлагают обе категории услуг не только в странах своего происхождения, но и по всему миру. Так, британский провайдер «Водафон» является владельцем и оператором сетей в 27 странах и имеет совместные с партнерами сети еще в более чем 50 странах. Базирующаяся в Финляндии и Швеции «ТелиаСонера» обслуживает рынки по всей Евразии, а «МТС Россия» предоставляет услуги внутри страны, а также обеспечивает телекоммуникационное обслуживание в Армении, Туркменистане и Узбекистане. Компании, подобные этим, зачастую имеют в собственности и обслуживают значительные элементы технической инфраструктуры, обеспечивающие сетевой и иной телекоммуникационный трафик, включая волоконно-оптические сети или линии спутниковой и беспроводной связи. Провайдеры интернет-услуг на местных и региональных рынках могут эксплуатировать ограниченное число таких сетей или арендовать сетевые мощности у владельцев крупных каналов передачи информации для того, чтобы обеспечить подсоединение своих абонентов к Интернету. Среди таких поставщиков услуг широкое распространение имеет государственная собственность: в Швейцарии, например, государству принадлежит 51% акций в «Свисском АГ»<sup>13</sup>, а в Уругвае государству принадлежит «Антел», один из ведущих телекоммуникационных провайдеров в стране<sup>14</sup>. Хотя в настоящее время доступ к Интернету предоставляют прежде всего провайдеры телекоммуникационных и интернет-услуг, растет число гибридных компаний, стремящихся предоставлять доступ к Интернету, а также другие связанные с Интернетом услуги<sup>15</sup>.

##### 2. Разработка и обслуживание аппаратных средств и операционных систем, облегчающих обработку информации и доступ к Интернету

17. Фирмы, выпускающие аппаратные средства, разрабатывают и изготавливают компьютерные устройства, которые предоставляют людям доступ к Интер-

<sup>12</sup> См., например, “Strategy panel: ICANN’s role in the Internet governance ecosystem” (23 February 2014); R. Mackinnon and others, *Fostering Freedom Online: The Role of Internet Intermediaries* (Paris, UNESCO, 2014); и D. A. Hope, *Protecting Human Rights in the Digital Age* (February 2011).

<sup>13</sup> См. [www.swisscom.ch/en/about/investors/shares/ownership-structure.html](http://www.swisscom.ch/en/about/investors/shares/ownership-structure.html).

<sup>14</sup> См. [www.antel.com.uy/antel/](http://www.antel.com.uy/antel/); <http://cs.stanford.edu/people/eroberts/cs181/projects/2006-07/latin-america/uruguayIntro.html>.

<sup>15</sup> «Гугл», например, будет, в числе прочего, предоставлять доступ к беспроводному обслуживанию через свой сервис «Гугл фибер» в дополнение к своим функциям поиска, хостинга контента и поддержки социальных сетей.

См. <https://fiber.google.com/about/>.

нету. Вместе с тем диапазон устройств, оснащенных функциями персонального компьютера, постоянно расширяется, и этот процесс неостановим, учитывая лавину цифровых связей, широко определяемых как «Интернет вещей», в котором цифровое подсоединение обеспечивается для всех аспектов современного существования. Автомобили, холодильники, телевизоры и часы – вот лишь некоторые из примеров «умных» устройств, которые в настоящее время объединяют в себе функции браузера, передающего устройства и другие связанные с Интернетом функции.

18. Кроме того, провайдеры телекоммуникационных и интернет-услуг приобретают оборудование и другие сетевые компоненты, составляющие физическую основу их сетей, у поставщиков инфраструктуры и производителей оборудования. Такие продукты имеют широкий диапазон: от простых маршрутизаторов и сетевых коммутаторов до устройств по углубленной проверке пакетов, сетевой фильтрации и устройств блокировки Интернета, а также центров мониторинга электронного слежения. Все чаще такие компании предусматривают также оказание услуг, консультирование, обучение и даже эксплуатационное управление.

### **3. Предоставление веб-доменов**

19. Предоставление и продажа адресов в Интернете (т.е. унифицированных указателей ресурсов (УУР)) осуществляются реестрами и регистраторами доменных имен под надзором некоммерческой структуры под названием «Корпорация по присвоению имен и номеров в Интернете» (ИКАНН). В настоящее время крупнейший в мире регистратор выполняет функции хостинга для более чем 61 млн. доменных имен.

### **4. Хостинг информации**

20. Услуги веб-хостинга позволяют пользователям загружать и отправлять файлы и другие материалы на браузеры своих читателей или клиентов. Обычно такие компании предоставляют также услуги хранения данных, электронной почты и другие услуги, ассоциируемые с веб-сайтами, которые приобретают их клиенты.

### **5. Содействие агрегированию, обмену и поиску информации**

21. Поисковые системы обеспечивают необходимую связь между пользователями, осуществляющими поиск информации, и теми, кто создает, агрегирует и публикует ее. На практике алгоритмы поисковых систем определяют то, что видит пользователь и в какой последовательности, и ими можно манипулировать в целях ограничения или установления порядка приоритетности контента. Однако возможности поиска информации не ограничиваются только поисковыми системами. Агрегаторы контента, специализированные поисковые сервисы, платформы социальных сетей и профессиональные сети также позволяют пользователям осуществлять поиск контента.

### **6. Предоставление и регулирование доступа к своему собственному контенту**

22. Компании, которые создают или покупают контент, размещаемый на их платформах, часто обладают авторским правом на такой контент, что позволяет им монетизировать и регулировать доступ к нему. В число наиболее влиятельных обладателей авторских прав входят медийные компании и компании индустрии развлечений, включая средства массовой информации, издательства, му-

зыкальные компании звукозаписи и студии художественных и телевизионных фильмов.

#### **7. Подсоединение пользователей и сообществ**

23. Компании предоставляют также комплекс услуг по подсоединению пользователей к множественным платформам, включая электронную почту, веб-чаты, дискуссионные форумы, социальные и профессиональные сети. В число наиболее видных субъектов в этой области входят провайдеры услуг электронной почты, социальные сети и другие сетевые платформы, а также веб-сайты с объявлениями. В дополнение к таким платформам возможности для обмена информацией и идеями посредством обзоров, комментариев и обсуждений предоставляют новостные веб-сайты, платформы электронной торговли и хранилища приложений. Возможности сетевого взаимодействия предусматривают также системы оплаты через Интернет.

#### **8. Продажа товаров и услуг и упрощение транзакций**

24. Электронная торговля упрощает продажу товаров и услуг и совершение других коммерческих транзакций между предприятиями и потребителями, предприятиями и другими предприятиями или потребителями и другими потребителями. Способы, используемые компаниями для предоставления доступа, продвижения или совершения таких транзакций и хранения значительного объема персональных данных, полученных в результате таких транзакций, могут оказывать воздействие на свободу выражения мнений и неприкосновенность частной жизни их клиентов.

#### **9. Сбор, переформатирование и продажа данных**

25. Подавляющее большинство описанных выше предприятий производит сбор информации от своих пользователей и о них, которая, в свою очередь, может использоваться для целенаправленной рекламы, адаптации предлагаемых услуг, снижения рисков с точки зрения безопасности или закрытия счетов недобросовестных пользователей. Вместе с тем компании могут также торговать услугами по сбору и анализу информации, предлагая такие услуги, как проектирование, адаптация или продажа технологий слежения и информационного анализа, либо предоставлять консалтинговые услуги, обеспечивающие правоприменение, сбор и анализ данных, кибербезопасность и операции по слежению.

### **В. Регулирование в эпоху цифровых технологий**

26. В Интернете существует обширная и разнообразная «экосистема» регулирования с участием различных субъектов на внутригосударственном, региональном и международном уровнях в частном и государственном секторах, в научных кругах и гражданском обществе. Определенные аспекты информационно-коммуникационных технологий – такие, как предоставление телекоммуникационных и сетевых услуг – уже давно привлекают к себе внимание на уровне государственного и международного регулирования, а также контроля со стороны общественности. Другие области, такие как поиск, социальные сети и продажа технологий слежения, также во все более значительной степени подвергаются такому контролю – сообразно их растущему воздействию и влиянию на осуществление свободы выражения мнений в Интернете.

