EUROPEAN COURT OF HUMAN RIGHTS
COUR EUROPÉENNE DES DROITS DE L'HOMME

ЕВРОПЕЙСКИЙ СУД ПО ПРАВАМ ЧЕЛОВЕКА
БОЛЬШАЯ ПАЛАТА

Дело «Центр правосудия (Centrum för rättvisa) против Швеции»[1]

(Жалоба № 35252/08)

ПОСТАНОВЛЕНИЕ[2]

г. Страсбург, 25 мая 2021 г.

По делу «Центр правосудия против Швеции» Европейский Суд по правам человека, заседая Большой Палатой в составе:

Роберта Спано, *Председателя Большой Палаты Суда*,
Йона Фридрика Кьёльбро,
Ангелики Нуссбергер,
Пауля Лемменса,
Йонко Грозева,
Винсента А. де Гаэтано,
Пауло Пинто де Альбукерке,
Фариса Вехабовича,
Юлии Антоанеллы Моток,
Карла Ранзони,
Мартиньша Митса,
Габриэль Кучко-Штадлмайер,
Марко Бошняка,
Тима Эйке,
Дариана Павли,
Эрика Веннерстрёма,
Саадет Юксель, *судей*,

а также при участии Сёрена Пребенсена, *заместителя Секретаря Большой Палаты Суда*,

рассмотрев дело в закрытых заседаниях 11 июля, 4 и 6 сентября 2019 г. и 17 февраля 2021 г.,

вынес в последнюю указанную дату следующее Постановление:

ПРОЦЕДУРА

1. Дело было инициировано жалобой (№ 35252/08), поданной против Королевства Швеция в Европейский Суд по правам человека (далее – Европейский Суд) в соответствии со статьей 34 Конвенции о защите прав человека и основных свобод (далее – Конвенция) шведским фондом «Центр правосудия» (далее – заявитель) 14 июля 2008 г.

2. Интересы заявителя представляли адвокаты Ф. Бергман (F. Bergman) и А. Эванс (A. Evans), практикующие в г. Стокгольме. Власти Швеции (далее также – власти государства-ответчика) были представлены их Уполномоченным при Европейском Суде Э. Хаммаршёльд (E. Hammarskjöld), руководителем юридического управления Министерства иностранных дел.

3. Заявитель утверждал, что законодательство и правоприменительная практика Швеции в области радиотехнической разведки нарушали его права, предусмотренные статьей 8 Конвенции, и что у него отсутствовало эффективное средство правовой защиты в этом отношении в нарушение статьи 13 Конвенции.

4. Жалоба была распределена в Третью Секцию Европейского Суда (пункт 1 правила 52 Регламента Европейского Суда). 1 ноября 2011 г. (в отношении приемлемости жалобы для рассмотрения по существу) и 14 октября 2014 г. (в отношении приемлемости жалобы для рассмотрения по существу и по ее существу) жалоба была коммуницирована властям Швеции. 19 июня 2018 г. Палата Третьей Секции Европейского Суда в следующем составе: Бранко Лубарды, Председателя, Хелены Ядерблом, Хелен Келлер, Пере Пастора Вилановы, Алёны Полачковой, Георгия А. Сергидеса, Жольены Шуккинг, судей, а также при участии Стивена Филлипса, Секретаря Секции Суда, – вынесла Постановление, в котором единогласно объявила жалобу приемлемой для рассмотрения по существу и постановила, что по делу не было допущено нарушения требований статьи 8 Конвенции и что отсутствовала необходимость отдельно рассматривать жалобу в соответствии со статьей 13 Конвенции.

5. 19 сентября 2018 г. заявитель ходатайствовал о передаче дела на рассмотрение Большой Палаты Европейского Суда в соответствии со статьей 43 Конвенции. 4 февраля 2019 г. коллегия судей Большой Палаты Европейского Суда удовлетворила это ходатайство.

6. Состав Большой Палаты Европейского Суда был определен в соответствии с положениями пунктов 4 и 5 статьи 26 Конвенции и правила 24 Регламента Европейского Суда. Председатель Большой Палаты Европейского Суда постановил, что в интересах надлежащего отправления правосудия настоящее дело должно быть передано тому же составу Большой Палаты Европейского Суда, что и в деле «Организация Big Brother Watch и другие против Соединенного Королевства» (Big Brother Watch and Others v. United Kingdom) (жалоба № 58170/13 и две другие жалобы) (правило 24, пункт 2 правила 42 и правило 71 Регламента Европейского Суда).

7. Заявитель и власти Швеции представили замечания по существу дела (пункт 1 правила 59 Регламента Европейского Суда).

[1] Перевод с английского ООО «Развитие правовых систем».

[2] Настоящее Постановление вступило в силу 25 мая 2021 г. в соответствии с положениями пункта 1 статьи 44 Конвенции (*примеч. редактора*).

8. Председатель Большой Палаты Европейского Суда разрешил властям Эстонии, Франции, Нидерландов и Норвегии представить письменные замечания (пункт 2 статьи 36 Конвенции, пункт 3 правила 44 Регламента Европейского Суда).

9. Открытое слушание по делу состоялось во Дворце прав человека в г. Страсбурге 10 июля 2019 г.

В заседании Большой Палаты Европейского Суда приняли участие:

(a) со стороны властей Швеции:

Э. Хаммаршёльд, руководитель юридического управления Министерства иностранных дел, *Уполномоченный Швеции при Европейском Суде*,

Г. Исакссон (G. Isaksson), заместитель руководителя, сотрудница Министерства иностранных дел,

Й. Шёстранд (J. Sjöstrand), старший юрисконсульт, сотрудница Министерства иностранных дел,

Й. Гартон (J. Garton), заместитель генерального директора, сотрудник Министерства обороны,

М. Андерссон (M. Andersson) старший юрисконсульт, сотрудник Министерства обороны,

Х. Селлман (H. Sellman), заместитель директора, сотрудник Министерства юстиции,

Ф. Кшижански (F. Krzyzanski) юрисконсульт, сотрудница Министерства инфраструктуры,

М. Драб (M. Dráb), старший юрисконсульт, сотрудница Радиотехнического центра Вооруженных сил Швеции,

К. Хеллстен (C. Hellsten), старший советник, сотрудник Радиотехнического центра Вооруженных сил Швеции, *консультанты*,

(b) со стороны заявителя:

Ф. Бергман,

А. Эванс,

А. Оттоссон (A. Ottosson), *адвокаты*,

Э. Пальм (E. Palm), *советник*.

Европейский Суд заслушал выступления А. Эванс, Ф. Бергмана и Э. Хаммаршёльд.

ФАКТЫ

10. Заявитель, фонд «Центр правосудия», был учрежден в 2002 году. Его штаб-квартира находится в г. Стокгольме.

11. Заявитель представляет интересы клиентов в судебных разбирательствах, касающихся конвенционных прав и свобод, а также в рамках сопутствующих судебных разбирательств в соответствии с законодательством Швеции. Он также принимает участие в образовательных и исследовательских проектах, в общественных дебатах по вопросам, связанным с правами и свободами человека.

12. Заявитель ежедневно общается с отдельными людьми, организациями и компаниями в Швеции и за рубежом по электронной почте, телефону и факсу. Он утверждает, что большая часть этого общения требует особой защиты с точки зрения неприкосновенности частной жизни. В связи с характером своей функции неправительственной организации, контролирующей деятельность представителей государства, заявитель считает, что существует риск того, что его сообщения были или будут перехвачены и изучены с помощью средств радиотехнической разведки.

13. Заявитель не обращался с какими-либо исками в суды Швеции, утверждая, что отсутствуют эффективные внутригосударственные средства правовой защиты для его жалоб в соответствии с Конвенцией.

СООТВЕТСТВУЮЩЕЕ ЗАКОНОДАТЕЛЬСТВО И ПРАВОПРИМЕНИТЕЛЬНАЯ ПРАКТИКА

I. ЗАКОНОДАТЕЛЬСТВО И ПРАВОПРИМЕНИТЕЛЬНАЯ ПРАКТИКА ШВЕЦИИ

A. Общие положения о радиотехнической разведке

14. Радиотехническую разведку можно определить как перехват, обработку, анализ и передачу сведений, полученных из электронных сигналов. Эти сигналы могут быть преобразованы в текст, изображения и звук. Информация, полученная с помощью таких способов, может касаться как содержания сообщения, так и связанных с ним данных (например, описывающих, каким образом, когда и между какими адресами осуществляется электронное общение). Информация может быть перехвачена по воздушным каналам связи, обычно по радиоканалам и спутникам, и по кабельным средствам связи. Передача сигнала воздушным или проводным путем контролируется провайдером услуг связи, то есть телекоммуникационными, кабельными компаниями, интернет-компаниями и иными подобными компаниями, которые обеспечивают различные формы электронной передачи информации. Бóльшая часть трафика, имеющего отношение к радиотехнической разведке, передается проводным путем. Термин «носители сообщений» (или «носители сигналов») относится к носителю, используемому для передачи одного или нескольких сигналов. Если иное не указано ниже, в нормах, регулирующих радиотехническую разведку в Швеции, не проводится различий между содержанием сообщений и данными о них, а также между воздушным и кабельным трафиком.

15. Согласно Закону о внешней разведке (*Lagen om försvarsunderrättelseverksamhet*, 2000:130) внешняя разведка проводится для защиты внешней политики, обороны и безопасности Швеции, а также в целях выявления внешних угроз для страны. Подобные мероприятия должны также способствовать участию Швеции в международном сотрудничестве в области безопасности. В соответствии

с данным законом разведка может проводиться только в отношении иностранных элементов (пункт 1 статьи 1). Это не исключает того, что некоторые обстоятельства, связанные с иностранными элементами, могут иметь последствия в Швеции, например, при отслеживании шпионажа иностранных государств против Швеции (подготовительные материалы к законодательству о внешней разведке, предложение № 2006/07:63, с. 43).

16. Власти Швеции определяют направления деятельности. Они также устанавливают, какие органы могут давать более детальные указания, и какой орган должен осуществлять разведывательную деятельность (пункты 2 и 3 статьи 1 Закона о внешней разведке). Власти Швеции ежегодно издают распоряжения общего характера с указанием задач. Внешняя разведка не может проводиться для решения задач в тех сферах правоохранительной деятельности или предупреждения преступлений, которые относятся к полномочиям органов Главного полицейского управления, Государственной службы безопасности и иных органов и которые регулируются другим законодательством. Однако органы, осуществляющие внешнюю разведку, могут оказывать помощь органам, занимающимся правоохранительной деятельностью или предупреждением преступлений (статья 4 Закона о внешней разведке). Примерами такой помощи являются криптоанализ и техническая помощь в отношении информационной безопасности (подготовительные материалы к законодательству о внешней разведке, предложение № 2006/07:63, с. 136).

17. Получение электронных сигналов представляет собой одну из форм внешней разведки, которая регулируется Законом о радиотехнической разведке (*Lagen om signalspaning i försv arsunderrättelseverksamhet*, 2008:717), вступившим в силу 1 января 2009 г. В данный закон 1 декабря 2009 г., 1 января 2013 г., 1 января 2015 г. и 15 июля 2016 г. были внесены изменения. Дополнительные положения содержатся в Постановлении о радиотехнической разведке (*Förordningen om signalspaning i försvarsunder rättelseverksamhet*, 2008:923). Законодательство уполномочивает Радиотехнический центр Вооруженных сил Швеции (*Försvarets radioanstalt*) (далее – Радиотехнический центр) осуществлять радиотехническую разведку (статья 2 Постановления по сравнению со статьей 1 Закона о радиотехнической разведке).

18. При проведении подобной разведки все проводные трансграничные сообщения передаются в определенные пункты приема. В этих пунктах информация не хранится, и ограниченный объем трафика данных передается в Радиотехнический центр с помощью носителей сообщений (доклад парламентского комитета, SOU2016:45, с. 107).

19. Радиотехнический центр может проводить разведку только на основании конкретного распоряжения с указанием задач, изданного властями Швеции, государственными учреждениями, Вооруженными силами или с января 2013 года Государственной службой безопасности и Национальным оперативным отделением Главного полицейского управления (*Nationella operativa avdelningen i Polismyndigheten*) (пункт 1 статьи 1 и пункт 1 статьи 4 Закона о радиотехнической разведке) в соответствии с точным разведывательным заданием соответствующего органа. При этом направление «деятельности Радиотехнического центра по разработке» может определяться исключительно властями Швеции (пункт 2 статьи 4 Закона о радиотехнической разведке). Подробное распоряжение с указанием задач определяет направление разведывательной деятельности и может касаться соответствующего явления или ситуации, но не может быть ориентировано исключительно на конкретное физическое лицо (пункт 3 статьи 4 Закона о радиотехнической разведке).

20. Полномочия Государственной службы безопасности и Национального оперативного отделения Главного полицейского управления по изданию детальных распоряжений с указанием задач направлены на улучшение способности этих органов на стратегическом уровне получать данные об иностранных элементах, связанных с международным терроризмом и иными серьезными международными преступлениями, которые могут угрожать важным национальным интересам. На момент введения новых правил власти Швеции заявили в подготовительных материалах (предложение № 2011/12:179, с. 19), что эти полномочия соответствуют запрету на ведение радиотехнической разведки в целях решения задач в области правоохранительной деятельности или предупреждения преступлений.

21. В соответствии с Постановлением о внешней разведке (*Förordningen om försvarsunderrättel severksamhet*, 2000:131) детальное распоряжение с указанием задач должно содержать информацию (i) об издавшем его органе, (ii) о той части ежегодного распоряжения, которую оно затрагивает, (iii) об явлении или ситуации, которые предполагается охватить, и (iv) о необходимости сбора информации об этом явлении или ситуации (статья 2(a) Постановления).

B. Сфера применения радиотехнической разведки

22. Цели, для которых могут быть получены электронные сигналы в рамках внешней разведки, указаны в Законе о радиотехнической разведке (пункт 2 статьи 1), который предусматривает, что

радиотехническая разведка может проводиться только для мониторинга:

1) внешних военных угроз для страны;

2) условий участия Швеции в международных миротворческих или гуманитарных миссиях или угроз для безопасности интересов Швеции при выполнении таких операций;

3) стратегических обстоятельств, связанных с международным терроризмом или другими серьезными трансграничными преступлениями, которые могут угрожать важным национальным интересам;

4) разработки и распространения оружия массового поражения, военной техники и иной подобной специальной продукции;

5) серьезных внешних угроз социальной инфраструктуре;

6) внешних конфликтов, имеющих последствия для международной безопасности;

7) операций внешней разведки против интересов Швеции, а также

8) действий или намерений иностранной державы, которые имеют существенное значение для внешней политики, политики безопасности или обороны Швеции.

23. Восемь указанных целей подробно разъяснены в подготовительных материалах к законодательству (предложение № 2008/09:201, с. 108–109):

> «Цели, для которых может быть разрешена радиотехническая разведка, перечислены в восьми пунктах. Первый пункт касается внешних военных угроз для страны. Под военными угрозами понимаются не только неминуемые угрозы, такие как угроза вторжения, но и явления, которые в долгосрочной перспективе могут перерасти в угрозы безопасности. Следовательно, формулировка охватывает изучение военных потенциала и мощностей в непосредственной близости от Швеции.
>
> Второй пункт включает в себя как исследования, необходимые для формирования надлежащей базы для принятия решения об участии в международных миротворческих или гуманитарных миссиях, так и исследования, проводимые при выполнении текущих миссий в отношении угроз для шведского персонала или для других интересов Швеции.
>
> Третий пункт относится к стратегическому изучению международного терроризма или иных серьезных трансграничных преступлений, таких как незаконный оборот наркотических средств или торговля людьми, настолько тяжких, что это может угрожать важным национальным интересам. Задача радиотехнической разведки в отношении подобных видов деятельности состоит в том, чтобы изучить их с точки зрения внешней политики и политики безопасности. Разведывательные данные, необходимые для оперативной борьбы с преступной деятельностью, в первую очередь относятся к сфере ответственности полиции.
>
> Четвертый пункт касается необходимости использования радиотехнической разведки, среди прочего, для отслеживания деятельности, имеющей отношение к обязательствам Швеции в отношении нераспространения и экспортного контроля оружия массового поражения, даже в тех случаях, когда такая деятельность не является преступлением или не противоречит международным конвенциям.
>
> Пятый пункт включает, среди прочего, серьезные угрозы, связанные с информационными технологиями, которые исходят из-за границы. Серьезный характер угроз означает, например, что они должны быть направлены на жизненно важные общественные системы энерго- и водоснабжения, связи или финансовых услуг.
>
> Шестой пункт относится к изучению конфликтов между другими странами и в других странах, которые могут иметь последствия для международной безопасности. Речь может идти о регулярных военных действиях между государствами, а также о внутренних или трансграничных конфликтах между разными этническими, религиозными или политическими группами. Исследование конфликтов предполагает изучение их причин и последствий.
>
> Седьмой пункт означает, что разведывательная деятельность, направленная против интересов Швеции, может осуществляться с помощью методов радиотехнической разведки.
>
> Восьмой пункт предоставляет возможность проводить радиотехническую разведку против иностранных держав и их представителей с целью изучить их намерения или действия, которые имеют существенное значение для внешней политики, политики безопасности или обороны Швеции. Такая разведывательная деятельность может осуществляться только в отношении лиц, представляющих иностранную державу. Условие наличия "существенного значения" подчеркивает недостаточность того, чтобы явление представляло общий интерес, напротив, разведывательные данные должны оказывать непосредственное воздействие на действия или позицию Швеции по различным вопросам внешней политики, политики безопасности или обороны…».

24. Радиотехнический центр также вправе осуществлять сбор электронных сигналов в целях мониторинга изменений в областях международной радиотехнической обстановки, технического прогресса и радиотехнической защиты, а также разрабатывать технологии, необходимые для радиотехнической разведки (пункт 3 статьи 1 Закона о радиотехнической разведке). Данные виды деятельности известны как «деятельность по разработке», и согласно соответствующим подготовительным материалам (предложение № 2006/07:63, с. 72) при их проведении не требуется составления каких-либо разведывательных донесений. Сигналы, перехватываемые в рамках деятельности Радиотехнического центра по разработке, представляют интерес для государственных органов не с точки зрения данных, которые они могут содержать, а только с точки зрения возможности проанализировать системы и способы передачи информации. Радиотехнический центр вправе обмениваться опытом в сфере технологических вопросов с другими органами. Деятельность по разработке,

как правило, не фокусируется на сообщениях физических лиц, хотя сведения о личных данных физических лиц могут перехватываться.

25. Радиотехническая разведка, осуществляемая по кабелям, может касаться только сигналов, пересекающих границу Швеции по кабелям, принадлежащим провайдеру услуг связи (статья 2 Закона о радиотехнической разведке). Сообщения между отправителем и получателем на территории Швеции не могут быть перехвачены независимо от того, имеет ли источник сигнала воздушное происхождение или передается по кабелю. Если такие сигналы не могут быть разделены в пункте приема, их запись или сведения о них должны быть уничтожены, как только будет установлено, что они были получены (статья 2(a) Закона о радиотехнической разведке).

26. Перехват кабельных сигналов автоматизирован и должен затрагивать только те сигналы, которые были идентифицированы с помощью селекторов (или «поисковых запросов»). Данные селекторы также используются для идентификации сигналов, передаваемых воздушным путем, если процедура автоматизирована. Селекторы должны быть сформулированы таким образом, чтобы в максимально возможной степени ограничить нарушение права на личную неприкосновенность. Селекторы, непосредственно относящиеся к конкретному физическому лицу, могут использоваться только в том случае, если это представляет исключительную важность для разведывательной деятельности (статья 3 Закона о радиотехнической разведке).

27. В подготовительных материалах к Закону о радиотехнической разведке (предложение № 2006/07:63, с. 90) уточняется, что требование исключительной важности, предусмотренное в его статье 3, необходимо вследствие того, что использование поисковых запросов, относящихся к конкретному лицу, например, личные имена, номера телефонов, адреса электронной почты или IP-адреса, вызывает особые риски с точки зрения защиты частной жизни. Возможность использования таких поисковых запросов должна рассматриваться только при исключительных обстоятельствах, и ей должна предшествовать тщательная оценка необходимости, в частности, того, является ли информация, которую можно получить подобным образом, настолько важной, чтобы оправдывать применение данной меры. В качестве примера приводится следующая гипотетическая ситуация: национальный кризис, вызванный информационной атакой на системы, имеющие жизненно важное значение для общества, когда необходимо принимать немедленные меры для установления личностей конкретных субъектов.

28. После перехвата сигналы обрабатываются. Это означает, что они, например, подвергаются криптоанализу или переводу. Затем информация анализируется и передается в орган, который поручил Радиотехническому центру сбор соответствующих разведывательных данных.

29. Согласно описанию, предоставленному властями Швеции, этот процесс состоит из шести этапов:

1) выбор наиболее актуальных сегментов радиотехнической обстановки;

2) автоматическое применение селекторов к сигналам в выбранных сегментах в целях перехвата и постепенного сокращения получаемых сведений;

3) дальнейшая обработка данных с помощью автоматизированных и ручных средств с применением, среди прочего, криптоанализа, структурирования и перевода с одного языка на другой;

4) изучение обработанных сведений аналитиком в целях выявления среди них разведывательных данных;

5) составление отчета и его распространение среди выбранных получателей, относящихся к внешней разведке;

6) запрос обратной связи об использовании предоставленных разведывательных данных и о последствиях такого использования, а также обмен обратной связью с участниками процесса.

C. Санкционирование проведения радиотехнической разведки

30. Для проведения всех видов радиотехнической разведки, включая деятельность по разработке, Радиотехнический центр должен обращаться за разрешением в Суд по вопросам внешней разведки (*Försvarsunderrättelsedomstolen*). Заявление должно содержать полученный Радиотехническим центром запрос на проведение разведки, включая информацию о соответствующем детальном распоряжении с указанием задач и необходимости в запрашиваемой разведывательной информации. Кроме того, должны быть перечислены носители сообщений, доступа к которым требует Радиотехнический центр, а также используемые селекторы или категории селекторов. Наконец, в заявлении должен быть указан срок, на который запрашивается разрешение (статья 4(a) Закона о Радиотехнической разведке).

31. Разрешение может быть предоставлено только в следующих случаях: миссия соответствует положениям Закона о внешней разведке и Закона о радиотехнической разведке; цель перехвата сигналов не может быть достигнута при меньшем вмешательстве; ожидается, что в ходе миссии может быть получена информация, ценность которой явно превышает возможное вмешательство в право на личную неприкосновенность; селекторы или категории селекторов соответствуют Закону о радиотехнической разведке; применение разведывательных мер не направлено исключительно

на конкретное физическое лицо (статья 5 Закона о радиотехнической разведке).

32. В случае его предоставления разрешение должно содержать следующие сведения: указание на миссию, в целях которой может проводиться радиотехническая разведка; о носителях, к которым Радиотехнический центр будет иметь доступ; о селекторах или категориях селекторов, которые могут быть использованы; о сроке действия разрешения и других условиях, необходимых для ограничения вмешательства в право на личную неприкосновенность (статья 5(a) Закона о радиотехнической разведке).

33. Радиотехнический центр сам может принять решение о выдаче разрешения, если заявление о выдаче разрешения Судом по вопросам внешней разведки может вызвать задержку или другие проблемы, имеющие существенное значение для одной из указанных целей радиотехнической разведки. Если Радиотехнический центр выдает разрешение, он должен незамедлительно уведомить об этом суд, который обязан незамедлительно принять решение по данному вопросу. Суд по вопросам внешней разведки вправе отозвать или изменить разрешение (статья 5(b) Закона о радиотехнической разведке).

34. Состав Суда по вопросам внешней разведки и его деятельность регулируются Законом о суде по вопросам внешней разведки (*Lagen om Försvarsunderrättelsedomstol*, 2009:966). В его состав входят один председатель, один или два вице-председателя и от двух до шести других членов. Председателем является постоянный судья, предложенный Советом по выдвижению кандидатур судей (*Domarnämnde*n) и назначаемый властями Швеции. Вице-председатели, которые должны иметь юридическое образование и опыт работы в качестве судей, а также другие члены суда, которые должны обладать специальными знаниями, имеющими отношение к работе суда, назначаются властями Швеции на четырехлетний срок. Заявления о выдаче разрешений на проведение радиотехнической разведки рассматриваются во время слушаний, которые могут проводиться за закрытыми дверями, если очевидно, что в ходе публичных слушаний будет раскрыта секретная информация. Разбирательство в Суде по вопросам внешней разведки проходит в присутствии сотрудников Радиотехнического центра и представителя по вопросам защиты частной жизни (*integritetsskyddsombud*). Представитель, который выражает интересы не какого-либо конкретного лица, а отдельных лиц в целом, осуществляет мониторинг вопросов, касающихся права на личную неприкосновенность, имеет доступ к материалам дела и вправе делать заявления. Представители по вопросам защиты частной жизни назначаются властями Швеции на четырехлетний срок и должны быть судьями на постоянной основе или адвокатами либо в прошлом являться таковыми. Суд по вопросам внешней разведки может проводить слушание и принимать решение по заявлению в отсутствие представителя только в том случае, если дело является настолько срочным, что задержка в его рассмотрении может серьезно нарушить цель подачи заявления. Решения Суда по вопросам внешней разведки являются окончательными.

D. Продолжительность радиотехнической разведки

35. Разрешение на проведение радиотехнической разведки может быть выдано на конкретный срок, не превышающий шести месяцев. После повторного рассмотрения указанный срок может продлеваться каждый раз на шесть месяцев (статья 5(a) Закона о радиотехнической разведке).

