Организация Объединенных Наций A/HRC/23/40

Генеральная Ассамблея

Distr.: General
17 April 2013
Russian
Original: English

Совет по правам человека
Двадцать третья 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 Франка Ла Рю*

Резюме

В настоящем докладе, представленном в соответствии с резолюцией 16/4 Совета по правам человека, анализируются последствия практики осуществления государствами слежения за сообщениями на осуществление прав человека на неприкосновенность личной жизни и на свободу мнений и их свободное выражение. В докладе описывается влияние существенного технологического прогресса в области коммуникации и одновременно подчеркивается неотложная необходимость дальнейшего изучения новых способов слежения и приведения национального законодательства, регулирующего эту практику, в соответствие с правозащитными стандартами.

* Представлен с опозданием.

Содержание

I. Введение

1. В настоящем докладе анализируются последствия практики осуществляемого государствами слежения за сообщениями на осуществление прав человека на неприкосновенность личной жизни и на свободу мнений и их свободное выражение. В докладе описывается влияние существенного технологического прогресса в области коммуникаций и одновременно подчеркивается неотложная необходимость дальнейшего изучения новых способов слежения и приведения национального законодательства, регулирующего эту практику, в соответствие с правозащитными стандартами.

2. Инновации в области технологий расширяют коммуникационные возможности и возможности защиты свободы выражения мнений, обеспечивая условия для анонимности, быстрого обмена информацией и межкультурного диалога. Технологические изменения одновременно расширяют возможности государства с точки зрения слежения за частными контактами и вмешательства в них.

3. Соображения, связанные с национальной безопасностью и противодействием преступной деятельности, могут оправдать использование в исключительных случаях технологий слежения за коммуникациями. Тем не менее национальные законы, регулирующие понятие необходимости, законности и соразмерности применительно к осуществляемому государством слежению за сообщениями, зачастую являются неадекватными или отсутствуют. Ненадлежащая национальная правовая база создает благодатную почву для произвольных и незаконных нарушений права на неприкосновенность личной жизни в области обмена информацией и, как следствие, также угрожает защите права на свободу мнений и их свободное выражение.

4. В предыдущих докладах (A/HRC/17/27 и A/66/290) Специальный докладчик проанализировал беспрецедентное влияние Интернета на расширение возможностей частных лиц по осуществлению своего права на свободу мнений и их свободное выражение. Он выразил озабоченность принимаемыми государствами многочисленными мерами по предупреждению или ограничению потоков информации в онлайновом режиме и подчеркнул неадекватность защиты права на неприкосновенность личной жизни в Интернете.

5. Целью настоящего доклада, который опирается на предыдущий анализ, является выявление угроз, которые несут новые средства и способы слежения за сообщениями для прав человека, включая право на неприкосновенность личной жизни и свободу выражения мнений.

6. Для описания наиболее распространенных способов слежения в докладе используются следующие термины:

a) слежение за сообщениями: мониторинг, перехват, сбор, хранение и удержание информации, которая была передана, ретранслирована или генерирована через коммуникационные сети;

b) коммуникационные данные: информация о сообщениях частных лиц (электронная почта, телефонные переговоры и полученные и отправленные текстовые сообщения, сообщения в социальных сетях и размещение постов), личности пользователей, сетевых учетных записях, адресах, посещенных вебсайтах, прочитанных, просмотренных или прослушанных книгах и других материалах, произведенных поисковых запросах, использованных ресурсах, обмене информацией (отправители и получатели сообщений, лица, с которыми

проводился обмен информацией, друзья, семья, знакомые), времени контактов и местонахождении частных лиц, включая близость к другим лицам);

c) фильтрация Интернета: автоматический или механический мониторинг интернет-контента (включая веб-сайты, блоги и онлайновые источники массовой информации, а также электронную почту) в целях ограничения или запрещения конкретных текстов, изображений, веб-сайтов, сетей, протоколов, услуг или деятельности.

II. Деятельность Специального докладчика

7. В течение отчетного периода Специальный докладчик принял участие в многочисленных международных и национальных мероприятиях, связанных с вопросами, которые он рассматривал в своих предыдущих докладах, такими как свобода выражения мнений в Интернете, недопущение ненавистнических высказываний и защита журналистов. Он уделял особое внимание национальным инициативам по поощрению защиты журналистов; в данном контексте он участвовал в совещаниях по таким инициативам, разработанным в Бразилии, Колумбии, Гондурасе и Мексике. Он также принял участие в Межучрежденческом совещании Организации Объединенных Наций по вопросам безопасности журналистов и безнаказанности, которое состоялось в Вене в ноябре 2012 года.

8. Его последний доклад Генеральной Ассамблее Организации Объединенных Наций был сосредоточен на недопущении ненавистнических высказываний и разжигания ненависти[1]. Эта же тема рассматривалась на параллельном мероприятии в ходе сессии Генеральной Ассамблеи, которое было организовано совместно Специальным докладчиком и Специальным советником по предупреждению геноцида в феврале 2013 года. В том же месяце он продолжил рассмотрение этих вопросов в ходе запуска в Женеве "Рабатского плана действий о запрете пропаганды национальной, расовой и религиозной ненависти, представляющей собой подстрекательство к дискриминации, вражде и насилию" и в ходе пятого Глобального форума Альянса цивилизаций Организации Объединенных Наций в Вене.

9. Специальный докладчик осуществил поездку в Гондурас с 7 по 14 августа 2012 года. Его основные выводы и рекомендации по итогам этого визита содержатся в приложении к настоящему докладу (A/HRC/20/40/Add.1). Он получил приглашение от индонезийского правительства посетить страну в январе 2013 года. К сожалению, правительство обратилось с просьбой о переносе этого визита, а новые даты поездки все еще ожидают подтверждения.

10. При подготовке данного доклада Специальный докладчик ознакомился с соответствующими исследованиями и провел консультации с экспертами по вопросам, относящимся к слежению за сообщениями. В декабре 2012 года он принял участие в рабочем совещании по проблеме электронного слежения и прав человека, которое было организовано Фондом электронных рубежей. В феврале 2013 года он организовал экспертные консультации по подготовке данного доклада, которые состоялись одновременно с проведением совещания "Всемирная встреча на высшем уровне по вопросам информационного общества + 10", состоявшегося в Организации Объединенных Наций по вопросам образования, науки и культуры (ЮНЕСКО) в Париже, где он также участвовал в первом пленарном заседании экспертной группы.

[1] A/67/357.

III. Эволюция технологий слежения

11. Инновации в области технологий расширили возможности коммуникации и свободы выражения мнений, обеспечивая условия для анонимности, быстрого обмена информацией и межкультурного диалога. В то же время технологические изменения также создали новые возможности для слежения и вмешательства в личную жизнь со стороны государства.

12. Начиная с зарождения первых форм дальней связи государства стремились осуществлять перехват и контроль частных сообщений в интересах правопорядка и национальной безопасности. Сообщения позволяют узнать в высшей степени личную и интимную информацию, в том числе о предыдущей или будущей деятельности частных лиц или групп. Сообщения представляют собой ценный источник доказательств, на основе которых государство может предотвращать и преследовать серьезные преступления или предупреждать потенциальные чрезвычайные ситуации в области национальной безопасности.

13. Сделанные в течение XX века технологические инновации изменили характер и последствия слежения за сообщениями. Существенно возросли число каналов связи и частота передачи сообщений. Переход от фиксированной телефонной связи к мобильной и снижение стоимости коммуникационных услуг привели к резкому росту использования телефона. С наступлением эпохи Интернета появился ряд новых инструментов и приложений для бесплатного общения или по весьма приемлемым ценам. Эти достижения открыли новые коммуникационные возможности, содействовали глобальному обмену информацией и идеями и усилили потенциал экономического роста и перемен в обществе.

14. По мере развития информационных и коммуникационных технологий эволюционировали и средства, с помощью которых государства стремились контролировать частные коммуникации. С участившимся использованием телефонов стал применяться перехват телефонных сообщений, который заключается в подсоединении подслушивающего устройства к телефонной линии для прослушивания частных телефонных переговоров. С заменой в 1990-х годах аналоговых телефонных сетей на волоконно-оптические и цифровые коммутаторы государства перепроектировали сетевые технологии для включения в них возможностей перехвата коммуникаций ("бэкдоры") в целях санкционирования государственного слежения, сделав современные телефонные сети дистанционно доступными и контролируемыми.

15. Динамичный характер технологий не только изменил способы слежения, но и набор объектов возможного контроля. Позволив создание различных возможностей для общения и обмена информацией, Интернет также облегчил накопление больших объектов транзакционных данных частными лицами и о частных лицах. Эта информация, известная как коммуникационные данные или метаданные, содержит персональные сведения о частных лицах, их местонахождении, онлайн-активности, логинах и связанную с этим информацию об адресах электронной почты и сообщениях, которые они отправляют или получают. Коммуникационные данные являются долгохранимыми, доступными и допускающими возможность поиска объекта, а их раскрытие и использование государственными органами практически не регулируется. Анализ этих данных имеет весьма разоблачительный и интрузивный характер, в особенности когда данные комбинируются и обобщаются. По существу государства во все большей степени используют коммуникационные данные для оказания содействия в проведении расследований правоохранительными органами или органами национальной безопасности. Государства также заставляют хранить и удерживать

коммуникационные данные для предоставления им возможности осуществлять отслеживание во времени.