## 1. Технические стандарты

27. Технические стандарты и процессы обеспечивают бесперебойную работу инфраструктуры, сетей и приложений, на основе которых функционируют Интернет и телекоммуникационные сети. Элементы физической инфраструктуры, обслуживающие потоки интернет-трафика, такие как сетевые кабели и спутники, устанавливаются и эксплуатируются в соответствии с различными техническими требованиями, которые обеспечивают их стабильное функционирование. Организации, разрабатывающие такие требования, включают в себя: Международный союз электросвязи, устанавливающий стандарты функциональной совместимости телекоммуникационных сетей; Институт инженеров по электротехнике и электронике, являющийся профессиональной ассоциацией, которая разрабатывает стандарты передачи информации по беспроводным сетям; и Ассоциация операторов сетей GSM, представляющая собой международную частную ассоциацию индустрии мобильной связи, которая разрабатывает стандарты для мобильных сетей.

28. Другая группа организаций устанавливает и разрабатывает технические стандарты передачи, хранения, размещения и представления данных в Интернете. Целевая группа по техническим аспектам организации Интернета разрабатывает и поддерживает протокол управления передачей/интернет-протокол, который определяет порядок соединения устройств в Интернете и обмена данными между ними. Консорциум Всемирной паутины устанавливает стандарты, касающиеся отображения веб-контента и взаимодействия с ним, что подразумевает урегулирование таких вопросов, как языковой контент и доступность для инвалидов. ИКАНН определяет политику регистрации доменных имен верхнего уровня, в том числе общих (таких, как .com, .org, .edu), страновых кодов (.cn, .tj, .sg) или используемых для обозначения конкретной отрасли или общества (таких, как .aero). Ее вспомогательное подразделение – Орган по присвоению номеров в Интернете – производит распределение адресов интернет-протокола, которые обозначают и отличают каждое подсоединенное к Интернету устройство уникальной цифровой отметкой.

29. Хотя технические стандарты имеют серьезные последствия для свободы выражения мнений, Комиссия Организации Объединенных Наций по науке и технике в целях развития отметила, что при разработке стандартов часто недостаточно учитываются озабоченности в области прав человека<sup>16</sup>. Разумеется, заинтересованные стороны и представители общественности допущены к участию в работе и к наблюдению за работой большинства из этих органов по установлению стандартов. Однако, поскольку для конструктивного участия, как правило, требуется высокий уровень технических знаний, правозащитная точка зрения не всегда учитывается в дискуссиях, даже несмотря на то, что технические и конструктивные решения могут оказать значительное воздействие на свободу выражения мнений<sup>17</sup>.

<sup>16</sup> См. Intersessional Panel of the Commission on Science and Technology for Development, “The mapping of international Internet public policy issues” (November 2014).

<sup>17</sup> Следует отметить, что несколько организаций выделили средства для учета аспектов прав человека в технических решениях. ИКАНН, например, создала объединяющую несколько сообществ рабочую группу по вопросу о своей корпоративной и социальной ответственности за соблюдение прав человека, которая стремится обозначить и представить проблемы и потенциальные решения в области корпоративной и социальной ответственности ИКАНН; взято из: <https://community.icann.org/display/gnsononcomstake/CCWP+on+ICANN's+Corporate+and+Social+Responsibility+to+Respect+Human+Rights>. Ряд неправительственных

## 2. Управление Интернетом и разработка соответствующей политики

30. Международно-правовые инструменты не содержат каких-либо прямых указаний о том, каким образом государствам и другим субъектам следует поддерживать свободный и открытый Интернет; при этом законодательное регулирование также не всегда является надлежащим подходом. Действительно, управление Интернетом не относится к исключительной компетенции специализированных органов или правительств. Совсем недавно на Всемирной встрече на высшем уровне по вопросам информационного общества подчеркивалась сохраняющаяся важность такого подхода к управлению, который предусматривал бы участие заинтересованных сторон от правительства, корпораций и гражданского общества, научных кругов и технических специалистов и учитывал бы их знания (см. резолюцию 70/125 Генеральной Ассамблеи). В контексте глобальной торговли принципы недискриминации, установленные в соответствии с международными соглашениями под эгидой Всемирной торговой организации, могут потребовать от государств ограничить или иным образом регулировать нейтральные услуги. Всемирная организация интеллектуальной собственности также сталкивалась с проблемой возросших запросов государств-членов на рекомендации по поводу законодательной базы, которая позволила бы им выполнять договорные обязательства в цифровой среде. Региональные органы, такие как Африканский союз, Европейская комиссия и Организация американских государств, стремятся гарантировать, чтобы глобальная политика в области Интернета разрабатывалась и осуществлялась с учетом законов, особенностей и озабоченностей их конкретных регионов<sup>18</sup>.

31. Ряд организаций, устанавливающих технические стандарты, наделены также функциями выработки политики. Глобальную политику в телекоммуникационной сфере, например, разрабатывает и координирует Международный союз электросвязи. ИКАНН принимает принципиальные решения о том, какие виды доменных имен верхнего уровня могут быть зарегистрированы и кто именно может притязать на владение ими, в рамках консультаций с правительствами, частным сектором, гражданским обществом и другими соответствующими субъектами.

32. На решение проблем управления Интернетом, которые недостаточно регулируются действующими законодательными положениями, направлены также отраслевые инициативы. Так, Система оповещения о нарушениях авторских прав объединяет профильные ассоциации киноиндустрии и индустрии звукозаписи, а также провайдеров интернет-услуг в целях разработки и применения единого подхода в области нарушений авторских прав в онлайн-режиме. Диалог телекоммуникационной отрасли привлекает к участию операторов и продавцов телекоммуникационных услуг для обсуждения вопросов, связанных со свободой выражения мнений и правом на неприкосновенность частной жизни в их секторе.

33. Хотя многие из этих инициатив реализуются частным сектором, порой они сотрудничают с государствами или получают от них поддержку. Например, Фонд по наблюдению за Интернетом Соединенного Королевства Великобрита-

---

организаций также поднимали тематику прав человека в ходе технических дискуссий. См., например, Neils ten Oever, "Research into human rights protocol considerations", размещено по адресу <https://datatracker.ietf.org/doc/draft-tenoever-hrpc-research/>.

<sup>18</sup> См., например, подготовленное Европейской комиссией *Руководство для сектора ИКТ* (пункт 14 выше); и Inter-American Commission on Human Rights, Office of the Special Rapporteur for Freedom of Expression, *Freedom of Expression and the Internet* (2013).

нии и Северной Ирландии, оказывающий провайдерам интернет-услуг и хостинговым платформам услуги, связанные с режимом «удаления после уведомления», предупреждающим их о наличии потенциально криминального контента в их сетях, предоставляет также правоохранительным органам «уникальные данные» в проводимых ими расследованиях в связи с таким контентом.

## IV. Правовые и политические вопросы

34. Множественные функции сектора информационно-коммуникационных технологий выдвигают на первый план правовые и политические вопросы, которые заслуживают внимания и изучения со стороны международных правозащитных механизмов.

### A. Регулирование контента

35. Многие вопросы, касающиеся частных субъектов в эпоху цифровых технологий, сопряжены с регулированием контента. Например, каким образом государства стимулируют или обеспечивают удаление контента, устанавливают цензуру или излишние или несоразмерные ограничения на право поиска, получения и распространения интернет-контента через частные компьютерные платформы и сети? Каким образом частные предприятия реагируют на такие требования и другие виды внешнего давления? Если частный сектор разрабатывает и осуществляет собственные внутренние меры политики и стандарты защиты и поощрения прав в сети, то какое влияние эти меры и стандарты оказывают на выражение мнений отдельными лицами и их доступ к информации?

36. Цифровой контент, передаваемый по частным сетям и размещенный на частных платформах, все больше зависит от государственного и корпоративного регулирования. Пространство создаваемого пользователями контента неуклонно расширяется: блоги, текстовые сообщения, форумы, фотографии, видеоролики и рассылка в социальных сетях являются лишь некоторыми из тех видов контента, которые создают и которыми обмениваются пользователи на ежедневной основе. Компании, которые управляют сетями и платформами для такого контента (именуемые посредниками), могут «предоставить доступ к разработанным третьими сторонами контенту, продуктам и услугам, обеспечить их размещение, передачу и индексацию», даже если сами они не создают и не производят такого контента<sup>19</sup>.