E. Порядок хранения, оценки, изучения, использования и уничтожения перехваченных данных

36. Государственная инспекция по надзору за разведывательной деятельностью (*Statens inspektion för försvarsunderrättelseverksamheten*) (далее – Инспекция по надзору) (см. также ниже §§ 50–54) контролирует доступ к носителям сообщений. Провайдеры услуг связи обязаны передавать кабельные сигналы, пересекающие границу Швеции, в «пункты сотрудничества», согласованные с Инспекцией по надзору которая, в свою очередь, предоставляет Радиотехническому центру доступ к носителям в той мере, в какой такой доступ охватывается разрешением на проведение радиотехнической разведки, и тем самым приводит в исполнение разрешения, выданные Судом по вопросам внешней разведки (статья 19(a) главы 6 Закона об электронной коммуникации (*Lagen om elektronisk kommunikation*, 2003:389). Совет по законодательству (*Lagrådet*) – орган, дающий заключения по запросу властей Швеции или парламентского комитета по определенным законопроектам, высказал мнение о том, что вмешательство в права на частную жизнь и корреспонденцию уже имеет место на данном этапе, поскольку власти получают доступ к средствам связи (предложение № 2006/07:63, с. 172).

37. В соответствии с Законом о радиотехнической разведке Радиотехнический центр должен немедленно уничтожать перехваченные данные в тех случаях, когда они (i) касаются конкретного физического лица и не имеют значения для радиотехнической разведки; (ii) защищены конституционными положениями об обеспечении конфиденциальности в целях защиты анонимных авторов и средств массовой информации; (iii) содержат информацию, которой обмениваются подозреваемый и его или ее адвокат и на которую

вследствие этого распространяется адвокатская тайна; (iv) содержат информацию, предоставленную в религиозном контексте исповеди или индивидуального консультирования, кроме случаев, когда имеются исключительные причины для изучения такой информации (статья 7).

38. Если были перехвачены сообщения между отправителем и получателем, которые находятся в Швеции, несмотря на запрет такого перехвата, соответствующие сообщения должны быть уничтожены, как только их внутренний характер станет очевидным (статья 2(a) Закона о радиотехнической разведке).

39. Если Суд по вопросам внешней разведки отменяет или изменяет разрешение, выданное Радиотехническому центру в срочном порядке (см. выше § 21), то все полученные разведывательные данные, которые, следовательно, более не санкционированы, должны быть немедленно уничтожены (пункт 3 статьи 5(b) Закона о радиотехнической разведке).

40. Закон об обработке персональных данных Радиотехническим центром (*Lagen om behandling av personuppgifter i Försvarets radioanstalts försvarsunderrättelse- och utvecklingsverksamhet*, 2007:259) содержит положения об обработке персональных данных в области радиотехнической разведки. Этот закон вступил в силу 1 июля 2007 г., а изменения к нему – 30 июня 2009 г., 15 февраля 2010 г. и 1 марта 2018 г. Целью данного закона является защита от нарушений права на личную неприкосновенность (статья 2 главы 1). Радиотехнический центр гарантирует, *inter alia*, сбор персональных данных только для конкретных явно названных и обоснованных целей. Подобные цели определяются направлением деятельности внешней разведки посредством детального распоряжения с указанием задач либо тем, что необходимо для отслеживания изменений радиотехнической обстановки, технического прогресса и радиотехнической защиты. Кроме того, обрабатываемые персональные данные должны быть соразмерны и соответствовать цели обработки. Нельзя обрабатывать персональные данные в большем объеме, чем это необходимо для достижения конкретной цели. Необходимо прилагать все разумные усилия для исправления, блокировки и удаления неверных или неполных персональных данных (статьи 6, 8 и 9 главы 1 Закона об обработке персональных данных Радиотехническим центром).

41. Обработка персональных данных не может осуществляться исключительно на основании того, что известно о расе или этнической принадлежности какого-либо лица, о его или ее политических, религиозных или философских взглядах, членстве в каком-либо союзе, состоянии здоровья или сексуальной жизни. Однако если обработка персональных данных осуществляется по иной причине, то данная информация может быть использована, если это абсолютно необходимо для ее обработки. Информация о внешнем виде лица всегда должна быть сформулирована объективно с уважением к его человеческому достоинству. При сборе разведывательных данных вышеупомянутые персональные критерии могут использоваться в качестве селекторов только в том случае, если это абсолютно необходимо для целей сбора данных (статья 11 главы 1 Закона об обработке персональных данных Радиотехническим центром).

42. Сотрудники Радиотехнического центра, занимающиеся обработкой персональных данных, проходят официальную процедуру допуска и обязаны обеспечивать конфиденциальность в отношении данных, к которым применяются положения о секретности. Сотрудники могут быть подвергнуты уголовному наказанию в случае ненадлежащего выполнения ими задач, связанных с обработкой персональных данных (статья 2 главы 6 Закона об обработке персональных данных Радиотехническим центром).

43. Персональные данные, подвергнутые автоматизированной обработке, подлежат уничтожению, как только потребность в них прекращается (статья 1 главы 6 Закона об обработке персональных данных Радиотехническим центром).

44. Дополнительные положения об обработке персональных данных изложены в Постановлении об обработке персональных данных Радиотехническим центром (*Förordningen om behandling av personuppgifter i Försvarets radioanstalts försvars-underrättelse- och utvecklingsverksamhet*, 2007:261). Постановление предусматривает, *inter alia*, что Радиотехнический центр вправе хранить базы данных исходных материалов, содержащих персональные данные. Под исходными материалами понимается необработанная информация, собранная посредством автоматизированной обработки данных. Персональные данные в таких базах данных должны быть уничтожены в течение одного года с момента их сбора (статья 2 указанного постановления).

F. Условия передачи перехваченных данных другим сторонам

45. Собранные разведывательные данные должны быть переданы соответствующим органам, как это определено в Законе о внешней разведке (статья 8 Закона о радиотехнической разведке).

46. Государственные учреждения, Вооруженные силы, Государственная служба безопасности, Национальное оперативное отделение Главного полицейского управления, Инспекция по стратегической продукции (*Inspektionen för strategiska produkter*), Управление военным имуществом (*Försvarets materialverk*), Агентство по оборонным

исследованиям (*Totalförsvarets forskningsinstitut*), Агентство по гражданским чрезвычайным ситуациям (*Myndigheten för samhällsskydd och beredskap*) и Таможенная служба Швеции (*Tullverket*) могут получить прямой доступ к полным разведывательным донесениям в том объеме, который определит Радиотехнический центр (статья 9 Постановления об обработке персональных данных Радиотехническим центром). Однако до настоящего времени Радиотехнический центр не принимал каких-либо решений, допускающих прямой доступ.

47. Радиотехнический центр также вправе предоставить Государственной службе безопасности и Вооруженным силам прямой доступ к данным, которые представляют собой результаты анализа в базе данных и необходимы властям для проведения стратегической оценки террористической угрозы против Швеции и ее интересов (статья 15 главы 1 Закона об обработке персональных данных Радиотехническим центром, а также статья 13(a) Постановления об обработке персональных данных Радиотехническим центром).

48. Согласно подготовительным материалам (предложение № 2017/18:36) вышеупомянутый доступ предоставляется в рамках сотрудничества между Радиотехническим центром, Государственной службой безопасности и Вооруженными силами в составе рабочей группы под названием Национальный центр оценки террористических угроз (*Nationellt centrum för terrorhotbedömning*), объединяющей аналитиков трех ведомств, которые совместно готовят отчеты, содержащие стратегические оценки террористических угроз. С разрешения Радиотехнического центра и до тех пор, пока соответствующие данные актуальны для оценки террористической угрозы, аналитики Национального центра оценки террористических угроз имеют прямой доступ к «результатам анализа», содержащимся в базах данных Радиотехнического центра. Однако у них нет прямого доступа к базам данных Радиотехнического центра для проведения собственного свободного поиска. Кроме того, хотя информация, предоставленная в распоряжение аналитиков посредством прямого доступа, может содержать персональные данные, оценки Национального центра оценки террористических угроз имеют общий стратегический характер и как таковые не направлены против отдельных лиц.

49. Персональные данные могут быть переданы другим государствам или международным организациям только в том случае, если это разрешено положениями о секретности и необходимо Радиотехническому центру для осуществления его деятельности в рамках международного сотрудничества в области обороны и безопасности. Власти Швеции могут устанавливать правила или при особых обстоятельствах разрешать такую передачу персональных данных и в других случаях, когда это необходимо для деятельности Радиотехнического центра (статья 17 главы 1 Закона об обработке персональных данных Радиотехническим центром). Радиотехнический центр вправе раскрывать персональные данные иностранному органу или международной организации, если это отвечает интересам Правительства Швеции (*statsledningen*), или для выработки комплексной стратегии обороны Швеции (*totalförsvaret*). Переданная подобным образом информация не должна причинять вред интересам Швеции (статья 7 Постановления об обработке персональных данных Радиотехническим центром).

G. Надзор за осуществлением радиотехнической разведки

50. Закон о внешней разведке (статья 5) и Закон о радиотехнической разведке (статья 10) предусматривают, что уполномоченный орган должен контролировать деятельность в области внешней разведки в Швеции и проверять соответствие проводимых Радиотехническим центром мероприятий положениям Закона о радиотехнической разведке. Надзорный орган – Инспекция по надзору – уполномочен, среди прочего, контролировать исполнение Закона и Постановления о внешней разведке и проверять соответствие мероприятий, проводимых в рамках внешней разведки, применимым директивам (статья 4 Постановления об инструкциях для Инспекции внешней разведки (*Förordningen med instruktion för Statens inspektion för försvarsunderrättelseverk samheten*, 2009:969)). Надзорный орган также проверяет соблюдение Закона о радиотехнической разведке, изучая, в частности, используемые селекторы, процедуру уничтожения разведывательных данных и передачи отчетов. Если по результатам проверки выяснится, что какой-либо конкретный сбор разведывательных данных не соответствует разрешению, Инспекция по надзору вправе принять решение о прекращении операции или об уничтожении разведывательных данных (статья 10 Закона о радиотехнической разведке). Радиотехнический центр должен сообщать Инспекции по надзору селекторы, которые напрямую связаны с конкретным физическим лицом (статья 3 Постановления о радиотехнической разведке).

51. Инспекцию по надзору возглавляет совет, члены которого назначаются властями Швеции на срок не менее четырех лет. Председатель и вице-председатель должны быть судьями на постоянной основе или в прошлом являться таковыми. Остальные члены Инспекции избираются из кандидатов, предложенных партийными группами в парламенте (пункт 3 статьи 10 Закона о радиотехнической разведке).

52. Любые заключения или предложения о принятии мер, вытекающие из проверок Инспекции по надзору, направляются в Радиотехнический центр, а при необходимости также и властям Швеции. Она также представляет властям Швеции ежегодные отчеты о своих проверках (статья 5 Постановления об инструкциях для Инспекции по надзору), которые доводятся до сведения общественности. Кроме того, если Инспекция по надзору обнаруживает потенциальные преступления, она должна сообщить об этом в Прокуратуру Швеции (*Åklagarmyndigheten*), а при выявлении недостатков, которые могут повлечь за собой ответственность властей за причиненный ущерб, отчет должен быть представлен канцлеру юстиции (*Justitiekanslern*). Отчет также может быть направлен в Инспекцию по защите данных (*Datainspektionen*), которая осуществляет надзор за обработкой персональных данных Радиотехническим центром (статья 15 Постановления об инструкциях для Инспекции по надзору).

53. С момента своего создания в 2009 году до 2017 года Инспекция по надзору провела всего 102 проверки. В результате 15 заключений были направлены в Радиотехнический центр, а одно – властям Швеции. По итогам проверок не было установлено оснований для прекращения сбора разведывательных данных или для уничтожения результатов. Согласно ежегодным отчетам Инспекции по надзору, которые содержат краткое описание проверок, последние включали неоднократное подробное изучение использованных селекторов, процедур уничтожения разведывательных данных, передачи отчетов, обработки персональных данных, а также проверку общего соблюдения законодательства, директив и разрешений, относящихся к разведывательной деятельности. Например, в период с 2010 по 2014 год использование селекторов проверялось 17 раз, по результатам чего были подготовлены одно заключение и предложение о внесении изменений в практику обработки данных Радиотехническим центром. За тот же период процедура уничтожения данных, относящихся к радиотехнической разведке, была проверена девять раз. В результате в 2011 году было вынесено одно заключение, в котором Радиотехническому центру предлагалось внести изменения в свои внутренние правила, что он и сделал в этом же году. В 2011 году Инспекция по надзору также проверила, собирал ли Радиотехнический центр данные для других стран в соответствии с законодательством, что не привело к вынесению какого-либо заключения. В 2014 году была проведена общая проверка сотрудничества Радиотехнического центра с другими государствами и международными организациями в вопросах разведки. Эта проверка не повлекла за собой вынесение мнений или предложений для Радиотехнического центра. В 2015 и 2016 годах по результатам общей проверки в целях оценки соблюдения ограничений, установленных в разрешениях Суда по вопросам внешней разведки, было вынесено одно замечание. В 2016 и 2017 годах Инспекция по надзору провела детальную проверку обработки Радиотехническим центром персональных данных. Проверка касалась обработки конфиденциальных персональных данных в связи со стратегическими обстоятельствами, связанными с международным терроризмом и иными серьезными трансграничными преступлениями, представляющими угрозу для важных национальных интересов. По результатам проверки не было вынесено каких-либо заключений или предложений. Однако в течение того же периода властям Швеции было направлено одно заключение после проверки соответствия разведывательной деятельности Радиотехнического центра вынесенным распоряжениям с указанием задач. В 2009–2017 годах Инспекция по надзору один раз выявила основание для направления отчета другому органу, Инспекции по надзору, в связи с толкованием положения закона. В своих ежегодных отчетах Инспекция по надзору отмечала, что ей предоставлялся доступ ко всей информации, необходимой для проведения проверок.

54. Проверка надзорной деятельности Инспекции по надзору проводилась Государственным ревизионным управлением (*Riksrevisionen*), органом, подотчетным парламенту. В отчете, опубликованном в 2015 году, оно отметило, что Радиотехнический центр внедрил практики обработки заключений Инспекции по надзору и что осуществляемый надзор способствовал развитию деятельности Радиотехнического центра. Предложения рассматривались серьезно и приводили к реформированию, если это требовалось сделать. За исключением одного случая, когда Радиотехнический центр передал вопрос на рассмотрение властям Швеции, он принимал меры, указанные Инспекцией по надзору. Вместе с тем Государственное ревизионное управление подвергло критике отсутствие у Инспекции по надзору документации по проверкам, а также неуказание четко определенных целей проверок.

55. В состав Радиотехнического центра входит Совет по защите конфиденциальности, которому поручается осуществлять постоянный мониторинг мер, принимаемых для обеспечения защиты права на личную неприкосновенность. Члены Совета назначаются властями Швеции. Совет передает свои замечания руководству Радиотехнического центра или Инспекции по надзору, если он считает, что для этого есть основания (статья 11 Закона о радиотехнической разведке).

56. Дополнительные положения о надзоре можно найти в Законе об обработке персональных данных Радиотехническим центром. Организация назначает одного или нескольких специалистов по защите данных и информирует об этом Инспекцию по надзору (статья 1 главы 4 Закона). Специалисту по защите данных поручается проводить независимый мониторинг законности и правильности обработки персональных данных Радиотехническим центром и указывать на любые недостатки. Если имеются подозрения о наличии недостатков и не были внесены соответствующие исправления, то необходимо направить отчет в Инспекцию по защите данных (статья 2 главы 4 Закона об обработке персональных данных Радиотехническим центром).

57. Инспекция по защите данных, которая подотчетна властям Швеции, по запросу получает доступ к персональным данным, обрабатываемым Радиотехническим центром, и к документации по обработке персональных данных, а также к информации о мерах безопасности, принятых в этом отношении, равно как и доступ на объекты, на которых обрабатываются персональные данные (статья 2 главы 5 Закона об обработке персональных данных Радиотехническим центром). Если Инспекция по надзору установит, что персональные данные обрабатываются или могут обрабатываться незаконно, она должна попытаться исправить ситуацию, передав свои замечания Радиотехническому центру (статья 3 главы 5 Закона об обработке персональных данных Радиотехническим центром). Она также может обратиться в Административный суд (*förvaltningsrätten*) г. Стокгольма, чтобы добиться уничтожения незаконно обрабатываемых персональных данных (статья 4 главы 5 Закона об обработке персональных данных Радиотехническим центром). Согласно копиям переписки по электронной почте от апреля 2019 года между заявителем и Административным судом в электронных документах этого суда не содержалось каких-либо свидетельств того, что Инспекция по защите данных воспользовалась указанной возможностью.

H. Уведомление о мерах скрытого наблюдения

58. При использовании селекторов, непосредственно связанных с конкретным физическим лицом, Радиотехнический центр должен уведомить это лицо в соответствии с Законом о радиотехнической разведке. Уведомление должно содержать информацию о дате и цели принятия мер. Такое уведомление должно быть направлено в кратчайшие сроки, когда это станет возможным без ущерба для внешней разведки, но не позднее, чем через один месяц после завершения разведывательной миссии (статья 11(a) Закона о радиотехнической разведке).

59. Однако направление уведомления может быть отложено в интересах секретности, в частности, в сфере обороны или в целях защиты международных отношений. Если по соображениям секретности уведомление не было направлено в течение года после завершения разведывательной миссии, отсутствует необходимость уведомлять соответствующее лицо. Кроме того, уведомление не направляется, если меры касаются исключительно условий иностранной державы или отношений между иностранными державами (статья 11(b) Закона о радиотехнической разведке).

60. В своем отчете за 2010 год Инспекция по защите данных отметила, *inter alia*, что Радиотехнический центр никогда не прибегал к уведомлению физических лиц по соображениям секретности (см. ниже § 75).

I. Средства правовой защиты

61. Закон о радиотехнической разведке предусматривает, что Инспекция по надзору по запросу конкретного лица должна расследовать, были ли сообщения этого лица перехвачены посредством радиотехнической разведки, и, если это да, проверить, соответствовали ли перехват и обработка информации закону. Инспекция по надзору уведомляет заинтересованное лицо о проведении такого расследования (статья 10(a) Закона о радиотехнической разведке). Запрос могут подавать юридические и физические лица независимо от гражданства и места жительства. За период с 2010 по 2017 год были обработаны 132 запроса и случаев нарушения законодательства не было выявлено. В 2017 году были обработаны 10 подобных запросов, в 2016 – 14. Решение Инспекции по надзору в связи с запросом является окончательным.

62. В соответствии с Законом об обработке персональных данных Радиотехническим центром последний также обязан предоставлять информацию по запросу. Один раз в календарном году физическое лицо может запросить информацию о том, обрабатываются или обрабатывались ли его или ее персональные данные. В случае положительного ответа Радиотехнический центр обязан сообщить, о какой информации идет речь, из каких источников она была получена, какова цель обработки и каким получателям или категориям получателей передаются или были переданы персональные данные. По общему правилу информация должна быть предоставлена в течение одного месяца с момента запроса (статья 1 главы 2 Закона об обработке персональных данных Радиотехническим центром). Однако указанное право на получение информации не применяется, если ее раскрытию препятствуют соображения секретности (статья 3 главы 2 Закона об обработке персональных данных Радиотехническим центром).

63. По запросу лица, персональные данные которого были зарегистрированы, Радиотехнический центр незамедлительно исправляет, блокирует или уничтожает такие данные, которые не были обработаны в соответствии с законом. Радиотехнический центр также уведомляет любую третью сторону, получившую данные, если этого требует физическое лицо или если посредством уведомления можно избежать причинять значительного ущерба или неудобств. Такое уведомление не должно направляться, если это невозможно или потребует несоразмерных усилий (статья 4 главы 2 Закона об обработке персональных данных Радиотехническим центром).

64. Решения Радиотехнического центра о раскрытии и корректирующих мероприятиях в отношении персональных данных могут быть обжалованы в Административный суд г. Стокгольма (статья 3 главы 6 Закона об обработке персональных данных Радиотехническим центром). Согласно копиям переписки по электронной почте от апреля 2019 года между заявителем и Административным судом в электронных документах этого суда не содержалось каких-либо свидетельств использования указанной возможности.

65. Власти несут ответственность за ущерб, причиненный нарушением правом на личную неприкосновенность в связи с обработкой персональных данных, осуществленной способом, не соответствующим Закону об обработке персональных данных Радиотехническим центром (статья 5 главы 2). Требование о возмещении ущерба подается канцлеру юстиции.

66. В дополнение к указанным выше средствам правовой защиты, установленным законодательством о радиотехнической разведке, законодательство Швеции предусматривает ряд других средств проверки и механизмов рассмотрения жалоб. Парламентские омбудсмены (*Justitieombudsmannen*) контролируют применение законов и постановлений при осуществлении государственной деятельности, суды и органы власти обязаны предоставлять информацию и заключения по запросу омбудсменов (статья 6 главы 13 Акта о форме правления (*Regeringsformen*)), а также доступ к протоколам и иным документам. Омбудсмены обязаны гарантировать, в частности, что суды и органы власти соблюдают положения Акта о форме правления об объективности и беспристрастности и что основные права и свободы граждан не ущемляются при осуществлении деятельности государством (статья 3 Закона об инструкциях для омбудсменов Риксдага (*Lagen med instruktion för Riksdagens ombudsman*, 1986:765)). Надзор, под который попадают Суд по вопросам внешней разведки и Радиотехнический центр, осуществляется посредством рассмотрения жалоб представителей общественности, а также в ходе проверок и проведения других расследований (статья 5 Закона об инструкциях для омбудсменов Риксдага). Анализ завершается вынесением решения, в котором приводится заключение омбудсмена, хотя и не имеющее обязательной силы, относительно того, нарушили ли суд или орган власти закон или совершили ли они иные противоправные или ненадлежащие действия. Омбудсмен может также инициировать уголовное или дисциплинарное производство в отношении государственного должностного лица, которое совершило уголовное преступление или пренебрегло своими служебными обязанностями (статья 6 Закона об инструкциях для омбудсменов Риксдага).

67. Будучи наделенным полномочиями, аналогичными полномочиям парламентских омбудсменов, канцлер юстиции проверяет, соблюдают ли должностные лица государственной администрации законы и постановления и выполняют ли они свои иные обязанности (статья 1 Закона о надзоре со стороны канцлера юстиции (*Lagen om justitiekanslerns tillsyn*, 1975:1339)). Канцлер юстиции осуществляет эти полномочия путем изучения индивидуальных жалоб или проведения проверок и других расследований, объектом которых могут быть, например, Суд по вопросам внешней разведки и Радиотехнический центр. Согласно копиям переписки по электронной почте от апреля 2019 года между заявителем и аппаратом канцлера юстиции в 2008 году были получены 12 таких жалоб, а в 2013 – одна. После их рассмотрения было установлено, что ни одна из этих жалоб не требует принятия каких-либо мер.

68. По запросу канцлера юстиции суды и органы власти обязаны предоставлять информацию и заключения, а также доступ к протоколам и иным документам (статьи 9 и 10 Закона о надзоре со стороны канцлера юстиции). Решения канцлера юстиции аналогичны по своему характеру решениям парламентских омбудсменов, включая отсутствие обязательной силы. Вместе с тем по традиции заключения канцлера юстиции и омбудсменов пользуются большим уважением в шведском обществе и, как правило, принимаются во внимание (см. Постановление Европейского Суда по делу «Сегерстедт-Виберг и другие против Швеции» (Segerstedt-Wiberg and Others v. Sweden), жалоба № 62332/00, § 118, ECHR 2006-VII). Канцлер юстиции обладает такими же полномочиями, что и омбудсмены по инициированию уголовного или дисциплинарного производства (статьи 5 и 6 Закона о надзоре со стороны канцлера юстиции).

69. Канцлер юстиции также уполномочен рассматривать жалобы и требования о возмещении ущерба, поданные против властей Швеции, в том числе о компенсации за предполагаемые нарушения Конвенции. Верховный суд Швеции и канцлер юстиции в последние годы создали прецедентную практику, подтверждающую, что принцип, согласно которому компенсация за нарушения

Конвенции может быть назначена без прямого основания в законодательстве Швеции в той мере, в какой Швеция обязана предоставлять компенсацию жертвам нарушений Конвенции в рамках права на компенсацию ущерба, является общим принципом права (см. Постановление Европейского Суда по делу «Адвокатское бюро "Линдстранд Партнерс Адвокатбюро АБ" против Швеции» (Lindstrand Partners Advokatbyrå AB v. Sweden) от 20 декабря 2016 г., жалоба № 18700/09, §§ 58–62 и 67, с дальнейшими ссылками). 1 апреля 2018 г. путем внесения нового положения, статьи 4 главы 3 Закона о гражданско-правовой ответственности (*Skadeståndslagen*, 1972:207), право на компенсацию за нарушения Конвенции было кодифицировано.

70. В дополнение к упомянутым выше надзорным функциям в соответствии с Постановлением об инструкциях для Инспекции по надзору и Законом об обработке персональных данных Радиотехническим центром (см. выше §§ 52, 56 и 57) на Инспекцию по защите данных, как правило, возлагается защита лиц от нарушений их права на личную неприкосновенность при обработке персональных данных в соответствии с Законом о дополнительных положениях к Общему регламенту ЕС о защите персональных данных (*Lagen med kompletterande bestämmelser till EU: s dataskyddsförordning*), который вступил в силу 25 мая 2018 г., в тот же день, что и новый Регламент Европейского союза, который указанный закон дополняет (см. ниже § 94). Что касается разведки, проводимой Радиотехническим центром, Закон о персональных данных (*Personuppgiftslagen*, 1998:204) продолжает применяться, хотя в остальных частях он заменяется новым Регламентом ЕС и дополнительным актом. Таким образом, Инспекция по защите данных имеет такую же общую надзорную задачу. При выполнении этой задачи она вправе получать и рассматривать индивидуальные жалобы.

J. Секретность в работе Радиотехнического центра

71. Закон о публичном доступе к информации и секретности (*Offentlighets och sekretesslagen*, 2009:400) содержит конкретное положение, касающееся деятельности Радиотехнического центра в процессе радиотехнической разведки. Требование секретности применяется к информации о личных или финансовых обстоятельствах лица, кроме случаев, когда очевидно, что эта информация может быть раскрыта без причинения ущерба заинтересованному лицу или лицу, тесно связанному с ним или с ней. Требование секретности является презумпцией (статья 4 главы 38 закона).