16. Технологические изменения сопровождались переменами в отношении к отслеживанию сообщений. Когда официальное прослушивание телефонных разговоров впервые было начато в Соединенных Штатах Америки, оно проводилось на ограниченной основе и весьма неохотно санкционировалось судами[2]. Как таковое оно рассматривалось в качестве серьезной угрозы праву на неприкосновенность личной жизни, и поэтому его использование должно было ограничиваться целями выявления и преследования наиболее тяжких преступлений. Однако с течением времени государства расширили свои полномочия по слежению, понизив порог ограничений и расширив набор оснований для такого слежения.

17. Во многих странах существующие законодательство и практика не были пересмотрены и обновлены в целях реагирования на угрозы и вызовы слежения за сообщениями в цифровую эпоху. Традиционные понятия доступа к письменной корреспонденции, например, были инкорпорированы в законы, позволяющие получать доступ к персональным компьютерам, другой информации и коммуникационным технологиям без учета широкого использования таких устройств и последствий для осуществления прав человека. В то же время отсутствие законов о регулировании глобального слежения за сообщениями и средств предоставления доступа к ним привело к появлению произвольной практики слежения, которая находится вне контроля независимых органов. Сегодня во многих государствах доступ к коммуникационным данным может предоставляться широкому кругу государственных органов в разнообразных целях зачастую без судебной санкции и независимого надзора. Кроме того, государства стремятся внедрить способы слежения, подразумевающие экстерриториальный характер.

18. Правозащитные механизмы в равной степени проявляли медлительность в оценке правозащитных последствий использования Интернета и новых технологий на слежение за сообщениями и доступ к коммуникационным данным. Последствия расширения полномочий и практики государств по слежению для прав на неприкосновенность личной жизни и на свободу мнений и их свободное выражение пока еще всесторонним образом не рассмотрены Советом по правам человека, мандатариями специальных процедур и договорными органами по правам человека. В данном докладе делается попытка исправить это.

[2] В первом судебном постановлении, санкционировавшем прослушивание телефонных разговоров, судья Верховного суда Соединенных Штатов Брэндис заявил о своем решительном несогласии, отметив, что прослушивание телефонных разговоров является "более утонченным и влекущим серьезные последствия средством вторжения в личную жизнь", которое не может быть оправдано по Конституции. Этот именитый юрист сделал ужасающее по своей точности предсказание: "Однажды могут быть разработаны средства, с помощью которых правительство, не вынимая документов из секретных ячеек, сможет представить их в суде и получит возможность демонстрировать присяжным глубоко личные подробности частной жизни. Прогресс в области психологии и смежных наук может позволить создать средства для изучения тайных убеждений, мыслей и переживаний". *Olmstead v. United States*, 277 U.S. 438 (1928).

IV. Международно-правовая база в области прав человека

19. Право на свободу мнений и их свободное выражение гарантируется статьей 19 Всеобщей декларации прав человека и статьей 19 Международного пакта о гражданских и политических правах, которые утверждают, что каждый человек имеет право беспрепятственно придерживаться мнений и искать, получать и распространять всякого рода информацию и идеи с помощью любых средств массовой информации и независимо от государственных границ. На региональном уровне данное право защищается Африканской хартией прав человека и народов (статья 9), Американской конвенцией по правам человека (статья 13) и Конвенцией о защите прав человека и основных свобод (статья 10).

20. Как на международном, так и на региональном уровне неприкосновенность личной жизни также безоговорочно признается в качестве одного из основополагающих прав человека. Право на неприкосновенность личной жизни закреплено во Всеобщей декларации прав человека (статья 12), Международном пакте о гражданских и политических правах (МПГПП, статья 17), Конвенции о правах ребенка (статья 16) и Международной конвенции о защите права всех трудящихся-мигрантов и членов их семей (статья 14). На региональном уровне право на неприкосновенность личной жизни защищается Европейской конвенцией по правам человека (статья 8) и Американской конвенцией по правам человека (статья 11).

21. Несмотря на широко распространенное признание обязательства по защите неприкосновенности личной жизни, конкретное содержание данного права не было полностью раскрыто международными механизмами по защите прав человека в момент его включения в вышеупомянутые правозащитные договоры. Отсутствие четкого определения содержания данного права создало трудности с его осуществлением и обеспечением соблюдения[3]. Поскольку право на неприкосновенность личной жизни является ограниченным правом, его толкование создает проблемы с определением того, что составляет сферу личной жизни, и понятийной базы "общественного интереса". Произошедшие в последние десятилетия фундаментальные достижения в области коммуникационных и информационных технологий также необратимо изменили наше понимание границ между личным и общественным.

22. Неприкосновенность личной жизни может быть определена как презумпция того, что частные лица должны иметь определенное поле для самостоятельного развития, взаимодействия и свободы, "частную сферу" во взаимодействии с другими лицами или без него, свободную от вмешательства государства и от чрезмерного инициативного вмешательства со стороны других незваных частных лиц[4]. Право на неприкосновенность личной жизни также представляет собой способность частных лиц определять, кто является держателем информации о них и каким образом используется эта информация.

23. В целях осуществления частными лицами своего права на неприкосновенность личной жизни в области коммуникаций они должны иметь возможность удостовериться, что коммуникации остаются конфиденциальными, безопасными и, если они того пожелают, анонимными. Неприкосновенность коммуникаций означает, что частные лица могут обмениваться информацией и идеями в пространстве, которое находится вне досягаемости других членов общества,

[3] UNESCO, Global Survey on Internet Privacy and Freedom of Expression, 2012, p. 51.

[4] Lord Lester and D. Pannick (eds.). *Human Rights Law and Practice.* London, Butterworth, 2004, para. 4.82.

частного сектора и в конечном счете самого государства. Безопасность коммуникаций означает, что частные лица должны иметь возможность удостовериться, что их сообщение получают только обозначенные ими адресаты без вмешательства или изменений и что получаемые ими сообщения в равной степени свободны от вторжения. Анонимность коммуникаций является одним из наиболее важных достижений, обеспечиваемых Интернетом, и позволяет частным лицам выражать свое мнение свободно, не опасаясь возмездия или осуждения.

A. Взаимосвязи между правом на неприкосновенность личной жизни и правом на свободу мнений и их свободное выражение

24. Право на неприкосновенность личной жизни часто понимается как одно из базовых условий реализации свободы выражения мнений. Чрезмерное вторжение в личную жизнь может как напрямую, так и косвенно ограничивать свободное развитие идей и свободный обмен ими. Ограничения на анонимность при передаче сообщений, например, оказывают очевидное пугающее воздействие на жертв всех форм насилия и посягательств, которые могут неохотно предоставлять соответствующую информацию, опасаясь двойной виктимизации. В этом отношении в статье 17 Пакта прямо упоминается о защите от вмешательства в "тайну корреспонденции" − термин, который должен толковаться как охватывающий все виды коммуникации как в онлайн-, так и в офлайн-режиме[5]. Как отметил Специальный докладчик в своем предыдущем докладе[6], право на неприкосновенность личной корреспонденции налагает всеобъемлющее обязательство на государство обеспечивать, чтобы электронная почта и другие виды онлайн-сообщений на деле доставлялись указанному адресату без вмешательства или контроля со стороны государственных органов или третьих сторон[7].

25. Комитет по правам человека проанализировал содержание права на неприкосновенность личной жизни (статья 17) в своем замечании общего порядка № 16 (1988 год), в соответствии с которым цель статьи 17 состоит в защите частных лиц от любого незаконного или произвольного вмешательства в их личную жизнь, включая семейную жизнь, жилище или тайну корреспонденции, а национальная правовая основа должна обеспечивать защиту этого права. Это положение налагает особые обязательства, относящиеся к защите личной жизни в области коммуникаций, подчеркивая, что "корреспонденция должна доставляться адресату без перехвата, не вскрываться или прочитываться так или иначе". "Должно быть запрещено электронное или иное наблюдение, перехватывание телефонных, телеграфных или иных сообщений, прослушивание и запись телефонных разговоров"[8]. В данном замечании общего порядка также указывается, что "законом должны регулироваться сбор и хранение личной информации государственными властями или частными лицами или органами в компьютерах, банках данных или как-либо иначе"[9]. На момент принятия данного замечания общего порядка понимание влияния достижений в области информационных и коммуникационных технологий на право на неприкосновенность личной жизни было весьма слабым.

[5] Комментарий к МПГПП, пункт 401.
[6] A/HRC/17/23.
[7] Комментарий к МПГПП, пункт 401.
[8] Центр гражданских и политических прав (ЦГПП), замечание общего порядка № 16 (замечания общего порядка), пункт 8.
[9] *Там же*, пункт 10.