37. Государства часто обосновывают свои требования удалить контент такими доводами, как диффамация, богохульство, положения о проведении выборов, оскорбления или ненавистнические высказывания, подстрекательство, интеллектуальная собственность, ругательства и непристойные выражения, вербовка или «восхваление» террористов, защита национальной безопасности и общественного порядка, защита детей и предупреждение гендерно-мотивированного насилия. Внимание систем государственного регулирования привлекают к себе также проблемы, которые в течение длительного времени были связаны со свободой выражения мнений, однако значительно усложнились в эпоху цифровых технологий, включая «право на забвение», а также плюрализм и многообразие (например, сетевой нейтралитет). Сами посредники устанавливают и поддерживают условия предоставления услуг, направленные на устранение многих из

<sup>19</sup> MacKinnon and others, *Fostering Freedom Online*, p. 19; K. Perset, *The Economic and Social Role of Internet Intermediaries* (OECD, 2010).

подобных проблем в силу правовых, коммерческих и иных причин. Многие из этих проблем вызывают вопросы, связанные с сохранением надлежащего баланса между свободой выражения мнений и другими правами человека (такими, как неприкосновенность частной жизни, недискриминация). Хотя регулирование контента часто является ограничительным по своей природе, оно может быть также связано с требованиями о передаче санкционированных или одобренных правительством сообщений<sup>20</sup> или с запрещением на установление дифференцированных цен на размещение контента и на услуги по распространению контента<sup>21</sup>.

## 1. Государственное регулирование

38. Государства регулируют цифровой контент с помощью различных законодательных, политических и технических средств. Обеспокоенность вызывают нижеуказанные общие тенденции.

### *Расплывчатые законы*

39. Положения о регулировании контента обычно отражены в законодательстве, судебных решениях или постановлениях или подзаконных актах, издаваемых административными органами с делегированными полномочиями на регулирование телекоммуникационных или связанных с Интернетом вопросов. Китай, например, недавно изменил свое законодательство о кибербезопасности, установив запрет для лиц и организаций на использование Интернета в целях «нарушения общественного порядка» или «причинения ущерба государственным интересам»<sup>22</sup>. Аналогичным образом, находящийся на рассмотрении в Нигерии законопроект запрещает любому лицу публиковать на «любом носителе» заявления с «преступным намерением дискредитировать» какое-либо лицо, группу или государственное учреждение, «либо настроить население против» них<sup>23</sup>. Такие формулировки наделяют органы власти широкими дискреционными полномочиями на определение того, какого рода выражения мнений в цифровой среде будут считаться нарушающими их условия. В результате частные лица и предприятия предпочитают проявлять осторожность во избежание обременительных санкций, производить фильтрацию контента сомнительного правового статуса и использовать другие методы цензуры и самоцензуры.

### *Чрезмерная ответственность посредников*

40. Государства часто настаивают на сотрудничестве посредников в целях обеспечения выполнения положений, касающихся частных сетей и платформ. Провайдеры сетевых и телекоммуникационных услуг, например, обязаны выполнять местные законы и положения в качестве условия выдачи им лицензии на осуществление своей деятельности, что является законным требованием, которое, однако, может стать проблематичным, если местные законы или порядок их осуществления сами по себе не соответствуют праву прав человека. Компании, менее ограниченные лицензионными требованиями, такие как платформы

<sup>20</sup> См. Vodafone Group Plc, “Response on issues relating to mobile network operations in Egypt” (2011).

<sup>21</sup> В Индии, например, поставщикам услуг запрещено предлагать или устанавливать дискриминационные тарифы на цифровые услуги в зависимости от контента (Prohibition of Discriminatory Tariffs for Data Services Regulations, 2016).

<sup>22</sup> Китай, Закон о кибербезопасности (2015 год), статья 9.

<sup>23</sup> Парламент Нигерии, проект закона о запрещении явно необоснованных заявлений и заявлений по другим связанным с этим вопросам, пункт 3 статьи 3.

социальных сетей, поисковые системы и регистраторы доменных имен, тем не менее, сталкиваются с угрозой того, что государства станут разрушать местную инфраструктуру, угрожать безопасности местных работников или блокировать местный доступ к их платформам.

41. Частные субъекты также могут потребовать от посредников ограничения или удаления контента. Например, жалобы на нарушение прав интеллектуальной собственности часто поступают тогда, когда частная сторона утверждает, что какое-либо лицо распространило или использовало контент с нарушением его авторского права, или создало доменное имя, которое нарушает его товарный знак. Хотя в отношении таких жалоб могут иметься аргументы добросовестного использования или другие средства защиты, рамки охраны интеллектуальной собственности могут ограничивать свободу культурного и художественного самовыражения (см. A/HRC/28/57).

42. В деле *Гугл, Испания, против Марио Костехи Гонсалеса* Европейский суд обязал «Гугл» в соответствии с Директивой Европейского союза о защите данных исключить из списка результаты поиска, основанные на веб-страницах, в которых указывался Гонсалес, даже несмотря на то, что оригинальная публикация этих страниц сама по себе не подвергалась удалению<sup>24</sup>. Это решение получило активное применение за пределами европейского контекста<sup>25</sup>. Сфера и порядок применения такого подхода вызывают вопросы по поводу надлежащего баланса между правами на неприкосновенность частной жизни и защиту личных данных, с одной стороны, и правом искать, получать и передавать информацию, содержащую такие данные, – с другой стороны.

43. Посредникам все чаще приходится оценивать обоснованность требований государства и частных претензий с точки зрения общих правовых критериев и удалять или отсоединять такой контент, опираясь на подобные оценки. Например, Закон Объединенной Республики Танзания о киберпреступности 2015 года освобождает провайдеров гиперссылок от ответственности за размещенную в ссылке информацию при условии, что они «незамедлительно удалят [ ] или закроют [ ] доступ к информации после получения распоряжения сделать это от соответствующего органа власти»<sup>26</sup>. В контексте авторских прав Закон Соединенных Штатов Америки о защите авторских прав в цифровое тысячелетие освобождает провайдеров «интернет-услуг и сетевого доступа» от ответственности за контент третьей стороны только в том случае, если они соглашаются «незамедлительно удалить или закрыть доступ к материалу, который, как утверждается, является нарушающим авторские права или является объектом правонарушающих действий», после направления уведомления о таком правонарушении<sup>27</sup>. Режим «удаления после уведомления» подвергался критике за стимулирование сомнительных претензий и неспособность обеспечить адекватную защиту для посредников, стремящихся применять справедливые и учитывающие права человека стандарты к регулированию контента.

44. Еще одна важная проблема заключается в том, что частные посредники обычно плохо подготовлены для того, чтобы делать заключения о законности контента. Межамериканская комиссия по правам человека отметила, что частные субъекты «не в состоянии производить оценку прав и толкование законода-

<sup>24</sup> Judgment of the European Court of Justice (Grand Chamber), case C-131/12 (13 May 2014).

<sup>25</sup> Информация, представленная организацией «Статья 19».

<sup>26</sup> Para. 43 (a).

<sup>27</sup> United States Code, title 17, sect. 512 (c) (1) (C).

тельства в соответствии с правом на свободу выражения мнений и другими правозащитными стандартами»<sup>28</sup>. Возможно, это объясняется нехваткой ресурсов, отсутствием надлежащего надзора и подотчетности или потенциальными конфликтами интересов. Перед лицом потенциальной ответственности компании могут проявлять склонность к самоцензуре либо к чрезмерной цензуре.

#### *Ограничения, не предусмотренные законом*

45. Государства стремятся также ограничивать цифровой контент, не прибегая к применению законодательства. Некоторые государства призывали компании, обслуживающие социальные сети, и другие компании, размещающие пользовательский контент, отслеживать и удалять контент по собственной инициативе, не дожидаясь законодательно обоснованных запросов от правительства. Должностные лица правительств пытаются также убедить компании принимать «контрпропагандистские» инициативы на публичных форумах, во время проведения различных кампаний и в частных дискуссиях. Кроме того, правительства все чаще указывают, что тот или иной контент в социальных сетях не соответствует условиям предоставления услуг платформой, с тем чтобы заставить компанию удалить контент или деактивировать аккаунт.