72. В соответствии с Законом о публичном доступе к информации и секретности требование секретности также применяется к деятельности в области внешней разведки в отношении информации, касающейся другого государства, международной организации, органа власти, гражданина или юридического лица в другом государстве, если можно предположить, что раскрытие такой информации повлияет на международные отношения Швеции или иным образом причинит ущерб стране (статья 1 главы 15).

73. Требование секретности также применяется к информации о деятельности, связанной с защитой страны или с планированием такой деятельности, либо к информации, которая иным образом затрагивает комплексную стратегию обороны страны, если можно предположить, что раскрытие данной информации причинит ущерб обороне страны или иным образом поставит под угрозу национальную безопасность (статья 2 главы 15 Закона о публичном доступе к информации и секретности).

74. Информация, которая защищена требованием секретности в соответствии с Законом о публичном доступе к информации и секретности, не может быть передана иностранному органу или международной организации, за исключением случаев, когда (i) такое раскрытие разрешено прямой правовой нормой (например, статьей 7 Постановления об обработке персональных данных Радиотехническим центром, см. выше § 34) или когда (ii) информация в аналогичной ситуации может быть доведена до сведения властей Швеции, и орган, раскрывающий информацию, считает очевидным, что передача информации иностранному органу или международной организации соответствует интересам Швеции (статья 3 главы 8 Закона о публичном доступе к информации и секретности).

K. Отчеты Инспекции по защите данных

75. 12 февраля 2009 г. власти Швеции поручили Инспекции по защите данных изучить обработку персональных данных в Радиотехническом центре с точки зрения соблюдения права на личную неприкосновенность. В своем отчете, опубликованном 6 декабря 2010 г., Инспекция по защите данных указала, что ее выводы в целом положительны. Радиотехнический центр с серьезностью относится к вопросам, связанным с обработкой персональных данных и личной неприкосновенностью, и уделяет много времени и ресурсов на создание процедур и обучение персонала, чтобы свести к минимуму риск неоправданного вмешательства в право на личную неприкосновенность. Кроме того, не было обнаружено каких-либо доказательств того, что Радиотехнический центр обрабатывал персональные данные в целях, не разрешенных действующим законодательством. Вместе с тем Инспекция по защите данных отметила, *inter alia*, что существует необходимость в улучшении методов разде-

ления внутренних и трансграничных сообщений. Даже несмотря на внедрение Радиотехническим центром соответствующих механизмов, отсутствовали гарантии того, что внутренние сообщения не будут перехвачены, и что фактически они перехватывались, хотя такие случаи были довольно редкими. Инспекция по защите данных также отметила, что Радиотехнический центр никогда не прибегал к процедуре уведомления физических лиц (см. выше §§ 58–60) по соображениям секретности.

76. Инспекция по защите данных подготовила второй отчет 24 октября 2016 г. Она вновь не обнаружила доказательств того, что сбор персональных данных осуществлялся для иных целей, кроме тех, что предусмотрены для радиотехнической разведки. Она также отметила, что Радиотехнический центр постоянно проверяет, необходимы ли перехваченные данные для указанных целей. Аналогичная проверка была проведена в отношении носителей сообщений, из которых Радиотехнический центр получал разведывательные данные. Кроме того, ничто не свидетельствовало об игнорировании положений законодательства об уничтожении персональных данных (см. выше §§ 37–39). Однако Радиотехнический центр был подвергнут критике за ненадлежащий мониторинг журналов, используемых для обнаружения неправомерного использования личных данных, то есть за недостаток, который отмечался еще в 2010 году.

L. Отчет Комитета по радиотехнической разведке

77. 12 февраля 2009 г. власти Швеции приняли решение создать Комитет по радиотехнической разведке (*Signalspaningskommittén*), состоящий преимущественно из членов парламента, в задачу которого входит мониторинг разведывательной деятельности Радиотехнического центра в целях изучения ее последствий для личной неприкосновенности. Отчет был представлен 11 февраля 2011 г. (*Uppföljning av signalspaningslagen*, SOU2011:13). В своем анализе Комитет по радиотехнической разведке в первую очередь сфокусировался на радиотехнической разведке, проводимой воздушным путем, поскольку подобная деятельность, осуществляемая по кабельным каналам, еще не была широкомасштабной.

78. Комитет по радиотехнической разведке пришел к выводу, что Радиотехнический центр серьезно относится к вопросам личной неприкосновенности, которые являются неотъемлемой частью разработки его процедур. При этом Комитет по радиотехнической разведке отметил, что существуют практические трудности в отделении внутренних сообщений, переданных по кабельным каналам, от сообщений, пересекающих границу Швеции. Любые внутренние сообщения, которые не отделялись автоматически, были отделены вручную на этапе обработки или анализа. Комитет по радиотехнической разведке также отметил, что селекторы, используемые для передачи данных о сообщениях, были менее специфичны по сравнению с теми, которые использовались для перехвата содержания сообщения, и, следовательно, хранящиеся в Радиотехническом центре данные могли затрагивать большее количество физических лиц.

79. Другой вывод, сделанный в отчете, заключался в том, что деятельность Радиотехнического центра по разработке (см. выше § 24) могла привести к перехвату нерелевантных сообщений и к их возможному прочтению или прослушиванию его сотрудниками. Вместе с тем Комитет по радиотехнической разведке отметил, что деятельность по разработке имеет непосредственное значение для способности Радиотехнического центра проводить разведывательные операции. Кроме того, информация, полученная в ходе деятельности по разработке, может быть использована в регулярной разведывательной деятельности только в том случае, если такое использование соответствует целям, установленным законодательством и соответствующими распоряжениями с указанием задач для радиотехнической разведки.

80. Как и Инспекция по защите данных, Комитет по радиотехнической разведке отметил, что на практике обязательство Радиотехнического центра информировать лиц, которые были лично и непосредственно затронуты мерами скрытого наблюдения, очень ограничено вследствие секретности. Таким образом, комитет пришел к выводу, что данное обязательство не является гарантией правовой определенности или невмешательства в право на личную неприкосновенность. Однако Комитет по радиотехнической разведке установил, что, в частности, процедура получения разрешения в Суде по вопросам внешней разведки при принятии решения о выдаче разрешений на проведение мероприятий радиотехнической разведки (см. выше §§ 30–34), а также надзорные функции Инспекции по надзору (см. выше §§ 36 и 50–54) и Совета по защите конфиденциальности (см. выше § 55) обеспечивают важную защиту права на личную неприкосновенность. В связи с этим Комитет по радиотехнической разведке отметил, что, хотя Совет по защите конфиденциальности входит в состав Радиотехнического центра, он действует независимо.

II. СООТВЕТСТВУЮЩЕЕ МЕЖДУНАРОДНОЕ ПРАВО

A. Организация Объединенных Наций

81. Резолюция № 68/167 «О праве на неприкосновенность личной жизни в цифровой век», при-

нятая Генеральной Ассамблеей ООН 18 декабря 2013 г., гласит:

«Генеральная Ассамблея…

4) призывает все государства…

(c) 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 в области прав человека;

(d) учредить новые или продолжать использовать уже имеющиеся независимые, эффективные внутренние надзорные механизмы, способные обеспечивать прозрачность в соответствующих случаях и подотчетность в отношении отслеживания властями сообщений, их перехвата и сбора личных данных…».

B. Совет Европы

1. Конвенция Совета Европы о защите физических лиц при автоматизированной обработке персональных данных от 1981 года и Дополнительный протокол к ней (CETS № 108)

82. Конвенция о защите физических лиц при автоматизированной обработке персональных данных, которая вступила в силу для Швеции 1 октября 1985 г., устанавливает стандарты защиты данных при автоматизированной обработке персональных данных в государственном и частном секторах. В соответствующих частях она гласит:

«**Преамбула**

Государства – члены Совета Европы, подписавшие настоящий документ,

учитывая, что цель Совета Европы заключается в достижении большего единства между его членами, основанного, в частности, на уважении принципа господства права, а также соблюдении прав человека и основных свобод;

учитывая желательность расширения гарантий прав и основных свобод для всех и, в частности, права на уважение частной жизни, с учетом увеличения трансграничного потока персональных данных, подвергающихся автоматизированной обработке;

подтверждая вместе с тем свою приверженность свободе информации невзирая на границы;

признавая необходимость согласования таких основных ценностей, как уважение частной жизни и свободное распространение информации между народами,

договорились о нижеследующем:

Статья 1. Предмет и цель

Цель настоящей Конвенции состоит в обеспечении на территории каждой Стороны для каждого физического лица, независимо от его гражданства или местожительства, уважения его прав и основных свобод и, в частности, его права на неприкосновенность частной жизни, в отношении автоматизированной обработки касающихся его персональных данных (“защита данных”)…

Статья 8. Дополнительные гарантии для субъекта данных

Любому лицу должна быть предоставлена возможность:

a) знать о существовании автоматизированного файла персональных данных, знать его основные цели, а также название и место обычного проживания или местонахождение контролера файла;

b) получить через разумный промежуток времени и без чрезмерной задержки или чрезмерных расходов подтверждение того, хранятся ли касающиеся его персональные данные в автоматизированном файле данных, а также получить такие данные в доступной для понимания форме;

c) добиваться в случае необходимости исправления или уничтожения таких данных, если они подвергались обработке в нарушение норм внутреннего законодательства, воплощающего основополагающие принципы, изложенные в статьях 5 и 6 настоящей Конвенции;

d) прибегать к средствам правовой защиты в случае невыполнения просьбы о подтверждении или в случае необходимости предоставлении данных, их изменении или уничтожении, как это предусмотрено в пунктах “b” и “c” настоящей статьи.

Статья 9. Изъятия и ограничения

1. Изъятия из положений статей 5, 6 и 8 настоящей Конвенции допускаются только в пределах, определенных в настоящей статье.

2. Отступление от положений статей 5, 6 и 8 настоящей Конвенции допускается, когда такое отступление предусматривается законодательством Стороны и является необходимой в демократическом обществе мерой, принимаемой в интересах:

a) защиты безопасности государства, общественной безопасности, валютно-кредитных интересов государства или пресечения уголовных преступлений;

b) защиты субъекта данных или прав и свобод других лиц…

Статья 10. Санкции и средства правовой защиты

Каждая Сторона обязуется предусмотреть надлежащие санкции и средства правовой защиты на случай нарушения норм внутреннего законодательства, воплощающих основополагающие принципы защиты данных, изложенные в настоящей главе».

83. Пояснительный доклад к указанной выше Конвенции содержит следующие пояснения в отношении ее статьи 9:

«…55. Изъятия из основополагающих принципов защиты данных ограничены теми, которые необходимы для защиты основных ценностей в демократическом обществе. Текст второго пункта этой статьи следует образцу второго пункта статей 6, 8, 10 и 11 Европейской конвенции по правам человека. Из постановлений Комиссии и Европейского Суда по правам человека, касающихся понятия "необходимые меры", следует, что критерии этого понятия не могут быть установлены для всех стран и на все времена, а должны рассматриваться в свете конкретной ситуации в каждой стране.

56. В литере "a" пункта 2 указанной статьи перечислены основные интересы государства, которые могут требовать исключений. Такие исключения имеют достаточно конкретный характер во избежание того, чтобы у властей была неоправданно большая свобода действий в отношении общего применения Конвенции.

В соответствии со статьей 16 Конвенции власти сохраняют возможность отказать в применении Конвенции в отдельных случаях по веским основаниям, включая те, что перечислены в статье 9 Конвенции.

Понятие "безопасность государства" следует понимать в традиционном смысле защиты национального суверенитета от внутренних или внешних угроз, включая защиту международных отношений государства…».

84. Дополнительный протокол к Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных, касающийся надзорных органов и трансграничной передачи данных, от 8 ноября 2001 г. (CETS № 181), который вступил в силу для Швеции 1 июля 2004 г., в соответствующих частях гласит:

«**Статья 1. Надзорные органы**

1. Каждая Сторона предусматривает наличие одного или нескольких органов, ответственных за обеспечение выполнения мер в своем внутригосударственном законодательстве для применения принципов, содержащихся в главах II и III Конвенции и в настоящем Протоколе.

2 (a). В указанных целях такие органы будут иметь, в частности, полномочия для проведения расследований и для вмешательства, а также полномочия возбуждать судебные производства или доводить до сведения компетентных судебных органов нарушения положений внутригосударственного законодательства, реализующего принципы, изложенные в пункте 1 статьи 1 настоящего Протокола.

b) Каждый надзорный орган рассматривает заявления со стороны любого лица в отношении защиты его прав и основных свобод в связи с обработкой персональных данных в рамках своей компетенции.

3. Надзорные органы выполняют свои функции, будучи полностью независимыми.

4. Решения надзорных органов, которые вызывают жалобы, могут быть обжалованы в судах…

Статья 2. Трансграничные потоки персональных данных получателю, который не попадает под юрисдикцию Стороны Конвенции

1. Каждая Сторона обеспечивает передачу персональных данных получателю, подпадающему под юрисдикцию государства или организации, которые не являются Сторонами Конвенции, только в том случае, если такие государство или организация гарантируют надлежащий уровень защиты при предполагаемой передаче данных.

2. В порядке отступления от пункта 1 статьи 2 настоящего Протокола каждая Сторона вправе разрешить передачу персональных данных, если:

a) это предусмотрено внутригосударственным законодательством ввиду:

– конкретных интересов субъекта данных, или

– преобладающих законных интересов, особо важных общественных интересов, или

b) контролер, ответственный за передачу данных, предоставляет гарантии, которые, в частности, могут вытекать из договорных положений и которые признаются компетентными органами надлежащими в соответствии с внутригосударственным законодательством».

2. Рекомендация Комитета Министров Совета Европы государствам-членам «О защите персональных данных в области услуг связи»

85. Рекомендация Комитета Министров Совета Европы государствам-членам № R(95)4 «О защите персональных данных в области услуг связи» с особым акцентом на услуги телефонной связи, принятая 7 февраля 1995 г., в соответствующих частях гласит:

«2.4. Вмешательство государственных органов в содержание сообщения, включая использование прослушивающих устройств или других средств наблюдения или перехвата сообщений, должно осуществляться только в том случае, если это предусмотрено законом и является необходимой мерой в демократическом обществе в интересах:

a) защиты безопасности государства, общественной безопасности, валютно-кредитных интересов государства или пресечения уголовных преступлений;

b) защиты субъекта данных или прав и свобод других лиц.

2.5. В случае вмешательства государственных органов в содержание сообщения внутригосударственное законодательство должно регулировать:

a) осуществление прав субъекта данных на доступ к данным и их исправление;

b) обстоятельства, при которых ответственные государственные органы вправе отказать в предоставлении информации заинтересованному лицу или отложить ее предоставление;

c) порядок хранения или уничтожения таких данных.

Если государственный орган поручает оператору сети или провайдеру услуг осуществить вмешательство, то полученные таким образом данные должны быть переданы только тому органу, который указан в разрешении на вмешательство».

3. Доклад Европейской комиссии за демократию через право (далее – Венецианская комиссия) от 2015 года «О демократическом контроле над органами радиотехнической разведки»

86. В своем докладе, опубликованном в декабре 2015 года, Венецианская комиссия прежде всего отметила важность массового перехвата информации для операций по обеспечению безопасности, поскольку он позволяет службам безопасности применять упреждающий подход, выявляя ранее неизвестные угрозы вместо того, чтобы расследовать уже известные. Вместе с тем она также отметила, что перехват большого количества данных при передаче или требование о том, чтобы телекоммуникационные компании хранили, а затем предоставляли данные или метаданные телекоммуникационного контента правоохранительным органам или органам безопасности, представляют собой вмешательство в частную жизнь и другие права человека значительной части мирового населения. В связи с этим Венецианская комиссия сочла, что основное вмешательство в частную жизнь имеет место в момент, когда органы получают доступ к хранящимся персональным данным и/или осуществляют их обработку. По этой причине компьютерный анализ (как правило, с помощью селекторов) является одним из важных этапов для установления баланса между опасениями, связанными с правом на личную неприкосновенность, и с другими интересами.

87. Согласно докладу разрешение (сбора и доступа) и надзор за процессом представляют собой две наиболее важные гарантии. Из прецедентной практики Европейского Суда следует, что надзор должен осуществляться независимым внешним органом. Хотя Европейский Суд отдает предпочтение судебному разрешению, он не считает это необходимым требованием. Скорее, система должна оцениваться в целом, и если независимый контроль отсутствует на этапе выдачи разрешения, то на этапе осуществления надзора должны существовать особенно строгие гарантии. В связи с этим Венецианская комиссия рассмотрела пример системы в Соединенных Штатах Америки, где разрешение выдается Судом по делам о наблюдении за иностранной разведывательной деятельностью. В то же время Венецианская комиссия отметила, что, несмотря на наличие судебной санкции, предметом критики является отсутствие независимого надзора за условиями и ограничениями, установленными судом.

88. Аналогичным образом Венецианская комиссия отметила, что уведомление объекта наблюдения не является абсолютным требованием статьи 8 Конвенции, поскольку общий порядок подачи жалоб в независимый надзорный орган может компенсировать отсутствие уведомления.

89. В докладе Венецианской комиссии внутренний контроль также рассматривается как «первичная гарантия». Набор и обучение персонала являются ключевыми проблемами. Кроме того, при принятии различными органами своих внутренних правил важно внедрять принцип соблюдения права на неприкосновенность частной жизни и другие права человека.

90. Венецианская комиссия в своем докладе также рассмотрела положение журналистов. В нем было указано, что данная группа лиц требует особой защиты, поскольку поиск их контактов мог выявить их источники (а риск обнаружения мог стать мощным сдерживающим фактором для осведомителей). Тем не менее Венецианская комиссия сочла, что абсолютный запрет на поиск контактов журналистов отсутствует при условии, что для такого поиска имеются веские основания. Вместе с тем она признала, что журналистов нелегко идентифицировать, поскольку неправительственные правозащитные организации также участвуют в формировании общественного мнения, и даже блогеры могут претендовать на эквивалентную защиту.

91. Наконец, в докладе были кратко рассмотрены вопрос об обмене разведывательными данными и, в частности, риск того, что государства могут таким образом обходить более строгие внутренние процедуры наблюдения или какие-либо правовые ограничения, которые могут применяться к их ведомствам при проведении внутренних разведывательных операций. Венецианская комиссия решила, что надлежащей гарантией стало бы обеспечение того, чтобы переданный объемный материал мог быть проанализирован только в случае выполнения всех существенных требований к анализу на внутригосударственном уровне, а также в случае получения разрешения в таком же порядке, как и для анализа объемного материала, полученного органами радиотехнической разведки с использованием собственных технологий.

III. ПРАВО ЕВРОПЕЙСКОГО СОЮЗА

A. Хартия Европейского союза об основных правах

92. Статьи 7, 8 и 11 Хартии Европейского союза об основных правах гласят следующее:

«**Статья 7. Уважение личной и семейной жизни**

Каждый имеет право на уважение его личной и семейной жизни, его жилища и его корреспонденции.

Статья 8. Защита персональных данных

1. Каждый имеет право на защиту относящихся к нему персональных данных.

2. Обработка таких данных должна производиться добросовестно в четко определенных целях с согласия заинтересованного лица либо при наличии других правомерных оснований, предусмотренных законом. Каждый имеет право на получение доступа к собранным в отношении него данным и право на внесение в них исправлений.

3. Соблюдение этих правил подлежит контролю со стороны независимого органа…

Статья 11. Свобода выражения мнений и свобода информации

1. Каждый имеет право свободно выражать свое мнение. Это право включает свободу придерживаться своего мнения и свободу получать и распространять информацию и идеи без какого-либо вмешательства со стороны публичных властей и независимо от государственных границ.

2. Соблюдаются свобода и плюрализм средств массовой информации».

B. Директивы и регламенты Европейского союза о защите и обработке персональных данных

93. Директива о защите данных (Директива 95/46/ЕС о защите физических лиц в отношении обработки персональных данных и о свободном обращении таких данных), принятая 24 октября 1995 г., в течение многих лет регулировала вопросы защиты и обработки персональных данных на территории Европейского союза. В силу того, что меры государств – членов ЕС в области общественной безопасности, обороны и безопасности государства не попадают под действие права Сообщества, эта директива не применяется к таким мерам (пункт 2 статьи 3 директивы).

94. Общий регламент по защите данных (далее – Общий регламент), принятый в апреле 2016 года, заменил собой Директиву о защите данных и вступил в силу 25 мая 2018 года. Общий регламент, непосредственно применимый в государствах – членах ЕС, содержит положения и требования, касающиеся обработки информации, позволяющей установить личность субъектов данных на территории Европейского союза, и применяется ко всем предприятиям независимо от их местонахождения, которые осуществляют свою деятельность в Европейской экономической зоне. Бизнес-процессы, в рамках которых обрабатываются персональные данные, должны быть оснащены проектируемой защитой данных и защитой по умолчанию. Это означает, что персональные данные должны храниться с использованием псевдонимизации или полной анонимности, а также с применением максимально возможных параметров конфиденциальности по умолчанию, чтобы данные не были общедоступны без явного согласия и не могли быть использованы для идентификации субъекта без дополнительной информации, хранящейся отдельно. Персональные данные могут обрабатываться только на законном основании, установленном в Общем регламенте, либо если контролер или лицо, осуществляющее обработку данных, получили явное согласие от владельца данных. Владелец данных вправе отозвать свое разрешение в любой момент.

95. Лицо, осуществляющее обработку персональных данных, обязано явным образом информировать о любом сборе данных, сообщить законное основание и цель обработки данных, срок хранения данных, а также факт их передачи каким-либо третьим лицам или за пределы Европейского союза. Пользователи имеют право запросить портативную копию данных, собранных лицом, осуществляющим обработку данных, в общем формате, а также право на удаление своих данных при определенных обстоятельствах. Государственные органы и предприятия, основная деятельность которых связана с регулярной или систематической обработкой персональных данных, должны нанять специалиста по защите данных, ответственного за соблюдение Общего регламента. Компании обязаны сообщать о любых нарушениях безопасности данных в течение 72 часов, если такие нарушения отрицательно сказываются на конфиденциальности пользователей.

96. Директива о конфиденциальности и электронных средствах связи (Директива 2002/58/ЕС в отношении обработки персональных данных и защиты конфиденциальности в секторе электронных средств связи), принятая 12 июля 2002 г., в пунктах 2 и 11 своей Преамбулы гласит:

«(2) Настоящая Директива стремится к соблюдению основополагающих прав и принципов, признанных в Хартии Европейского союза об основных правах. В частности, настоящая Директива стремится к обеспечению полного соблюдения прав, установленных статьями 7 и 8 названной Хартии…

(11) Так же, как и Директива 95/46/ЕС, настоящая Директива не обращается к проблемам защиты основных прав и свобод, связанных с осуществлением видов деятельности, не регулируемых законодательством Сообщества. Поэтому она не изменяет существующий баланс между правом индивида на частную жизнь и возможностью государств – членов ЕС принять меры, упомянутые в статье 15(1) настоящей Директивы, необходимые для защиты общественной безопасности, обороны, государственной безопасности (включая экономическое благосостояние государства, когда деятельность имеет отношение к делам государственной безопасности) и для применения уголовного права. Следовательно, настоящая Директива не оказывает влияния на

способность государств – членов ЕС производить законный перехват информации, передаваемой с помощью электронной связи, или принимать другие необходимые меры для любой из этих целей в соответствии с Конвенцией о защите прав человека и основных свобод и разъяснениями, содержащимися в постановлениях Европейского Суда по правам человека. Такие меры должны быть уместными, строго пропорциональными намеченной цели и необходимыми в пределах демократического общества и должны относиться к адекватным мерам безопасности в соответствии с Европейской конвенцией о защите прав человека и основных свобод».

Далее в соответствующих частях Директивы указывается:

«**Статья 1. Цели и область применения**

1. Настоящая Директива обеспечивает гармонизацию национальных положений, необходимых для обеспечения гарантий соответствующего уровня защиты основных прав и свобод, и, в частности, права на частную жизнь и конфиденциальность информации о частной жизни в связи с обработкой персональных данных в сфере электронных коммуникаций, и для обеспечения свободного движения таких данных, передвижения оборудования для электронной связи и услуг электронной связи в пределах Сообщества.

2. Положения настоящей Директивы конкретизируют и дополняют Директиву 95/46/ЕС в целях, указанных в пункте 1 настоящей статьи. Кроме того, положения настоящей Директивы предусматривают защиту законных интересов абонентов, являющихся юридическими лицами.

3. Настоящая Директива не должна применяться в отношении видов деятельности, которые выходят за пределы регулирования Договора об учреждении Европейского сообщества, таких как те, что под действие разделов V и VI Договора о Европейском союзе, и в любом случае не должна применяться в отношении видов деятельности, касающихся общественной безопасности, обороны, государственной безопасности (включая экономическое благосостояние государства, когда речь идет о делах государственной безопасности) и в отношении деятельности государства в области уголовного права…

Статья 15. Применение отдельных положений Директивы 95/46/ЕС

1. Государства – члены ЕС могут принять законодательные меры для ограничения области прав и обязанностей, предусмотренных статьями 5, 6, пунктами 1, 2, 3 и 4 статьи 8 и статьей 9 настоящей Директивы, если такое ограничение представляет собой необходимую, соответствующую и пропорциональную меру в демократическом обществе для осуществления защиты национальной (государственной) безопасности, обороны, общественной безопасности, предотвращения, расследования, обнаружения и судебного преследования преступных действий или несанкционированного использования системы электронной связи, как об этом говорится в пункте 1 статьи 13 Директивы 95/46/ЕС. В связи с этим государства – члены ЕС могут, *inter alia*, принять законодательные меры, предусматривающие сохранение данных на определенный период по основаниям, предусмотренным в настоящем пункте. Все меры, упоминаемые в настоящем пункте, должны соответствовать общим принципам законодательства Сообщества, включая те, что содержатся в пунктах 1 и 2 статьи 6 Договора о Европейском союзе».

