КОМИТЕТУ МИНИСТРОВ СОВЕТА ЕВРОПЫ

Об исполнении Постановления Европейского суда по правам человека по делу «Роман ЗАХАРОВ против Российской Федерации» (жалоба №47143/06)

меморандум

Международной правозащитной группы Агора,

и

Объединения альтернативных операторов связи

в соответствии с Правилом 9(2) Регламента
Комитета министров Совета Европы от 10 мая 2006 года
о порядке контроля за исполнением постановлений Европейского Суда по правам человека
и условий мировых соглашений

17 декабря 2018

I. ВВЕДЕНИЕ

1. Настоящий доклад подготовлен Международной правозащитной группой Агора, компанией Telegram Messenger LLP и Ассоциацией операторов телефонной связи в соответствии с Правилом 9(2) Регламента Комитета министров Совета Европы от 10 мая 2006 года о порядке контроля за исполнением постановлений Европейского Суда по правам человека и условий мировых соглашений.

2. *Международная Агора* – правозащитная организация, объединяющая более 50 юристов-правозащитников, работающих по резонансным делам о нарушении прав человека, преимущественно на территории Российской Федерации. Одним их приоритетных направлений работы Международной Агоры является защита права на уважение частной жизни и свободу выражения мнения, как онлайн, так и офлайн.

3. *Объединение альтернативных операторов связи (ОАОС)* – общественное объединение, включающее в себя руководителей небольших операторов связи (преимущественно из Санкт-Петербурга). ОАОС существует с 2014 года, активно участвует в законотворческой деятельности (входит в экспертные группы при Министерстве цифрового развития, связи и массовых коммуникаций, Правительстве РФ, Федеральной антимонопольной службе). ОАОС также представляет операторов в антимонопольных делах.

4. Настоящий Доклад посвящен исполнению Российской Федерацией Постановления Европейского суда по правам человека (далее – «Суд») по делу «Роман ЗАХАРОВ против Российской Федерации», жалоба №47143/06 (далее – «Постановление»).

5. В Постановлении Суд на основе анализа соответствующих нормативных правовых актов и практики их применения пришел к выводу о том, что российские правовые нормы, регулирующие перехват сообщений, не предусматривают адекватных и эффективных гарантий против произвола и риска злоупотребления, который присущ любой системе тайного наблюдения, и который является особенно высоким в системе, где спецслужбы и полиция

обладают прямым доступом, с помощью технических средств, ко всем мобильным телефонным переговорам[1].

6. Правительство Российской Федерации 3 августа 2018 года представило Комитету Министров Обновленный план действий по исполнению Постановления, в котором предложило ряд мер, направленных на устранение и предотвращение обозначенных нарушений Конвенции, отмеченных Судом.

7. В настоящем Докладе мы хотели бы дать оценку некоторым предложениям Правительства Российской Федерации, а также проинформировать Комитет Министров о значительном ухудшении ситуации с правом на уважение частной жизни в России в связи с принятием новых законодательных положений, разрешающих правоохранительным органам и спецслужбам получать доступ ко всем электронным коммуникациям.

ОЦЕНКА СУДА

8. Рассматривая обстоятельства дела Суд отметил, что, когда полномочия, принадлежащие исполнительной власти, исполняются в тайне, риск произвола очевиден. Поэтому важно иметь чёткие, подробные правила перехвата телефонных разговоров, особенно с учётом того, что доступные для использования технологии постоянно становятся всё более совершенными. Национальное законодательство должно быть достаточно чётким, чтобы дать гражданам надлежащее указание на обстоятельства и условия, при которых государственные органы уполномочены прибегать к таким мерам[2].

9. Формулируя соответствующие критерии, Суд, в частности, указал, что требование о предоставлении разрешения на перехват поставщику услуг связи до получения доступа к сообщениям лица является одной из важных гарантий против злоупотребления со стороны правоохранительных органов, гарантирующей, что

[1] См. *Roman ZAKHAROV v. Russian Federation*, application No. 47143/06, 4 December 2015, §302
[2] См. там же, §229

надлежащее разрешение должно быть получено для всех случаев перехвата[3].

10. В Постановлении Суд указал, в частности, на следующие недостатки российских законодательных норм, регламентирующих перехват телефонных переговоров.