#### *Фильтрация*

46. Государства часто блокируют или фильтруют контент при содействии частного сектора. Провайдеры интернет-услуг могут блокировать доступ к определенным ключевым словам, веб-страницам или целым веб-сайтам. На платформах, размещающих контент, способ фильтрации зависит от характера платформы и соответствующего контента. Регистраторы доменных имен могут отказать в регистрации тем, кто фигурирует в черном списке правительства; компании, обслуживающие социальные сети, могут удалять сообщения или блокировать аккаунты; поисковые системы могут удалять результаты поиска, предоставляющие доступ к нелегальному контенту. Такой метод установления ограничений, требуемый правительствами или применяемый компаниями, может вызывать вопросы, связанные как с необходимостью, так и соразмерностью, в зависимости от обоснованности приводимых аргументов в пользу удаления и опасности удаления легального или защищаемого выражения мнений.

47. Отсутствие четкости в государственном регулировании в сочетании с обременительными обязательствами, связанными с ответственностью посредников, может приводить к чрезмерной фильтрации. Даже в тех случаях, когда касающиеся контента нормативные положения приняты и применяются надлежащим образом, пользователи, тем не менее, могут сталкиваться с излишними ограничениями в отношении доступа. Например, фильтрация контента в одной юрисдикции может затронуть выражение пользователями мнения в цифровой среде в других юрисдикциях. Хотя компании могут разрабатывать фильтры для установки только в одной конкретной юрисдикции или в конкретном регионе, имели место случаи, когда такие фильтры все же оказывали воздействие на другие сети или области применения платформы. Например, в 2013 году предписанная государством фильтрация, которую проводила компания «Эйртел

---

<sup>28</sup> Inter-American Commission on Human Rights, *Freedom of Expression and the Internet*, pp. 47–48.

Индия», привела к тому, что тот же контент оказался заблокированным в ряде сетей в Омане, принадлежавших ее партнеру, компании «Омантел»<sup>29</sup>.

#### *Отключения сетей или обслуживания*

48. Отключения обслуживания и связанные с ними ограничения являются особенно вредоносными средствами практического регулирования контента. В оправдание подобных мер часто приводят интересы национальной безопасности, необходимость поддержания общественного порядка или недопущение общественных беспорядков. В 2015 году Специальный докладчик вместе с представителями Организации по безопасности и сотрудничеству в Европе, Организации американских государств и Африканской комиссии по правам человека и народов осудили незаконные блокировки Интернета<sup>30</sup>. Только за один год поступили сообщения об отключениях в Бангладеш, Бразилии, Бурунди, Демократической Республике Конго, Индии и Пакистане<sup>31</sup>. Специальный докладчик подтвердил случаи отключения провайдера телекоммуникационных услуг и предоставляемого им обслуживания в Таджикистане, имевшие место во время его официального визита в марте 2016 года<sup>32</sup>.

#### *Нейтральные сети*

49. В дополнение к тому, чтобы воздерживаться от излишних и несоразмерных ограничений на цифровой доступ, на государства возлагается также обязанность обеспечивать свободный и открытый Интернет. Сетевой нейтралитет является принципом, согласно которому любые интернет-данные, контент и услуги пользуются равным режимом без какой-либо ненадлежащей дискриминации. Однако провайдеры интернет-услуг могут применять технологии, которые ускоряют доступ к определенному контенту и определенным услугам или каким-либо иным образом способствуют такому доступу, замедляя при этом доступ к остальным услугам (практика, известная также как «троттлинг»). Рост числа совместных проектов провайдеров интернет-услуг и платформ для размещения контента, которые предлагают бесплатную беспроводную информацию для доступа к интернет-контенту или услугам, предоставляемым последними (известны также как предоставление услуг по «нулевым ставкам»), вызывает разногласия. В то время как такие меры представляют собой отход от принципа сетевого нейтралитета, предметом полемики остается вопрос о том, являются ли они допустимыми в тех районах, где существуют реальные проблемы с доступом к Интернету.

50. Государственное регулирование в данной области является бессистемным и неопределенным. Ряд государств признали важное значение сетевого нейтралитета в целом. Так, Румыния заявила, что она «поддерживает все инициативы по обеспечению того, чтобы размещенная в сети информация была реально доступна для населения в целом»<sup>33</sup>. Меньшее число государств предусмотрели

<sup>29</sup> Citizen Lab, “Routing gone wild: documenting upstream filtering in Oman via India” (2012).

<sup>30</sup> Совместная декларация о свободе выражения мнений и реагировании на ситуации конфликта (2015 год).

<sup>31</sup> Информация, представленная Институтом по правам человека и предпринимательской деятельности, примечание 3.

<sup>32</sup> 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 (9 March 2016).

<sup>33</sup> Информация, представленная правительством Румынии.

конкретные меры правовой защиты<sup>34</sup>. В начале 2016 года Управление телекоммуникационного регулирования Индии издало предписание, запрещающее провайдерам услуг предлагать или применять «дискриминационные тарифы на информационные услуги, предлагаемые или начисляемые потребителю в зависимости от контента»<sup>35</sup>. В определенных формах сетевой нейтралитет был признан в законодательстве или политике таких стран, как Бразилия, Нидерланды, Соединенные Штаты и Чили.

## 2. Внутренняя политика и практика

51. Проводимая посредниками политика и устанавливаемые ими правила могут оказывать значительное воздействие на свободу выражения мнений. Хотя основным источником регулирования являются условия предоставления услуг, конструктивные и технологические решения также могут оказывать влияние на предоставление контента.

### *Условия предоставления услуг*

52. Условия предоставления услуг, которые отдельные лица обычно должны принять для получения доступа к платформе, часто содержат ограничения, касающиеся размещаемого контента. Эти ограничения устанавливаются в соответствии с местными законами и нормативными положениями и отражают аналогичные запреты, включая запрещение оскорблений, ненавистнических высказываний, поддержки преступной деятельности, неспровоцированного насилия и прямых угроз<sup>36</sup>. Сформулированные условия предоставления услуг часто бывают настолько общими, что бывает трудно предсказать с достаточной степенью уверенности, какого рода контент может оказаться под запретом. Непоследовательное применение условий предоставления услуг также привлекает внимание со стороны общественности. Некоторые утверждают, что наиболее популярные в мире платформы не уделяют должного внимания потребностям и интересам уязвимых групп; например, выдвигались обвинения в нежелании «уделять непосредственное внимание техногенному насилию в отношении женщин, пока эта проблема не получила общественного резонанса»<sup>37</sup>. В то же время платформы подвергаются критике за чрезмерную цензуру широкого спектра законных, но (очевидно, для некоторых аудиторий) «некомфортных» выражений<sup>38</sup>. Отсутствие процедуры обжалования или недостаточно четкое озвучивание позиции компании по поводу удаления того или иного контента или деактивации аккаунта усугубляют такую обеспокоенность. Условия предоставления услуг, которые требуют регистрации с указанием подлинного имени конкретного лица или доказательства, подтверждающего надлежащее использование псевдонима, также могут несоразмерно ограничивать способность уязвимых групп или субъектов гражданского общества в закрытых обществах пользоваться сетевыми платформами для выражения мнений, ассоциации или отстаивания своих взглядов.

53. Государства все чаще используют также условия предоставления услуг для устранения контента, который они считают нежелательным. Специальный докладчик по вопросу о поощрении и защите прав человека в условиях борьбы

<sup>34</sup> Mackinnon and others, *Fostering Freedom Online*, p. 80.

<sup>35</sup> Prohibition of Discriminatory Tariffs for Data Services Regulations, 2016.

<sup>36</sup> См., например, Facebook terms of service, sect. 3 (7); Twitter terms of service; YouTube Community Guidelines; и Reddit.

<sup>37</sup> См. [https://ourinternet-files.s3.amazonaws.com/publications/no24\\_web\\_2.pdf](https://ourinternet-files.s3.amazonaws.com/publications/no24_web_2.pdf).

<sup>38</sup> См. [onlinencensorship.org](http://onlinencensorship.org).