97. 15 марта 2006 г. была принята Директива о сохранении данных (Директива 2006/24/ЕС о сохранении данных, сгенерированных или обработанных в связи с предоставлением общедоступных услуг электронной связи или сетей связи общего пользования, и о внесении изменений в Директиву 2002/58/ЕС). До вынесения в 2014 году Судом Европейского союза постановления об объявлении указанной Директивы недействительной (см. следующий пункт) она предусматривала, *inter alia*, следующее:

«**Статья 1. Предмет и сфера применения**

1. Настоящая Директива направлена на гармонизацию положений национального законодательства, касающегося обязательств провайдеров общедоступных услуг электронной связи или сетей связи общего пользования в отношении хранения определенных данных, которые они генерируют или обрабатывают, в целях обеспечения доступности данных для расследования, обнаружения и судебного преследования преступных действий, как это определено каждым государством – членом ЕС в его внутригосударственном законодательстве.

2. Настоящая Директива применяется к данным о трафике и местоположении как юридических, так и физических лиц, а также к сопутствующим данным, необходимым для идентификации абонента или зарегистрированного пользователя. Она не применяется к содержанию электронных сообщений, включая информацию, полученную с использованием сети электронной связи…

Статья 3. Обязательство по сохранению данных

1. В порядке отступления от статей 5, 6 и 9 Директивы 2002/58/ЕС государства – члены ЕС должны принять меры для обеспечения сохранения данных, указанных в статье 5 настоящей Директивы, в соответствии с ее положениями в том объеме, в котором такие данные генерируются или обрабатываются провайдерами общедоступных услуг электронной связи или сетей связи общего пользования в пределах их юрисдикции в процессе предоставления соответствующих услуг связи…».

С. Соответствующая прецедентная практика Суда Европейского союза (далее – Суд ЕС)

1. Постановление по делу «Компания “Диджитал Райтс Айлэнд Лтд” против министра по делам связи, морским

делам и природным ресурсам и других и Правительство австрийской земли Каринтия и другие» (Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others) (дела №№ C-293/12 и C-594/12, ECLI: EU: C:2014:238)

98. В Постановлении от 8 апреля 2014 г. Суд ЕС объявил недействительной Директиву 2006/24/ЕС о сохранении данных, устанавливающую обязательство провайдеров общедоступных услуг электронной связи или сетей связи общего пользования хранить все данные о трафике и местоположении в течение периода от шести месяцев до двух лет в целях обеспечения доступности данных для расследования, обнаружения и судебного преследования преступных действий, как это определено каждым государством – членом ЕС в его внутригосударственном законодательстве. Как отметил Суд ЕС, хотя указанная директива не разрешала хранить содержание сообщения, охватываемые ею данные о трафике и местоположении могли позволить сделать достаточно точные выводы относительно частной жизни лиц, данные о которых были сохранены. Соответственно, обязательство хранить данные само по себе является вмешательством в право на уважение частной жизни и корреспонденции, гарантированное статьей 7 Хартии Европейского союза об основных правах, и в право на защиту персональных данных, предусмотренное ее статьей 8.

99. Доступ компетентных внутригосударственных органов к данным также представлял собой вмешательство в указанные основные права, которое Суд ЕС счел «особенно серьезным». Тот факт, что данные хранились и впоследствии использовались без уведомления абонента или зарегистрированного пользователя, по мнению Суда ЕС, мог породить в сознании заинтересованных лиц ощущение того, что их частная жизнь является предметом постоянного наблюдения. Вмешательство соответствовало цели, представляющей общий интерес, а именно оказывать содействие в борьбе с серьезными преступлениями и терроризмом и в итоге в содействии обеспечению общественной безопасности. Однако оно не отвечало требованию соразмерности.

100. Во-первых, рассматриваемая директива в обобщенном виде охватывала всех лиц и все средства электронной связи, а также все данные о трафике без каких-либо различий, ограничений или исключений в свете цели борьбы с серьезными преступлениями. Следовательно, это влекло за собой вмешательство в основные права практически всего населения Европейского союза. Она была применима даже к лицам, в отношении которых не было доказательств, позволяющих предположить, что их действия могли иметь связь, даже косвенную или отдаленную, с серьезным преступлением.

101. Во-вторых, обжалуемая директива не содержала материально-правовых и процессуальных условий, касающихся доступа компетентных внутригосударственных органов к данным и их последующему использованию. Просто ссылаясь в целом на серьезное преступление, как определено каждым государством – членом ЕС в его внутригосударственном законодательстве, директива не устанавливала какой-либо объективный критерий, позволявший определить, какие преступления могут считаться достаточно серьезными, чтобы оправдать такое широкомасштабное вмешательство в основные права, закрепленные в статьях 7 и 8 хартии. Прежде всего доступ компетентных внутригосударственных органов к хранящимся данным не зависел от предварительной проверки со стороны суда или независимого административного органа, решение которого было бы направлено на ограничение доступа к данным и их использования до объема, строго необходимого для достижения преследуемой цели.

102. В-третьих, директива требовала, чтобы все данные хранились в течение как минимум шести месяцев без какого-либо различия между категориями данных на основе их предполагаемой пользы для преследуемой цели или в зависимости от различных заинтересованных лиц. Суд ЕС пришел к выводу, что эта директива влекла за собой широкомасштабное и особенно серьезное вмешательство в основные права, предусмотренные статьями 7 и 8 хартии, которое не было точно очерчено положениями, гарантирующими, что такое вмешательство действительно ограничивается лишь строго необходимым. Суд ЕС также отметил, что рассматриваемая директива не обеспечивала достаточных гарантий посредством принятия технических и организационных мер в целях обеспечения эффективной защиты хранящихся данных от риска злоупотребления и от любого незаконного доступа и использования таких данных.

2. Постановления по делам «Компания “Теле2 Сверие АБ” против Управления почты и телекоммуникаций Швеции» (Tele2 Sverige AB v. Post- och telestyrelsen) и «Министр внутренних дел против Тома Уотсона и других» (Secretary of State for the Home Department v. Tom Watson and Others) (дела №№ C203/15 и C698/15, ECLI: EU: C:2016:970)

103. В деле «Министр внутренних дел против Тома Уотсона и других» (Secretary of State for the Home Department v. Tom Watson and Others) заявители требовали судебной проверки законности статьи 1 Закона Соединенного Королевства о хранении данных и следственных полномочиях от 2014 года (далее – Закон о хранении данных), в соответствии с которой министр внутренних дел может потребовать от оператора телекомму-

никационной сети общего пользования хранить соответствующие данные о сообщениях, если министр сочтет это необходимым и соразмерным для одной или нескольких целей, попадающих под действие подпунктов «a»–«h» пункта 2 статьи 22 Закона о правовом регулировании следственных полномочий 2000 года. Заявители утверждали, *inter alia*, что статья 1 Закона о хранении данных несовместима со статьями 7 и 8 Хартии и статьей 8 Конвенции.

104. Постановлением от 17 июля 2015 г. Высокий суд определил, что Решение Суда ЕС по делу «Компания "Диджитал Райтс Айлэнд Лтд" против министра по делам связи, морским делам и природным ресурсам и других и Правительство австрийской земли Каринтия и другие» (Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others) устанавливало «обязательные требования права Европейского союза», применимые к законодательству государств – членов ЕС в отношении хранения данных о сообщениях и доступа к таким данным. Поскольку Суд ЕС в этом деле постановил, что Директива 2006/24 несовместима с принципом соразмерности, то внутригосударственное законодательство, содержащее те же положения, что и указанная директива, в равной мере не могло быть совместимо с этим принципом. Фактически из основной логики постановления по названному делу следовало, что законодательство, устанавливающее общий свод правил для хранения данных о сообщениях, нарушало права, гарантированные статьями 7 и 8 Хартии, кроме случаев, когда такое законодательство было дополнено правилами доступа к данным, определенным внутригосударственным законодательством, которые обеспечивают достаточные гарантии для защиты указанных прав. Соответственно, статья 1 Закона о хранении данных несовместима со статьями 7 и 8 хартии, поскольку она не устанавливает четких и точных правил доступа к хранящимся данным и правил их использования и поскольку доступ к этим данным не зависел от предварительной проверки со стороны суда или независимого административного органа.

105. В порядке рассмотрения жалобы министра внутренних дел Апелляционный суд обратился в Суд ЕС за вынесением предварительного заключения.

106. Суд ЕС объединил это дело с запросом о вынесении предварительного заключения от Административного апелляционного суда (*kammarrätten*) г. Стокгольма по делу № C-203/15 «Компания "Теле2 Сверие АБ" против Управления почты и телекоммуникаций Швеции» (Tele2 Sverige AB v Post- och telestyrelsen) для их рассмотрения в одном производстве. По результатам устного слушания, в котором участвовали власти около 15 государств – членов ЕС, Суд ЕС 21 декабря 2016 г. вынес постановление, в котором указал, что пункт 1 статьи 15 Директивы 2002/58, рассматриваемый в свете статей 7, 8 и 11 и пункта 1 статьи 52 хартии, следовало толковать как запрет принятия внутригосударственного законодательства, регулирующего защиту и безопасность данных о трафике и местоположении и, в частности, доступ компетентных внутригосударственных органов к хранящимся данным, если цель такого доступа в контексте борьбы с преступностью не ограничивалась только борьбой с серьезными преступлениями, если доступ не подлежал предварительной проверке со стороны суда или независимого административного органа и если отсутствовало требование о том, что соответствующие данные должны храниться в пределах Европейского союза.

107. Суд ЕС объявил вопрос Апелляционного суда о том, была ли защита, предоставляемая статьями 7 и 8 Хартии, шире, чем защита в соответствии со статьей 8 Конвенции, неприемлемым для рассмотрения по существу.

108. После вынесения указанного постановления Суда ЕС дело было повторно передано в Апелляционный суд. 31 января 2018 г. он предоставил декларативную защиту в следующих формулировках: статья 1 Закона о хранении данных несовместима с правом ЕС в том объеме, в котором она разрешает доступ к хранящимся данным, если цель такого доступа не ограничивается исключительно борьбой с серьезными преступлениями или если доступ не подлежит предварительной проверке со стороны суда или независимого административного органа.

3. Постановление по делу «Прокуратура Испании» (Ministerio Fiscal) (дело № C-207/16, ECLI: EU: C:2018:788)

109. Запрос о вынесении предварительного заключения был направлен после того, как полиция Испании в ходе расследования кражи кошелька и мобильного телефона обратилась к следственному судье с ходатайством о предоставлении ей доступа к данным, позволяющим идентифицировать пользователей телефонных номеров, активированных с помощью украденного телефона, за 12 дней, предшествовавших краже. Следственный судья отклонил ходатайство, *inter alia*, ввиду того что деяния, послужившие основанием для проведения уголовного расследования, не составляли «серьезного» преступления. Суд, направивший запрос, впоследствии запросил у Суда ЕС указания относительно установления порога тяжести преступлений, при превышении которого вмешательство в основные права, например, доступ компетентных внутригосударственных органов к персональным данным, хранящимся у провайдеров услуг электронной связи, может быть оправдан.

110. 2 октября 2018 г. Большая Палата Суда ЕС постановила, что пункт 1 статьи 15 Директивы 2002/58/ЕС, рассмотренный в свете статей 7 и 8 Хартии Европейского союза об основных правах, следовало толковать как означающий, что доступ государственных органов к данным в целях идентификации владельцев сим-карт, активированных с помощью украденного мобильного телефона, таким как фамилии, имена и при необходимости адреса владельцев, представлял собой вмешательство в их основные права, которое не было достаточно серьезным, чтобы повлечь за собой ограничение этого доступа в сфере предотвращения, расследования, обнаружения и судебного преследования преступных действий в целях борьбы с серьезными преступлениями. В частности, Большая Палата Суда ЕС отметила следующее:

> «В соответствии с принципом соразмерности серьезное вмешательство в сферах предотвращения, расследования, обнаружения и судебного преследования преступных действий может быть оправдано только целью борьбы с преступлениями, которые должны быть определены как “серьезные”.
>
> Напротив, когда вмешательство, которое влечет за собой такой доступ, не является серьезным, доступ может быть оправдан целью предотвращения, расследования, обнаружения и судебного преследования “преступных действий” в целом».

111. Большая Палата Суда ЕС не сочла доступ к данным, ставшим предметом запроса, особенно серьезным вмешательством, поскольку оно:

> «просто позволяло связать сим-карту или сим-карты, активированные в течение определенного периода с помощью украденного мобильного телефона, с личностью владельцев сим-карт. Без перекрестных ссылок на данные о сообщениях, отправленных с этих сим-карт, и на данные о местоположении, указанные выше данные не позволяют установить дату, время, продолжительность и получателей сообщений, отправленных с помощью таких сим-карт, равно как и место, где происходил обмен сообщениями, и частоту отправки сообщений конкретным лицам в течение определенного периода. Следовательно, указанные выше данные не позволяли сделать точные выводы о частной жизни лиц, которых они затрагивали».

4. Постановление по делу «Максимилиан Шремс против Уполномоченного по защите данных» (Maximillian Schrems v. Data Protection Commissioner) (дело № C362/14, ECLI: EU: C:2015:650)

112. Указанный запрос о вынесении предварительного заключения был направлен в результате жалобы на компанию «Фейсбук Айлэнд Лтд» (*Facebook Ireland Ltd*), поданной Уполномоченному по защите данных Ирландии австрийским юристом и активистом по защите персональных данных М. Шремсом (M. Schrems). Он обжаловал передачу его данных компанией «Фейсбук Айлэнд Лтд» в Соединенные Штаты Америки и хранение его данных на серверах, расположенных в США. Уполномоченный по защите данных отклонил жалобу, поскольку в Решении от 26 июля 2000 г. Европейская комиссия сочла, что США обеспечивают надлежащий уровень защиты передаваемых персональных данных (далее – Решение о безопасной гавани).

113. В Постановлении от 6 октября 2015 г. Суд ЕС указал, что Решение Европейской комиссии о том, что третья страна обеспечивает надлежащий уровень защиты передаваемых персональных данных, не может устранить или даже уменьшить полномочия внутригосударственных надзорных органов в соответствии с Хартией или Директивой о защите данных. Следовательно, даже если Европейская комиссия приняла решение, внутригосударственные надзорные органы должны иметь возможность изучить полностью независимо, соответствовала ли передача данных лица в третью страну требованиям, установленным указанной директивой.

114. Однако только Суд ЕС мог признать решение Европейской комиссии недействительным. В связи с этим он отметил, что механизм безопасной гавани применим исключительно к предприятиям США, которые его придерживаются, а власти США ему не подчиняются. Кроме того, требования национальной безопасности, охраны общественных интересов и правопорядка Соединенных Штатов Америки преобладали над механизмом безопасной гавани, поэтому предприятия США были обязаны игнорировать без каких-либо ограничений защитные правила, установленные механизмом, если они противоречили этим требованиям. Следовательно, указанный механизм позволял властям США вмешиваться в основные права лиц, и Европейская комиссия в Решении о безопасной гавани не упомянула о существовании в США норм, направленных на ограничение такого вмешательства, или о наличии эффективной правовой защиты от вмешательства.

115. Что касается того, был ли уровень защиты в США по существу эквивалентен основным правам и свободам, гарантированным в Европейском союзе, Суд ЕС установил, что законодательство не ограничивалось строго необходимым, поскольку оно разрешало на обобщенной основе хранение всех персональных данных всех лиц, данные которых были переданы из Европейского союза в США без каких-либо различий, ограничений или исключений в свете преследуемой цели и без наличия объективного критерия, установленного для определения пределов доступа государственных органов к данным и их последующего использования. Таким образом, в соответствии с правом ЕС законодательство, разрешающее органам госу-

дарственной власти иметь доступ к содержанию электронных сообщений на обобщенной основе, должно рассматриваться как подрывающее сущность основного права на уважение частной жизни. Аналогичным образом законодательство, не предусматривающее возможности физического лица использовать средства правовой защиты, чтобы иметь доступ к относящимся к нему персональным данным или добиваться исправления либо удаления этих данных, ставило под угрозу сущность основного права на эффективную судебную защиту.

116. Наконец, Суд ЕС установил, что Решение о безопасной гавани лишает внутригосударственные надзорные органы их полномочий, если лицо ставит под сомнение совместимость решения с защитой частной жизни, а также основных прав и свобод человека. Европейская комиссия не компетентна ограничивать полномочия внутригосударственных надзорных органов подобным образом, и, следовательно, Суд ЕС признал Решение о безопасной гавани недействительным.

5. Постановление по делу «Уполномоченный по защите данных против компании "Фейсбук Айлэнд Лтд" и Максимилиана Шремса» (дело № C-311/18, ECLI: EU: C:2020:559)

117. После вынесения Судом ЕС Постановления от 6 октября 2015 г. суд, направивший запрос, аннулировал отклонение жалобы М. Шремса и вернул решение Уполномоченному по защите данных. В ходе расследования Уполномоченного по защите данных компания «Фейсбук Айлэнд Лтд» пояснила, что большая часть персональных данных была передана компании «Фейсбук Инк.» (*Facebook Inc.*) в соответствии со стандартными положениями о защите данных, изложенными в приложении к Решению Европейской комиссии 2010/87/ЕС в действующей редакции.

118. М. Шремс переформулировал свою жалобу, утверждая, *inter alia*, что законодательство США требовало от компании «Фейсбук Инк.» предоставлять переданные ей персональные данные в распоряжение некоторых государственных органов США, например, Агентству национальной безопасности (далее – АНБ) и Федеральному бюро расследований. В силу того, что эти данные использовались в контексте различных программ мониторинга способом, несовместимым со статьями 7, 8 и 47 хартии, Решение 2010/87/ЕС не могло оправдать передачу таких данных в США. В связи с этим он просил Уполномоченного по защите данных запретить или приостановить передачу его персональных данных компании «Фейсбук Инк.».

119. В проекте решения, опубликованном 24 мая 2016 г., Уполномоченный по защите данных высказал предварительное мнение о том, что персональные данные граждан Европейского союза, переданные в Соединенные Штаты Америки, скорее всего, будут использоваться и обрабатываться властями США в порядке, несовместимом со статьями 7 и 8 хартии, и что законодательство США не предоставляет этим гражданам средства правовой защиты, совместимые со статьей 47 хартии. Уполномоченный по защите данных утверждал, что стандартные положения о защите данных, содержащиеся в приложении к Решению 2010/87/ЕС, не могут исправить этот недостаток, поскольку они не являются обязательными для властей США.

120. Проанализировав разведывательную деятельность США в соответствии со статьей 702 Закона о негласном наблюдении в целях внешней разведки и Указом Президента США № 12333, Высокий суд пришел к выводу, что в Соединенных Штатах Америки осуществляется массовая обработка персональных данных без обеспечения уровня защиты, по существу эквивалентного тому, который гарантируется статьями 7 и 8 хартии, и что граждане Европейского союза не имеют доступа к тем же средствам правовой защиты, что и граждане США. Следовательно, законодательство США не предоставляет гражданам ЕС уровень защиты, по существу эквивалентный тому, что гарантируется статьей 47 хартии. Высокий суд приостановил производство по делу и передал ряд вопросов в Суд ЕС для вынесения предварительного заключения. Он спрашивал, *inter alia*, о том, применяется ли право ЕС к передаче данных от частной компании в Европейском союзе частной компании в третьей стране, и если да, то как следует оценивать уровень защиты в третьей стране, и соответствует ли уровень защиты, предоставляемый в США, сущности прав, гарантированных статьей 47 хартии.

121. В Постановлении от 16 июля 2020 г. Суд ЕС указал, что Общий регламент по защите данных (Общий регламент) применяется к передаче персональных данных в коммерческих целях экономическим оператором, учрежденным в государстве – члене ЕС, другому экономическому оператору, учрежденному в третьей стране, независимо от того, подлежат ли такие данные в момент передачи или впоследствии обработке властями соответствующей третьей страны в целях защиты общественной безопасности, обороны и государственной безопасности. Кроме того, надлежащие гарантии, подлежащие исполнению права, и эффективные средства правовой защиты, требуемые Общим регламентом, должны гарантировать предоставление субъектам данных, чьи персональные данные были переданы в третью страну в соответствии со стандартными положениями о защите данных, уровня защиты, по существу эквивалентного тому, что предоставляется в пределах Европейского союза.

В указанных целях оценка уровня защиты, предоставляемого в контексте такой передачи, должна учитывать как договорные положения, согласованные между контролером или лицом, осуществляющим обработку данных, которые учреждены в Европейском союзе, и получателем данных, учрежденным в соответствующей третьей стране, так и соответствующие аспекты правовой системы этой третьей страны в отношении доступа ее государственных органов к переданным персональным данным.

122. Кроме того, в отсутствие действительного решения Европейской комиссии о достаточном уровне защиты компетентный надзорный орган должен приостановить или запретить передачу данных в третью страну, если, по мнению этого надзорного органа и в свете всех обстоятельств передачи, стандартные положения о защите данных, принятые Европейской комиссией, не соблюдались или не могли соблюдаться в третьей стране, и защита передаваемых данных (в соответствии с требованиями права Европейского союза) не могла быть обеспечена с помощью других средств.

123. Для того, чтобы Европейская комиссия могла принять решение о достаточном уровне защиты, она должна установить с указанием надлежащих оснований, что соответствующая третья страна в силу своего внутригосударственного законодательства или своих международных обязательств обеспечивает уровень защиты основных прав, по существу эквивалентный тому, что гарантирован правовым режимом Европейского союза. По мнению Суда ЕС, Решение о безопасной гавани было недействительным. Статья 702 Закона о негласном наблюдении в целях внешней разведки не содержала каких-либо ограничений полномочий, которые она предоставляла для внедрения программ наблюдения в целях внешней разведки, или на наличие гарантий для лиц, не являющихся гражданами США, которых такие программы могут затрагивать. В указанных обстоятельствах статья 702 Закона о негласном наблюдении в целях внешней разведки не могла обеспечивать уровень защиты, по существу эквивалентный тому, что гарантируется хартией. Кроме того, что касается программ мониторинга, основанных на Указе Президента США № 12333, было очевидно, что он также не предоставлял прав, которые могли быть принудительно исполнены в отношении властей США в судах.

6. Постановления по делам «Организация “Прайваси интернэшнл” против министра иностранных дел и по делам содружества и других» (Privacy International v. Secretary of State for Foreign and Commonwealth Affairs and Others) (дело № C-623/17, ECLI: EU: C:2020:790) и «Организация “Ла Квадратюр дю Нет” и другие» (La Quadrature du Net and Others), «Французская сеть передачи данных и другие» (French Data Network and Others) и «Коллегия франкоязычных и немецкоязычных адвокатов и другие» (Ordre des barreaux francophones et germanophone and Others) (дела №№ C-511/18, C-512/18 и C-520/18, ECLI: EU: C:2020:791)

124. 8 сентября 2017 г. Следственный трибунал Соединенного Королевства вынес Решение по делу «Организация “Прайваси интернэшнл” против министра иностранных дел и по делам содружества и других» (Privacy International v. Secretary of State for Foreign and Commonwealth Affairs and Others), которое касалось получения разведывательными службами массива данных о сообщениях в соответствии со статьей 94 Закона о телекоммуникациях 1984 года и массива персональных данных. Следственный трибунал установил, что после их открытого признания эти режимы не нарушали статью 8 Конвенции. Однако он определил следующие четыре требования, которые, по-видимому, следовали из Постановления Суда ЕС по делу «Министр внутренних дел против Тома Уотсона и других» (Secretary of State for the Home Department v. Tom Watson and Others) и, казалось, выходили за рамки требований статьи 8 Конвенции: ограничение нецелевого доступа к массиву данных; необходимость предварительного разрешения (кроме случаев, когда правомерно установлено наличие чрезвычайной ситуации) до получения доступа к данным; положение о последующем уведомлении затронутых лиц и хранение всех данных на территории Европейского союза.

125. 30 октября 2017 г. Следственный трибунал направил в Суд ЕС запрос о вынесении предварительного заключения, разъясняющего, в какой степени требования, установленные в деле «Министр внутренних дел против Тома Уотсона и других» (Secretary of State for the Home Department v. Tom Watson and Others), могут применяться в тех случаях, когда получение массива данных и их автоматизированная обработка необходимы для защиты национальной безопасности. При этом Следственный трибунал выразил серьезную обеспокоенность тем, что, если требования, установленные в указанном деле, должны применяться к мерам, принимаемым для защиты национальной безопасности, то такие меры будут невыполнимы, а национальная безопасность государств – членов ЕС окажется под угрозой. В частности, он отметил следующие факторы: преимущества получения массива данных в контексте национальной безопасности; риск того, что необходимость получения предварительного разрешения может подорвать способность разведывательных служб устранять угрозы

национальной безопасности; опасность и непрактичность внедрения требования об уведомлении в отношении получения или использования массива данных, особенно когда на карту поставлена национальная безопасность; возможное влияние абсолютного запрета на передачу данных за пределы Европейского союза на договорные обязательства государств – членов ЕС.

126. Публичное слушание состоялось 9 сентября 2019 г. Дело «Организация "Прайваси интернэшнл" против министра иностранных дел и по делам содружества и других» (Privacy International v. Secretary of State for Foreign and Commonwealth Affairs and Others) рассматривалось совместно с делами «Организация "Ла Квадратюр дю Нет" и другие» (La Quadrature du Net and Others) (№№ C-511/18 и C-512/18) и «Коллегия франкоязычных и немецкоязычных адвокатов и другие» (Ordre des barreaux francophones et germanophone and Others) (№ C-520/18), которые также касались применения Директивы 2002/58 к мероприятиям, связанным с национальной безопасностью и борьбой с терроризмом. В поддержку заинтересованных государств выступили власти 13 стран.