В отношении сферы применения тайных мер наблюдения:

11. Российское законодательство допускает тайный перехват сообщений в отношении очень широкого спектра уголовных преступлений, включая, например, карманные кражи (§ 244).

12. Приказ о перехвате может быть издан не только в отношении подозреваемого или обвиняемого, но также в отношении лица, способного располагать информацией о преступлении или иной информацией, относящейся к уголовному делу. Соответствующие термины в законодательстве и практике не определены (§ 245).

13. Закон об ОРД предусматривает, что телефонные и иные сообщения могут быть перехвачены после получения информации о событиях или деятельности, представляющей угрозу для национальной, военной, экономической или экологической безопасности России. Какие события или деятельность можно рассматривать, как представляющие угрозу таким видам безопасности, не определено нигде в российском законодательстве, что дает российским властям практически неограниченную свободу усмотрения (§§ 246-247).

14. Перехват в рамках уголовного дела связан с большим количеством мер предосторожности, чем перехват, проведенный вне таких рамок, в частности, в связи с «событиями или действиями, представляющими угрозу для национальной, военной, экономической или экологической безопасности» (§ 251).

В отношении процедур разрешения перехвата сообщений

15. Судебная проверка ограничена по объёму. Материалы, содержащие информацию о тайных агентах или информаторах

[3] См. там же, §269

полиции, или об организации и тактике оперативно-розыскных мероприятий, не могут быть переданы судье, и, следовательно, исключаются из сферы судебного рассмотрения (§ 261).

16. Ни УПК, ни Закон об ОРД не поручают судьям проверять наличие «обоснованного подозрения» в отношении заинтересованного лица, или применять проверку «необходимости» и «соразмерности» (§ 262).

В отношении доступа властей к сообщениям

17. В соответствии с национальным законодательством, правоохранительные органы не обязаны предъявлять судебное разрешение поставщикам услуг связи до получения доступа к сообщениям лица, за исключением случае запроса информация о фактах соединений между абонентскими устройствами (§ 269).

18. Манера, в которой система тайного наблюдения работает в России, даёт службам безопасности и полиции технические средства, позволяющие обойти процедуру разрешения и перехватывать любые сообщения без получения предварительного судебного разрешения (§ 270).

В отношении надзора за перехватом:

19. Суд, который выдал разрешение на перехват, не имеет полномочий контролировать его осуществление. Он не ставится в известность о результатах перехвата и не обладает полномочиями по рассмотрению того, были ли соблюдены требования решения, разрешающего перехват. Также российские суды в целом не обладают полномочиями по осуществлению общего надзора за перехватом. Судебный надзор ограничен стадией первоначального разрешения (§ 274).

В отношении извещений о перехвате сообщений и доступных средства правовой защиты

20. Лица, чьи сообщения были перехвачены, не уведомляются об этом, ни в какой момент времени и ни при каких обстоятельствах. Отсюда следует, что если в отношении субъекта перехвата не было возбуждено уголовное дело и перехваченные данные не были

использованы в качестве доказательств, или если не было утечки, заинтересованное лицо вряд ли сможет когда-либо узнать, что его или её сообщения были перехвачены (§ 289).

21. Человек, который каким-либо образом узнал, что его сообщения перехватывались, может потребовать информацию о соответствующих данных , однако доступ к информации зависит от способности человека доказать, что его или её сообщения были перехвачены. Кроме того, субъект перехвата не имеет права на получение доступа к документам, связанным с перехватом его сообщений; он или она в лучшем случае имеет право получить «информацию» о собранных данных (§ 280).

МЕРЫ, ПРЕДЛОЖЕННЫЕ ПРАВИТЕЛЬСТВОМ

22. В Обновленном плане действий, представленном Правительством Российской Федерации 3 августа 2018 года, отмечается следующее.

23. В соответствии с планом законопроектной деятельности России на 2018 года Министерство юстиции Российской Федерации в октябре 2018 года должно разработать и направить в Правительство Российской Федерации проекты Федеральных законов «О внесении изменений в статью 9 Федерального закона «Об оперативно-розыскной деятельности» (в части совершенствования гарантий прав и свобод человека при санкционировании проведения и обжаловании оперативно-разыскных мероприятий)» и «О внесении изменений в Кодекс административного судопроизводства Российской Федерации (в части урегулирования порядка судебного рассмотрения материалов об ограничении конституционных прав граждан при проведении оперативно-разыскных мероприятий)». Соответствующие законопроекты должны быть внесены в Государственную Думу в декабре 2018 года (п.1 Обновленного плана действий).