с терроризмом отмечал, что ряд государств установили механизмы удаления контента, которые часто используются для удаления такого контента, который, будучи законным, может, тем не менее, рассматриваться как экстремистский (см. A/HRC/31/65). Так, Контртеррористическое подразделение по контролю интернет-пространства в Соединенном Королевстве призвано удалять сетевой контент «насильственно экстремистского или террористического характера», в том числе посредством методов «используемых механизмами маркировки контента для отправки сообщения о контенте как о нарушающем условия [предоставления услуг] сайта»<sup>39</sup>. Такая практика повышает вероятность того, что государства будут опираться на частные условия предоставления услуг в обход норм в области прав человека или внутренних законодательных норм по недопущению ограничения контента.

54. Деятельность частной цензуры осложняется уже одним объемом жалоб и маркированного контента, которые идентифицируются посредниками на ежедневной основе. Крупные платформы могут также передавать на внешние функции по модерации контента, тем самым еще более увеличивая дистанцию между модераторами контента и принятием внутренних стратегических решений и усугубляя нестыковки в сфере правоприменения. Посредники, осуществляющие свою деятельность на самых разных рынках, неизбежно сталкиваются с проблемой «сложных оценочных суждений», проблемами культурных особенностей и многообразия, а также «трудных решений, связанными с коллизией законов»<sup>40</sup>.

#### *Проектные и технологические решения*

55. От того, каким образом посредники отбирают, классифицируют и располагают контент, зависит, какую именно информацию пользователи получают и видят на своих платформах. Например, платформы используют алгоритмические прогнозы пользовательских предпочтений и на этой основе определяют, какие рекламные объявления могут увидеть отдельные лица, как происходит организация подачи им материалов сетей и в каком порядке появляются результаты поиска<sup>41</sup>. Другие меры саморегулирования, такие как инициативы в области противодействия языку ненависти в поддержку мер по борьбе с терроризмом и недопущению притеснений<sup>42</sup>, также влияют на то, каким образом пользователи могут получать и обрабатывать интернет-контент по деликатным вопросам. По-прежнему открытым остается вопрос о том, каким образом озабоченности в области свободы выражения мнений, сопряженные с проектными и техническими решениями, должны учитываться в увязке со свободой частных субъектов конструировать и адаптировать собственные платформы по своему усмотрению.

<sup>39</sup> National Police Chiefs' Council, Counter Terrorism Internet Referral Unit; информация, представленная Центром развития технологии и демократии.

<sup>40</sup> Emily Taylor, *The Privatization of Human Rights: Illusions of Consent, Automation and Neutrality*, GCIG Paper No. 24 (2016).

<sup>41</sup> Информация, представленная Центром технологии и общества; проект «Классификация цифровых прав».

<sup>42</sup> См., например, Home Affairs Committee, Oral testimony of Anthony House, Google Europe, Middle East and Africa (2 February 2016).

## **В. Слежение и цифровая безопасность**

56. Слежение со стороны государства, а также корпоративный сбор и хранение данных затрагивают важные вопросы свободы выражения мнений. Например, каким образом государство осуществляет слежение при содействии частного сектора и каким образом такое сотрудничество влияет на свободу выражения мнений? Что обязаны предпринять частные субъекты, если они обнаружат, что государство скрытно получает доступ к сетевым и телекоммуникационным данным, передаваемым или хранимым в их сетях или на их платформах? Каковы обязанности частного сектора по защите безопасности и анонимности в сетях?

57. Цифровые сообщения, а также данные, передаваемые или хранимые в частных сетях и на частных платформах, все чаще становятся объектом слежения и других форм воздействия со стороны как государств, так и частных субъектов. Излишнее и несоразмерное слежение может подрывать безопасность в сетевой среде и доступ к информации и идеям (см. A/HRC/23/40). Слежение может оказывать сковывающее воздействие на выражение мнений в сетях обычными гражданами, которые могут заниматься самоцензурой, опасаясь того, что за ними постоянно следят. Слежение оказывает несоразмерное воздействие на свободу выражения мнений широкого круга уязвимых групп, включая расовые, религиозные, этнические, гендерные и сексуальные меньшинства, членов определенных политических партий, гражданского общества, правозащитников, таких специалистов, как журналисты, юристы и профсоюзные деятели, жертв насилия и надругательств, а также детей (см. A/HRC/29/32). Способность государства осуществлять слежение может зависеть от степени сотрудничества или противодействия такому слежению со стороны частных предприятий.

### **1. Запросы о предоставлении пользовательских данных**

58. Поскольку провайдеры интернет-услуг, платформы социальных сетей, информационно-поисковые системы, провайдеры «облачных услуг» и другие компании передают или накапливают огромное количество пользовательских данных, объем запросов правительств о предоставлении пользовательской информации на основании местных законов и нормативных положений также начал возрастать. Об увеличении таких запросов сообщили несколько крупных интернет-компаний<sup>43</sup>. Инициаторами многих подобных запросов являются правоохранительные органы и спецслужбы. Государственный контроль над такими запросами варьируется: от получения предварительной судебной санкции<sup>44</sup> до утверждения исполнительным органом власти высокого уровня<sup>45</sup> либо полного его отсутствия. Лицензионные соглашения и законодательство могут ограничивать способность частного сектора противостоять подобным запросам или принуждать к обязательному представлению отчетности. Даже платформы для размещения контента, не имеющие физического присутствия в определенных юрисдикциях, где они осуществляют свою деятельность, могут сталкиваться с полным блокированием своих услуг и попытками запугивания сотрудников корпоративных дочерних организаций. Тем не менее компании во всех областях индустрии информационно-коммуникационных технологий способны в различ-

<sup>43</sup> См. последнюю отчетность о прозрачности компаний «Гугл», «Фейсбук», «Дропбокс», «Твиттер» и «Майкрософт».

<sup>44</sup> Sweden, Act on Signal Surveillance for Defense Intelligence Activities, sect. 4 (3).

<sup>45</sup> Australia, Telecommunications (Interception and Access) Act 1979, sect. 9 (1).

ной степени создавать или приводить в действие механизмы влияния в своих отношениях с государствами в целях противодействия причинению или смягчения ущерба, наносимого неправомочным применением законодательства. К эффективным стратегиям противодействия относятся: включение в лицензионные соглашения и другие соответствующие контракты гарантий прав человека; ограничительное толкование запросов правительства; переговоры с государственными должностными лицами о рамках подобных запросов; оспаривание в судебном порядке чрезмерно расширенных запросов или законов; предоставление соответствующей информации затрагиваемым лицам, средствам массовой информации или общественности; а также приостановление предоставления услуг на конкретном рынке, уход с него или принятие решения не выходить на такой рынок.

## **2. Продажа оборудования, предназначенного для слежения и цензуры**

59. Частный сектор поставляет аппаратуру, программное обеспечение и другие технологии, позволяющие государствам перехватывать, хранить или анализировать сообщения и другую информацию. Поставщики инфраструктуры, производители оборудования и разработчики программного обеспечения могут разрабатывать или изготавливать по специальным требованиям продукцию по поручению государств либо поставлять оборудование и технологии двойного назначения, которые государства впоследствии адаптируют для использования в соответствии со своими собственными потребностями. Провайдеры интернет-услуг и провайдеры телекоммуникационных услуг могут также приобретать оборудование или программное обеспечение у этих компаний для установки на своих сетевых компонентах в целях обеспечения соблюдения предусмотренных местным законодательством протоколов перехвата в тех государствах, где они осуществляют свою деятельность. Государства могут использовать такие продукты и услуги для оказания адресного воздействия на представителей уязвимых групп, их запугивания или устрашения.

## **3. Скрытое слежение**

60. Государства могут также скрытно подключаться к технической инфраструктуре, принадлежащей провайдерам услуг и платформам для размещения контента, в целях перехвата широкого диапазона различной информации, включая сообщения, информацию о пользовательских аккаунтах, а также телефонные разговоры и записи интернет-данных. Государства, согласно сообщениям, перехватывают контроль над компьютерным оборудованием во время его доставки потребителям и проникают в частные сети и платформы с помощью вредоносного программного обеспечения, взламывают конкретные устройства и используют другие лазейки в системе цифровой безопасности. Когда частным предприятиям становится известно о таком слежении, могут возникнуть вопросы, касающиеся их обязательств в области прав человека, таких как уведомление потребителей или смягчение последствий такого вреда за счет принятия мер безопасности. Компании, поставляющие оборудование и услуги правительствам для применения методов скрытого слежения, могут оказаться причастными к нарушениям прав человека, происходящим в результате их поставок.