127. 6 октября 2020 г. были вынесены два отдельных постановления. В деле «Организация "Прайваси интернэшнл" против министра иностранных дел и по делам содружества и других» (Privacy International v. Secretary of State for Foreign and Commonwealth Affairs and Others) Суд ЕС постановил, что внутригосударственное законодательство, разрешающее органам власти требовать, чтобы провайдеры услуг электронной связи направляли данные о трафике и местоположении в органы внешней разведки и государственной безопасности в целях защиты национальной безопасности, попадало под действие Директивы о конфиденциальности и электронных средствах связи. При толковании этой директивы следовало учитывать право на неприкосновенность частной жизни, право на защиту персональных данных и право на свободу выражения мнений, гарантированные статьями 7, 8 и 11 хартии соответственно. Ограничения на осуществление этих прав должны быть предусмотрены законом, не должны затрагивать сущность прав, а также должны быть соразмерными, необходимыми и действительно отвечать целям общего интереса, признанным Европейским союзом, или необходимости защиты прав и свобод других лиц. Кроме того, ограничения защиты персональных данных должны применяться только в той мере, в какой это строго необходимо. Для того, чтобы отвечать требованию соразмерности, законодательство должно содержать четкие и точные правила, регулирующие объем и сферу применения рассматриваемой меры, а также устанавливающие минимальные гарантии, чтобы лица, персональные данные которых были затронуты, имели достаточные гарантии того, что их данные будут эффективно защищены от риска злоупотреблений.

128. По мнению Суда ЕС, внутригосударственное законодательство, требующее от провайдеров услуг электронной связи раскрывать данные о трафике и местоположении органам внешней разведки и государственной безопасности посредством общей и неизбирательной передачи данных, которая затрагивала всех лиц, пользующихся услугами электронной связи, превышало пределы строгой необходимости и не могло считаться обоснованным в соответствии с Директивой о конфиденциальности и электронных средствах связи, рассматриваемой во взаимосвязи с хартией.

129. Однако в деле «Организация "Ла Квадратюр дю Нет" и другие» (La Quadrature du Net and Others) Суд ЕС подтвердил, что, хотя Директива о конфиденциальности и электронных средствах связи, рассматриваемая во взаимосвязи с хартией, исключает законодательные меры, предусматривающие общее и неизбирательное хранение данных о трафике и местоположении, в ситуациях, когда государство – член ЕС сталкивается с серьезной угрозой для национальной безопасности, в отношении которой доказано, что она является реальной и существующей или ожидаемой, указанная директива не препятствует принятию законодательных мер, требующих, чтобы провайдеры услуг осуществляли общее и неизбирательное хранение данных о трафике и местоположении в течение периода, ограниченного строго необходимым, но который может быть продлен, если угроза сохраняется. В целях борьбы с серьезными преступлениями и предотвращения серьезных угроз для общественной безопасности государство – член ЕС также вправе предусмотреть, если это строго ограничено по времени, целевое хранение данных о трафике и местоположении на основе объективных и недискриминационных факторов в зависимости от категорий затронутых лиц либо с использованием географических критериев или IP-адресов, присвоенных источнику интернет-соединения. Государство – член ЕС также может осуществлять общее и неизбирательное хранение данных о гражданской личности пользователей средств электронной связи без ограничения срока такого хранения.

130. Кроме того, Директива о конфиденциальности и электронных средствах связи, рассматриваемая во взаимосвязи с хартией, не препятствовала принятию внутригосударственных норм, которые обязывали провайдеров услуг электронной связи прибегать, во-первых, к автоматизированному анализу и сбору данных о трафике и местоположении в режиме реального времени и, во-вторых, к сбору в режиме реального вре-

мени технических данных о местонахождении используемого оконечного оборудования, если такие нормы ограничивались ситуациями, когда государство – член ЕС сталкивалось с серьезной угрозой для национальной безопасности, которая была реальной и существующей или ожидаемой, и когда обращение к такому анализу могло подлежать эффективной проверке со стороны суда или независимого административного органа, решение которого являлось обязательным, а также ситуациями, когда сбор данных о трафике и местонахождении в режиме реального времени был ограничен лицами, в отношении которых имелись веские основания подозревать, что они были причастны к террористической деятельности, и в отношении которых проводились предварительные проверки со стороны суда или независимого административного органа, решение которого являлось обязательным.

IV. СООТВЕТСТВУЮЩИЕ СРАВНИТЕЛЬНОЕ ПРАВО И ПРАВОПРИМЕНИТЕЛЬНАЯ ПРАКТИКА

А. Государства – участники Конвенции

1. Обзор

131. Как минимум семь государств – участников Конвенции (Финляндия, Франция, Германия, Нидерланды, Швеция, Швейцария и Соединенное Королевство) официально используют режимы массового перехвата данных по кабельным и/или воздушным путям.

132. Еще в одном государстве (в Норвегии) обсуждается законопроект: если он будет принят, то массовый перехват данных также будет разрешен.

133. Режим массового перехвата данных в Соединенном Королевстве подробно описан в упомянутом выше Постановлении Европейского Суда по делу «Организация Big Brother Watch и другие против Соединенного Королевства» (Big Brother Watch and Others v. United Kingdom).

134. Что касается соглашений об обмене разведывательными данными, по крайней мере 39 государств – участников Конвенции либо заключили соглашения об обмене разведывательными данными с другими государствами, либо имеют возможность для заключения подобных соглашений. Два государства прямо запрещают, а два разрешают властям просить иностранное государство перехватывать материалы в их интересах. В остальных государствах позиция по этому вопросу не ясна.

135. Наконец, в большинстве государств применимые гарантии в целом такие же, как и для внутригосударственных операций, с различными ограничениями на использование полученных данных и в некоторых случаях с обязательством уничтожить их, если они станут неактуальными.

2. Постановление Федерального конституционного суда Германии от 19 мая 2020 г. (1 BvR2835/17)

136. В указанном постановлении Федеральный конституционный суд Германии рассмотрел вопрос о том, нарушают ли полномочия Федеральной разведывательной службы Германии по проведению стратегической (или «радиотехнической») разведки в отношении внешних телекоммуникационных сообщений основные права, содержащиеся в Основном законе Германии (*Grundgesetz*).

137. Рассматриваемый режим предполагал перехват как содержания, так и связанных с ним данных о сообщениях и был направлен только на мониторинг внешних телекоммуникационных сетей за пределами территории Германии. Данный мониторинг мог осуществляться в целях получения информации по вопросам, которые федеральные власти Германии в соответствии со своей компетенцией считали значимыми для внешней политики и политики безопасности государства. Однако этот мониторинг мог осуществляться и в отношении конкретных лиц. Допустимость и необходимость распоряжения о проведении такого мониторинга контролировались независимой комиссией. Согласно постановлению Федерального конституционного суда Германии за перехватом следовал многоэтапный, полностью автоматизированный процесс фильтрации и оценки. В указанных целях Федеральная разведывательная служба использовала шестизначное число поисковых запросов, которые подлежали контролю внутренним подразделением, ответственным за обеспечение того, чтобы связь между используемыми поисковыми запросами и целью запроса данных объяснялась разумным и исчерпывающим образом. После применения автоматизированного процесса фильтрации перехваченный материал удалялся или сохранялся и передавался аналитику для проведения оценки.

138. Обмен перехваченными материалами с иностранными разведывательными службами сопровождался заключением соглашения о сотрудничестве, которое должно было содержать ограничения на использование и гарантии для обеспечения обработки и удаления данных в соответствии с принципом верховенства права.

139. Федеральный конституционный суд Германии постановил, что рассматриваемый режим не соответствовал Основному закону Германии. Признавая преобладающий государственный интерес к эффективному сбору данных внешней разведки, он, тем не менее, счел, *inter alia*, что режим не был ограничен достаточно конкретными целями, что его структура не позволяла осуществлять надлежащий надзор и контроль и что отсутствуют раз-

личные гарантии, особенно в отношении защиты журналистов, адвокатов и иных лиц, сообщения которых требуют особой защиты конфиденциальности.

140. Что касается обмена разведывательными данными, полученными в результате наблюдения за внешними телекоммуникационными сообщениями, Федеральный конституционный суд Германии вновь установил отсутствие гарантий. В частности, не было достаточно четко указано, когда важные интересы могут оправдывать передачу данных. В дополнение, хотя Федеральный конституционный суд Германии не счел необходимым, чтобы государство-получатель имело сопоставимые правила обработки персональных данных, он, вместе с тем, счел, что данные могут быть переданы за границу только при обеспечении надлежащего уровня защиты данных и в отсутствие оснований опасаться того, что информация будет использована для нарушения основных принципов верховенства права. В более общем плане, в контексте обмена разведывательными данными, Федеральный конституционный суд Германии отметил, что сотрудничество с иностранными государствами не должно использоваться для ослабления гарантий на внутригосударственном уровне, и если Федеральная разведывательная служба хочет использовать поисковые запросы, предоставленные ей иностранной разведывательной службой, она должна сначала удостовериться в наличии необходимой связи между поисковыми запросами и целью запроса данных, а также в том, что полученные в результате данные не свидетельствуют об особой потребности в обеспечении конфиденциальности (например, в силу того, что они касаются осведомителей или диссидентов). Хотя Федеральный конституционный суд Германии не исключил возможности передачи массива данных иностранным разведывательным службам, он установил, что этот процесс не может быть непрерывным и основанным на единственной цели.

141. Наконец, Федеральный конституционный суд Германии постановил, что рассматриваемые полномочия по наблюдению также не являлись предметом всестороннего независимого и постоянного надзора в целях обеспечения соблюдения закона и компенсации фактического отсутствия гарантий, обычно предусмотренных в соответствии с принципом верховенства права. Законодатель должен был предусмотреть два различных вида надзора, которые также должны были быть отражены в организационной структуре: во-первых, орган, подобный суду, которому поручено проводить надзор и принимать решения в рамках формальной процедуры, обеспечивающей юридическую защиту *ex ante* или *ex post*, и, во-вторых, надзор административного характера, который позволял бы проводящему его органу по собственной инициативе в случайном порядке проверять весь процесс стратегического наблюдения на предмет его законности. По мнению Федерального конституционного суда Германии, некоторые ключевые процессуальные действия в принципе потребуют *ex ante* разрешения со стороны органа, подобного суду, а именно формальное определение различных мер наблюдения (освобождения от этого требования в случаях срочности не исключались); использование поисковых запросов в той мере, в какой они непосредственно затрагивали лиц, которые могли представлять угрозу и, следовательно, вызывали прямой интерес Федеральной разведывательной службы; использование поисковых запросов, направленных непосредственно на лиц, чьи сообщения требовали особой защиты конфиденциальности; обмен с иностранными разведывательными службами данными журналистов, юристов и представителей других профессий, заслуживающих особой защиты конфиденциальности.

B. Соединенные Штаты Америки

142. Разведывательные службы США применяли программу Upstream в соответствии со статьей 702 Закона о негласном наблюдении в целях внешней разведки.

143. Генеральный прокурор и директор национальной разведки ежегодно выдают сертификаты, разрешающие наблюдение за лицами, не являющимися гражданами США, которые по обоснованным предположениям находятся за пределами США. Им не нужно указывать Суду по делам о наблюдении за иностранной разведывательной деятельностью на конкретных лиц, не являющихся гражданами США, или доказывать возможное основание полагать, что лицо, ставшее объектом наблюдения, является агентом иностранной державы. Вместо этого в сертификатах, выдаваемых в соответствии со статьей 702 Закона о негласном наблюдении в целях внешней разведки, указываются категории собираемой информации, которая должна соответствовать установленному законом определению информации о деятельности иностранной разведки. Выданные сертификаты включают информацию о международном терроризме и приобретении оружия массового поражения.

144. В соответствии с разрешением Агентство национальной безопасности (АНБ) при вынужденном содействии провайдеров услуг копирует и осуществляет поиск потоков интернет-трафика по мере передачи данных через Интернет. Осуществляется сбор как телефонных звонков, так и интернет-сообщений. До апреля 2017 года АНБ получало данные об интернет-сообщениях «в адрес» целевого селектора, «от» него и «о» нем. Для сообщений «в адрес» и «от» отправителем или получателем являлся пользователь целевого селектора в соответствии со статьей 702 Закона о негласном наблюдении в целях внешней развед-

ки. В сообщениях «о» целевой селектор упоминался в получаемом интернет-сообщении, но искомый объект необязательно являлся участником общения. Таким образом, сбор сообщений «о» предполагал поиск содержания сообщений, передаваемых через Интернет. Однако с апреля 2017 года АНБ не получало и не собирало сообщения просто «об» искомом объекте. Кроме того, АНБ заявило, что в связи с таким сокращением оно удалит подавляющее большинство ранее полученных в рамках программы Upstream интернет-сообщений, как только это станет практически возможным.

145. Статья 702 Закона о негласном наблюдении в целях внешней разведки требует от властей разработки процедур адресного воздействия и минимизации, которые находятся под контролем Суда по делам о наблюдении за иностранной разведывательной деятельностью.

146. Указ Президента США № 12333, подписанный в 1981 году, разрешает сбор, хранение и распространение информации, полученной в ходе законных мероприятий по внешней разведке, контрразведке, международных расследований преступлений, связанных с наркотиками или международным терроризмом. Наблюдение за иностранными гражданами согласно Указу Президента США № 12333 не подлежит внутригосударственному регулированию в соответствии с Законом о негласном наблюдении в целях внешней разведки. Неизвестно, сбор какого объема данных осуществляется в соответствии с Указом Президента США № 12333 по сравнению со сбором данных на основании статьи 702 Закона о негласном наблюдении в целях внешней разведки.

ПРАВО

I. ПРЕДВАРИТЕЛЬНЫЙ ВОПРОС: ДАТА ОЦЕНКИ

147. В Палате Европейского Суда заявитель просил вынести постановление о совместимости с Конвенцией соответствующего законодательства Швеции, которое применялось в течение трех различных периодов времени (см. § 82 Постановления Палаты Европейского Суда). Палата Европейского Суда сосредоточила свое внимание на законодательстве Швеции по состоянию на момент рассмотрения настоящего дела (см. §§ 96–98 Постановления Палаты Европейского Суда).

148. В ходе производства по делу в Большой Палате Европейского Суда заявитель не повторил свой запрос относительно трех периодов времени, но в своих доводах ссылался, *inter alia*, на события 2018 и 2019 годов, которые произошли позднее рассмотрения дела Палатой Европейского Суда.

149. По мнению властей Швеции, с учетом прецедентной практики Европейского Суда, согласно которой «содержание и пределы рассмотрения дела, переданного в Большую Палату Европейского Суда… ограничиваются решением Палаты Европейского Суда о приемлемости жалобы для рассмотрения по существу», проверка со стороны Большой Палаты Европейского Суда должна ограничиваться законодательством Швеции по состоянию на момент рассмотрения дела Палатой Европейского Суда.

150. Большая Палата Европейского Суда согласна с Палатой Европейского Суда в том, что при рассмотрении соответствующего законодательства *in abstracto*, как в настоящем деле, задачей Европейского Суда не может быть проверка его совместимости с Конвенцией до и после внесения каждого отдельного изменения.

151. Таким образом, временные пределы рассмотрения дела Большой Палатой Европейского Суда ограничиваются законодательством и правоприменительной практикой Швеции по состоянию на май 2018 года, то есть на момент рассмотрения дела Палатой Европейского Суда.

II. ПРЕДПОЛАГАЕМОЕ НАРУШЕНИЕ СТАТЬИ 8 КОНВЕНЦИИ

152. Заявитель жаловался, что соответствующие законодательство и правоприменительная практика Швеции в отношении массового перехвата сообщений, также называемого радиотехнической разведкой, нарушали его право на уважение частной жизни и корреспонденции, предусмотренное статьей 8 Конвенции. Власти Швеции оспорили этот довод.

153. Статья 8 Конвенции гласит:

> «1. Каждый имеет право на уважение его личной и семейной жизни, его жилища и его корреспонденции.
>
> 2. Не допускается вмешательство со стороны публичных властей в осуществление этого права, за исключением случаев, когда такое вмешательство предусмотрено законом и необходимо в демократическом обществе в интересах национальной безопасности и общественного порядка, экономического благосостояния страны, в целях предотвращения беспорядков или преступлений, для охраны здоровья или нравственности или защиты прав и свобод других лиц».

A. Предварительное возражение властей Швеции относительно статуса жертвы

1. Постановление Палаты Европейского Суда

154. Применяя критерии, разработанные в Постановлении Большой Палаты Европейского Суда по делу «Роман Захаров против Российской Федерации» (Roman Zakharov v. Russia), жалоба № 47143/06[1], ECHR 2015, и в Постановлении

[1] См.: Бюллетень Европейского Суда по правам человека. 2016. № 6 (*примеч. редактора*).

Европейского Суда по делу «Кеннеди против Соединенного Королевства» (Kennedy v. United Kingdom) от 18 мая 2010 г., жалоба № 26839/05[1], Палата Европейского Суда сочла, что оспариваемое законодательство о радиотехнической разведке устанавливало систему скрытого наблюдения, которое потенциально затрагивало всех пользователей, и что внутригосударственные средства правовой защиты не содержали подробных оснований для ответа заявителю, который подозревает, что его или ее сообщения были перехвачены. При таких обстоятельствах Палата Европейского Суда признала рассмотрение соответствующего законодательства *in abstracto* оправданным и пришла к выводу, что заявитель может считать, что он является жертвой нарушения Конвенции, хотя он и не мог утверждать, что в отношении него применялись конкретные меры по перехвату сообщений. По тем же причинам Палата Европейского Суда пришла к выводу, что сам по себе факт наличия оспариваемого законодательства представляет собой вмешательство в права заявителя, предусмотренные статьей 8 Конвенции.

2. Доводы сторон в Большой Палате Европейского Суда

(a) Власти Швеции

155. Власти Швеции утверждали, что заявитель не принадлежал к «группе лиц или организаций, попадающих под действие законодательства» о радиотехнической разведке как направления внешней разведки.

156. Кроме того, по мнению властей Швеции, обжалуемое законодательство не затрагивало напрямую всех пользователей услуг мобильной телефонной связи и Интернета, поскольку оно было ограничено внешней разведкой и, следовательно, иностранными элементами.

157. Ссылаясь на описанные ими шесть этапов деятельности по радиотехнической разведке (см. выше § 29), власти Швеции утверждали, что сообщения заявителя по телефону и интернет-связи, вероятно, не будут затронуты по следующим причинам: большинство исключительно внутренних сообщений не достигнет пунктов передачи по трансграничным проводным путям. Однако даже если это произойдет, селекторы, используемые для идентификации соответствующих сигналов, разработаны с большой точностью в отношении целевых иностранных элементов и подлежат утверждению Судом по вопросам внешней разведки. В результате вышеизложенного сообщения заявителя вряд ли будут подвергнуты указанной выше автоматизированной обработке, поскольку любые данные, проходящие через каналы сообщений, которые не были отобраны, исчезают без какой-либо возможности для воспроизведения и проверки Радиотехническим центром. Даже если данные или сообщения заявителя достигли третьей стадии процесса массового перехвата данных, то дальнейшая детализация будет проводиться автоматически и вручную, и риск того, что сообщения заявителя будет сохранены для их дальнейшего изучения после этого этапа, практически отсутствует.

158. По мнению властей Швеции, вмешательство в права, предусмотренные статьей 8 Конвенции, отсутствует до этапа, на котором становится возможным аналитическое изучение отдельных сигналов.

159. Власти Швеции также придерживались мнения о том, что внутригосударственное законодательство предоставляет эффективные средства правовой защиты для лица, которое подозревает, что оно подверглось мерам по перехвату сигналов, включая возможность подать запрос в Инспекцию по надзору и, как следствие, получить уведомление о том, имел ли место ненадлежащий сбор данных. По мнению властей Швеции, требование Палаты Европейского Суда о том, чтобы в дополнение к вышеизложенному в ответ должны быть приведены «подробные основания», не опиралось на предыдущую прецедентную практику и неоправданно расширяло существующие требования.

160. На основании этого власти Швеции считали, что заявитель мог утверждать, что он является жертвой нарушения, вызванного самим фактом наличия оспариваемого законодательства, только в том случае, если он мог доказать, что в силу своей «личной» ситуации он потенциально подвергался риску применения в отношении него мер радиотехнической разведки. Это было далеко не так. Напротив, телефонные и интернет-сообщения заявителя вряд ли будут перехвачены и проанализированы, и в любом случае риск того, что они будут сохранены для дальнейшего изучения за пределами стадии автоматизированной обработки данных, практически отсутствовал.

161. Таким образом, власти Швеции просили Большую Палату Европейского Суда признать жалобу неприемлемой для рассмотрения по существу ввиду отсутствия статуса жертвы или установить отсутствие вмешательства в права заявителя, предусмотренные статьей 8 Конвенции.

162. Что касается других вопросов, связанных с приемлемостью жалобы для рассмотрения по существу, власти Швеции заявили об отсутствии у них возражений относительно исчерпания внутригосударственных средств правовой защиты.

(b) Заявитель

163. Заявитель считал, что в настоящем деле были соблюдены два необходимых условия для того, чтобы утверждать о наличии статуса жертвы

[1] См.: там же. 2017. № 11 (*примеч. редактора*).

в жалобах, касающихся самого факта существования правового режима скрытого наблюдения, как изложено в упомянутом выше Постановлении Большой Палаты Европейского Суда по делу «Роман Захаров против Российской Федерации» (Roman Zakharov v. Russia).

164. В частности, Закон о радиотехнической разведке разрешает перехват любых сообщений по кабельным путям, которые пересекают границу Швеции, или передаются по воздушным путям, и, следовательно, по словам заявителя, напрямую затрагивает всех пользователей таких услуг связи. Хотя было разрешено перехватывать только сообщения, относящиеся к иностранным элементам, практически все пользователи услуг связи могут участвовать в трансграничном общении, либо намеренно контактируя с иностранным получателем, либо ненамеренно посредством связи через сервер, расположенный за границей. Кроме того, Закон о радиотехнической разведке разрешает перехват в целях разработки, не связанных с иностранными элементами.

165. Заявитель также утверждал, что на внутригосударственном уровне отсутствуют эффективные средства правовой защиты как для заявителя, так и для иных лиц, которые подозревают, что они могли стать объектом массового перехвата данных властями Швеции. Таким образом, заявитель должен иметь возможность добиться рассмотрения его дела Европейским Судом и может утверждать, что сам факт существования оспариваемого режима является вмешательством в его права, предусмотренные статьей 8 Конвенции.

3. Мнение Большой Палаты Европейского Суда

166. Как отметил Европейский Суд в упомянутых выше Постановлении Европейского Суда по делу «Кеннеди против Соединенного Королевства» (Kennedy v. United Kingdom) и в Постановлении Большой Палаты Европейского Суда по делу «Роман Захаров против Российской Федерации» (Roman Zakharov v. Russia), в делах, касающихся скрытых мер, имеются особые причины, обосновывающие отступление Европейским Судом от своего общего подхода, который отрицает права лица оспаривать внутригосударственное законодательство *in abstracto*. Основной причиной для этого является обеспечение того, чтобы секретность мер наблюдения не приводила к фактической невозможности их обжаловать и к тому, что они окажутся за пределами надзора внутригосударственных судебных органов и Европейского Суда (см. упомянутое выше Постановление Большой Палаты Европейского Суда по делу «Роман Захаров против Российской Федерации» (Roman Zakharov v. Russia), § 169).

167. В настоящее время в прецедентной практике установлено, что при оценке того, может ли заявитель утверждать, что он стал жертвой нарушения его прав, предусмотренных Конвенцией, в результате самого существования мер скрытого наблюдения или законодательства, разрешающего такие меры, применяется несколько критериев. Эти критерии были сформулированы в упомянутом выше Постановлении Большой Палаты Европейского Суда по делу «Роман Захаров против Российской Федерации» (Roman Zakharov v. Russia), § 171):

> «…Во-первых, Европейский Суд будет учитывать область законодательства, разрешающего меры скрытого наблюдения, проверив, может ли заявитель испытать на себе их воздействие, поскольку он принадлежит к группе лиц, попадающих под действие оспариваемого законодательства, или потому что законодательство напрямую влияет на всех пользователей услуг связи за счет введения системы, где сообщения любого человека могут прослушиваться.
>
> Во-вторых, Европейский Суд примет во внимание наличие средств правовой защиты на внутригосударственном уровне и будет регулировать уровень тщательности рассмотрения в зависимости от эффективности такого средства правовой защиты… [Е]сли внутригосударственная система не предусматривает наличия эффективного средства правовой защиты для лица, которое подозревает, что подверглось скрытому наблюдению, широко распространенные подозрение и озабоченность общественности по поводу того, что власти незаконно используют скрытое наблюдение, не могут считаться необоснованными… При таких обстоятельствах угроза наблюдения может рассматриваться как ограничение свободы общения посредством почтовых и телекоммуникационных услуг, тем самым составляя для всех пользователей или потенциальных пользователей прямое вмешательство в право, гарантированное статьей 8 Конвенции. Поэтому необходимость для тщательного рассмотрения Европейским Судом возрастает, и исключение из правила, которое отрицает право лица оспорить закон *in abstracto*, является обоснованным. В таких случаях лицо не нуждается в том, чтобы продемонстрировать существование какого-либо риска того, что к нему были применены меры скрытого наблюдения.
>
> Напротив, если внутригосударственная система предусматривает эффективные средства правовой защиты, широко распространенное подозрение в превышении полномочий становится труднее оправдать. В данных ситуациях лицо может считаться жертвой нарушения, вызванного фактом существования скрытых мер или законодательства, допускающего скрытые меры, только если он способен доказать, что вследствие его личной ситуации он потенциально имеет риск подвергнуться подобным мерам».

168. Применяя указанные критерии к настоящему делу, Европейский Суд согласен с властями Швеции в том, что заявитель не принадлежит к группе лиц или организаций, на которые распространяется действие законодательства Швеции о радиотехнической разведке и соответствующих мер. Действительно, заявитель не утверждал обратное.

169. Следовательно, необходимо проанализировать, устанавливает ли оспариваемое законодательство, как утверждал заявитель, систему скрытого наблюдения, потенциально затрагивающую всех лиц, которые общаются по телефону или используют Интернет.

170. В этом отношении очевидно, что сообщения или данные о сообщениях любого физического или юридического лица в Швеции могут передаваться через перехваченные каналы сообщений и, таким образом, могут подвергаться, по крайней мере, начальным этапам автоматизированной обработки со стороны Радиотехнического центра в соответствии с обжалуемым законодательством.