24. Принято Постановление Конституционного Суда Российской Федерации №12-П от 9 июня 2011 года, согласно которому органы, обращающиеся за разрешением на проведение оперативно-разыскных мероприятий, должны предоставить суду материалы, указывающие на конкретные фактические обстоятельства,

подтверждающие наличие обоснованного подозрения, а также ряд определений Конституционного Суда (в частности, №114-О от 22 января 2014 года, №86-О от 28 января 2016 года и 568-О от 28 марта 2017 года).

25. За период с 2014 по 2017 годы к уголовной ответственности по части 2 статьи 138 УК РФ (Нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений с использованием служебного положения) было привлечено 79 человек.

26. За период с 2016 по первую половину 2018 года по результатам 630 000 прокурорских проверок было прекращено 295 оперативно-разыскных мероприятий.

ОЦЕНКА МЕР, ПРЕДЛОЖЕННЫХ ПРАВИТЕЛЬСТВОМ

27. По сути, усилия Правительства Российской Федерации, предпринимаемые во исполнение Постановления, сводятся к намерению принять поправки в статью 9 Федерального закона «Об оперативно-розыскной деятельности» и дополнении Кодекса административного судопроизводства положениями особо урегулирующими порядок судебного рассмотрения материалов об ограничении конституционных прав граждан при проведении оперативно-розыскных мероприятий.

28. Между тем, в соответствии с Постановлением Правительства РФ от 25 августа 2012 г. №851 «О порядке раскрытия федеральными органами исполнительной власти информации о подготовке проектов нормативных правовых актов и результатах их общественного обсуждения» проекты орган исполнительной власти, которому поручена подготовка проекта нормативного правового акта, обязан разместить на Официальном сайте для размещения информации о подготовке федеральными органами исполнительной власти проектов нормативных правовых актов и результатах их общественного обсуждения уведомление о подготовке соответствующего акта, а также его проект для

общественного обсуждения, срок которого не может быть меньше 15 дней. Размещение информации о подготовке проектов федеральных законов является обязательным.

29. До настоящего времени проекты федеральных законов, упомянутых в Дополненном плане действий Правительства (п.1), на официальном портале не опубликованы, информация о подготовке таких документов отсутствует в открытом доступе и общественного обсуждения не проводилось.

30. Упомянутое в Обновленном плане действий Постановление Конституционного Суда Российской Федерации №12-П от 9 июня 2011 года, в котором подчеркивается необходимость при решении вопроса о разрешении производства оперативно-разыскных мероприятий, устанавливать наличие конкретных фактических обстоятельств, подтверждающих обоснованность подозрения лица в причастности к преступлению, распространяется лишь на случаи проведения оперативно-разыскных мероприятий лишь в отношении судей, что прямо отмечается в п.1 указанного Постановления Конституционного Суда: «предметом рассмотрения Конституционного Суда Российской Федерации по настоящему делу являются взаимосвязанные положения пункта 7 статьи 16 Закона Российской Федерации «О статусе судей в Российской Федерации» и части первой статьи 9 Федерального закона «Об оперативно-розыскной деятельности».

31. В отношении упомянутых в Обновленном плане действий определений Конституционного Суда Российской Федерации следует отметить отсутствие свидетельств учета их положений национальными судами, дающими разрешение на проведение оперативно-разыскных мероприятий и следственных действий, связанных с ограничением конституционных прав граждан.

32. В этой связи также следует отметить, что Суд, рассматривая дело Романа Захарова, пришел к выводу, что национальное законодательство не требует отчётливо, чтобы суды общей юрисдикции следовали мнению Конституционного Суда в отношении того, как следует толковать законодательное положение, если оно выражено в определении, а не в

постановлении (§263). С момента вынесения указанного Постановления описанная ситуация не изменилась.

33. Далее, Правительство Российской Федерации отмечает, что за период с 2014 по 2017 годы к уголовной ответственности по части 2 статьи 138 УК РФ было привлечено 79 человек (п.4 Обновленного плана действий).

34. Однако, Правительством не представлено сведений о количестве привлеченных к уголовной ответственности представителей власти, в частности - сотрудников полиции и ФСБ.