26. В своем замечании общего порядка № 34 (2011 год) о праве на свободу выражения мнений Комитет по правам человека отметил, что государства-участники должны учитывать существенную степень, в которой прогресс в области информационных и коммуникационных технологий изменил коммуникационную практику. Комитет также призвал государства-участники принять все необходимые меры для укрепления независимости этих новых средств массовой информации. В этом замечании общего порядка также анализируется связь между защитой личной жизни и свободой выражения мнений и рекомендуется, чтобы государства-участники уважали элемент права на свободу выражения мнений, который включает в себя ограниченную привилегию журналистов не раскрывать источники информации[10].

27. Существуют также противоречия между правом на неприкосновенность личной жизни и правом на свободу выражения мнений, например, когда информация, рассматривающаяся как персональная, распространяется через средства массовой информации. В этом смысле в статье 19 (3) предусматриваются ограничения на свободу выражения мнений и информации для защиты прав других лиц. Тем не менее по аналогии со всеми допустимыми ограничениями права на свободу выражения мнений (см. ниже), здесь необходимо строго соблюдать принцип соразмерности, поскольку в ином случае существует опасность нарушения свободы выражения мнений. В частности, в политической жизни не все нападки на добрую репутацию политиков должны быть разрешены, поскольку в ином случае свобода выражения мнений и информации будет лишена ее ключевой значимости для процесса формирования политических убеждений[11] в рамках отстаивания транспарентности и борьбы с коррупцией. Международная практика на региональном уровне показывает, что в случае возникновения конфликта между неприкосновенностью личной жизни и свободой выражения мнений следует ссылаться на общественный интерес в соответствующих вопросах[12].

B. Допустимые ограничения неприкосновенности личной жизни и свободы выражения мнений

28. Рамки статьи 17 МПГПП предоставляют возможность для необходимой, законной и соразмерной рестрикции права на неприкосновенность личной жизни посредством допустимых ограничений. В отличие от положений пункта 3 статьи 19, в котором разъясняются элементы допустимых ограничительных критериев[13], формулировка статьи 17 не содержит ограничительной оговорки. Несмотря на эти различия в формулировках, подразумевается, что статья 17 Пакта должна также толковаться как содержащая элементы допустимых ограничительных критериев, уже описанных в других замечаниях общего порядка Комитета по правам человека[14].

[10] Замечание общего порядка № 34 к МПГПП.

[11] Nowak, Manfred, United Nations Covenant on Civil and Political Rights: CCPR Commentary (1993), p. 462.

[12] UNESCO, Global Survey on Internet Privacy and Freedom of Expression, 2012, pp. 53 and 99.

[13] Перечни допустимых ограничений также включены в статью 12 (3) о праве на свободу передвижения и свободу на выбор местожительства; в статью 18 (3) о праве на свободу мысли, совести и религии; статью 21 о праве на свободу мирных собраний; и статью 22 (2) о праве на свободу ассоциаций.

[14] *Там же*.

29. В этом отношении позиция Специального докладчика заключается в том, что право на неприкосновенность личной жизни должно быть подвержено таким же допустимым ограничительным критериям, что и право на свободу передвижения, как это разъясняется в замечании общего порядка № 27[15]. В соответствии с этим замечанием критерии включают в себя, помимо прочего, следующие элементы:

a) любые ограничения должны быть предусмотрены законом (пункты 11−12);

b) существо права человека не является предметом ограничений (пункт 13);

c) ограничения должны являться необходимыми в демократическом обществе (пункт 11);

d) любые дискреционные полномочия по применению ограничений не должны быть неограниченными (пункт 13);

e) для допустимости ограничений недостаточно того, чтобы они служили достижению одной из перечисленных законных целей. Они должны являться необходимыми для достижения законной цели (пункт 14);

f) Ограничительные меры должны соответствовать принципу соразмерности; они должны являться уместными для выполнения своей защитной функции; они должны представлять собой наименее ограничительное средство из числа тех, с помощью которых может быть достигнут желаемый результат; и они должны являться соразмерными защищаемому интересу (пункты 14−15).

C. Последние соображения международных механизмов по защите прав человека

30. В предыдущих докладах Специальный докладчик оценил воздействие Интернета на осуществление права на свободу мнений и их свободное выражение (A/HRC/17/27 и A/66/290). Он отметил, что, хотя пользователи Интернета могут обладать относительной анонимностью в Интернете, государства и частные субъекты также имеют доступ к новым технологиям для мониторинга и сбора информации о коммуникациях и деятельности частных лиц. Такие технологии потенциально могут нарушать право на неприкосновенность личной жизни, подрывая таким образом доверие и безопасность в Интернете и препятствуя свободному обмену информацией и идеями в онлайновом режиме. Специальный докладчик настоятельно призвал государства принять эффективные законы о защите неприкосновенности личной жизни и персональных данных в соответствии с правозащитными стандартами и предпринять все необходимые меры к обеспечению того, чтобы частные лица могли анонимно выражать свое мнение в онлайновом режиме[16].

31. Другие мандатарии специальных процедур рассматривали вопрос о вмешательстве в осуществление права на неприкосновенность личной жизни. Специальный докладчик по вопросу о поощрении и защите прав человека и основных свобод в ходе борьбы с терроризмом исследовал изменения в практике слежения и технологиях, которые негативно влияли на право на неприкосновен-

[15] См. также замечание общего порядка № 34 к МПГПП.

[16] A/HRC/17/27, пункт 22.

ность личной жизни под предлогом борьбы с терроризмом[17]. Специальный докладчик подчеркнул, что эти меры не только привели к нарушениям права на неприкосновенность личной жизни, но также оказали отрицательное воздействие на права в области надлежащего судопроизводства и права на свободу передвижения, свободу ассоциации и свободу выражения мнений. Он настоятельно призвал правительства подробно пояснить, каким образом их политика в области слежения согласуется с принципами соразмерности и необходимости в соответствии с международными правозащитными стандартами и какие меры были приняты для защиты от злоупотреблений. Специальный докладчик также призвал принять всеобъемлющее законодательство по защите данных и личной жизни и учредить сильные независимые органы по надзору, уполномоченные пересматривать интрузивные методы слежения и обработки информации личного характера. Кроме того, он призвал к проведению исследований и развитию ресурсов, направленных на совершенствование технологий по обеспечению неприкосновенности личной жизни.

32. Другие правозащитные механизмы также в последнее время уделяли внимание вопросу о воздействии, которое оказывает слежение за сообщениями на защиту прав на неприкосновенность личной жизни и свободу выражения мнений. Комитет по правам человека, например, выразил озабоченность в связи с утверждениями о мониторинге использования Интернета и блокировании доступа к некоторым веб-сайтам со стороны государств[18] и рекомендовал пересмотреть законодательство, предоставляющее исполнительной власти широкие полномочия в области слежения за электронными сообщениями[19]. В рамках Универсального периодического обзора также были сделаны рекомендации, например, по обеспечению того, чтобы в законодательстве о регулировании Интернета и других новых коммуникационных технологий соблюдались международные обязательства в области прав человека[20].

V. Способы слежения за сообщениями

33. Современные технологии и средства, позволяющие государствам вторгаться в личную жизнь частных лиц, несут угрозу размывания разделительной линии между частной и общественной сферами. Они способствуют интрузивному и произвольному контролю деятельности частных лиц, которые могут даже и не знать о том, что они подвергаются такому слежению, не говоря уже о противодействии этому. Технологические достижения снимают ограничения с возможностей государства по осуществлению слежения с точки зрения охвата или продолжительности. Снижение стоимости технологий и хранения данных устраняет финансовые или практические препятствия осуществлению слежения. По сути, в настоящее время государство обладает большими, чем когда-либо, возможностями осуществления одновременного, интрузивного, адресного или широкомасштабного слежения.

[17] A/HRC/13/37.
[18] CCPR/C/IRN/CO/3.
[19] CCPR/C/SWE/CO/6.
[20] A/HRC/14/10.

A. Адресное слежение за сообщениями

34. Государства имеют доступ к различным методам и технологиям слежения за конкретными частными сообщениями. Технические возможности перехвата в реальном времени позволяют государствам прослушивать и записывать телефонные разговоры любого частного лица, использующего фиксированную линию связи или мобильный телефон, посредством применения технических средств государственного слежения, которые все коммуникационные сети обязаны встраивать в свои системы[21]. Местоположение частных лиц может быть установлено, а их текстовые сообщения могут быть прослушаны и записаны. За счет подключения устройства слежения к интернет-кабелю, относящегося к определенному помещению или лицу, государственные власти также могут контролировать интернет-активность частных лиц, включая посещение ими веб-сайтов.

35. Доступ к хранящемуся контенту электронной почты и сообщений частных лиц, в дополнение к другим соответствующим коммуникационным данным, может быть получен через интернет-компании и провайдеров услуг. Озабоченность вызывает инициатива Европейского агентства по стандартизации и Европейского института стандартов связи, направленная на то, чтобы задействовать провайдеров "облачных" услуг[22] встраивать "законные технические возможности для перехвата" в "облачные" технологии, с тем чтобы государственные органы могли получать прямой доступ к контенту, хранимому этими провайдерами, включая электронную почту, сообщения и голосовую почту[23].