171. Доводы властей Швеции о том, что радиотехническая разведка ограничена внешними угрозами и обстоятельствами и что вследствие этого практически отсутствует риск того, что сообщения заявителя будут сохранены для дальнейшего изучения за пределами этапа автоматизированной обработки данных при массовом перехвате, имеют отношение к оценке интенсивности и соразмерности вмешательства в права, предусмотренные статьей 8 Конвенции, включая гарантии, предлагаемые оспариваемым режимом перехвата сигналов, но не имеют решающего значения для установления статуса жертвы заявителя в соответствии со статьей 34 Конвенции. Какой-либо иной подход может привести к тому, что доступ к процедуре рассмотрения жалоб в соответствии с Конвенцией будет обусловлен доказыванием того, что сообщения лица представляют интерес для органов, которым поручено осуществление внешней разведки, что представляет собой практически невозможную задачу, учитывая секретность, присущую деятельности по внешней разведке.

172. При таких обстоятельствах Европейский Суд должен принимать во внимание средства правовой защиты, доступные в Швеции лицам, которые подозревают, что к ним применяются меры, предусмотренные Законом о радиотехнической разведке, чтобы оценить, можно ли утверждать, как это делает заявитель, что угроза наблюдения сама по себе ограничивает свободное общение, тем самым представляя собой прямое вмешательство в права всех пользователей или потенциальных пользователей, гарантированные статьей 8 Конвенции.

173. В этом отношении Европейский Суд отмечает, что на практике лица, которых затрагивает массовый перехват данных, не получают каких-либо уведомлений. Вместе с тем в ответ на запрос любого лица, независимо от его гражданства и места жительства, Инспекция по надзору должна расследовать, были ли сообщения такого лица перехвачены посредством радиотехнической разведки, и, если это так, проверять, соответствовали ли перехват и обработка информации закону. Инспекция по надзору вправе принять решение о прекращении операции по радиотехнической разведке или об уничтожении разведывательной информации. В ряде случаев любое лицо может также добиваться привлечения к участию в разбирательстве парламентских омбудсменов и канцлера юстиции.

174. Однако заявитель утверждал, что единственная информация, которая могла быть предоставлена Инспекцией по надзору, без каких-либо оснований для сделанных выводов и в форме окончательного решения, не подлежащего обжалованию, заключалась в том, что было совершено противоправное деяние. Иные средства правовой защиты не могли привести к тому, чтобы заявитель получил дополнительную информацию об обстоятельствах возможного перехвата данных и об использовании его или ее сообщений или связанных с ними данных, равно как и о характере противоправных действий, если они имели место.

175. В контексте вопроса о статусе жертвы, без ущерба для выводов, которые должны быть сделаны в отношении материально-правовых требований пункта 2 статьи 8 и статьи 13 Конвенции в настоящем деле, Европейский Суд отмечает, что внутригосударственные средства правовой защиты, доступные в Швеции лицам, которые подозревают, что они подвергаются массовому перехвату данных, имеют ряд ограничений. По мнению Европейского Суда, даже если эти ограничения следует признать неизбежными или оправданными, их практическое последствие заключается в том, что наличие средств правовой защиты не может в достаточной степени рассеять опасения общественности, связанные с угрозой скрытого наблюдения.

176. Следовательно, отсутствует необходимость проверять, подвергается ли заявитель в силу своей личной ситуации потенциальному риску перехвата и анализа его сообщений или связанных с ними данных.

177. На основании вышеизложенного Европейский Суд полагает, что рассмотрение соответствующего законодательства *in abstracto* является оправданным. Возражение властей Швеции о том, что заявитель не может утверждать, что он является жертвой нарушения его прав, предусмотренных Конвенцией, предположительно вследствие самого факта наличия законодательства Швеции о массовом перехвате данных и соответствующей деятельности, должно быть отклонено.

В. Существо жалобы

1. Постановление Палаты Европейского Суда

178. Палата Европейского Суда пришла к выводу, что действующая система наблюдения явно основывалась на законодательстве Швеции и ее наличие было оправдано интересами национальной безопасности. Действительно, учитывая современные угрозы глобального террориз-

ма и серьезных трансграничных преступлений, а также возросшее усложнение коммуникационных технологий, Европейский Суд постановил, что власти Швеции обладают широкими пределами свободы усмотрения (далее – широкие пределы усмотрения) для принятия решения о создании такой системы массового перехвата данных. Однако дискреционные полномочия властей в отношении фактического использования такой системы перехвата были более узкими, и Европейский Суд должен был удостовериться в наличии надлежащих и эффективных гарантий против злоупотреблений. Европейский Суд оценил минимальные гарантии против злоупотребления властью, сформулированные в его прецедентной практике, в частности, в упомянутом выше Постановлении Большой Палаты Европейского Суда по делу «Роман Захаров против Российской Федерации» (Roman Zakharov v. Russia) (см. §§ 99–115 Постановления Палаты Европейского Суда).

179. В целом, хотя Палата Европейского Суда выявила некоторые области, в которых есть потенциал для совершенствования системы, в частности, относительно регулирования передачи персональных данных другим государствам и международным организациям и отсутствия публичных доводов после рассмотрения индивидуальных жалоб (см. §§ 150, 173 и 177 Постановления Палаты Европейского Суда), она решила, что отсутствуют существенные недостатки в структуре и функционировании системы. В этом контексте она отметила, что нормативно-правовая база Швеции пересматривалась несколько раз в целях усиления защиты частной жизни и что фактически она была разработана таким образом, чтобы минимизировать риск вмешательства в частную жизнь и компенсировать закрытость системы (см. §§ 180 и 181 Постановления Палаты Европейского Суда).

180. Так, пределы перехвата и обработка перехваченных данных были ясно определены законом; продолжительность мер была четко регламентирована (любое разрешение действовало не более шести месяцев, а для продления требовалось новое рассмотрение); процедура выдачи разрешения была детализирована и поручена судебному органу – Суду по вопросам внешней разведки; нескольким независимым органам, в частности, Инспекции по надзору и Инспекции по защите данных, было поручено осуществлять надзор и пересмотр системы. Кроме того, по запросу Инспекция по надзору должна была расследовать индивидуальные жалобы на перехваченные сообщения, как это делали парламентские омбудсмены и канцлер юстиции (см. §§ 116–147 и 153–178 Постановления Палаты Европейского Суда).

181. С учетом изложенного Палата Европейского Суда пришла к выводу, что система радиотехнической разведки Швеции содержит надлежащие и достаточные гарантии против произвола и риска злоупотреблений. Соответствующее законодательство отвечало требованию «качества закона», и вмешательство можно было считать «необходимым в демократическом обществе». Структура и функционирование системы были соразмерны преследуемой цели. Вместе с тем Палата Европейского Суда отметила, что ее анализ проводился *in abstracto* и не препятствовал пересмотру ответственности властей в соответствии с Конвенцией в случае, если, например, заявителю станет известно о фактическом перехвате (см. §§ 179–181 Постановления Палаты Европейского Суда).

2. Доводы сторон

(a) Заявитель

(i) Мнение заявителя относительно подлежащего применению стандарта

182. По мнению заявителя, режимы массового перехвата данных по своей природе несовместимы с Конвенцией. В Постановлении по делу «Класс и другие против Германии» (Klass and Others v. Germany) (от 6 сентября 1978 г., § 51, Series A, № 28; и в Постановлении по делу «Ассоциация “21 декабря 1989 года” и другие против Румынии» (Association 21 December 1989 and Others v. Romania) от 24 мая 2011 г., жалобы №№ 33810/07 и 18817/08[1], §§ 174–175, Европейский Суд признал, что «разведочное» или «общее наблюдение» вызывает вопросы. Что касается нецелевого перехвата данных, только гораздо более узкие по своим пределам режимы, чем действующий в Швеции, были признаны совместимыми с Конвенцией. Учитывая, что Радиотехнический центр может получить доступ практически ко всем проводным коммуникациям, пересекающим границу Швеции, объем частных, персональных и конфиденциальных данных, которые могут быть изучены в рамках режима радиотехнической разведки Швеции, был намного больше. В связи с этим заявитель считал, что только режимы адресного перехвата и нецелевого перехвата данных меньшего масштаба могут относиться к пределам усмотрения государства. Иной подход может привести к непоследовательной прецедентной практике с учетом подхода Европейского Суда к другим вопросам в соответствии с Конвенцией, таким как всеобъемлющее хранение отпечатков пальцев и профилей ДНК, рассмотренным в Постановлении Большой Палаты Европейского Суда по делу «S. и Марпер против Соединенного Королевства» (S. and

[1] См.: Избранные постановления Европейского Суда. 2012. № 1 (*примеч. редактора*).

Marper v. United Kingdom), жалобы №№ 30562/04 и 30566/04, § 115, ECHR 2008).

183. Если Европейский Суд решит, что массовый перехват может быть оправдан в соответствии с Конвенцией, заявитель считал, что необходимо разработать строгие минимальные гарантии. Факторы, изложенные в упомянутом выше Постановлении Большой Палаты Европейского Суда по делу «Роман Захаров против Российской Федерации» (Roman Zakharov v. Russia) (§ 238), могут служить первоначальной основой, однако нецелевое наблюдение влечет за собой повышенные риски для частной жизни и требует адаптации указанных стандартов.

184. В частности, основные составляющие режима должны быть достаточно подробно изложены в законах. Это может гарантировать, что именно представители народа обеспечивают баланс противоречащих друг другу интересов.

185. Что касается предварительного разрешения, то, хотя Европейский Суд признал, что орган, которому эта задача поручена в Швеции, является судебным, заявитель предложил Европейскому Суду сделать еще один шаг в развитии его прецедентной практики и постановить, что предварительное разрешение всегда должно быть вынесено судебным органом.

186. Кроме того, по мнению заявителя, орган, выдающий разрешение, должен иметь возможность проверять наличие разумных подозрений в отношении любого обособленного или выбранного в качестве объекта изучения лица. Заявитель счел неубедительным отступление Палаты Европейского Суда в настоящем деле и в упомянутом выше Постановлении по делу «Организация Big Brother Watch и другие против Соединенного Королевства» (Big Brother Watch and Others v. United Kingdom)) от этого предположительно установленного требования. Что касается использования персонализированных селекторов для обособления и сбора данных о лице, хотя и в контексте массового перехвата данных, должен применяться тот же порог, что и в отношении адресного перехвата данных. В противном случае такие селекторы можно будет использовать как обходной метод для сбора информации об отдельных лицах.

187. Вместе с тем в отсутствие заранее определенных целей орган, выдающий разрешение, должен иметь возможность проверить, что персональные данные используются в селекторах только в той степени, в которой это является важным для узко определенной цели внешней разведки. Последнее условие необходимо в связи с тем, что использование селекторов, относящихся к конкретным лицам, подвергает их определенным рискам для их частной жизни, в том числе в отношении глубоко личных вопросов и мнений.

188. Кроме того, по мнению заявителя, судебному органу, выдающему разрешение, следует пояснять, каким образом данные будут анализироваться и использоваться (например, с помощью анализа на основе шаблонов или тематики, и будут ли составляться профили лиц).

189. Что касается надзора на этапах проведения мероприятий по наблюдению и после их прекращения, заявитель признал, что надзорные органы Швеции отвечают требованию достаточной независимости от исполнительной власти.

190. В то же время надзорный орган должен быть наделен достаточными полномочиями для принятия юридически обязательных решений, включая пресечение и устранение нарушений и привлечение к ответственности лиц, виновных в таких нарушениях. Он должен иметь доступ к секретным документам, а его функционирование должно быть открытым для контроля со стороны общественности. Надзорные полномочия должны касаться как содержания сообщений, так и данных о них и должны осуществляться на этапах, когда собранные сообщения подвергаются автоматизированному компьютерному анализу, когда над ними работает специалист-аналитик и когда информация передается внутригосударственным органам, властям иностранных государств или международным организациям. Также необходимо контролировать хранение данных на каждом этапе.

191. В дополнение, по мнению заявителя, физические лица должны располагать эффективными средствами правовой защиты, которые могут существовать в трех формах: уведомление объекта наблюдения после его проведения, возможность запросить информацию о наблюдении или наличие органа, который будет иметь право рассматривать жалобы, не требуя от физического лица представления доказательств.

192. Что касается передачи перехваченных материалов иностранным органам, заявитель подчеркнул, что государства – участники Конвенции не обладают возможностью неограниченного усмотрения, поскольку они не могут привлекать третьих лиц для обработки и анализа данных таким образом, чтобы избежать ответственности в соответствии с Конвенцией. По мнению заявителя, минимальные стандарты должны включать в себя доступные законодательные положения, четкие правовые условия для обмена данными, в том числе обязательство предпринимать разумные меры для обеспечения защиты данных принимающей стороной посредством предоставления гарантий, аналогичных тем, что существуют на внутригосударственном уровне, а также надлежащие надзорные и корректирующие механизмы.

(ii) Анализ заявителем оспариваемого режима Швеции

193. Применяя вышеуказанные стандарты к оспариваемому режиму, действующему в Шве-

ции, заявитель утверждал, что общие пределы применения Радиотехническим центром своих полномочий достаточно ограничены, за исключением широкого усмотрения, которым он наделен в отношении своей деятельности по разработке. Вместе с тем заявитель выразил обеспокоенность в связи с тем, что с 1 января 2013 г. Государственная служба безопасности и Национальное оперативное отделение Главного полицейского управления были уполномочены издавать распоряжения с указанием задач для радиотехнической разведки и что с 1 марта 2018 г. Государственной службе безопасности может быть предоставлен прямой доступ к базам данных Радиотехнического центра с материалами анализа. Риск использования методов радиотехнической разведки за пределами деятельности по внешней разведке должен в достаточной мере сдерживаться четкими правовыми положениями и эффективным надзором.

194. Заявитель также отмечал, что, хотя разрешение, выдаваемое согласно Закону Швеции о радиотехнической разведке, имеет четко определенный срок действия, отсутствует требование его аннулировать, если необходимость сбора сообщений в соответствии с разрешением отпадает.

195. Заявитель также считал, что пределы судебной проверки со стороны органа, выдающего разрешения в Швеции, а именно Суда по вопросам внешней разведки, были слишком узкими, чтобы проверка была эффективной. В частности, наличие разумного подозрения в отношении конкретного лица не проверялось, а критерий «исключительной важности», оправдывающий селекторы, которые относятся непосредственно к физическому лицу, распространяется только на селекторы, используемые при автоматизированном сборе данных, а не на этапе дальнейшего изучения собранных данных. Кроме того, Суд по вопросам внешней разведки не обязан проверять предполагаемое последующее использование собранных данных. В запросе на выдачу разрешения действительно не указывается, каким образом будет проводиться анализ данных, например, путем предметного анализа данных или составления профилей лиц.

196. Что касается хранения, доступа, изучения, использования и уничтожения перехваченных данных, заявитель указал на два основных недостатка в системе Швеции: отсутствие у Радиотехнического центра правового обязательства вести подробный учет перехвата, использования и передачи данных, за что она неоднократно подвергалась критике со стороны Инспекции по защите данных Швеции, а также отсутствие правил, специально адаптированных к массовому перехвату данных, в отличие от общих правил обработки данных. Заявитель также выразил обеспокоенность тем, что с 1 марта 2018 г. Государственной службе безопасности может быть предоставлен прямой доступ к базам данных Радиотехнического центра с материалами анализа.

197. Заявитель также утверждал, что юридические лица не пользуются надлежащей защитой, поскольку Закон об обработке данных Радиотехническим центром применяется только к перехвату материалов, содержащих персональные данные. Это предположительно приводит к ситуации, когда материалы, не содержащие персональных данных, могут храниться вечно и использоваться в целях, несовместимых с первоначальной целью сбора.

198. Заявитель критиковал следующие особенности существующей системы надзора. Во-первых, хотя Инспекция по защите данных может принять решение о прекращении операции или об уничтожении полученных разведывательных данных, если она установит несовместимость с разрешением, выданным Судом по вопросам внешней разведки, у нее нет полномочий выносить обязательные решения, если разрешение признается незаконным. Инспекция не может предоставить компенсацию или требовать привлечения к ответственности виновных в нарушениях. Во-вторых, ни Инспекция по защите данных, ни канцлер юстиции, ни омбудсмены не могут принимать юридически обязательные решения. Инспекция по защите данных может обратиться в Административный суд г. Стокгольма только с ходатайством об уничтожении незаконно обработанных данных. Кроме того, ни одна из жалоб, которые были поданы канцлеру юстиции и омбудсменам в связи с деятельностью Радиотехнического центра, не были удовлетворены. Указанные органы не специализируются на деятельности Радиотехнического центра и не обладают знаниями и возможностями для эффективного надзора за ней.

199. Заявитель представил следующие доводы относительно средств правовой защиты, доступных в рамках оспариваемого режима, действующего в Швеции.

Во-первых, по его мнению, уведомление, предусмотренное статьей 11(a) Закона о радиотехнической разведке, касается только физических лиц, а не организаций, и соответствующее положение может не применяться по причинам секретности, что постоянно и происходит на практике. Следовательно, это средство правовой защиты является «теоретическим и иллюзорным». Возможность обратиться в Радиотехнический центр с запросом об информировании лица о том, подвергались ли обработке его персональные данные, также попадает под действие правила секретности. При этом Административный суд, который рассматривает последующие жалобы, не имеет доступа к секретным документам и не может пересмотреть оценку Радиотехнического центра относительно применения положения о секретности. Указанное средство правовой защиты также недо-

ступно для юридических лиц, каковым является заявитель.

Во-вторых, заявитель сослался на полномочия Следственного трибунала в Соединенном Королевстве рассматривать жалобы о незаконном перехвате данных без необходимости того, чтобы податель жалобы доказывал факт проведения в отношении него наблюдения. Следственный трибунал – независимый судебный орган – имеет доступ к секретным документам, может принимать обязательные решения и присуждать компенсацию. Его решения публикуются. Заявитель утверждал, что в Швеции отсутствует аналогичное средство правовой защиты.

В-третьих, что касается возможности в соответствии с законодательством Швеции обратиться в Инспекцию по надзору с ходатайством о проведении расследования в отношении того, были ли перехвачены сообщения физического лица, заявитель отметил, что она не сообщала заинтересованному лицу свои выводы, а только отправляла стандартные ответы о том, что неправомерное наблюдение не имело места. Заявитель повторил свое утверждение о том, что Инспекция по надзору не имела полномочий контролировать соблюдение закона и Конституции и не могла выносить распоряжения о выплате компенсации.

В-четвертых, по мнению заявителя, обращение за компенсацией к канцлеру юстиции не является эффективным средством правовой защиты по следующим причинам: (i) лицо несет бремя доказывания того, что имело место незаконное наблюдение; (ii) компенсация без удаления незаконно обработанных данных не может считаться эффективным средством правовой защиты; (iii) до настоящего момента канцлер юстиции, который по своему усмотрению определяет жалобы к рассмотрению, отклонял все жалобы, касающиеся деятельности Радиотехнического центра; (iv) власти Швеции не доказали эффективность этого средства правовой защиты, поскольку неясно, какие действия должен совершить канцлер юстиции после получения отчета Инспекции по надзору с информацией о действиях Радиотехнического центра, которые могут привести к подаче иска о возмещении ущерба. В частности, если бы канцлер юстиции предоставил физическому лицу возможность требовать возмещения ущерба, это вызвало бы необходимость информировать данное лицо о незаконных действиях Радиотехнического центра, что может быть исключено требованием секретности.

В-пятых, в отсутствие уведомления или доступа к документам у физического лица практически отсутствует возможность представить доказательства в гражданском процессе по иску о возмещении ущерба.

В-шестых, омбудсмены не могут выносить распоряжение о возмещении ущерба, и не было приведено каких-либо примеров эффективности указанного средства правовой защиты.

В-седьмых, процедура, в ходе которой Радиотехнический центр мог исправить или уничтожить незаконно обработанные персональные данные, была обусловлена осведомленностью лица об обработке его данных и была неэффективной ввиду требования секретности. Кроме того, в Административный суд никогда не поступали ходатайства от Инспекции по защите данных об удалении незаконно обработанных данных.

Наконец, возможность добиваться судебного преследования также зависела от осведомленности лица о соответствующем правонарушении и, следовательно, была неэффективной.

200. Что касается передачи перехваченных данных иностранным третьим лицам, заявитель считал, что недостатки правового режима Швеции и практики его применения очевидны. Правовые ограничения такой передачи представляют собой не что иное, как неопределенные и широкие обязательства действовать в национальных интересах. Отсутствует требование о необходимости учитывать возможный вред для лица или о том, что получатель должен защищать данные посредством гарантий, аналогичных тем, что применялись в Швеции.

201. Заявитель не согласился с выводом Палаты Европейского Суда о том, что вышеуказанные недостатки уравновешивались надзорными механизмами, существующими в Швеции. Он полагал, что подобный надзор был недостаточным и в любом случае не охватывал передачу перехваченных данных иностранным получателям. Радиотехнический центр должен был просто проинформировать Инспекцию по надзору о принципах, регулирующих его сотрудничество с иностранными получателями, указать страны или международные организации, которым были переданы данные, и предоставить общие сведения об операции. Поскольку Инспекция по надзору осуществляет мониторинг деятельности Радиотехнического центра на предмет соблюдения действующих правовых требований, а закон наделяет ее чрезмерной свободой усмотрения в этой области, то даже самый строгий контроль со стороны Инспекции мало что мог сделать для защиты от злоупотреблений. По мнению заявителя, описанные выше механизмы не могут составлять практику, совместимую с Конвенцией, поскольку они позволяют привлечь третьих лиц для осуществления видов деятельности, которые в ином случае были бы незаконными, без соответствующих ограничений, защищающих основные права.

(b) Власти Швеции

202. Власти Швеции утверждали, что цель радиотехнической разведки заключается в получе-

нии информации и обнаружении явлений, имеющих значение для внешней разведки. Внешняя разведка крайне важна для обеспечения национальной безопасности Швеции, а также имеет отношение к позитивным обязательствам Швеции в соответствии с Конвенцией по защите жизни и безопасности населения.

203. По мнению властей Швеции, в связи с тем, что прецедентная практика Европейского Суда, устанавливающая минимальные гарантии для мер скрытого наблюдения, касается уголовных расследований, за исключением настоящего дела и упомянутого выше Постановления по делу «Организация Big Brother Watch и другие против Соединенного Королевства» (Big Brother Watch and Others v. United Kingdom), то некоторые минимальные гарантии, требуемые Европейским Судом, предполагают связь с конкретным человеком или конкретным местом. Это сильно отличается от системы радиотехнической разведки, которая не может использоваться для расследования уголовных преступлений, и одна из обязанностей Суда по вопросам внешней разведки заключается в обеспечении того, чтобы она не использовалась подобным образом. Радиотехническая разведка как направление внешней разведки во многих случаях может определять объектом своего изучения конкретные сообщения отдельных лиц, но такие лица чаще всего не представляют интереса *per se*: они являются лишь носителями информации.

204. Следовательно, необходимо адаптировать соответствующие требования, в том числе изменить формулировку некоторых критериев, изложенных в прецедентной практике Европейского Суда, следующим образом: ввести критерий «обстоятельств, при которых меры могут применяться», вместо «характера преступления» и «категорий лиц, являющихся объектом изучения». Также необходимо учитывать тот факт, что угрозы национальной безопасности по своей природе изменчивы и их трудно определить заранее.

205. Власти Швеции категорически не согласились с заявителем, который утверждал, ссылаясь на упомянутое выше Постановление Большой Палаты Европейского Суда по делу «Роман Захаров против Российской Федерации» (Roman Zakharov v. Russia) и на Постановление Европейского Суда по делу «Сабо и Виши против Венгрии» (Szabó and Vissy v. Hungary) от 12 января 2016 г., жалоба № 37138/14[1], что наличие разумного подозрения требовалось как минимум при использовании селекторов, связанных с конкретным лицом. По мнению властей Швеции, из приведенной выше прецедентной практики нельзя сделать вывод о наличии такого требования. Власти Швеции поддержали доводы Палаты Европейского Суда, изложенные в § 317 упомянутого выше Постановления Европейского Суда по делу «Организация Big Brother Watch и другие против Соединенного Королевства» (Big Brother Watch and Others v. United Kingdom), в котором он постановил, что требования «обоснованного подозрения» и «последующего уведомления» несовместимы с режимами массового перехвата данных.

206. Власти Швеции также утверждали, что массовый перехват данных в стране регулировался комплексным правовым режимом, основанным на опубликованных правовых положениях, и предусматривал существенные гарантии, в том числе независимый надзор, охватывающие деятельность по наблюдению как в связи с данными о сообщениях, так и относительно содержания сообщений. Закон четко определял пределы деятельности по наблюдению, полномочия, предоставленные компетентным органам в этом отношении, и порядок осуществления этой деятельности.

207. Что касается деятельности Радиотехнического центра по разработке, власти Швеции подчеркнули, что она строго регулируется и подчиняется всем материально-правовым и процессуальным требованиям, применимым к радиотехнической разведке в целом. В рамках деятельности по разработке, которая имеет решающее значение для того, чтобы Радиотехнический центр мог адаптировать свои инструменты, системы и методы к постоянно изменяющейся радиотехнической обстановке и техническому прогрессу, интерес представляют поток трафика и системы, через которые передается информация. Для поддержания возможностей Радиотехнического центра ограничение деятельности по разработке только восьмью целями, которые ограничивают радиотехническую разведку, представлялось бы чрезмерным.

208. Кроме того, существует процедура получения предварительного разрешения в Суде по вопросам внешней разведки, председателем которого является постоянный судья, а другие члены назначаются властями Швеции на четырехлетний срок. В исключительных случаях срочности, когда Радиотехнический центр может самостоятельно выдать разрешение на проведение радиотехнической разведки, необходимо незамедлительно уведомить указанный суд, который может изменить или отозвать разрешение, после чего собранные данные должны быть уничтожены. Если разрешение, выданное Радиотехническим центром, а не судом, предусматривает доступ к определенным носителям сообщений, такой доступ может быть осуществлен только Инспекцией по надзору Швеции, которая имеет возможность оценить соответствующие правовые аспекты.