35. Между тем, при оценке представленных статистических сведений следует учитывать, что по части 2 статьи 138 УК РФ к ответственности могут привлекаться, к примеру, сотрудники операторов связи, которые в нарушение должностных инструкций, как правило из корыстной заинтересованности, незаконно получаются доступ к телефонным переговорам абонентов и детализации звонков.

36. Таким образом, а также учитывая общее незначительное число уголовных дел и приговоров за нарушение тайны телефонных переговоров (менее 20 в год), представленные Правительством Российской Федерации сведения не подтверждают, что указанная норма уголовного законодательства является эффективным средством предупреждения злоупотреблений в этой сфере.

37. Необходимо также отметить, что Обновленный план не предусматривает действий, направленных на исправление фундаментальных недостатков, отмеченных Судом, прежде всего таких, как крайне широкий спектр преступлений по которым допускается перехват, возможность перехвата в отношении неопределенного круга лиц, а также существование технической возможности обойти процедуру разрешения и перехватывать любые сообщения без получения предварительного судебного разрешения и отсутствие эффективного судебного контроля *ex post factum*.

ТЕКУЩАЯ СИТУАЦИЯ

38. Начиная с 2015 года российские власти предприняли целый ряд шагов, направленных на серьезное ограничение права на уважение частной жизни и тайну переписки, фактически распространив систему постоянного прямого контроля телефонных переговоров на все интернет-коммуникации.

39. Наиболее серьезной мерой является принятый 6 июля 2016 года так называемый «Закон Яровой» - Федеральный закон № 374-ФЗ «О внесении изменений в Федеральный закон «О противодействии терроризму» и отдельные законодательные акты Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности» (далее – «Закон №374», «Закон Яровой»).

40. Закон представляет собой пакет поправок, в частности, в Федеральный закон «Об информации, информационных технологиях и о защите информации» и Федеральный закон «О связи» под предлогом противодействия терроризму, затронувших различные аспекты регулирования телекоммуникаций, в том числе касающиеся приватности и анонимности.

Дополнение законодательства об оперативно-розыскной деятельности получением компьютерной информации

41. Закон №374 также дополняет перечень оперативно-розыскных мероприятий, содержащийся в статье 6 Федерального закона от 12 августа 1995 года №144-ФЗ «Об оперативно-розыскной деятельности», получением компьютерной информации.

42. Дополнительных гарантий соблюдения прав человека при проведении оперативно-розыскных мероприятий соответствующие поправки в законодательство не предусматривают.

Возложение на операторов связи обязанности собирать и хранить метаданные и сообщения абонентов

43. 16 апреля 2014 года принят Приказ Министерства связи и массовых коммуникаций Российской Федерации №83, устанавливающий обязательные требования к оборудованию коммутации и маршрутизации пакетов информации, входящему в состав сети связи общего пользования и выделенных сетей связи, включая программное обеспечение, обеспечивающему выполнение установленных действий при проведении оперативно-розыскных мероприятий (далее – «технические средства ОРМ»), согласно которому каждый оператор связи должен обеспечить как минимум следующее:

- подключение 16-ти пунктов управления техническими средствами ОРМ, запрет подключения иных интерфейсов управления;
- хранение в кольцевом буфере в течение не менее 12 часов всех поступающих пакетов данных, а также их обработку в соответствии со следующими заданными параметрами контроля: постоянные и динамические IP-адреса, имя учетной записи, электронные почтовые адреса (включая mail.ru, yandex.ru, rambler.ru, gmail.com, yahoo.com), идентификаторы телефонной линии и телефонные номера вызываемого и вызывающего абонента, идентификатор служб обмена сообщениями, IMEI, IMSI, MAC-адреса устройств, данные о местоположении абонентских терминалов и т.п.

44. Постановлением Правительства РФ от 31 июля 2014 г. №758 Правила оказания телематических услуг дополнены пунктом 22.1, обязывающим операторов связи дополнить договоры с абонентами-юридическими лицами, а также индивидуальными предпринимателями, обязанностью таких лиц ежеквартально предоставлять оператору связи списки лиц, использующих оконечное оборудование юридического лица с указанием их места жительства, и реквизитов основного документа, удостоверяющего личность. Постановление не содержит требований по безопасности хранения и не определяют процедуру обработки данных.