36. Государства могут с помощью различных методов отслеживать перемещения конкретных мобильных телефонов, определять всех частных лиц с мобильными телефонами в рамках определенного района и перехватывать звонки и текстовые сообщения. Некоторые государства используют мобильные мониторинговые устройства перехвата, называемые "ловушками международного идентификатора абонента мобильной связи (IMSI)", которые могут устанавливаться временно (например, при проведении протестов или демонстраций) или на постоянной основе (например, в аэропортах или других местах пересечения границы). Эти ловушки маскируются под базовую станцию сотовой телефонной сети, посылая сигналы на мобильный телефон и отвечая на них в целях получения номера карточки индивидуального модуля идентификации абонента (SIM) из всех мобильных телефонов в пределах определенной территории.

37. Государства также все чаще приобретают программное обеспечение, которое может использоваться для проникновения в персональные компьютеры, мобильные телефоны или другие цифровые устройства[24]. Программное обеспечение по агрессивному проникновению в компьютерные сети, включая так на-

[21] См., например, Закон Соединенных Штатов о коммуникационном содействии правоохранительным органам 1994 года (Соединенные Штаты); Закон о телекоммуникациях 1997 года, часть 15 (Австралия); Закон о регулировании полномочий следствия 2000 года, разделы 12−14 (Великобритания); Закон о телекоммуникациях (средствах перехвата) 2004 года.

[22] "Облачный" провайдер предоставляет услуги по хранению данных в объединенной онлайновой сетевой структуре.

[23] ETSI DTR 101 567 VO.0.5 (2012-14), Draft Technical Report: Lawful Interception (LI); Cloud/Virtual Services (CLI).

[24] Toby Mendel, Andrew Puddephatt, Ben Wagner, Dixi Hawtin, and Natalia Torres, Global Survey on Internet Privacy and Freedom of Expression, *UNESCO Series on Internet Freedom* (2012), p. 41.

зываемые "программы-трояны" (также известные как шпионящее или вредоносное ПО), может использоваться для включения микрофона или камеры устройства в целях отслеживания осуществляемой на нем деятельности и в целях доступа к хранящейся на устройстве любой информации либо ее изменения или удаления. Такое программное обеспечение, практически не поддающееся обнаружению, позволяет государству полностью контролировать зараженное устройство.

B. Слежение за массовыми коммуникациями

38. Задачи и материально-технические препятствия в области осуществления слежения в массовом масштабе продолжают быстро снижаться по мере распространения технологий, позволяющих вести широкий перехват, мониторинг и анализ коммуникаций. В настоящее время некоторые государства обладают техническими возможностями по отслеживанию и записи сообщений в Интернете и телефонных сообщений в национальном масштабе. С помощью установки устройств слежения на волоконно-оптических кабелях, через которые проходит основной поток цифровой коммуникационной информации, и применяя технологии распознавания слов, голоса и речи, государства могут достичь практически полного контроля за телефонными и онлайновыми сообщениями. Как сообщается, такие системы были внедрены, например, египетским и ливийским правительствами в преддверии "арабской весны"[25].

39. Во многих государствах обязательное хранение данных упрощает массовый сбор коммуникационных данных, которые затем могут стать предметом вмешательства и анализа. Технологии позволяют государствам отслеживать телефонные переговоры и текстовые сообщения для выявления использования определенных слов, голосов или фраз или для контроля веб-деятельности в целях определения, когда то или иное частное лицо заходит на определенные вебсайты или получает доступ к конкретным онлайновым ресурсам. Могут проектироваться так называемые "черные ящики" для проверки проходящих через Интернет данных в целях фильтрации и анализа всей информации об онлайновой активности. Данный метод, называемый "глубоким анализом пакетов (DPI)", позволяет государствам выйти за пределы получения простой информации о сайтах, посещаемых частными лицами, и анализировать контент посещаемых веб-сайтов. Как сообщается, "глубокий анализ пакетов" применялся, например, государствами, столкнувшимися с недавними народными восстаниями на Ближнем Востоке и в регионе Северной Африки[26].

40. Мониторинг социальных сетей является еще одним инструментом, который в настоящее время регулярно используется государствами. Государства обладают возможностями физического мониторинга активности на сайтах социальных сетей, в блогах и на медийных каналах для выявления подключений и связей, убеждений и объединений и даже местонахождения соответствующих лиц. Государства также могут применять наиболее передовые технологии извлечения данных в отношении находящейся в общественном доступе информации или в отношении коммуникационных данных, предоставляемых провайдерами-посредниками. Кроме того, на более базовом уровне у государств появи-

[25] European Parliament, Directorate-General for External Policies, Policy Department, After the Arab Spring: New Paths for Human Rights and the Internet in European Foreign Policy (2012), pp. 9-10.

[26] Mendel *et al.*, *op. cit.*, p. 43.

лись технические средства для получения имен пользователей и паролей на сайтах социальных сетей, таких как "Фейсбук"[27].

C. Доступ к коммуникационным данным

41. Помимо перехвата и отслеживания содержания сообщений частных лиц, государства могут также пытаться получить доступ к коммуникационным данным, хранящимся у провайдеров-посредников и интернет-компаний. Поскольку частный сектор постепенно собирает все большее количество различных данных, которые содержат чувствительную информацию о ежедневной жизни людей, а частные лица и предприятия сохраняют содержание своих сообщений, в том числе в голосовой почте, электронной почте и документах при помощи провайдеров-посредников, доступ к коммуникационным данным становится все более продуктивным методом слежения, используемым государствами.

42. Коммуникационные данные, собранные провайдерами-посредниками, включая крупные интернет-компании, могут использоваться государствами для составления всестороннего портрета соответствующих частных лиц. Доступ даже, казалось бы, к безобидным транзакционным записям о сообщениях и их анализ могут позволить составить картину личной жизни частных лиц, включая состояние здоровья, политические и религиозные взгляды и/или участие в политических и религиозных организациях, общение с другими людьми и интересы, раскрывая столько же или даже больше подробностей, которые могли бы быть получены из содержания самих сообщений[28]. Комбинируя информацию о связях людей, их местонахождении, личности и деятельности, государства могут отслеживать перемещение частных лиц и их деятельность в самых различных областях, в том числе, где они путешествуют и получают образование, какую литературу они читают или с кем они общаются.

43. Примеры доступа государств к коммуникационным данным быстро увеличиваются. За три года отчетности компании "Гугл" о получаемых запросах на предоставление коммуникационных данных число таких запросов практически удвоилось с 12 539 за последние шесть месяцев 2009 года до 21 389 за последние шесть месяцев 2012 года[29]. В Соединенном Королевстве, где правоохранительные органы уполномочены сами санкционировать свои собственные запросы на получение коммуникационных данных, сообщается о подаче 500 000 таких запросов ежегодно[30]. В Республике Корея, население которой насчитывает примерно 50 млн. человек, сообщается о подаче приблизительно 37 млн. запросов на предоставление коммуникационных данных ежегодно[31].

[27] European Parliament, *op. cit.*, p. 6.

[28] Alberto Escudero-Pascual and Gus Hosein, “Questioning lawful access to traffic data”, *Communications of the ACM*, Volume 47 Issue 3, March 2004, pp. 77–82.

[29] См. http://www.google.com/transparencyreport/userdatarequests/.

[30] См. http://www.intelligencecommissioners.com/docs/0496.pdf.

[31] Газета "Money Today", 23 октября 2012 года, в которой приводится обнародованная по запросу члена парламента Ю Сын Хи информация корейской Комиссии по вопросам коммуникаций в рамках подготовки к ежегодному Национальному аудиту 2013 года, http://www.mt.co.kr/view/mtview.php?type=1&no=2012102309430241764&outlink=1.

D. Фильтрация и цензура Интернета

44. Достижения в области технологий не только упростили перехват сообщений и доступ к ним в отдельных случаях, но также позволили государствам проводить широкую и даже общенациональную фильтрацию онлайновой активности. Во многих странах фильтрация Интернета проводится под предлогом поддержания социального согласия или искоренения "ненавистнической риторики", однако на деле используется для подавления инакомыслия, критических выступлений или оппозиционной деятельности.

45. Упомянутые выше технологии фильтрации также способствуют мониторингу веб-активности, с тем чтобы позволить государствам выявлять запрещенные изображения, высказывания, адреса сайтов или другой контент, подвергать его цензуре или изменять. Государства могут использовать такие технологии для выявления использования отдельных слов и предложений в целях их цензурирования или регулирования их применения или для выявления лиц, которые их используют. В странах с высоким уровнем проникновения государства в Интернет фильтрация Интернета, как сообщается, позволяет подвергать цензуре содержание веб-сайтов и сообщений и упрощает наблюдение за правозащитниками и оппозиционерами[32].