209. Суд по вопросам внешней разведки проводит публичные слушания, за исключением случаев, когда соображения секретности требуют иного. Власти Швеции утверждали, что указанное огра-

[1] См.: Прецеденты Европейского Суда по правам человека. 2016. № 7 (*примеч. редактора*).

ничение прозрачности было оправдано и компенсировалось гарантиями, такими как присутствие представителя по вопросам защиты частной жизни на закрытых судебных заседаниях. Представитель защищает общественные интересы, имеет полный доступ к материалам дела и может делать заявления. Представитель является судьей на постоянной основе, бывшим судьей на постоянной основе или членом Коллегии адвокатов Швеции.

210. Власти Швеции подчеркнули, что Радиотехнический центр должен запрашивать разрешение в отношении каждой миссии и обязан указывать задачу, носители, к которым требуется доступ, и селекторы или как минимум категории селекторов, которые будут использоваться. Суд проверяет не только формальную законность, но и соразмерность ожидаемого вмешательства. В разрешении должны быть перечислены все параметры, включая условия, необходимые для ограничения такого вмешательства.

211. Что касается гарантий продолжительности перехвата, законодательство Швеции ограничило ее шестью месяцами с возможностью продления после полной проверки со стороны Суда по вопросам внешней разведки. Кроме того, перехват прекращается, если распоряжение с указанием задач отменяется или срок его действия истекает, а также если перехват не соответствует разрешению либо он более не требуется.

212. Существуют надлежащие гарантии в отношении процедур хранения, доступа, изучения, использования и уничтожения перехваченных данных. Эти гарантии включают в себя ограничение обработки данных тем, что является достаточным и соответствующим ее цели, а также подбор сотрудников, их обязанность соблюдать конфиденциальность и санкции в случае ненадлежащего управления данными. При некоторых условиях разведывательные данные должны быть немедленно уничтожены, в том числе, *inter alia*, когда они касаются защищенных на конституционном уровне средств массовой информации или адвокатской тайны в отношениях между подозреваемым в совершении уголовного преступления и его адвокатом. Если перехваченные сообщения окажутся полностью внутренними, они должны быть уничтожены.

213. Что касается условий передачи перехваченных данных другим сторонам, Радиотехнический центр имеет регулируемое обязательство передавать информацию соответствующим властям Швеции, но гарантирует, что персональные данные передаются только в том случае, если они относятся к целям, для которых может проводиться внешняя разведка. Инспекция по надзору контролирует соблюдение этого требования.

214. Власти Швеции подчеркнули, что, несмотря на положение, разрешающее Радиотехническому центру предоставлять прямой доступ к его полным разведывательным донесениям государственным учреждениям, Вооруженным силам, Государственной службе безопасности и трем другим органам, Радиотехнический центр до сих пор не принимал каких-либо решений, разрешающих такой доступ. Власти Швеции дополнительно пояснили, что с 1 марта 2018 г. в соответствии со статьей 15 Закона о защите персональных данных Радиотехническим центром Государственной службе безопасности и Вооруженным силам может быть предоставлен прямой доступ к данным, которые представляют собой результаты анализа в базе данных, чтобы эти органы могли проводить стратегическую оценку террористических угроз. Это ничего не меняет в отношении запрета использовать методы радиотехнической разведки как направления внешней разведки для расследования уголовных преступлений.

215. Наконец, что касается передачи персональных данных другим государствам и международным организациям, власти Швеции не согласились с Палатой Европейского Суда, которая выявила недостатки в соответствующем правовом режиме (см. § 150 Постановления Палаты Европейского Суда). Они утверждали, *inter alia*, что Радиотехнический центр должен отчитываться перед Министерством обороны, прежде чем устанавливать и поддерживать сотрудничество с другими государствами и международными организациями, а также информировать Министерство о важных проблемах, возникающих в процессе этого сотрудничества. Кроме того, Радиотехнический центр обязан информировать Инспекцию по надзору Швеции о принципах, применимых к такому сотрудничеству, и сообщать подробную информацию о странах и организациях, с которыми он сотрудничает. При установлении сотрудничества Радиотехнический центр должен уведомлять Инспекцию о масштабах сотрудничества и, если это оправдано, о результатах, опыте и постоянном направлении сотрудничества.

216. Власти Швеции также отметили тот факт, что в рамках международного сотрудничества данные передаются исключительно тем сторонам, которые сами занимаются внешней разведкой, а это означает, что в интересах получателя защитить полученные данные. Доверие между сторонами основано на взаимной заинтересованности в обеспечении безопасности данных. Кроме того, общие руководящие принципы Радиотехнического центра предусматривают, что международное сотрудничество обусловлено соблюдением принимающим государством законодательства Швеции. Иностранные партнеры получают информацию по вопросам содержания соответствующего законодательства Швеции и проходят необходимую подготовку. Поскольку у Инспекции по надзору есть четкие полномочия по контролю за международным сотрудничеством Радиотехнического центра, любое изменение его внутренних руководящих

принципов не останется незамеченным. Таким образом, существуют четкие гарантии против обхода законодательства Швеции.

217. По мнению властей Швеции, созданная в стране система наблюдения за радиотехнической разведкой содержит важные гарантии. Инспекция по надзору независима, имеет доступ ко всем соответствующим документам, проверяет используемые селекторы и вправе принимать решение о прекращении сбора данных или об уничтожении собранных данных, если не были соблюдены условия соответствующего разрешения. Инспекция также гарантирует, что Радиотехнический центр получает доступ к носителям сообщений только в том объеме, в котором это предусмотрено разрешением. Инспекция по надзору представляет ежегодные публичные отчеты и подлежит проверке со стороны Государственного ревизионного управления и контролю со стороны парламентских омбудсменов и канцлера юстиции. Что касается персональных данных, Инспекция по защите данных Швеции выполняет общие надзорные функции. Власти Швеции считали, подобный надзор со стороны независимых несудебных органов является надлежащим и соответствует прецедентной практике Европейского Суда.

218. Власти Швеции утверждали, что в период с 2009 по 2018 год Инспекция по надзору провела 113 проверок в отношении Радиотехнического центра, по результатам которых были вынесены 18 заключений. Как минимум 17 проверок проводились, *inter alia*, в целях контроля использования Радиотехническим центром селекторов в соответствии с разрешением, выданным Судом по вопросам внешней разведки, а как минимум девять проверок включали в себя вопросы уничтожения данных. Ряд проверок также касался обработки Радиотехническим центром персональных данных. В результате проверок было вынесено лишь несколько замечаний или заключений. В течение того же срока Инспекция по надзору провела 141 проверку по запросам физических лиц на предмет того, проводились ли в отношении их сообщений незаконные мероприятия радиотехнической разведки. По результатам этих проверок не было выявлено ненадлежащих мероприятий в сфере радиотехнической разведки. Также было проведено несколько целевых проверок деятельности Радиотехнического центра, например, проверка соблюдения ограничений, установленных разрешениями.

219. Власти Швеции также отмечали, что существует несколько средств правовой защиты, с помощью которых физические лица могут инициировать проверку законности мер, принятых в период функционирования системы радиотехнической разведки. К ним относятся запрос в Инспекцию по надзору, в результате которого может быть направлено уведомление о каких-либо неправомерных действиях; запрос в Радиотехнический центр относительно того, подвергались ли обработке персональные данные, касающиеся заинтересованного лица; заявления в адрес парламентских омбудсменов, канцлера юстиции и Инспекции по защите данных; предъявление иска о возмещении ущерба; заявление о проблеме в целях возбуждения уголовного дела. Некоторые из указанных средств правовой защиты не зависят от предварительного уведомления физического лица. Хотя отсутствует возможность систематического уведомления, важное значение имеет тот факт, что Радиотехнический центр обязан информировать физическое лицо при использовании селекторов, напрямую касающихся его, за исключением случаев, когда применяются положения о секретности.

220. Власти Швеции также утверждали, что внутригосударственное законодательство о массовом перехвате данных не проводит различий между данными о содержании и данными о сообщениях, и все гарантии в равной мере применяются к тем и другим категориям. На практике использование данных о сообщениях для обнаружения неизвестных угроз требует объединения различных фрагментов таких данных для создания общего представления, на основе которого можно сделать выводы. Это требует, чтобы селекторы, используемые для перехвата данных о сообщениях, были менее конкретны, чем те, что используются для перехвата содержания сообщений, и чтобы данные были доступны аналитику для анализа в течение определенного срока. Другие отличия отсутствуют.

221. В заключение власти Швеции отметили, что в оспариваемом режиме радиотехнической разведки как направлении внешней разведки не выявлено существенных недостатков в части его структуры и функционирования. Риск вмешательства в частную жизнь сведен к минимуму, и предусмотрены достаточные гарантии против произвола. Режим в целом является правомерным и соразмерным законной цели защиты национальной безопасности.

3. Третьи стороны, вступившие в производство по делу

(a) Власти Эстонской Республики

222. Власти Эстонии считали, что критерии оценки совместимости режимов скрытого наблюдения с Конвенцией, разработанные в прецедентной практике Европейского Суда, нуждаются в адаптации, чтобы отразить особый характер массового перехвата сообщений как мероприятия внешней разведки. Следует учитывать различия между этим видом деятельности и наблюдением в контексте уголовного расследования. Внешняя разведка направлена на выявление угроз для наци-

ональной безопасности и, следовательно, шире по своему охвату. Кроме того, это долгосрочная деятельность, требующая более высокого уровня секретности в течение достаточно длительного периода времени.

223. На этом основании власти Эстонии, ссылаясь на критерии оценки, примененные в упомянутом выше Постановлении Большой Палаты Европейского Суда по делу «Роман Захаров против Российской Федерации» (Roman Zakharov v. Russia) (§ 231), согласились с Палатой Европейского Суда в том, что критерии «характера преступления» и «обоснованного подозрения» не были надлежащими, и утверждали, что вместо критерия «категории лиц» внутригосударственное законодательство должно содержать указание на «области, в которых массовый перехват трансграничных сообщений может быть использован для сбора разведывательных данных». Что касается уведомления затронутых лиц, то, по мнению властей Эстонии, не следует накладывать такое обязательство ввиду важности обеспечения секретности для внешней разведки.

(b) Власти Французской Республики

224. Власти Франции, подчеркивая важность мероприятий по массовому перехвату данных для выявления неизвестных угроз, считали, что критерии оценки совместимости таких мероприятий с Конвенцией, разработанные в Решении Европейского Суда по делу «Вебер и Саравия против Германии» (Weber and Saravia v. Germany), жалоба № 54934/00, ECHR 2006-XI, и в упомянутом выше Постановлении Большой Палаты Европейского Суда по делу «Роман Захаров против Российской Федерации» (Roman Zakharov v. Russia), имели отношение к настоящему делу. Однако, по их мнению, не следует вводить требование о наличии «разумных подозрений» с учетом особого характера операций по массовому перехвату данных, которые отличаются от скрытого наблюдения за конкретным лицом.

225. Власти Франции также считали, что государства пользуются широкими пределами усмотрения при использовании режимов массового перехвата данных и что оценка достаточности применимых гарантий против злоупотреблений всегда должна проводиться *in concreto* с учетом соответствующего законодательства, рассматриваемого в целом. Палата Европейского Суда в настоящем деле сделала именно это, отметив, что, несмотря на целесообразность некоторых усовершенствований, действующая в Швеции система в целом не содержала существенных недостатков. Однако в упомянутом выше Постановлении по делу «Организация Big Brother Watch и другие против Соединенного Королевства» (Big Brother Watch and Others v. United Kingdom) Палата Европейского Суда провела более строгую проверку и необоснованно установила нарушения статей 8 и 10 Конвенции. Власти Франции выступили против такого подхода. В частности, они считали, что режим массового перехвата данных, который не предусматривает наличия предварительного разрешения судебного органа, совместим со статьей 8 Конвенции, если существует механизм надзора со стороны независимого органа *a posteriori*.

226. Власти Франции также выразили мнение, обосновав его ссылками на прецедентную практику, о том, что перехват и обработка данных о сообщениях представляют собой значительно меньшее вмешательство в право на частную жизнь, чем перехват и обработка данных о содержании сообщений, и, следовательно, к ним не должны применяться те же гарантии защиты права на частную жизнь.

227. Что касается обмена разведывательными данными, власти Франции подчеркнули важность обеспечения секретности и тот факт, что применяемые процедуры и гарантии могут отличаться в разных государствах. Они также подробно остановились на нескольких критериях, в частности, в контексте получения перехваченных данных от иностранных партнеров и использования таких данных.

(c) Власти Королевства Нидерландов

228. Власти Нидерландов утверждали, что массовый перехват данных необходим в целях выявления ранее неизвестных угроз для национальной безопасности. Для защиты национальной безопасности разведывательным службам требуются инструменты для проведения своевременного и эффективного расследования возникающих угроз. Им также нужны полномочия, необходимые для выявления и/или предотвращения не только террористической деятельности (например, планирования атак, вербовки, пропаганды и финансирования), но и интрузивной кибердеятельности государственных или негосударственных субъектов, направленной на подрыв демократии (например, путем оказания влияния на национальные выборы или воспрепятствования расследованиям, проводимым внутригосударственными и международными организациями). Примером подобной деятельности была попытка компьютерной атаки в связи с расследованием применения химического оружия в Сирии Организацией по запрещению химического оружия в г. Гааге. Кроме того, растущая зависимость жизненно важных секторов от цифровой инфраструктуры означает, что такие сектора, в том числе управления водными ресурсами, энергетики, телекоммуникаций, транспорта, логистики, а также порты и аэропорты, становятся всё более уязвимыми для кибератак. Последствия перебоев в функционировании этих секторов оказывают глубокое воздействие на общество, выходя-

щее далеко за пределы значительного материального ущерба.

229. Усложняющим фактором являются разработка новых средств цифровой связи и стремительный рост данных, которые передаются и хранятся по всему миру. Во многих случаях характер и происхождение конкретной угрозы неизвестны, и отсутствует возможность использовать адресный перехват данных. Однако хотя массовый перехват данных не был так четко определен, как адресный перехват, он никогда не был полностью случайным. Скорее, он применялся для конкретных целей.

230. По мнению вступивших в производство по делу властей Нидерландов, отсутствует необходимость в дополнительных или обновленных минимальных требованиях, поскольку минимальные гарантии, ранее установленные Европейским Судом, являются достаточно надежными и «выдержали проверку временем». Дополнительные требования, предложенные заявителем, в частности, требование доказать наличие «разумного подозрения», неприемлемо снизят эффективность деятельности разведывательных служб без обеспечения какой-либо значимой дополнительной защиты основных прав лиц.

231. Кроме того, по мнению вступивших в производство по делу властей Нидерландов, попрежнему необходимо проводить различие между данными о содержании и данными о сообщениях в связи с тем, что содержание сообщений, скорее всего, имеет более конфиденциальный характер, чем данные о сообщениях. Власти Нидерландов согласились с Палатой Европейского Суда в том, что неправильно автоматически предполагать, что массовый перехват данных представляет собой большее вторжение в частную жизнь лица, чем адресный перехват, поскольку, если имеет место адресный перехват, то, вероятно, все или почти все перехваченные сообщения будут проанализированы. В случае массового перехвата данных это не так по той причине, что ограничения на изучение и использование данных определяют степень вмешательства перехвата в основные права лиц.

232. Наконец, вступившие в производство по делу власти Нидерландов утверждали, что требование объяснять или обосновывать селекторы или критерии поиска в разрешении серьезно ограничит эффективность массового перехвата данных ввиду высокой степени неопределенности относительно источника угрозы. Надзор *ex post* обеспечивает достаточные гарантии.

(d) Власти Королевства Норвегия

233. Власти Норвегии утверждали, что государства должны иметь широкие пределы усмотрения в том, что касается введения и использования той или иной формы режима массового перехвата данных в целях национальной безопасности. Это связано с тем, что разведывательным службам приходится идти в ногу с быстрым развитием информационных и коммуникационных технологий. Враждебно настроенные субъекты изменяют свои устройства и цифровую идентичность с такой скоростью, что их сложно отслеживать с течением времени. Также трудно своевременно выявлять враждебные кибероперации и противодействовать им без инструментов, способных к обнаружению отклонений и соответствующих характерных признаков. Следовательно, современные возможности, такие как массовый перехват данных, несомненно, необходимы для обнаружения неизвестных угроз в цифровой среде, а также для того, чтобы службы могли выявлять и отслеживать соответствующие угрозы для разведки.

234. В связи с этим надзор Европейского Суда должен основываться на общей оценке того, являются ли существующие процессуальные гарантии против злоупотреблений достаточными и надлежащими, поэтому следует избегать количественно установленных и абсолютных требований. Ему также не следует применять критерии, которые косвенно могут ослабить широкие пределы усмотрения, предоставленные государствам при принятии решения о применении режима массового перехвата данных по соображениям национальной безопасности. Требования «обоснованного подозрения» или «последующего уведомления» будут иметь такие последствия.

235. Наконец, власти Норвегии призвали Европейский Суд воздержаться от привнесения концепций и критериев, разработанных Судом ЕС. Во-первых, на соответствующий момент времени 19 государств – членов Совета Европы не входят в состав Европейского союза. Во-вторых, хотя Конвенция и Хартия Европейского союза об основных правах имеют много общего, существуют и различия, в первую очередь это касается статьи 8 Хартии, которая содержит право на защиту персональных данных. Кроме того, Суд ЕС иначе сформулировал критерий «соразмерности», используя метод «строгой необходимости», который несопоставим с методом, применяемым Европейским Судом.

4. Мнение Большой Палаты Европейского Суда

(a) Предварительные замечания

236. Настоящая жалоба касается массового перехвата трансграничных сообщений разведывательными службами. Хотя Европейский Суд не в первый раз рассматривает указанный вид наблюдения (см. упомянутое выше Решение Европейского Суда по делу «Вебер и Саравия против Германии» (Weber and Saravia v. Germany), а также упомянутое выше Постановление Евро-

пейского Суда по делу «Организация “Либерти” и другие против Соединенного Королевства» (Liberty and Others v. United Kingdom)[1], в ходе производства по делу стало очевидно, что при оценке любого подобного режима возникает ряд трудностей. В современную цифровую эпоху подавляющее большинство сообщений принимает цифровую форму и передается по глобальным телекоммуникационным сетям посредством сочетания самых быстрых и самых дешевых каналов без каких-либо значимой отсылки к национальным границам. Таким образом, наблюдение, которое не направлено непосредственно на отдельных лиц, действительно может иметь очень широкий охват как в пределах, так и за пределами территории государства, осуществляющего наблюдение. В связи с этим гарантии имеют решающее значение, однако они труднодостижимы. В отличие от адресного перехвата данных, которому посвящена значительная часть прецедентной практики Европейского Суда и который в основном используется для расследования преступлений, массовый перехват данных также (возможно, даже преимущественно) используется для сбора данных внешней разведки и выявления новых угроз со стороны как известных, так и неизвестных субъектов. При работе в этой сфере у государств – участников Конвенции есть законная потребность в обеспечении секретности. Это означает, что будет очень мало общедоступной информации, если она вообще будет, о функционировании механизма, и эта информация может быть сформулирована в неопределенных выражениях, которые могут значительно отличаться в разных государствах.

237. В то время как технологические возможности значительно увеличили объем сообщений, проходящих через мировой Интернет, возросли и угрозы, с которыми сталкиваются государства – участники Конвенции и их граждане. К ним относятся, помимо прочего, международный терроризм, незаконный оборот наркотических средств, торговля людьми и сексуальная эксплуатация детей. Многие из этих угроз исходят от международных сетей враждебно настроенных субъектов, имеющих доступ ко всё более сложным технологиям, позволяющим им общаться, оставаясь незамеченными. Доступ к подобным технологиям также позволяет враждебным государственным и негосударственным субъектам разрушать цифровую инфраструктуру и даже препятствовать надлежащему функционированию демократических процессов путем совершения кибератак, что представляет собой для национальной безопасности серьезную угрозу, которая по определению существует только в цифровой среде и как таковая может быть обнаружена и изучена только в ней. Следовательно, Европейский Суд должен провести оценку режимов государств – участников Конвенции по массовому перехвату данных – ценной технологической возможности по выявлению новых угроз в цифровой среде – на предмет соответствия Конвенции с учетом наличия гарантий против произвола и злоупотреблений на основе ограниченной информации о функционировании этих режимов.

(b) Наличие вмешательства

238. Власти Швеции утверждали, что отсутствовало вмешательство в права заявителя, предусмотренные статьей 8 Конвенции, поскольку он не принадлежал к группе лиц или организаций, на которые распространяется действие соответствующего законодательства, а ввиду весьма незначительной вероятности того, что сообщения заявителя станут предметом аналитического изучения, вмешательство в права в соответствии со статьей 8 Конвенции предположительно отсутствовало на предшествующих этапах массового перехвата сообщений в Швеции.

239. Европейский Суд рассматривает массовый перехват данных как поэтапный процесс, при котором степень вмешательства в права отдельных лиц по статье 8 Конвенции возрастает по мере продвижения процесса. Не все режимы массового перехвата данных имеют одну и ту же модель, и разные этапы процесса необязательно будут отдельными или следовать в строго хронологическом порядке. Тем не менее с учетом указанных оговорок Европейский Суд считает, что подлежащие изучению этапы процесса массового перехвата данных можно описать следующим образом:

(a) перехват и первоначальное хранение сообщений и связанных с ними данных (то есть данных трафика, связанных с перехваченными сообщениями);

(b) применение специальных селекторов к хранящимся сообщениям/данным, связанным с сообщениями;

(c) изучение отобранных сообщений/связанных с ними данных аналитиками, а также

(d) последующее хранение данных и использование «конечного продукта», включая обмен данными с третьими сторонами.

240. В ходе того, что Европейский Суд назвал первым этапом, разведывательные службы осуществляют массовый перехват электронных сообщений (или «блоков» электронных сообщений). Такие сообщения принадлежат большому количеству лиц, многие из которых не представляют интереса для разведывательных служб. Некоторые

[1] Так в тексте. Имеется в виду Постановление Европейского Суда по делу «Организация “Либерти” и другие против Соединенного Королевства» (Liberty and Others v. United Kingdom) от 1 июля 2008 г., жалоба № 58243/00. В настоящем Постановлении оно упоминается впервые (*примеч. переводчика*).

подобные сообщения, которые вряд ли представляют интерес для разведки, могут быть исключены на этом этапе.

241. Первоначальный анализ, который в основном автоматизирован, происходит в процессе того, что, по мнению Европейского Суда, является вторым этапом, когда к сохраненным блокам сообщений и связанным с ними данными применяются различные типы селекторов, включая «жесткие селекторы» (например, адрес электронной почты) и/или комплексные запросы. На этом этапе процесс начинает адресно выявлять отдельных лиц посредством использования жестких селекторов.

242. На третьем этапе, в соответствии с определением Европейского Суда, перехваченные материалы впервые изучаются аналитиком.

243. В ходе того, что Европейский Суд считает заключительным этапом, перехваченные материалы фактически используются разведывательными службами. Это использование может включать в себя составление разведывательного донесения, обмен материалами с другими разведывательными службами в пределах государства, осуществляющего перехват, или даже передачу материалов иностранным разведывательным службам.

244. По мнению Европейского Суда, статья 8 Конвенции применяется на каждом из вышеуказанных этапов. В то время как первоначальный перехват с последующим немедленным удалением фрагментов сообщений не представляет собой существенного вмешательства, степень вмешательства в права отдельных лиц, предусмотренные статьей 8 Конвенции, будет увеличиваться по мере продвижения процесса массового перехвата сообщений. В этом отношении Европейский Суд четко заявил, что даже простое хранение данных, касающихся частной жизни лица, составляет вмешательство по смыслу статьи 8 Конвенции (см. Постановление Европейского Суда по делу «Леандер против Швеции» (Leander v. Sweden) от 26 марта 1987 г., § 48, Series A, № 116) и что необходимость наличия гарантий еще больше возрастает, когда речь идет о защите персональных данных, подвергающихся автоматизированной обработке (см. упомянутое выше Постановление Большой Палаты Европейского Суда по делу «S. и Марпер против Соединенного Королевства» (S. and Marper v. United Kingdom), § 103). Тот факт, что хранящийся материал закодирован, понятен только с использованием компьютерных технологий и может быть интерпретирован только ограниченным количеством лиц, не может иметь отношения к этому выводу (см. Постановление Большой Палаты Европейского Суда по делу «Аманн против Швейцарии» (Amann v. Switzerland), жалоба № 27798/95, § 69, ECHR 2000-II; упомянутое выше Постановление Большой Палаты Европейского Суда по делу «S. и Марпер против Соединенного Королевства» (S. and Marper v. United Kingdom), §§ 67 и 75). Наконец, на заключительном этапе процесса, когда аналитик будет изучать информацию о конкретном лице или содержание сообщений, потребность в гарантиях будет максимальной. Этот подход Европейского Суда соответствует выводу Венецианской комиссии, которая в своем докладе «О демократическом контроле над органами радиотехнической разведки» пришла к выводу, что при массовом перехвате данных основное вмешательство в частную жизнь происходило на этапе, когда сохраненные персональные данные обрабатывались и/или становились доступны для ведомств (см. выше §§ 86–91).

245. Таким образом, степень вмешательства в право на неприкосновенность частной жизни будет усиливаться по мере прохождения процесса через различные этапы. При анализе обоснованности этого возрастающего вмешательства Европейский Суд проведет оценку соответствующего режима Швеции, исходя из указанного понимания природы вмешательства.