45. Согласно новой редакции части 1 статьи 64 Федерального закона «О связи», введенной Законом №374, операторы связи обязаны хранить на территории Российской Федерации: (1) информацию о фактах приема, передачи, доставки и (или) обработки голосовой информации, текстовых сообщений, изображений, звуков, видео- или иных сообщений пользователей услугами связи — в течение трех лет с момента окончания осуществления таких действий; (2) текстовые сообщения пользователей услугами связи, голосовую информацию, изображения, звуки, видео-, иные сообщения пользователей услугами связи — до шести месяцев с момента окончания их приема, передачи, доставки и (или) обработки.

46. Операторы связи при этом обязаны обеспечивать реализацию оперативно-розыскных мероприятий в установленном законом порядке.

47. 30 декабря 2017 года внесены поправки в Постановление Правительства РФ от 27.08.2005 №538 «Об утверждении Правил взаимодействия операторов связи с уполномоченными государственными органами, осуществляющими оперативно-разыскную деятельность», согласно которым оператор связи обязан в течение 3 лет хранить на территории Российской Федерации информацию, содержащуюся в базах данных об абонентах оператора связи и оказанных им услугах связи, в том числе информацию о фактах приема, передачи, доставки и (или) обработки голосовой информации, текстовых сообщений, изображений, звуков, видео- или иных сообщений, и предоставлять ее органам ФСБ и МВД путем осуществления круглосуточного удаленного доступа к базам данных.

48. 12 апреля 2018 года Постановлением Правительства Российской Федерации №445 утверждены «Правила хранения операторами связи текстовых сообщений пользователей услугами связи, голосовой информации, изображений, звуков, видео- и иных сообщений пользователей услугами связи».

49. В соответствии с Правилами, оператор связи осуществляет хранение на территории Российской Федерации текстовых

сообщений, голосовой информации, изображений, звуков, видео- и иных сообщений пользователей услугами связи данного оператора (далее - сообщения электросвязи) в принадлежащих оператору связи технических средствах накопления информации.

50. В целях исполнения этой обязанности оператор обеспечивает с 1 июля 2018 г. хранение сообщений электросвязи в нулевом объеме, а с 1 октября 2018 г. - хранение в полном объеме сообщений электросвязи в технических средствах накопления информации емкостью, равной объему сообщений электросвязи, отправленных и полученных пользователями указанного оператора за 30 суток, предшествующих дате ввода технических средств накопления информации в эксплуатацию. Емкость технических средств накопления информации увеличивается ежегодно на 15 процентов в течение 5 лет с даты ввода технических средств накопления информации в эксплуатацию.

Возложение на интернет-сервисы обязанности хранить метаданные, а также хранить и расшифровывать сообщения пользователей

51. Законом №374 также внесены поправки в часть 3 статьи 10.1 Федерального закона «Об информации, информационных технологиях и о защите информации», согласно которым организатор распространения информации обязан хранить на территории Российской Федерации (1) информацию о фактах приема, передачи, доставки и (или) обработки голосовой информации, письменного текста, изображений, звуков, видео- или иных электронных сообщений пользователей и информацию об этих пользователях в течение одного года с момента окончания осуществления таких действий; (2) текстовые сообщения пользователей, голосовую информацию, изображения, звуки, видео-, иные электронные сообщения до шести месяцев с момента окончания их приема, передачи, доставки и (или) обработки.

52. Организаторы распространения информации должны предоставлять указанную информацию органам, осуществляющим

оперативно-розыскную деятельность или обеспечение безопасности Российской Федерации в случаях, предусмотренных федеральными законами.

53. Сервисы, использующие шифрование, кроме того, должны предоставить Федеральной службе безопасности ключи, позволяющие расшифровать любые передаваемые, принимаемые и обрабатываемые с их помощью сообщения (часть 4.1 статьи 10.1 Федерального закона «Об информации, информационных технологиях и о защите информации»). При этом, **действующее национальное законодательство не обязывает спецслужбы получать предварительное судебное разрешение на доступ к такой информации.**

54. В настоящее время реестр интернет-компаний, на которые распространяется действие закона, насчитывает 152 сервиса, включая такие популярные платформы как ВКонтакте, Одноклассники, Mail.ru, Яндекс, Threema, Badoo, а также СМИ, городские и профессиональные форумы и т.д. По заявлениям представителей российских телекоммуникационных властей в настоящее время рассматривается вопрос о включении в реестр Apple, Twitter, Facebook и WhatsApp, Google, Microsoft, Viber и других международных компаний, представляющих миллиарды пользователей по всему миру.