46. В дополнение к технологиям, облегчающим фильтрацию и цензуру, многие государства используют ручную интернет-фильтрацию путем создания онлайновой полиции и инспекторов в целях физического мониторинга содержания веб-сайтов, социальных сетей, блогов и других форм медийных каналов. В некоторых государствах "киберполиция" уполномочена инспектировать и контролировать Интернет, осуществляя поиск веб-сайтов и критических узлов веб-сайтов (в частности, онлайновых дискуссионных форумов) в целях блокирования или закрытия веб-сайтов во всех случаях, когда содержащийся на них контент не одобряется правительством, включая критику руководства страны. Обязанности по такому слежению возложены на частных посредников, в частности поисковые системы и платформы социальных сетей путем принятия законов, которые расширяют ответственность за размещение запрещенного контента с первоначальных выразителей мнения на всех посредников.

E. Ограничения анонимности

47. Одним из наиболее важных достижений, которому способствовало наступление эпохи Интернета, стала возможность получения анонимного доступа к информации и ее распространения, а также безопасного общения без необходимости раскрытия личности. Первоначально это стало возможным благодаря отсутствию "уровня идентификации личности" при доступе к Интернету; изначально было невозможно выяснить, кто стоит за конкретным сообщением, адресом электронной почты или даже за соответствующим компьютером. Тем не менее во имя безопасности и поддержания правопорядка государства постепенно стали ликвидировать возможности для анонимного общения. Во многих государствах частные лица должны раскрывать свою личность в интернет-кафе, а их транзакции на общедоступных компьютерах должны регистрироваться. Идентификация и регистрация все чаще требуются при покупке сим-карты или

[32] European Parliament, Directorate-General for External Policies, Policy Department, After the Arab Spring: New Paths for Human Rights and the Internet in European Foreign Policy (2012), p. 12.

сотового телефона, при посещении определенных крупных веб-сайтов или при размещении комментариев на сайтах средств массовой информации или в блогах.

48. Ограничения на анонимность способствуют отслеживанию государствами сообщений, упрощая идентификацию частных лиц, получающих или распространяющих запрещенный контент, делая таких частных лиц более уязвимыми для других форм государственного слежения.

49. В этом смысле ограничения на анонимность оказывают отрицательное воздействие, препятствуя свободному распространению информации и идей. Они также могут приводить к исключению частных лиц де-факто из жизненно важных социальных сфер, подрывая их права на выражение мнений и на информацию и обостряя социальное неравенство. Кроме того, ограничения на анонимность позволяют частному сектору собирать и компилировать значительный объем данных, что накладывает на корпоративных субъектов существенное бремя и ответственность по защите неприкосновенности личной жизни и безопасности таких данных.

VI. Вызывающие озабоченность проблемы, связанные с национальными правовыми нормами

50. Как правило, законодательство не идет в ногу с изменениями в области технологий. В большинстве государств правовые нормы, отвечающие на современные вызовы в области отслеживания сообщений, либо отсутствуют, либо являются неадекватными. В результате государства все чаще пытаются оправдать использование новых технологий с помощью старой нормативно-правовой базы и не признают, что имеющиеся у них в настоящее время широкие технические возможности выходят далеко за пределы того, что предусматривалось такой нормативно-правовой базой. Во многих странах данный факт означает, что расплывчатые и широко понимаемые правовые нормы используются в качестве обоснования для легализации и санкционирования использования серьезных интрузивных методов. В отсутствие четких законов, разрешающих применение таких технологий и методов и устанавливающих пределы их использования, частные лица не в состоянии не только предвидеть их применение, но даже знать о нем. В то же время принимаются законы о расширении охвата исключений по соображениям национальной безопасности, предусматривающие легализацию интрузивных методов слежения без надзора или независимого наблюдения за ними.

51. Неадекватные правовые нормы повышают степень подверженности частных лиц нарушениям их прав человека, включая право на неприкосновенность личной жизни и право на свободу выражения мнений. Они также оказывают негативное влияние на определенные группы населения – например, членов некоторых политических партий, членов профсоюзов или национальные, этнические и языковые меньшинства, − которые могут быть в большей степени подвержены слежению за их сообщениями со стороны государства. В отсутствие надежных механизмов правовой защиты журналисты, правозащитники и политические активисты могут подвергаться произвольному слежению за их деятельностью.

52. Факты слежения за правозащитниками во многих странах должным образом задокументированы. В данном контексте правозащитники и политические активисты сообщают о прослушивании их телефонных переговоров, про-

смотре их электронной почты и об отслеживании их передвижений. Журналисты также подвержены повышенному риску стать жертвами отслеживания их сообщений в силу их зависимости от онлайновых средств связи. В целях получения и поиска информации из конфиденциальных источников, в том числе от разоблачителей, журналисты должны иметь возможность полагаться на неприкосновенность, безопасность и анонимность своих контактов. Среда, в которой слежение широко распространено и не регламентировано надлежащими правовыми процедурами или судебным надзором, не может обеспечить презумпцию защиты источников информации. Даже узкое, нетранспарентное, не задокументированное и служебное слежение может иметь негативные последствия в отсутствие тщательного и публичного документирования использования этой практики и известной системы контроля и противовесов для предотвращения злоупотреблений в данной области.

53. В нижеследующих подразделах перечисляются общие вызывающие озабоченность вопросы, связанные с законами, которые позволяют государствам осуществлять отслеживание сообщений в обстоятельствах, которые угрожают правам на свободу выражения мнений и на неприкосновенность личной жизни.

A. Отсутствие судебного надзора

54. Несмотря на то, что традиционно для отслеживания сообщений требовалась судебная санкция, данное требование все чаще ослабляется или отменяется. В некоторых странах перехват сообщений может быть санкционирован министром, его заместителем или комитетом. В Великобритании, например, перехват сообщений санкционируется Государственным секретарем[33]; в Зимбабве он санкционируется Министром транспорта и коммуникаций[34]. Отслеживание сообщений все чаще может санкционироваться на широкой и неизбирательной основе без необходимости для правоохранительных органов представлять доказательную базу, обосновывающую необходимость слежения в каждом конкретном случае.

55. Многие государства освободили правоохранительные органы от обязанности информировать суд о продолжающемся наблюдении после вынесения судебного предписания о перехвате сообщений. Например, в соответствии с кенийским Законом о предупреждении терроризма 2012 года перехват сообщений может проводиться в течение неопределенного времени без какого бы то ни было требования для правоохранительных органов отчитываться перед судом или запрашивать у него санкцию на продление слежения. Некоторые государства налагают временные ограничения на исполнение судебных предписаний на перехват сообщений, однако позволяют правоохранительным органам возобновлять такие предписания неоднократно и на неограниченной основе.

56. Даже когда судебная санкция требуется по закону, зачастую она де-факто является произвольным одобрением запросов правоохранительных органов. Это особенно касается случаев, когда объем доказательств, который должны предъявить правоохранительные органы, является небольшим. Например, угандийский Закон о регулировании перехвата сообщений 2010 года требует от правоохранительных органов только демонстрации наличия "разумных" оснований для разрешения перехвата сообщений. В таких случаях бремя доказывания необходимости слежения является чрезвычайно слабым с учетом того, что потен-

[33] Раздел 5, Закон о регулировании полномочий следствия 2000 года.

[34] Раздел 5, Закон о перехвате коммуникаций 2006 года.

циально слежение может привести к расследованию, дискриминации или нарушениям прав человека. В других странах доступ к сообщениям и их отслеживание по самым различным основаниям санкционирует сложная совокупность законов. В Индонезии, например, законы о психотропных веществах, наркотиках, электронной информации и транзакциях, телекоммуникациях и коррупции содержат компоненты, относящиеся к отслеживанию сообщений. В Великобритании более 200 органов, полиция и тюремная администрация уполномочены получать коммуникационные данные в соответствии с Законом о регулировании полномочий следствия 2000 года. В результате частным лицам сложно предвидеть, когда и какой государственный орган может осуществлять за ними слежение.

57. Во многих государствах провайдеры коммуникационных услуг принуждаются к модификации их инфраструктуры для обеспечения прямого слежения, что устраняет возможность судебного надзора. Например, в 2012 году колумбийские министерства юстиции, информации и коммуникационных технологий издали постановление, требующее от провайдеров телекоммуникационных услуг создать инфраструктуру, позволяющую получать судебной полиции прямой доступ к сообщениям без постановления Генерального прокурора[35]. Упоминавшийся выше угандийский Закон о регулировании перехвата сообщений 2010 года (раздел 3) предусматривает учреждение мониторингового центра и обязывает телекоммуникационных провайдеров обеспечивать, чтобы перехваченные сообщения передавались в мониторинговый центр (раздел 8 (1) f)). Правительство Индии предлагает сформировать централизованную мониторинговую систему, которая направляла бы все сообщения центральному правительству, предоставляя органам безопасности возможность не взаимодействовать с провайдерами услуг[36]. Такие меры выводят отслеживание сообщений за рамки требования о получении судебной санкции и позволяют вести нерегулируемое, секретное слежение, устраняя любую транспарентность и подотчетность со стороны государства.