## **4. Договоры о взаимной правовой помощи и локализация данных**

61. Важно отметить, что на слежение влияют другие требования, касающиеся хранения частной информации. Например, если режим договора о взаимной правовой помощи не позволяет удовлетворить трансграничные запросы о предоставлении данных, это может заставить государства прибегнуть к исполь-

зованию в обход закона экстерриториальных мер слежения. Законы, обязывающие компании сохранять данные о пользователях или хранить такие данные в местных центрах сбора данных, также могут стимулировать такое слежение.

## 5. Шифрование и анонимность

62. С тех пор как Специальный докладчик рассмотрел в своем докладе вопрос о важном значении шифрования и анонимности для защиты свободы мнений и их свободного выражения, давление правительств на корпорации в стремлении обойти систему безопасности цифровых устройств пользователей, их сообщений и информации возросло. Целый ряд частных субъектов – от производителей аппаратуры до служб электронной почты и передачи сообщений – принимают меры по разработке и внедрению технологий, повышающих уровень безопасности пользователей, их анонимности и неприкосновенности частной жизни. К числу таких мер относится: межэбонентское шифрование цифровых сообщений, шифрование дисков и своевременное обновление программного обеспечения для ликвидации изъянов в системе безопасности. Государства в свою очередь стремятся заставить компании создавать или использовать технические лазейки в их продуктах и услугах в своих интересах. В Соединенных Штатах, например, Федеральное бюро расследований обратилось в федеральный суд с целью заставить компанию «Эппл» создать программное обеспечение, отказывающее доступ к «айфонам» подозреваемых лиц в рамках расследования террористической деятельности. Представленный на рассмотрение британского парламента 1 марта 2016 года проект закона о следственных полномочиях позволит спецслужбам обращаться за выдачей санкции, обязывающей частные субъекты «обеспечивать доступ к любому оборудованию в целях получения сообщений [...], данных оборудования и любой другой информации»<sup>46</sup>.

## С. Транспарентность

63. Транспарентность может оказать содействие в обеспечении того, чтобы субъекты интернет-регулирующие могли реально прогнозировать свои правовые обязательства и оспаривать их в случае необходимости. Пробелы в соблюдении этих стандартов угрожают способности отдельных лиц понимать рамки, ограничивающие их свободу выражения мнений в сетевой среде, и обращаться за надлежащим возмещением в случае нарушения их прав. Проблемы транспарентности возникают как в контексте государства, так и в контексте частного сектора и затрагивают государственно-частное партнерство, участие частного сектора в торговых переговорах и цифровую «гонку вооружений».

64. Несмотря на многочисленные попытки реформирования, транспарентность в отношении правительственных запросов по-прежнему отсутствует. Хотя налицо определенные улучшения в отношении отчетности по вопросам транспарентности, касающиеся запросов правительства на получение пользовательских данных, гораздо меньше информации имеется в отношении объема и характера запросов правительства, касающихся запрещения или удаления контента<sup>47</sup>. Остается неясным, обеспечивается ли вообще хранение подобных статистических данных. Ограничения, налагаемые государством на раскрытие частными компаниями соответствующей информации, могут представлять со-

<sup>46</sup> Investigatory Powers Bill (2015), Cl. 88 (2).

<sup>47</sup> Информация, представленная Рабочей группой по вопросам защиты персональных данных и транспарентности в сетевом пространстве коалиции «Фридом онлайн» и Диалогом телекоммуникационной отрасли.

бой одно из основных препятствий для обеспечения корпоративной прозрачности. Ряд государств запрещают раскрытие информации о запросах правительства, касающихся удаления контента или доступа к данным пользователей. Индия, например, запрещает интернет-посредникам раскрывать подробности о распоряжениях правительства заблокировать доступ к интернет-контенту, а также о любых принимаемых ими мерах в ответ на такие распоряжения<sup>48</sup>. Находящийся на рассмотрении в Великобритании проект закона о следственных полномочиях запретит провайдерам телекоммуникационных услуг раскрывать, в числе прочего, «существование и содержание» распоряжений правительства о хранении данных, касающихся сообщений клиентов<sup>49</sup>. В других государствах расплывчатые законы и нормативные положения затрудняют для корпораций определение того, какого рода информацию им разрешено раскрывать. В Южной Африке, например, раскрытие частными компаниями запросов правительства по данным клиентов запрещено<sup>50</sup>, однако остается неясным, распространяется ли такое ограничение на запросы об удалении контента<sup>51</sup>.

65. В случае частного сектора провайдеры услуг и платформы для размещения контента часто раскрывают по меньшей мере часть информации об обстоятельствах, при которых они удаляют контент или выполняют запросы правительства на предоставление пользовательских данных. Тем не менее имеются широкие расхождения в отношении того, сообщают ли они о толкованиях или разъяснениях постановлений государства и условий предоставления услуг, а также внутренних процессов по обеспечению выполнения и соблюдения и если да, то каким образом. Существуют также пробелы в раскрытии корпорациями статистических данных по объему, частотности и типам запросов, касающихся удаления контента и представления пользовательских данных, в связи с наличием введенных государством ограничений или решений, связанных с внутренней политикой. В любом случае компании более склонны раскрывать статистические данные по запросам правительства, чем по частным запросам. Кроме того, гораздо менее изучен вопрос о том, в какой степени другие посредники (например, финансовые посредники или посредники в сфере электронной торговли) и компании раскрывают информацию, касающуюся удаления контента и запросов на получение пользовательских данных.

66. Продолжающиеся дебаты по поводу минимальных стандартов раскрытия корпоративной информации и соответствующей передовой практики отражают отсутствие определенности в отношении надлежащего баланса между прозрачностью и такими коллидирующими ценностями, как индивидуальная безопасность и коммерческая тайна. Несмотря на все более широкое признание того, что корпорациям следует раскрывать информацию о толковании и применении ограничений, менее однозначным является согласие в вопросе о том, каким образом это следует делать. Аналогичным образом существует широкое согласие в отношении важного значения количественной прозрачности, однако менее понятно, каким образом следует контекстуализировать, представлять и делать доступной такую информацию.

<sup>48</sup> India, Information Technology (Procedures and Safeguards for Blocking for Access of Information by Public) Rules, 2009, rule 16.

<sup>49</sup> Investigatory Powers Bill, Cl. 84 (2).

<sup>50</sup> South Africa, Regulation of Interception of Communications and Provision of Communication-Related Information Act 70 of 2002, sect. 42 (1).

<sup>51</sup> South Africa, National Key Points Act 102 of 1980, sect. 10 (c).

## D. Средства правовой защиты

67. Ограничения свободы выражения мнений в сетевом пространстве происходят на ежедневной основе и часто связаны с корпоративным поведением, будь то регламентируемым законодательством или отвечающим корпоративной политике и практике (например, закрепленным в условиях предоставления услуг). Наиболее распространенными примерами таких ограничений являются, в частности, незаконные или иные вызывающие сомнение случаи удаления контента, ограничения на обслуживание и временные закрытия аккаунтов, а также нарушения режима безопасности данных.

68. В соответствии с пунктом 3 статьи 2 Международного пакта о гражданских и политических правах государство-участники обязуются обеспечить любому лицу, права которого, признаваемые в Пакте, нарушены, эффективное средство правовой защиты. В Руководящих принципах предпринимательской деятельности в аспекте прав человека предусмотрено, что корпорации должны обеспечивать механизмы предоставления средств правовой защиты и подачи жалоб, которые являлись бы легитимными, доступными, предсказуемыми, справедливыми, соответствующими нормам прав человека, транспарентными, основанными на диалоге и взаимодействии и представляли бы собой источник непрерывного обучения<sup>52</sup>. Вместе с тем весьма ограниченными являются руководящие ориентиры в отношении того, каким образом эти элементы должны реализовываться или оцениваться в контексте информационно-коммуникационных технологий. Например, ненадлежащее удаление ссылок на сайты из результатов поиска может потребовать от поисковой системы восстановления таких ссылок. Однако остается неясным, каким образом следует разрабатывать и внедрять механизмы рассмотрения жалоб или апелляций для обеспечения того, чтобы такие удаления эффективно помечались, оценивались и исправлялись. Исключительно разветвленная клиентская база поисковых систем еще более усугубляет проблемы проектирования. Неясно также, должны ли компании предоставлять такие дополнительные средства защиты, как финансовая компенсация упущенной выгоды за период удаления или гарантии неповторения в будущем.