55. В апреле-мае 2017 года за отказ зарегистрироваться в качестве организатора распространения информации и предоставить российским властям доступ к данным и сообщениям пользователей в России были заблокированы сервис обмена голосовыми сообщениями Zello, мессенджеры Imo, Line, Blackberry Messenger и сервис видеочатов Vchat.

56. 28 июня 2017 года интернет-мессенджер Telegram по решению Роскомнадзора был принудительно включен в Реестр организаторов распространения информации, что, согласно позиции российских властей, означает обязанность администратора сервиса хранить на территории России разнообразные метаданные и всю переписку пользователей и предоставлять их спецслужбам по запросу.

57. 14 июля 2017 года ФСБ России направила компании Telegram Messenger LLP требование предоставить информацию, необходимую для декодирования переписки, по 6 телефонным номерам. Судебных разрешений на доступ к переписке компании предоставлено не было. Ключи шифрования предлагалось направить по обычной электронной почте на общедоступный адрес интернет-приемной ФСБ. Компания отказалась выполнить этот запрос.

58. 16 октября 2017 года мировой судья в Москве вынес постановление о признании Telegram Messenger LLP виновной в совершении административного правонарушения, предусмотренного частью 2.1 статьи 13.31 Кодекса Российской Федерации об административных правонарушениях (неисполнение обязанности предоставить информацию, необходимую для декодирования сообщений) и оштрафовал на 800 000 рублей.

59. 13 апреля 2018 года Таганский районный суд Москвы обязал Федеральную службу по надзору в сфере связи, информационных технологий и массовых коммуникаций, а также третьих лиц заблокировать доступ пользователей к сервису Telegram на территории Российской Федерации[4].

60. Как следует из апелляционного определения Верховного суда Российской Федерации от 9 августа 2018 года по делу №АПЛ18-298, содержащего отсылку к статье 9 Федерального закона «Об информации, информационных технологиях и о защите информации», информация, необходимая для декодирования сообщений, не отнесена к информации ограниченного доступа и не составляет охраняемой Конституцией и федеральными законами тайны сообщений. При этом, организаторы распространения информации (т.е. компании-владельцы интернет-сервисов) не являются лицами, осуществляющими контроль и надзор за законностью проведения оперативно-разыскных мероприятий.

[4] Жалоба Telegram Messenger LLP зарегистрирована Европейским Судом по правам человека (application No.13232/18)

61. 1 сентября 2015 года также вступил в силу Федеральный закон от 21 июля 2014 г. N 242-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации в части уточнения порядка обработки персональных данных в информационно-телекоммуникационных сетях», которым внесены поправки в федеральные законы «О персональных данных» и «Об информации, информационных технологиях и о защите информации», устанавливающее обязанность операторов персональных данных (в том числе – интернет-сервисов) обрабатывать персональные данные граждан Российской Федерации с использованием баз данных, находящихся на территории страны.

62. В ноябре 2016 года из-за отказа перенести данные пользователей на российские серверы по решению Московского городского суда на территории Российской Федерации была заблокирована социальная сеть LinkedIn.

Обеспечение безопасности данных

63. В соответствии с Постановлением Правительства №445 оператор связи обеспечивает защиту технических средств накопления информации от несанкционированного доступа к ним и хранящейся в них информации в соответствии с требованиями, установленными Министерством связи и массовых коммуникаций Российской Федерации.

64. Такие требования закреплены в приказе Минкомсвязи №83 (см. п.43 настоящего Доклада) и заключаются в том, что технические средства ОРМ должны быть выполнены в отдельном корпусе, оснащенном запирающими устройствами, исключающими возможность свободного доступа к аппаратным элементам технических средств ОРМ и запрете альтернативных интерфейсов управления.

65. В соответствии с пунктом 4 указанных правил, технические средства накопления информации входят в состав и идентифицируются как оборудование средств связи, включая

программное обеспечение, обеспечивающее выполнение установленных действий при проведении оперативно-розыскных мероприятий.