B. Исключения по соображениям национальной безопасности

58. Размытые и не конкретизированные понятия "национальной безопасности" стали приемлемым обоснованием для перехвата сообщений и доступа к ним во многих странах. В Индии, например, Закон об информационных технологиях 2008 года позволяет осуществлять перехват сообщений в интересах, помимо прочего, "суверенитета, целостности или защиты Индии, дружественных отношений с зарубежными государствами, общественного порядка и расследования любых правонарушений" (раздел 69).

59. Во многих случаях национальные разведывательные службы также пользуются всесторонними исключениями в отношении требования о получении судебной санкции. Например, в Соединенных Штатах Закон о надзоре за иностранными разведками уполномочивает Национальное агентство безопасности перехватывать сообщения без судебной санкции в случаях, когда одна из сторон обмена сообщениями находится за пределами Соединенных Штатов, а другой участник обоснованно рассматривается в качестве члена признанной государством в качестве террористической организации. Германское законодательство

[35] Ministries of Justice and ICTs Decree 1704. Rooted in the Criminal Procedure Code of 2004.

[36] Department of Communications. Government of India. Annual Report 2011-2012 pg. 58 – http://www.dot.gov.in/annualreport/AR%20Englsih%2011-12.pdf.

разрешает не санкционированное судом слежение за национальными и международными сообщениями государственными разведслужбами в целях защиты свободного демократического порядка и безопасности государства[37]. В Швеции Закон о радиоперехвате разведданных в ходе оборонительных операций разрешает шведскому разведывательному управлению перехватывать без каких-либо постановлений или судебных предписаний весь телефонный и интернет-трафик в пределах территории Швеции. В Объединенной Республике Танзания Закон о службах разведки и безопасности 1996 года позволяет разведслужбам страны проводить любые расследования и собирать сведения о любых лицах или органах, которых они имеют разумные основания считать представляющими риск, источником риска или угрозой для безопасности государства.

60. Использование аморфной концепции национальной безопасности для обоснования интрузивных ограничений пользования правами человека является предметом серьезной обеспокоенности[38]. Данная концепция имеет широкое определение и в этой связи является уязвимой для манипуляций со стороны государства, которое рассматривает ее в качестве средства для оправдания действий, которые направлены против таких уязвимых групп, как правозащитники, журналисты или оппозиционеры. Она также используется для обоснования зачастую ненужной секретности вокруг расследований или действий правоохранительных органов, подрывая принципы транспарентности и подотчетности.

C. Нерегулируемый доступ к коммуникационным данным

61. Доступ к коммуникационным данным, хранящимся у национальных провайдеров коммуникационных услуг, часто санкционируется законодательством или обуславливается при выдаче лицензий. В результате государствам, как правило, предоставляется полная свобода действий в плане доступа к коммуникационным данным при низком уровне надзора или регулирования. Так, например, бразильский Закон о борьбе с отмыванием денежных средств 2012 года наделяет полицию полномочиями доступа к регистрационной информации, хранящейся в Интернете и у провайдеров коммуникационных услуг, без судебного постановления[39]. На международном уровне предоставление доступа к коммуникационным данным регулируется двусторонними договорами об оказании взаимной правовой помощи. Однако это сотрудничество часто осуществляется вне правовых рамок на основе добровольного согласия провайдеров услуг или интернет-компаний. По сути, во многих государствах доступ к коммуникационным данным может быть получен без независимого санкционирования и при ограниченном надзоре.

D. Не подпадающее под действие закона слежение

62. Ряд вышеперечисленных технических возможностей слежения выпадают из существующего правового поля, но, тем не менее, продолжают широко применяться государствами. Программное обеспечение агрессивного проникновения в компьютеры, такое как "программы-трояны" или технические средства массового перехвата сообщений, создают такие серьезные вызовы для традици-

[37] G-10 law.

[38] Резолюции Совета по правам человека о борьбе с терроризмом.

[39] Бразильский Федеральный закон 12683/2012. Статья 17-B. Доступен по адресу http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2012/Lei/L12683.htm.

онных понятий слежения, что не могут быть совмещены с существующими законами о слежении и доступе к информации личного характера. Они представляют собой не только новые методы слежения, но и новые его формы. С точки зрения прав человека использование таких технологий вызывает чрезвычайную обеспокоенность. "Программы-трояны", например, не только позволяют государствам получать доступ к устройствам, но также и дают им возможность изменять – непреднамеренно или преднамеренно – содержащуюся в них информацию. Это угрожает не только праву на неприкосновенность личной жизни и правам, относящимся к процессуальной законности, применительно к использованию таких доказательств в ходе судопроизводства. Технологии массового перехвата устраняют любые соображения соразмерности, позволяя осуществлять неизбирательное слежение. Они предоставляют возможность государствам копировать и контролировать любой отдельный акт общения в отдельно взятой стране или районе без получения санкции на каждый индивидуальный случай перехвата.

63. Правительства часто не признаются в использовании таких технологий для осуществления слежения или же утверждают, что они применяются на законных основаниях в рамках существующего законодательства о слежении. Хотя очевидно, что многие страны обладают программным обеспечением агрессивного вторжения в компьютеры, таким как технологии "программ-троянов", правовая основа их использования публично не обсуждалась ни в одном государстве, за исключением Германии. В данном контексте земля Северный Рейн-Вестфалия в 2006 году приняла законодательство, разрешающее "секретный доступ к системам информационных технологий" (пункт 5.2 № 11, Закон о защите Конституции Северного Рейна-Вестфалии), под которым понималось техническое проникновение, осуществляемое либо путем инсталляции шпионской программы, либо путем использования дыр в безопасности системы. В феврале 2008 года Федеральный конституционный суд Германии отменил этот закон, постановив, что такие меры только в том случае соответствовали бы правам человека, если они бы они являлись предметом судебной санкции или надзора и применялись бы исключительно в ситуациях, когда может существовать конкретная угроза особо важным законным интересам[40].

E. Экстерриториальное применение законов о слежении

64. В ответ на растущий трансграничный поток данных и с учетом того факта, что большинство сообщений хранятся у зарубежных провайдеров-посредников, ряд государств стали принимать законы, предусматривающие предоставление им полномочий на проведение экстерриториального слежения или перехват сообщений в иностранных юрисдикциях. Это вызывает серьезную озабоченность в отношении совершения экстерриториальных нарушений прав человека и в связи с отсутствием у частных лиц возможности выяснить, что они могут подвергаться иностранному слежению, оспорить решения об иностранном слежении или добиваться возмещения ущерба. В Южно-Африканской Республике, например, Закон о внесении изменений в общие законы о разведывательной деятельности позволяет отслеживать зарубежные сообщения, которые передаются за пределами Южно-Африканской Республики или проходят через

[40] Доступно на немецком языке. BVerfG, 1 BvR 370/07 vom 27.2.2008, Absatz-Nr. (1 - 67), http://www.bverfg.de/entscheidungen/rs20080227_1bvr037007.html.

нее[41]. В октябре 2012 года голландское Министерство юстиции и безопасности внесло законодательную поправку в голландский парламент, которая позволяет полиции взламывать компьютеры и мобильные телефоны как в Нидерландах, так и за рубежом в целях инсталляции шпионского программного обеспечения, поиска и уничтожения данных[42]. В декабре 2012 года Национальное собрание Пакистана приняло Закон о справедливом судебном разбирательстве, пункт 31 которого предусматривает приведение в исполнение судебных постановлений в зарубежных юрисдикциях. Позже в этом же месяце Соединенные Штаты обновили Закон о внесении поправок в Закон о надзоре за иностранными разведками 2008 года, расширив полномочия правительства по осуществлению слежения за иностранцами, находящимися за пределами Соединенных Штатов (пункт 1881 a), включая любых иностранных частных лиц, чьи сообщения хранятся "облачными" провайдерами, расположенными в Соединенных Штатах (такими, как "Гугл", и другими крупными интернет-компаниями)[43]. Кроме того, в 2012 году Европейский институт стандартов связи подготовил проекты стандартов по перехвату зарубежных "облачных" услуг европейскими правительствами[44]. Эти события свидетельствуют о тревожной тенденции расширения полномочий по слежению за пределы территориальных границ, что повышает риск заключения соглашений о сотрудничестве между государственными правоохранительными органами и службами безопасности, с тем чтобы обойти национальные законодательные ограничения.

F. Обязательное хранение данных

65. В целях увеличения объемов коммуникационных данных, к которым они могут иметь доступ, некоторые государства принимают законы об обязательном хранении данных, обязывающие интернет-провайдеров и провайдеров телекоммуникационных услуг (называемых совместно как "провайдеры коммуникационных услуг") постоянно собирать и хранить содержание сообщений и информацию об онлайновой активности пользователей. Такие законы позволяют компилировать предыдущие данные об электронной почте и сообщениях частных лиц, их местонахождении, общении с друзьями и семьями и т.д.