69. Для обеспечения соблюдения условий предоставления услуг компании, возможно, не всегда имеют достаточные процедуры для обжалования решений об удалении контента или деактивации аккаунта, если пользователь считает такую меру ошибочной или результатом неправомерных кампаний маркировки контента. Полезными могут оказаться дополнительные исследования по рассмотрению передовой практики в области распространения компаниями информации о выполнении решений, связанных с условиями предоставления услуг, и использования ими механизмов обжалования.

70. Рамки ответственности корпораций за устранение последствий также являются предметом споров. На кого следует возлагать бремя ответственности за необоснованные удаления или запросы на передачу данных в тех случаях, когда компании чрезмерно строго толкуют или соблюдают соответствующие законы государства? Если продукты или услуги компании используются для совершения нарушений прав человека, то на каком уровне причинно-следственная связь влечет за собой обязательства предоставлять средства защиты? Когда компаниям предъявляются обвинения в совершении правонарушений, предусматривает ли это обязанность проводить внутренние расследования и должны ли такие

---

<sup>52</sup> Руководящие принципы, глава III (A) (31).

расследования отвечать определенным стандартам? Если ограничение затрагивает отдельных лиц в разных странах, какая юрисдикция должна применяться для рассмотрения вопроса о средствах правовой защиты? Эти вопросы отражают ту неопределенность, с которой жертвы нарушений прав человека сталкиваются в ситуациях, когда действия корпораций и государств невозможно отделить друг от друга.

71. Вопрос о надлежащей роли государства в дополнении или регулировании корпоративных механизмов правовой защиты также требует более подробного анализа. Для потребителей, чьи права были ущемлены действиями корпораций, часто существуют возможности гражданского судебного разбирательства и другие средства судебной защиты, но они часто бывают обременительными и дорогостоящими. Разумными альтернативами могут быть, в частности, механизмы подачи и рассмотрения жалоб, создаваемые и обслуживаемые органами по защите потребителей и отраслевыми регуляторами. Ряд государств санкционировали также создание внутренних механизмов правовой защиты или рассмотрения жалоб: Индия, например, предписывает корпорациям, владеющим, занимающимся или оперирующим конфиденциальными персональными данными, назначать сотрудника по претензиям, с тем чтобы он занимался «любыми недостатками и жалобами [...] в связи с обработкой информации»<sup>53</sup>.

## V. Дальнейшая проработка тематики

72. Учитывая диапазон частной деятельности в области информационно-коммуникационных технологий, которая очерчивает контуры осуществления свободы мнений и их свободного выражения в онлайн-режиме, а также оказывает на него воздействие, Специальный докладчик уделит особое внимание обязательствам государств и ответственности предприятий в конкретных областях, вызывающих беспокойство. Затронутые выше вопросы права и политики будут определять особенности представления докладов по данной тематике, контактов с правительствами, посещений стран и компаний, региональных консультаций и совещаний экспертов, а также иной деятельности.

73. К числу приоритетов Специального докладчика в области проведения тематических исследований и составления руководств относятся следующие:

### **Ограничения на предоставление телекоммуникационных и интернет-услуг**

74. Правительства все чаще обязывают частные предприятия, предоставляющие телекоммуникационные и интернет-услуги, соблюдать требования цензуры. В дополнение к практике сетевой фильтрации государства обязывают или принуждают компании отключать сети или блокировать любое предоставление услуг. Эта тенденция нуждается в дополнительном документировании и тщательном изучении. В рамках дальнейшей работы будут изучаться законы, политика и не предусмотренные законом меры, которые позволяют правительствам вводить подобные ограничения, а также издержки и последствия таких ограничений. Специальный докладчик изучит также обязанности компаний по реагированию на такие меры с учетом необходимости соблюдения прав, смягчения ущерба и предоставления возможностей для возмещения вреда в случае злоупотреблений.

<sup>53</sup> India, Information Technology Act, 2008, sect. 43 A; Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011, rule 5 (9).

**Ограничения контента в соответствии с условиями предоставления услуг и стандартами, принятыми в сообществе**

75. Частные субъекты подвергаются значительному давлению со стороны правительств и отдельных лиц на предмет ограничения выражения мнений, которые считаются экстремистскими или ненавистническими, враждебными или оскорбительными. Кроме того, частные субъекты в свою очередь могут задаться целью способствовать тому, что, по их мнению, является гражданским дискурсом, на своих платформах, регулировать доступ посредством требования указывать подлинное имя и других методов, связанных с регистрацией, либо размещать или ранжировать определенный контент исходя из коммерческих соображений. В рамках дальнейшей работы будет произведена оценка возможностей государства в деле злоупотреблений частными инициативами, воздействия частных мер на свободу выражения мнений и соответствующих правозащитных обязательств и обязанностей в данной области. В этих докладах внимание будет сосредоточено на роли не только социальных сетей и поисковых систем, но и таких менее известных субъектов, как посредники в сфере электронной торговли и финансовые посредники.

**Ответственность за размещение контента**

76. Посредники все чаще привлекаются к ответственности за размещаемый ими контент третьих сторон либо в рамках режимов ответственности посредников, либо в рамках требований цензуры. Широко приводимыми обоснованиями для таких ограничений являются, в частности, кибербезопасность, авторское право, клевета и защита данных. Дальнейшее исследование будет посвящено законности таких обоснований, необходимости сопутствующих ограничений и отсутствию при существующих системах процедурных гарантий при устранении контента третьих сторон. Будущая работа позволит также изучить источники и виды ответственности посредников в конкретных контекстах и регионах, а также поможет разработать основные принципы и виды применимой практики в целях обеспечения способности посредников поощрять и защищать свободу выражения мнений.

**Цензура и индустрия средств слежения**

77. Частные компании играют важную роль в разработке, производстве и передаче программного обеспечения и аппаратных средств, которые правительства могут использовать для правоприменения, сбора и анализа данных и обеспечения общественной безопасности. Хотя у этих инструментов могут быть законные цели, они часто используются правительствами для установления цензуры и неправомерного слежения. Дальнейшая работа позволит рассмотреть эти проблемы с точки зрения нормативно-правовой базы прав человека, а также будет способствовать повышению должной осмотрительности при определении методов применения такой технологии в целях, подрывающих свободу выражения мнений.

**Усилия, направленные на подрыв цифровой безопасности**

78. Компании, которые передают, хранят или генерируют сообщения и другие формы пользовательских данных, – особенно провайдеры телекоммуникационных и интернет-услуг и платформы для размещения контента – сталкиваются с проблемой растущего числа требований правоохранительных органов и спецслужб по поводу предоставления доступа к информации своих пользователей. Дальнейшая деятельность будет направлена на выявление подходов, кото-

рые могли бы максимально расширить свободу выражения мнений, но при этом учитывать законные государственные интересы в сферах национальной безопасности и общественного порядка.

### **Доступ к Интернету**

79. Миллиарды людей, подключенные к сетям, пользуются доступом к информации и идеям, которые недоступны многим миллиардам людей, не обладающим соответствующей инфраструктурой или лишенным соответствующих возможностей по соображениям политики, безопасности, а также правовых и социальных условий, необходимых для подсоединения. Поскольку частный сектор все более стремится предоставить доступ еще многим миллиардам людей, будет важно обеспечить, чтобы такой доступ являлся свободным, открытым и безопасным. В ходе дальнейшей деятельности будут изучены проблемы, связанные с доступом, участием частного сектора и инвестициями в обеспечение финансовой и физической доступности, особенно с учетом интересов маргинализированных групп.