66. Технически и организационно хранилища информации, создаваемые в рамках Закона №374 («Закон Яровой»), должны предусматривать постоянный удаленный неограниченный доступ спецслужб с помощью технических средств ко всем пользовательских данным.

67. Таким образом, эти хранилища являются дальнейшей эволюцией системы СОРМ, которая была предметом рассмотрения Европейского Суда в деле «Роман Захаров против Российской Федерации».

Отсутствие эффективного судебного контроля

68. По сведениям Судебного департамента при Верховном суде Российской Федерации с 2015 по 2017 годы национальные суды выдали более 1,8 миллиона разрешений об ограничении конституционных прав граждан на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений, передаваемых по сетям электрической и почтовой связи в рамках оперативно-разыскных мероприятий, удовлетворяя в среднем 99,32% соответствующих запросов.

69. За этот же период выдано более 0,8 миллиона разрешений на контроль и запись телефонных и иных переговоров, а также получение информации о соединениях между абонентами в рамках следственных действий, удовлетворяя в среднем 97,39% запросов.

70. Таким образом предварительный судебный контроль за деятельностью органов, осуществляющих оперативно-разыскную деятельность является иллюзорным и не может гарантировать соблюдение прав граждан при перехвате переписки.

71. Закон «Об оперативно-розыскной деятельности» по-прежнему предусматривает возможность перехвата сообщений и

информации в некоторых случаях без решения суда, с последующим уведомлением суда в течение 24 часов. То есть, даже в рамках закона суд, даже признав перехват незаконным, не может предотвратить нарушение прав граждан, которое уже имело место. В ряде случаев, например, в избирательном процессе, законодательство Российской Федерации предусматривает принятие экстренных судебных решений (ч.4 ст. 78 Федерального закона от 12 июня 2002 г. N 67-ФЗ «Об основных гарантиях избирательных прав и права на участие в референдуме граждан Российской Федерации»). Таким образом имеется возможность предусмотреть законом возможность вынесения при необходимости экстренного решение суда, не допуская перехвата с последующим уведомлением.

Экономический эффект вводимых мер по контролю коммуникаций

72. Согласно различным оценкам расходы операторов связи на реализацию мероприятий, предусмотренных Законом №374, могут составить от нескольких миллиардов[5] до 10 триллионов рублей в год[6].

73. Неизбежным последствием новых мер станет рост цен на услуги связи, банкротство небольших компаний, оказывающих услуги связи, дальнейшая монополизация рынка телекоммуникаций. Выполнение Закона № 374 чрезвычайно сложно для большинства телекоммуникационные компаний, однако его требования к приобретению и установке оборудования для хранения данных фатально для небольших сервисов. Это вынудит региональных операторов продавать бизнес, либо нарушать законодательство.

[5] https://www.rbc.ru/business/05/03/2018/5a9ce5939a794745f656c133

[6] https://meduza.io/news/2017/04/10/rspp-otsenil-zatraty-na-zakon-yarovoy-v-10-trillionov-rubley-on-razgonit-inflyatsiyu

74. Начиная с весны 2018 года, операторы связи начали повышать тарифы, объяснив это необходимостью компенсировать стоимость реализация «Закона Яровой». Увеличение цены в среднем 5-10%.

ЗАКЛЮЧЕНИЕ И РЕКОМЕНДАЦИИ

75. Исходя из изложенного можно сделать вывод о том, что ситуация в сфере перехвата сообщений при осуществлении правоохранительной деятельности в России после вынесения Европейским Судом Постановления по делу «Роман Захаров против Российской Федерации», но, напротив, значительно ухудшилась.

76. Предпринимаемые российскими властями шаги, в том числе принятие законов, обязывающих операторов связи и интернет-сервисы хранить гигантские объемы пользовательских данных и сообщений в отсутствие эффективных механизмов контроля, а также обжалования незаконных действий и возмещения ущерба от разглашения личной информации, неизбежно приведут к массовому нарушению прав граждан на приватность и анонимность, ухудшению экономического положения небольших частных компаний, ущемлению конкуренции и дальнейшей монополизации рынка телекоммуникационных услуг.

77. Установленные законодательством меры по обеспечению безопасности хранимых данных и гарантии защиты от недобросовестного доступа к ним со стороны государственных и негосударственных субъектов, представляются явно недостаточными.