66. При оказании услуг своим пользователям провайдеры коммуникационных услуг присваивают устройствам или сети абонента IP-адрес[45], который периодически меняется. Информация о IP-адресе может использоваться для установления личности и местонахождения частных лиц и слежения за их онлайновой активностью. Законы об обязательном хранении данных обязывают провайдеров коммуникационных услуг хранить регистрационные данные о предоставленных ими IP-адресах в течение определенного периода времени, что расширяет возможности государств требовать от провайдеров коммуникационных услуг раскрытия личности частных лиц с помощью присвоенного им IP-адреса на

[41] Раздел 1. c. Закон о внесении изменений в общие законы о разведдеятельности. Доступен по адресу http://www.parliament.gov.za/live/commonrepository/Processed/20111201/385713_1.pdf.

[42] См. http://www.edri.org/edrigram/number10.20/dutch-proposal-state-spyware.

[43] См. European Parliament Directorate-General for Internal Policies Policy Department C: Citizens Rights and Constitutional Affairs, Fighting crime and protecting privacy in the cloud: study, 2012.

[44] Draft ESTI DTR 101 567 Lawful Interception (LI) Vo.1.0 (2012 - 05); Cloud/Virtual Services (CLI). Доступно по адресу www.3gpp.org.

[45] IP-адрес является уникальным цифровым кодом, который идентифицирует все компьютеры или другие устройства, подключенные к Интернету.

определенную дату и время. Некоторые государства в настоящее время также пытаются обязать провайдеров-посредников осуществлять сбор и хранение информации, которую они обычно не собирают.

67. Национальные законы о хранении данных являются интрузивными и затратными, несут угрозу для прав на неприкосновенность личной жизни и свободу выражения мнений. Обязывая провайдеров коммуникационных услуг создавать обширные информационные базы данных об общении людей по телефону или Интернету, продолжительности обмена информацией, местонахождении пользователей и хранить эту информацию (иногда годами), законы об обязательном хранении данных существенно расширяют охват государственного слежения и, таким образом, масштабы нарушений прав человека. Базы коммуникационных данных становятся уязвимыми для хищения, мошенничества или для случайного раскрытия.

G. Законы о раскрытии личности

68. Во многих государствах законы требуют удостоверения личности в интернет-кафе. Такие законы создают особые проблемы в странах, где собственные персональные компьютеры являются редкостью, и частные лица в высокой степени зависят от компьютеров, находящихся в общественном доступе. В Индии, например, Правила в области информационных технологий (руководящие принципы для интернет-кафе) 2011 года требуют от владельцев интернет-кафе просить предъявлять удостоверяющие личность документы у любых частных лиц, посещающих интернет-кафе, чьи регистрационные данные должны храниться как минимум в течение года (Правило 4 (2)). Интернет-кафе должно хранить как минимум в течение года регистрационную информацию о подключении к Сети, содержащую, помимо прочего, время подключения к Сети, время выхода из Сети и идентификацию терминала компьютера (Правило 5 (1) и 5 (2)); хранить резервные копии регистрационных записей каждого доступа в Сеть или сеанса работы любого пользователя как минимум в течение года (Правило 5 (4)).

69. В настоящее время во многих государствах частные лица также обязаны использовать свои подлинные имена в Интернете и предоставлять официальные документы в целях установления их личности. В Республике Корея принятый в 2007 году Закон об информационных коммуникациях обязывал пользователей регистрировать свои настоящие имена перед входом на веб-сайты, которые ежедневно насчитывают более 100 000 посетителей, якобы в целях снижения уровня агрессии и ненавистнической риторики в онлайне. Данный закон был недавно отменен Конституционным судом на том основании, что он ограничивал свободу слова и подрывал демократию[46]. В Китае недавно было принято Решение об укреплении защиты онлайновой информации, обязывающее провайдеров Интернета и телекоммуникационных услуг осуществлять сбор персональной информации о пользователях, когда они оформляют подключение к Интернету, проводной линии связи или услугам мобильной телефонной связи. Провайдеры услуг, разрешающие пользователям размещать информацию в Сети, должны быть в состоянии увязывать их ники с настоящими именами. Эти требования по регистрации настоящего имени позволяют властям легче выяв-

[46] Решение Конституционного суда 2010Hun-Ma47 (решение о "настоящих именах"), 23 августа 2012 года. Официальный сборник решений Суда доступен на веб-сайте Суда по адресу http://www.ccourt.go.kr/home/bpm/sentence01_list.jsp only in Korean.

лять сетевых комментаторов или устанавливать связь между использованием мобильных телефонов и конкретными частными лицами, ликвидируя тем самым анонимное выражение мнений[47].

70. Еще одной инициативой, препятствующей анонимности сообщений, является постепенное принятие правил, требующих регистрировать сим-карты на настоящие имена абонентов или по удостоверяющим личность документам, выданным правительством. В 48 странах Африки законы, обязывающие частных лиц регистрировать свою персональную информацию у своих сетевых провайдеров до активации сим-карт предоплаты, согласно сообщениям, упрощают создание широких баз данных о пользователях, ликвидируя возможности для анонимности сообщений, позволяя отслеживать местонахождение частных лиц и облегчая отслеживание сообщений[48]. В отсутствие законодательства о защите данных информация о пользователях сим-карт может передаваться правительственным учреждениям и сопоставляться с другими закрытыми или открытыми базами данных, позволяя государствам составлять всеобъемлющие характеристики на конкретных граждан. Частным лицам также угрожает отключение услуг мобильной телефонной связи (которая предоставляет возможность не только для коммуникаций, но и для получения доступа к финансовым услугам) в случае, если они не могут или не хотят предоставлять данные о своей личности для регистрации.

H. Законы об ограничениях на шифрование и о раскрытии ключей

71. Безопасность и анонимность сообщений также подрываются законами, которые ограничивают использование повышающих конфиденциальность инструментов, которые могут использоваться для защиты сообщений, таких как шифрование. В настоящее время многие государства приняли законы, которые обязывают частных лиц осуществлять дешифрование сообщений в случае соответствующего распоряжения. Закон Южно-Африканской Республики 2002 года о регулировании перехвата сообщений и предоставлении коммуникационной информации обязывает всех лиц, обладающих дешифровочным ключом, оказывать содействие в дешифровании[49]. Аналогичные законы существуют в Финляндии (раздел 4 (4) a) Закона о принудительных мерах 1987/450), Бельгии (статья 9 Закона о киберпреступности от 28 ноября 2000 года) и Австралии (разделы 12 и 28 Закона о киберпреступности 2001 года).

VII. Роль и обязанности частного сектора

72. Важные технологические прорывы, позволившие развитие новых и динамичных форм связи, были совершены в основном в частном секторе. В этом смысле многие нововведения, с помощью которых мы отправляем, получаем и

[47] "China to Strengthen Internet Information Protection" - http://www.ebeijing.gov.cn/BeijingInformation/BeijingNewsUpdate/t1292298.htm.

[48] Kevin P. Donovan and Aaron K. Martin, “The Rise of African SIM Registration: Mobility, Identity, Surveillance and Resistance,” Information Systems and Innovation Group Working Paper Series, no. 186, London School of Economics and Political Science (20012).

[49] Раздел 29. Южно-африканский Закон 2002 года о регулировании перехвата сообщений и предоставлении коммуникационной информации. Доступен по адресу http://www.dac.gov.za/acts/Regulation%20of%20Interception%20of%20Communications%20Act.pdf.

распространяем информацию, основываются на исследованиях и инновациях корпоративных субъектов.

73. Частный сектор также сыграл в ряде отношений ключевую роль в упрощении государственного слежения за частными лицами. Корпоративные субъекты были вынуждены реагировать на требования о проектировании цифровых сетей и коммуникационной инфраструктуры таким образом, чтобы предоставить государству возможности для проникновения в них. Такие требования были первоначально одобрены государствами в 1990-х годах и стали обязательными для всех провайдеров коммуникационных услуг. Все чаще государства принимают законодательство, обязывающее провайдеров коммуникационных услуг предоставлять государствам прямой доступ к коммуникационным данным или изменять инфраструктуру для облегчения новых форм государственного проникновения в системы.

74. Развивая и внедряя новые технологии и средства коммуникации конкретными способами, корпоративные субъекты также добровольно приняли меры, облегчающие отслеживание сообщений государствами. В самом простом проявлении данное сотрудничество обрело форму решений о порядке сбора и обработки информации корпоративными субъектами, что позволяет превращать их в крупные хранилища персональных данных, которые затем становятся доступными для государств по их требованию. Корпоративные субъекты приняли спецификации, которые предоставляют возможности для доступа государственных органов к данным или проникновения в системы, для сбора избыточной и разоблачительной информации или для ограничения применения шифрования и других методов, позволяющих ограничить доступ к информации как со стороны компаний, так и со стороны правительств. Частный сектор также зачастую не внедрял повышающие конфиденциальность технологии или же реализовывал их не такими безопасными путями, которые отвечали бы современному уровню развития техники.