### **Управление Интернетом**

80. Итоги Всемирной встречи на высшем уровне по вопросам информационного общества показали сохранение активной поддержки управления Интернетом при участии широкого круга заинтересованных сторон. Тем не менее существующая модель испытывает на себе усиливающееся давление в виде конкретных мер национальной политики (таких, как локализация данных) и таких стратегий, как «киберсуверенитет». Кроме того, налицо сохраняющаяся необходимость поддерживать или расширять участие правозащитного компонента на всех уровнях управления, включая установление технических стандартов, а также обеспечивать, чтобы рамки управления Интернетом и нацеленные на реформы усилия отвечали потребностям женщин, сексуальных меньшинств и других уязвимых групп общества.

81. В рамках этой будущей деятельности Специальный докладчик будет уделять особое внимание изменениям в правовой области (законодательным, нормативным и судебным) на национальном и региональном уровнях. В связи с этим он доводит до сведения всех соответствующих субъектов свою заинтересованность в сборе таких материалов для будущих сообщений и докладов и призывает заинтересованные стороны обеспечивать сбор и представление таких материалов в ходе всей этой работы.

## **VI. Выводы и рекомендации**

82. Сектор информационно-коммуникационных технологий постоянно находится в процессе стремительного развития, что позволяет непрерывно обновлять технологию и «оцифровывать» повседневную жизнь. В результате этого рассмотрение правовых вопросов и вопросов политики через призму существующих сегодня нормативных пробелов чревато определенным риском оставить без внимания те тенденции, которые сейчас только проявляются или которым предстоит еще проявиться. Это естественно для эпохи цифровых технологий, однако даже с учетом стремительных изменений в технологии в цифровом пространстве будут сохраняться постоянные угрозы для свободы мнений и их свободного выражения. К числу таких угроз относятся господство или стремление к господству государств над источниками информации при помощи цензуры в отношении интернет-

услуг и инфраструктуры; борьба предприятий за продвижение своих продуктов и услуг в среде, враждебной для свободы выражения мнений; неспособность многих предприятий обеспечить поощрение и защиту прав при преследовании своих коммерческих интересов; а также зачастую противоречивые требования отдельных лиц, рассчитывающих на то, что предпринимательские структуры будут обеспечивать им не только безопасность, но и удобство в пользовании, сетевое взаимодействие и подключенность к сообществам. По мере дальнейшего осуществления проекта изучения ответственности в области информационно-коммуникационных технологий Специальный докладчик будет обращаться к экспертам в этой области (в правительстве, частном секторе, гражданском обществе, техническом сообществе, академических кругах), рассчитывая на получение содействия в проведении анализа и подготовке докладов, посвященных как текущим проблемам на стыке технологии и свободы выражения мнений, так и долгосрочным особенностям эпохи цифровых технологий.

83. Специальный докладчик настоятельно призывает все заинтересованные стороны – включая государственные органы, предприятия частного сектора или организации гражданского общества и отдельных лиц – принять активное участие в разработке предстоящих проектов. Он призывает прежде всего заинтересованные стороны из наименее развитых стран и уязвимые сообщества поделиться своими мнениями относительно возможного воздействия сектора информационно-коммуникационных технологий на пользование правами и той роли, которую могут играть государства в связи либо с нарушением, либо с укреплением таких прав.

84. Хотя данный проект находится на своих начальных стадиях, тем не менее крайне важно, чтобы государства и частные субъекты принимали меры по обеспечению соблюдения свободы мнений и их свободного выражения. Эти меры должны предусматривать как минимум нижеследующее с последующим анализом, который будет проводиться на протяжении всего срока действия мандата Специального докладчика.

#### Государства

85. Главную ответственность за защиту и соблюдение права на осуществление свободы мнений и их свободного выражения несут государства. В контексте информационно-коммуникационных технологий это означает, что государства не должны обязывать или каким-либо иным образом принуждать частный сектор принимать меры, неоправданно или несоразмерно ограничивающие свободу выражения мнений, с помощью законов, политики или неюридических средств. Любые требования, запросы или иные меры по удалению цифрового контента или получению доступа к информации пользователей должны основываться на принятых в установленном порядке законах, подлежать внешнему и независимому надзору и представлять собой необходимые и соразмерные средства достижения одной или более целей, предусмотренных пунктом 3 статьи 19 Международного пакта о гражданских и политических правах. Прежде всего в контексте регулирования частного сектора государственные законы и меры политики должны приниматься и осуществляться транспарентным образом.

86. Кроме того, правительства должны принимать и выполнять законы и меры политики, обеспечивающие защиту разработки и реализации частным сектором технических мер, продуктов и услуг, способствующих укреплению свободы выражения мнений. Они должны обеспечивать

надлежащие процессы осуществления законов, разработки политики и установления других норм в отношении прав и ограничений, касающихся Интернета, с тем чтобы предоставить частному сектору, гражданскому обществу, техническому сообществу и научным кругам возможности для конструктивного вклада и участия.

#### Частный сектор

87. Государства оказывают на частный сектор информационно-коммуникационных технологий явное давление, которое зачастую приводит к серьезным ограничениям свободы выражения мнений. Вместе с тем частный сектор также выполняет независимые функции, которые могут либо продвигать, либо ограничивать права, что было должным образом признано Советом по правам человека, который в 2011 году принял Руководящие принципы предпринимательской деятельности в аспекте прав человека в качестве общего руководства в данной области. О деятельности частных субъектов следует судить по принимаемым ими мерам, как способствующим, так и препятствующим осуществлению свободы выражения мнений, даже в негативных условиях, подрывающих осуществление прав человека.

88. К числу наиболее важных мер, которые надлежит принимать частным субъектам, относятся разработка и внедрение транспарентных процедур оценки соблюдения прав человека. Они должны разрабатывать и проводить политику, учитывающую их потенциальное воздействие на права человека. Необходимо, чтобы такая оценка предусматривала критический обзор широкого спектра различных видов деятельности частного сектора, таких как разработка и обеспечение соблюдения условий предоставления услуг и стандартов сообщества, касающихся свободы выражения мнений пользователями, включая передачу функции по их применению на подряд сторонним организациям; воздействие продуктов, услуг и иных коммерческих инициатив, по мере их разработки, на свободу выражения мнений пользователями, включая конструктивные и технические решения, а также планы по установлению дифференцированных цен на интернет-контент и интернет-услуги или доступ к ним; и воздействие на соблюдение прав человека коммерческих отношений с потенциальными государственными клиентами, таких как обслуживание телекоммуникационной инфраструктуры или передача технологий для регулирования контента или осуществления слежения.

89. Кроме того, исключительно важно, чтобы частные субъекты обеспечивали максимально возможную транспарентность в своей политике, стандартах и действиях, затрагивающих свободу выражения мнений и другие основные права. Оценки соблюдения прав человека должны подвергаться транспарентному обзору с точки зрения применяемых методологий, толкования предусмотренных законом обязательств и воздействия таких оценок на принятие деловых решений. Транспарентность имеет важное значение во всех аспектах, в том числе в контексте регулирования контента, и должна предусматривать отчетность по запросам правительств, касающимся удаления контента.

90. Сверх принятия мер политики частные субъекты должны также интегрировать обязательства по соблюдению свободы выражения мнений в свои внутренние процессы разработки политики, конструирования изделий, развития предпринимательской деятельности, подготовки персонала

и другие соответствующие внутренние процессы. Специальный докладчик будет стремиться изучать меры политики и весь спектр шагов по их осуществлению, используя для этого различные способы, включая посещения компаний.

#### **Международные организации и многосторонние процессы**

91. Как показал настоящий доклад, многие международные организации играют определенную роль в процессах управления информационно-коммуникационными технологиями. Исключительно важно, чтобы такие организации обеспечивали реальный публичный доступ к мерам политики, стандартам, докладам и иной информации относительно управления Интернетом, разработанным или подготовленным этими организациями и/или их членами, в том числе за счет облегчения доступа к бесплатным интерактивным ресурсам и общественно-просветительским инициативам. В более общем плане многосторонний процесс управления Интернетом является важным стимулом для осуществления политики, способствующей свободе выражения мнений. С учетом этого международным организациям следует обеспечивать конструктивное участие гражданского общества в разработке политики и других процессах установления стандартов, в том числе посредством расширенного привлечения технических экспертов, разбирающихся в вопросах соблюдения прав человека.

---