78. Нормативные правовые акты, устанавливающие все новые механизмы массовой слежки за гражданами, фактически принимаются в чрезвычайном порядке - без широкого публичного обсуждения и учета позиция заинтересованных сторон, в том числе представителей гражданского общества и интернет-отрасли.

79. Считаем важным отметить, что за последние годы Организация Объединенных Наций и ее специализированные институты сформулировали развернутые стандарты соблюдения

прав человека онлайн, в том числе права на свободное выражение мнения, а также на приватность и анонимность, значительно опередив в этом Совет Европы.

80. Так, Резолюция, принятая Генеральной Ассамблеей ООН 18 декабря 2013 года «Право на неприкосновенность частной жизни в цифровой век», прямо призывает все государства провести обзор своих процедур, практики и законодательства, касающихся слежения за сообщениями, их перехвата и сбора личных данных, включая массовое слежение, перехват и сбор, в целях защиты права на неприкосновенность личной жизни путем обеспечения полного и эффективного выполнения всех их обязательств по международному праву прав человека (A/Res/68/167).

81. Согласно Докладу Верховного комиссара ООН по правам человека неизбирательное тайное массовое слежение и перехват коммуникаций, сбор, хранение и анализ данных о всех пользователях в рамках широкого круга средств коммуникации (например, электронная почта, телефонные и видеозвонки, текстовые сообщения и посещаемые веб-сайты), не допускается международным правом прав человека, поскольку при таких мерах невозможно проводить анализ каждого конкретного случая на предмет необходимости и соразмерности применяемых мер (п.17, A/HRC/39/29).

82. В Докладе Специального докладчика ООН по вопросу о поощрении и защите права на свободу мнений и их свободное выражение отмечается, что законодательные предложения о пересмотре или принятии ограничений в отношении личной безопасности в онлайновой среде подлежат публичному обсуждению и утверждаются только на основе обычного, публичного, обоснованного и транспарентного законодательного процесса. Государства обязаны поощрять действенное участие широкого круга представителей гражданского общества и групп меньшинств в таких обсуждениях и процессах и избегать принятия такого законодательства на основании ускоренных законодательных процедур (п.58, A/HRC/29/32).

83. Создание новых механизмов хранения, обработки и перехвата всех видов интернет-трафика в рамках СОРМ, «Закона Яровой» и сопутствующих им нормативных правовых актов, предпринятое российскими властями в последние годы представляет собой дальнейшее развитие системы неизбирательной и неподконтрольной обществу массовой слежки, что прямо противоречит как международному праву прав человека в целом, так и Постановлению Европейского Суда по делу «Роман Захаров против Российской Федерации».

84. В этой связи мы просим Комитет Министров Совета Европы:

A) обратить внимание Правительства на необходимость отмены Федерального закона № 374-ФЗ «О внесении изменений в Федеральный закон «О противодействии терроризму» и отдельные законодательные акты Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности» в части, касающейся поправок в законы «О связи», и «Об информации, информационных технологиях и о защите информации»;

B) обратить внимание Правительства на необходимость усиления ответственности операторов связи и интернет-сервисов за соблюдение прав человека, в частности, законодательного закрепления обязанности регулярно публиковать развернутые отчеты о количествах обращениях государственных органов и частных лиц, связанных с ограничением доступа к контенту, а также о количествах запросов со стороны государственных органов на раскрытие пользовательской информации (transparency reports);

C) обратить внимание Правительства на необходимость изменения технологии перехвата, позволяющей органам, осуществляющим оперативно-розыскную деятельность иметь постоянный прямой доступ ко всем телефонным переговорам и интернет-коммуникациям всех пользователей.

D) предложить Правительству включить в проект поправок в законодательство об оперативно-розыскной деятельности, требование обязательного предварительного предоставления

поставщикам услуг связи и организаторам распространения информации судебного разрешения на доступ к сообщениям пользователей и метаданным;

E) сформулировать требование обязательного предварительного публичного и транспарентного обсуждения всех принимаемых норм, ограничивающих цифровые права граждан, на основе мультистейкхолдерного подхода с привлечением представителей гражданского общества и интернет-отрасли.

F) продолжить контроль за исполнением Российской Федерацией постановления по делу «Роман Захаров против Российской Федерации».

От Агоры	_____	Павел Чиков
От ОАОО	_____	Рамиль Ахметгалиев