75. В наиболее серьезных случаях частный сектор являлся соучастником разработки технологий, которые позволяли вести массовое или интрузивное слежение в нарушение существующих правовых норм[50]. Корпоративный сектор породил глобальную индустрию, сфокусированную на обмене технологиями слежения. Такие технологии часто продаются в страны, в которых существует серьезный риск их использования для нарушения прав человека, в том числе прав правозащитников, журналистов или других уязвимых групп. Эта индустрия практически не регулируется, поскольку государствам не удалось идти в ногу с технологической и политической эволюцией.

76. Обязательства государств в области прав человека требуют, чтобы они не только соблюдали и поощряли права на свободу выражения мнений и неприкосновенность личной жизни, но и защищали частных лиц от нарушений прав человека, совершенных корпоративными субъектами. Кроме того, государства должны осуществлять надлежащий контроль в целях выполнения своих международных обязательств в области прав человека при заключении контрактов с предприятиями или принятия законодательных актов в их интересах, которые

[50] Примеры технологий слежения, разработанных частным сектором и используемых в Ливии, Бахрейне, Сирийской Арабской Республике, Египте и Тунисе, см. в European Parliament, Directorate-General for External Policies, Policy Department, After the Arab Spring: New Paths for Human Rights and the Internet in European Foreign Policy (2012), pp. 9−10.

могут оказывать воздействие на осуществление прав человека[51]. Соответствующие обязательства в области прав человека также применяются, когда корпоративные субъекты действуют за рубежом[52].

77. Государства должны обеспечивать, чтобы частный сектор мог выполнять свои функции на независимой основе и таким способом, который поощряет права человека частных лиц. В то же время корпоративные субъекты не могут допускаться к участию в деятельности, которая нарушает права человека, а государства обязаны в этой связи привлекать компании к ответственности.

VIII. Выводы и рекомендации

78. **Коммуникационные методы и технологии существенным образом эволюционировали, изменив способ государственного слеживания за сообщениями. В этой связи государства должны модернизировать свои подходы к регулированию практики слежения за сообщениями и изменить эту практику в целях обеспечения соблюдения и защиты прав человека частных лиц.**

79. **Государства не могут обеспечить возможность частным лицам свободно искать, получать информацию и выражать свое мнение без соблюдения, защиты и поощрения их права на неприкосновенность личной жизни. Неприкосновенность личной жизни и свобода выражения мнений взаимосвязаны и взаимозависимы, причем посягательство на одно из этих прав может стать причиной и следствием нарушения другого. В отсутствие адекватного законодательства и правовых норм по обеспечению конфиденциальности, безопасности и анонимности сообщений журналисты, правозащитники и разоблачители не могут, например, удостовериться, что их сообщения не станут объектом контроля со стороны государств.**

80. **В целях выполнения своих правозащитных обязательств государства должны обеспечить, чтобы права на свободу выражения мнений и неприкосновенность личной жизни лежали в основе их нормативно-правовых механизмов слежения за сообщениями. В этой связи Специальный докладчик рекомендует следующее:**

A. Обновление и укрепление законов и правовых норм

81. **Слежение за сообщениями должно рассматриваться как крайне интрузивное деяние, которое потенциально препятствует осуществлению прав на свободу выражения мнений и неприкосновенность личной жизни и угрожает основам демократического общества. Законодательство должно предусматривать, что слежение государством за сообщениями должно осуществляться только в самых исключительных обстоятельствах и только под надзором независимого судебного органа. В законе должны быть четко прописаны гарантии, касающиеся характера, охвата и продолжительности возможных мер слежения, оснований, требующихся для их применения,**

[51] Руководящие принципы предпринимательской деятельности в аспекте прав человека: осуществление рамок Организации Объединенных Наций в отношении "защиты, соблюдения и средств правовой защиты", Принцип 5.

[52] Комитет по правам человека, заключительные замечания, Германия, декабрь 2012 года.

органов власти, уполномоченных санкционировать, осуществлять такие меры и надзирать за ними, и типа средств правовой защиты, предусмотренных национальным законодательством.

82. **Частные лица должны иметь законное право на уведомление о том, что их сообщения отслеживались или что к их коммуникационным данным получило доступ государство. Учитывая, что заблаговременное или совпадающее по времени уведомление может поставить под угрозу эффективность слежения, частные лица должны, тем не менее, уведомляться об этом сразу же после окончания слежения. Они также должны иметь возможность добиваться возмещения ущерба в связи с применением к ним мер по слежению за сообщениями после их завершения.**

83. **Законодательная база должна обеспечивать, чтобы меры по слежению за сообщениями:**

a) были предписаны законом и удовлетворяли нормам ясности и четкости, что является достаточным для обеспечения того, чтобы частные лица были заблаговременно уведомлены о них и могли предвидеть их применение;

b) являлись строго и очевидно необходимыми для достижения законной цели; и

c) соответствовали принципу соразмерности и не применялись в случаях наличия или неисчерпания менее интрузивных методов.

84. **Государства должны криминализировать незаконное слежение с государственными или частными субъектами. Такие законы не должны использоваться для борьбы с разоблачителями или другими частными лицами, стремящимися предать гласности нарушения прав человека. Они также не должны препятствовать законному надзору за деятельностью правительства со стороны граждан.**

85. **Предоставление частным сектором коммуникационных данных государствам должно надлежащим образом регулироваться для обеспечения того, чтобы правам человека частных лиц уделялось первостепенное внимание во всех случаях. Вопрос о доступе к коммуникационным данным, хранящимся у национальных корпоративных субъектов, должен ставиться только в таких обстоятельствах, когда были исчерпаны другие доступные менее интрузивные методы.**

86. **Предоставление коммуникационных данных государствам должно контролироваться независимым органом, таким как суд или надзорный механизм. На международном уровне государства должны использовать договоры о взаимной правовой помощи для регулирования доступа к коммуникационным данным, хранящимся у зарубежных корпоративных субъектов.**

87. **Методы и практика слежения, применяющиеся вне правового поля, должны быть поставлены под законодательный контроль. Их внеправовое использование подрывает базовые принципы демократии и может привести к пагубным политическим и социальным последствиям.**

B. Содействие обеспечению конфиденциальных, безопасных и анонимных каналов связи

88. **Государства должны воздерживаться от принуждения к идентификации пользователей как предварительного условия для доступа к каналам связи, включая онлайновые службы, интернет-кафе или мобильную телефонию.**

89. **Частные лица должны обладать свободой выбора в области использования какой бы то ни было технологии для обеспечения безопасности своих сообщений. Государства не должны вторгаться в использование технологий шифрования и принуждать к предоставлению дешифровочных ключей.**

90. **Государства не должны хранить персональную информацию или требовать ее хранения исключительно в целях слежения.**

C. Расширение публичного доступа к информации, понимание угроз неприкосновенности личной жизни и повышение осведомленности о них

91. **Государства должны демонстрировать полную транспарентность в отношении применения и охвата методов и полномочий слежения. Они должны публиковать как минимум обобщенную информацию о количестве одобренных и отклоненных запросов, данные о запросах в разбивке по провайдерам услуг, расследованиям и целям.**

92. **Государства должны предоставлять частным лицам достаточную информацию, с тем чтобы позволить им полностью уяснить охват, характер и применение законов, разрешающих слежение за сообщениями. Государства должны разрешить провайдерам услуг публикацию информации о применяемых ими процедурах при слежении государства за сообщениями, соблюдении ими этих процедур и отчетов о слежении государства за сообщениями.**

93. **Государства должны учредить независимые надзорные механизмы, способные обеспечить транспарентность и подотчетность практики слежения государства за сообщениями.**

94. **Государства должны повышать осведомленность общественности об использовании новых коммуникационных технологий в целях оказания содействия частным лицам в плане должной оценки связанных с обменом информацией рисков, их регулирования, снижения их вероятности и принятия осознанных решений в этой области.**

D. Регулирование коммерциализации технологий слежения

95. **Государства должны обеспечивать, чтобы коммуникационные данные, собираемые корпоративными субъектами в ходе оказания коммуникационных услуг, соответствовали наивысшим стандартам защиты данных.**

96. **Государства должны воздерживаться от принуждения частного сектора к принятию мер, дискредитирующих конфиденциальность, безопас-**

ность и анонимность коммуникационных услуг, включая требование о создании технических средств перехвата для целей государственного слежения или запрет на использование шифрования.

97. **Государства должны принимать меры по предотвращению коммерциализации технологий слежения, уделяя особое внимание технологическим исследованиям, развитию, торговле, экспорту и использованию этих технологий с учетом возможности их содействия систематическим нарушениям прав человека.**

E. Содействие оценке соответствующих международных обязательств в области прав человека

98. **Существует значительная потребность в углублении понимания на международном уровне вопроса о защите права на неприкосновенность личной жизни в свете технологических достижений. Комитет по правам человека должен рассмотреть вопрос о выпуске нового замечания общего порядка о праве на неприкосновенность личной жизни взамен замечания общего порядка № 16 (1988 год).**

99. **Правозащитные механизмы должны продолжить оценку обязательств частного сектора в области разработки и поставки технологий слежения.**