(c) Было ли вмешательство обоснованным

(i) Общие принципы, касающиеся мер скрытого наблюдения, включая перехват сообщений

246. Любое вмешательство в права лица, гарантированные статьей 8 Конвенции, может быть оправдано только в соответствии с пунктом 2 статьи 8 Конвенции, если оно предусмотрено законом, преследует одну или несколько законных целей, на которые ссылается пункт 2 статьи 8 Конвенции, и является необходимым в демократическом обществе для достижения любой из этих целей (см. упомянутое выше Постановление Большой Палаты Европейского Суда по делу «Роман Захаров против Российской Федерации» (Roman Zakharov v. Russia), § 227; упомянутое выше Постановление Европейского Суда по делу «Кеннеди против Соединенного Королевства» (Kennedy v. United Kingdom), § 130). Формулировка «предусмотрено законом» требует, чтобы оспариваемая мера имела некоторую основу во внутригосударственном законодательстве (в противоположность практике, которая не имеет специальной законодательной основы, см. Постановление Европейского Суда по делу «Хеглас против Чешской Республики» (Heglas v. Czech Republic) от 1 марта 2007 г., жалоба № 5935/02, § 74). Оспариваемая мера также должна быть совместима с принципом верховенства права, который прямо упомянут в Преамбуле к Конвенции и воплощен в объекте и цели статьи 8 Конвенции. Следовательно, закон должен быть доступен для заинтересованного лица и предсказуем в своих последствиях (см. упомянутое выше Постановление Большой Палаты Европейского Суда по делу «Роман Захаров против

Российской Федерации» (Roman Zakharov v. Russia), § 228; см. также среди многих прочих примеров Постановление Большой Палаты Европейского Суда по делу «Ротару против Румынии» (Rotaru v. Romania), жалоба № 28341/95, ECHR 2000-V, § 52; упомянутое выше Постановление Большой Палаты Европейского Суда по делу «S. и Марпер против Соединенного Королевства» (S. and Marper v. United Kingdom), § 95; упомянутое выше Постановление Европейского Суда по делу «Кеннеди против Соединенного Королевства» (Kennedy v. United Kingdom), § 151).

247. Значение термина «предсказуемость» в контексте мер скрытого наблюдения не может быть таким же, как во многих других областях. Предсказуемость в особом контексте мер скрытого наблюдения, таких как перехват сообщений, не может означать, что лицо должно иметь возможность предвидеть, когда власти могут прибегнуть к указанной мере, чтобы адаптировать свое поведение соответствующим образом. Тем не менее особенно в случаях, когда полномочия, которыми наделены исполнительные органы власти, осуществляются секретно, риски произвола очевидны. В связи с этим крайне важно, чтобы существовали четкие, подробные правила, касающиеся мер скрытого наблюдения, особенно когда доступные для использования технологии постоянно становятся всё более изощренными. Внутригосударственное законодательство должно быть достаточно ясным, чтобы давать лицам адекватное представление об обстоятельствах и условиях, при которых органы власти имеют право прибегать к подобным мерам (см. упомянутое выше Постановление Большой Палаты Европейского Суда по делу «Роман Захаров против Российской Федерации» (Roman Zakharov v. Russia), § 229; Постановление Европейского Суда по делу «Мэлоун против Соединенного Королевства» (Malone v. United Kingdom) от 2 августа 1984 г., § 67, Series A, № 82; упомянутое выше Постановление Европейского Суда по делу «Леандер против Швеции» (Leander v. Sweden), § 51; Постановление Европейского Суда по делу «Ювиг против Франции» (Huvig v. France) от 24 апреля 1990 г., § 29, Series A, № 176-B; Постановление Европейского Суда по делу «Валенсуэла Контрерас против Испании» (Valenzuela Contreras v. Spain) от 30 июля 1998 г., § 46, *Reports of Judgments and Decisions* 1998-V; упомянутое выше Постановление Большой Палаты Европейского Суда по делу «Ротару против Румынии» (Rotaru v. Romania), § 55; упомянутое выше Решение Европейского Суда по делу «Вебер и Саравия против Германии» (Weber and Saravia v. Germany), § 93; Постановление Европейского Суда по делу «Ассоциация за европейскую интеграцию и права человека и Экимджиев против Болгарии» (Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria) от 28 июня 2007 г., жалоба № 62540/00, § 75). Кроме того, закон должен с достаточной ясностью определять пределы любого усмотрения, предоставленного компетентным органам, и способ его реализации, чтобы обеспечить лицу надлежащую защиту от произвольного вмешательства (см. упомянутое выше Постановление Большой Палаты Европейского Суда по делу «Роман Захаров против Российской Федерации» (Roman Zakharov v. Russia), § 230; см. также среди прочих примеров упомянутое выше Постановление Европейского Суда по делу «Мэлоун против Соединенного Королевства» (Malone v. United Kingdom), § 68; упомянутое выше Постановление Европейского Суда по делу «Леандер против Швеции» (Leander v. Sweden), § 51; упомянутое выше Постановление Европейского Суда по делу «Ювиг против Франции» (Huvig v. France), § 29; упомянутое выше Решение Европейского Суда по делу «Вебер и Саравия против Германии» (Weber and Saravia v. Germany), § 94).

248. В делах, где в Европейском Суде оспаривается законодательство, разрешающее скрытое наблюдение, вопрос о законности вмешательства тесно связан с вопросом о проверке «необходимости», поэтому Европейский Суд считает целесообразным совместно рассматривать критерии «соответствия закону» и «необходимости». «Качество закона» в этом смысле предполагает, что внутригосударственное законодательство не только должно быть доступным и предсказуемым в его применении, но и должно гарантировать, что меры скрытого наблюдения применяются только при их «необходимости в демократическом обществе», в частности, обеспечивая надлежащие и эффективные гарантии против произвола (см. упомянутое выше Постановление Большой Палаты Европейского Суда по делу «Роман Захаров против Российской Федерации» (Roman Zakharov v. Russia), § 236; упомянутое выше Постановление Европейского Суда по делу «Кеннеди против Соединенного Королевства» (Kennedy v. United Kingdom), § 155).

249. В этом отношении следует напомнить, что в своей прецедентной практике о перехвате сообщений в рамках уголовного расследования Европейский Суд разработал следующие минимальные гарантии, которые должны быть установлены в законодательстве во избежание злоупотребления полномочиями: (1) указание на характер правонарушений, которые могут привести к выдаче разрешения на перехват; (2) определение категорий лиц, сообщения которых подлежат перехвату; (3) ограничение продолжительности перехвата; (4) определение порядка изучения, использования и хранения полученных данных; (5) определение мер предосторожности при передаче данных другим лицам и (6) указание обстоятельств, при которых перехваченные данные могут или должны быть удалены или уничтожены (см. упомянутое выше Постановление Европейского

Суда по делу «Ювиг против Франции» (Huvig v. France), § 34; упомянутое выше Постановление Европейского Суда по делу «Валенсуэла Контрерас против Испании» (Valenzuela Contreras v. Spain), § 46; упомянутое выше Решение Европейского Суда по делу «Вебер и Саравия против Германии» (Weber and Saravia v. Germany), § 95; упомянутое выше Постановление Европейского Суда по делу «Ассоциация за европейскую интеграцию и права человека и Экимджиев против Болгарии» (Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria), § 76). В упомянутом выше Постановлении Большой Палаты по делу «Роман Захаров против Российской Федерации» (Roman Zakharov v. Russia) (§ 231) Европейский Суд подтвердил, что те же шесть гарантий применимы и в делах, когда перехват сообщений осуществляется по соображениям национальной безопасности. Однако при определении того, нарушало ли оспариваемое законодательство статью 8 Конвенции, Европейский Суд также учитывал порядок надзора за осуществлением мер скрытого наблюдения, наличие любых механизмов уведомления и средств правовой защиты, предусмотренных внутригосударственным законодательством (см. упомянутое выше Постановление Большой Палаты Европейского Суда по делу «Роман Захаров против Российской Федерации» (Roman Zakharov v. Russia), § 238).

250. Проверка мер скрытого наблюдения и надзор за ними могут осуществляться на трех этапах: вначале, когда наблюдение санкционируется, в ходе его проведения или после его завершения. Что касается первых двух этапов, сама природа и логика скрытого наблюдения предполагают, что не только наблюдение, но и сопутствующая ему проверка должны осуществляться без ведома лица. Следовательно, поскольку у лица неизбежно не будет возможности использовать эффективное средство правовой защиты по собственной инициативе или принимать непосредственное участие в каком-либо надзорном производстве, важно, чтобы установленные процедуры сами предусматривали надлежащие и эквивалентные гарантии защиты его прав. В сферах, где злоупотребления могут быть совершены потенциально легко и иметь пагубные последствия для демократического общества в целом, Европейский Суд отмечал, что в принципе желательно передать надзорные полномочия судье, поскольку судебный контроль предлагает наилучшие гарантии независимости, беспристрастности и соблюдения надлежащей процедуры (см. упомянутое выше Постановление Большой Палаты Европейского Суда по делу «Роман Захаров против Российской Федерации» (Roman Zakharov v. Russia), § 233; а также упомянутое выше Постановление Европейского Суда по делу «Класс и другие против Германии» (Klass and Others v. Germany), §§ 55 и 56).

251. Что касается третьего этапа, после прекращения наблюдения вопрос о последующем уведомлении о мерах наблюдения представляет собой значимый фактор для оценки эффективности средств правовой защиты в судах и, следовательно, для изучения существования эффективных гарантий против злоупотребления полномочиями по наблюдению. В принципе у заинтересованного лица мало возможностей для обращения в суды кроме случаев, когда это лицо получило уведомление о мерах, принятых без его ведома, и, таким образом, имеет возможность оспорить их законность после их применения (см. упомянутое выше Постановление Большой Палаты Европейского Суда по делу «Роман Захаров против Российской Федерации» (Roman Zakharov v. Russia), § 234; упомянутое выше Постановление Европейского Суда по делу «Класс и другие против Германии» (Klass and Others v. Germany), § 57; упомянутое выше Решение Европейского Суда по делу «Вебер и Саравия против Германии» (Weber and Saravia v. Germany), § 135), или в качестве альтернативы, когда любое лицо, которое подозревает, что в отношении него осуществляется наблюдение, может обратиться в суд, юрисдикция которого не зависит от уведомления объекта наблюдения о принятых мерах (см. упомянутое выше Постановление Большой Палаты Европейского Суда по делу «Роман Захаров против Российской Федерации» (Roman Zakharov v. Russia), § 234; см. также упомянутое выше Постановление Европейского Суда по делу «Кеннеди против Соединенного Королевства» (Kennedy v. United Kingdom), § 167).

252. Что касается вопроса о «необходимости вмешательства в демократическом обществе» для достижения законной цели, Европейский Суд признал, что властям государства-ответчика предоставлены широкие пределы свободы усмотрения при выборе наилучшего способа достижения законной цели защиты национальной безопасности (см. упомянутое выше Решение Европейского Суда по делу «Вебер и Саравия против Германии» (Weber and Saravia v. Germany), § 106).

253. Однако такие пределы подлежат контролю со стороны Европейского Суда, который охватывает как законодательство, так и имплементирующие его решения. С учетом риска того, что система скрытого наблюдения, учрежденная в целях защиты национальной безопасности (и других важных государственных интересов), может воспрепятствовать надлежащему функционированию демократических процессов или даже уничтожить их под предлогом их защиты, Европейскому Суду необходимо удостовериться в наличии надлежащих и эффективных гарантий против злоупотреблений. Эта оценка зависит от всех обстоятельств дела, таких как характер, объем и продолжительность возможных мер, основания, необходимые для их санкционирования, компетентные органы,

правомочные выдавать разрешение, выполнять и контролировать такие меры, а также вид средства правовой защиты, предусмотренного внутригосударственным законодательством. Европейский Суд должен определить, будет ли порядок надзора за санкционированием и осуществлением ограничительных мер достаточным для того, чтобы «вмешательство» не выходило за рамки «необходимого в демократическом обществе» (см. упомянутое выше Постановление Большой Палаты Европейского Суда по делу «Роман Захаров против Российской Федерации» (Roman Zakharov v. Russia), § 232; см. также упомянутое выше Постановление Европейского Суда по делу «Класс и другие против Германии» (Klass and Others v. Germany), §§ 49, 50 и 59; упомянутое выше Решение Европейского Суда по делу «Вебер и Саравия против Германии» (Weber and Saravia v. Germany), § 106; упомянутое выше Постановление Европейского Суда по делу «Кеннеди против Соединенного Королевства» (Kennedy v. United Kingdom), §§ 153 и 154).

(ii) Наличие необходимости развивать прецедентную практику

254. В упомянутом выше Решении по делу «Вебер и Саравия против Германии» (Weber and Saravia v. Germany) и в упомянутом выше Постановлении по делу «Организация “Либерти” и другие против Соединенного Королевства» (Liberty and Others v. United Kingdom) Европейский Суд признал, что режимы массового перехвата данных *per se* не выходят за пределы усмотрения властей. С учетом увеличения количества угроз, с которыми в настоящее время сталкиваются власти со стороны групп международных субъектов, использующих Интернет как для общения, так и в качестве инструмента, а также ввиду наличия изощренной технологии, которая позволяет этим субъектам избегать обнаружения, Европейский Суд считает, что пределы усмотрения по-прежнему охватывают решение применять режим массового перехвата данных в целях выявления угроз для национальной безопасности или важных национальных интересов.

255. В упомянутом выше Решении по делу «Вебер и Саравия против Германии» (Weber and Saravia v. Germany) и в упомянутом выше Постановлении по делу «Организация “Либерти” и другие против Соединенного Королевства» (Liberty and Others v. United Kingdom) Европейский Суд применил указанные выше шесть минимальных гарантий, разработанных в его прецедентной практике в отношении адресного перехвата. Вместе с тем, несмотря на то, что режимы массового перехвата данных, рассмотренные в этих делах, на первый взгляд аналогичны режиму, анализируемому в настоящем деле, оба вышеуказанных дела рассматривались более 10 лет назад, и за прошедшие годы технологические разработки значительно изменили способ общения людей. Жизнь всё чаще проходит в режиме онлайн, при этом генерируется значительно больший объем электронных сообщений, существенно отличающихся по характеру и качеству от тех, что, по всей видимости, создавались 10 лет назад. Следовательно, масштабы деятельности по наблюдению, рассмотренной в указанных выше делах, были гораздо у́же.

256. То же самое относится и к сопутствующим данным о сообщениях. Представляется, что в настоящее время доступны бóльшие объемы данных о сообщениях в отношении отдельного лица, чем относительно содержания сообщения, поскольку каждому фрагменту содержания сопутствует множество фрагментов данных о сообщениях. Несмотря на то, что содержание может быть зашифровано и в любом случае может не раскрывать значимой информации об отправителе или получателе, сопутствующие данные о сообщениях могут раскрывать большой объем персональной информации, такой как идентичность и географическое местоположение отправителя и получателя, а также оборудование, через которое передавалось сообщение. Кроме того, любое вмешательство, вызванное получением сопутствующих данных о сообщениях, будет возрастать при массовом получении таких данных, поскольку в настоящее время их можно анализировать и изучать в целях создания детального образа лица посредством сравнения социальных сетей, отслеживания местоположения, отслеживания просмотра интернет-страниц, соотнесения моделей общения и понимания того, с кем человек взаимодействовал.

257. Однако гораздо важнее тот факт, что в упомянутом выше Решении по делу «Вебер и Саравия против Германии» (Weber and Saravia v. Germany) и в упомянутом выше Постановлении по делу «Организация “Либерти” и другие против Соединенного Королевства» (Liberty and Others v. United Kingdom) Европейский Суд прямо не отметил, что он имел дело с наблюдением иного характера и масштаба, чем то, что рассматривалось в предыдущих делах. Тем не менее адресный перехват и массовый перехват различаются по ряду важных аспектов.

258. Прежде всего предметом массового перехвата обычно становятся международные сообщения (то есть сообщения, физически пересекающие государственные границы), и, хотя нельзя исключать перехват и даже анализ сообщений лиц, находящихся на территории государства, осуществляющего наблюдение, во многих случаях заявленная цель массового перехвата заключается в отслеживании сообщений лиц, находящихся за пределами территориальной юрисдикции государства, которые не могут быть проконтролированы с помощью иных форм наблюдения. Например, система, действующая в Германии, предназначена только

для мониторинга внешних телекоммуникаций за пределами территории Германии (см. выше § 137).

259. Кроме того, как уже отмечалось, массовый перехват данных может применяться для иных целей. В той части, в которой Европейский Суд рассматривал адресный перехват, он в большинстве случаев использовался властями государств-ответчиков для расследования преступлений. Однако хотя массовый перехват данных может использоваться для расследования некоторых серьезных преступлений, государства – члены Совета Европы, в которых действует режим массового перехвата, по-видимому, используют его для сбора данных внешней разведки, раннего выявления и расследования кибератак, контрразведки и борьбы с терроризмом (см. выше §§ 131–146).

260. Даже если массовый перехват данных необязательно направлен на обнаружение конкретных лиц, очевидно, что он может использоваться (и используется) для этой цели. Вместе с тем в этом случае устройства лиц, являющихся объектами наблюдения, не отслеживаются. Скорее, лица становятся «объектами» наблюдения путем применения жестких селекторов (таких, как адреса электронной почты) к сообщениям, перехватываемым разведывательными службами в массовом порядке. Таким способом будут перехвачены только те «блоки» сообщений лиц, являющихся объектами наблюдения, которые проходили через носители, отобранные разведывательными службами, и только те перехваченные сообщения, которые соответствовали жесткому селектору или комплексному запросу, могут быть изучены аналитиком.

261. Как и при любом режиме перехвата данных, режим массового перехвата имеет значительный потенциал для злоупотреблений, которые отрицательно скажутся на праве лиц на уважение их частной жизни. Хотя статья 8 Конвенции не запрещает использование массового перехвата данных для защиты национальной безопасности и иных важных национальных интересов от серьезных внешних угроз и властям предоставлены широкие пределы свободы усмотрения при принятии решения о том, какой режим перехвата необходим для этих целей, при использовании такой системы предоставленные им пределы усмотрения должны быть у́же, и должен быть предусмотрен ряд гарантий. Европейский Суд уже определил те гарантии, которые должны быть предусмотрены режимом адресного перехвата данных, соответствующего Конвенции. Несмотря на то, что указанные принципы представляют собой практическую основу для этой задачи, их необходимо адаптировать, чтобы отразить особенности режима массового перехвата и, в частности, возрастающую степень вмешательства в права отдельных лиц, предусмотренные статьей 8 Конвенции, по мере прохождения операции через этапы, указанные выше в § 239.

(iii) Подход, которого следует придерживаться в делах о массовом перехвате данных

262. Очевидно, что первые две из шести «минимальных гарантий», которые, как установил Европейский Суд в контексте адресного перехвата данных, должны быть четко установлены во внутригосударственном законодательстве во избежание злоупотреблений полномочиями (а именно характер правонарушений, которые могут привести к выдаче разрешения на перехват, и категории лиц, сообщения которых подлежат перехвату; см. выше § 249), не всегда применимы к режиму массового перехвата данных. Аналогичным образом требование «разумного подозрения», которое выработано в прецедентной практике Европейского Суда, касающейся адресного перехвата данных в контексте уголовных расследований, имеет меньшее значение в отношении массового перехвата данных, который в принципе является превентивным, а не направлен на изучение конкретного объекта и/или на расследование идентифицируемого уголовного преступления. Тем не менее Европейский Суд считает крайне важным, чтобы при наличии в государстве такого режима внутригосударственное законодательство содержало подробные нормы, регламентирующие использование властями подобных мер. В частности, во внутригосударственном законодательстве следует с достаточной ясностью указать основания, на которых может быть разрешен массовый перехват данных, и обстоятельства, при которых сообщения отдельных лиц могут быть перехвачены. Остальные четыре минимальные гарантии, установленные Европейским Судом в его предыдущих постановлениях, а именно необходимость установления во внутригосударственном законодательстве ограничений продолжительности перехвата, порядка изучения, использования и хранения полученных данных, мер предосторожности при передаче данных другим лицам и обстоятельств, при которых перехваченные данные могут или должны быть удалены или уничтожены, в равной степени относятся к массовому перехвату данных.

263. В своей прецедентной практике, касающейся адресного перехвата данных, Европейский Суд принимал во внимание механизмы контроля и проверки режимов перехвата (см. упомянутое выше Постановление Большой Палаты Европейского Суда по делу «Роман Захаров против Российской Федерации» (Roman Zakharov v. Russia), §§ 233–234). В контексте массового перехвата данных значимость контроля и проверки такого режима возрастает ввиду присущего ему риска злоупотреблений и того, что законная потребность в обеспечении секретности неизбежно будет означать, что по причинам нацио-

нальной безопасности власти зачастую не будут вправе раскрывать информацию о функционировании оспариваемого режима.

264. Таким образом, по мнению Европейского Суда, в целях минимизации риска злоупотреблений при массовом перехвате данных к процессу должны применяться «сквозные» гарантии. Иными словами, на внутригосударственном уровне следует проводить оценку необходимости и соразмерности принимаемых мер на каждом этапе процесса. В самом начале в момент определения пределов и цели массового перехвата данных должно быть выдано независимое разрешение на его проведение, и операция должна подлежать надзору и независимой проверке *ex post facto*. По мнению Европейского Суда, это основополагающие гарантии, которые являются ключевым элементом любого режима массового перехвата данных, соответствующего статье 8 Конвенции (см. также доклад Венецианской комиссии выше в § 86, где аналогичным образом было установлено, что выдача разрешения и контроль процесса представляют собой важнейшие гарантии в рамках режима массового перехвата данных).

265. Обращаясь прежде всего к вопросу о разрешении, Большая Палата Европейского Суда считает, что, хотя разрешение судебного органа составляет «важную гарантию против произвола», оно не является «необходимым требованием». Тем не менее массовый перехват данных должен быть санкционирован независимым органом, то есть органом, независимым от органов исполнительной власти.

266. Кроме того, чтобы обеспечить эффективную защиту от злоупотреблений, независимый орган, выдающий разрешение, должен быть уведомлен как о цели перехвата, так и о носителях сообщений или о способах связи, которые могут быть перехвачены. Это позволит независимому органу, выдающему разрешение, оценить необходимость и соразмерность массового перехвата, а также установить, является ли выбор носителей необходимым и соразмерным целям, для которых проводится перехват.

267. Использование селекторов, в частности, жестких селекторов, – одна из наиболее важных мер в процессе массового перехвата данных, поскольку именно в этот момент разведывательные службы могут отслеживать сообщения конкретного лица. При этом Европейский Суд отмечает, что, как утверждали вступившие в производство по делу власти Нидерландов, любое требование объяснять или обосновывать селекторы или критерии поиска в разрешении серьезно ограничит эффективность массового перехвата данных (см. выше §§ 228–232). В Соединенном Королевстве Следственный трибунал установил, что включение селекторов в разрешение «чрезмерно ослабит и ограничит действие ордера и в любом случае будет совершенно нереальным» (см. упомянутое выше Постановление Европейского Суда по делу «Организация Big Brother Watch и другие против Соединенного Королевства» (Big Brother Watch and Others v. United Kingdom), § 49).

268. Принимая во внимание характеристики массового перехвата данных (см. выше §§ 258 и 259), большое количество используемых селекторов и неотъемлемую потребность в гибкости при выборе селекторов, которые на практике могут быть выражены в виде технического сочетания цифр или букв, Европейский Суд согласен с тем, что на практике может оказаться невозможным включить в разрешение все селекторы. Тем не менее, учитывая, что выбор селекторов и критериев поиска определяет, какие сообщения будут переданы для дальнейшего изучения аналитиком, в разрешении как минимум должны быть указаны типы или категории используемых селекторов.

269. Кроме того, необходимо предусматривать повышенные гарантии, когда разведывательные службы применяют жесткие селекторы, связанные с поддающимися идентификации лицами. Разведывательные службы должны обосновывать использование каждого такого селектора с учетом принципов необходимости и соразмерности. Это обоснование должно быть тщательно зафиксировано и подвергнуто процедуре предварительного внутреннего разрешения в целях отдельной и объективной проверки того, соответствует ли обоснование указанным выше принципам.

270. Каждый этап процесса массового перехвата данных, включая первоначальное разрешение и любое последующее продление срока его действия, отбор носителей, выбор и применение селекторов и критериев поиска, равно как и использование, хранение, дальнейшая передача и удаление перехваченных материалов, также должны подлежать надзору со стороны независимого органа, и такой надзор должен быть достаточно строгим для того, чтобы «вмешательство» не выходило за рамки «необходимого в демократическом обществе» (см. упомянутое выше Постановление Большой Палаты Европейского Суда по делу «Роман Захаров против Российской Федерации» (Roman Zakharov v. Russia), § 232; упомянутое выше Постановление Европейского Суда по делу «Класс и другие против Германии» (Klass and Others v. Germany), §§ 49, 50 и 59; упомянутое выше Решение Европейского Суда по делу «Вебер и Саравия против Германии» (Weber and Saravia v. Germany), § 106; и упомянутое выше Постановление Европейского Суда по делу «Кеннеди против Соединенного Королевства» (Kennedy v. United Kingdom), §§ 153 и 154). В частности, надзорный орган должен быть в состоянии оценить необходимость и соразмерность принимаемых мер с надлежащим учетом соответствующей степени вмешательства в конвенционные права

лиц, которые могут быть затронуты. В целях облегчения такого надзора разведывательные службы обязаны вести подробные записи на каждом этапе процесса.

271. Наконец, любому лицу, которое подозревает, что его сообщения были перехвачены разведывательными службами, должно быть предоставлено эффективное средство правовой защиты для оспаривания законности предполагаемого перехвата данных или совместимости режима массового перехвата с Конвенцией. В контексте адресного перехвата Европейский Суд неоднократно признавал последующее уведомление о мерах наблюдения важным фактором при оценке эффективности средств правовой защиты в судах и, следовательно, в оценке наличия эффективных гарантий против злоупотребления полномочиями по осуществлению наблюдения. При этом он считал, что не требуется уведомления, если система внутригосударственных средств правовой защиты позволяет любому лицу, которое подозревает, что его сообщения перехватываются или были перехвачены, обратиться в суд. Иными словами, если юрисдикция суда не зависит от уведомления объекта наблюдения о перехвате его сообщений (см. упомянутое выше Постановление Большой Палаты Европейского Суда по делу «Роман Захаров против Российской Федерации» (Roman Zakharov v. Russia), § 234; упомянутое выше Постановление Европейского Суда по делу «Кеннеди против Соединенного Королевства» (Kennedy v. United Kingdom), § 167).

272. По мнению Европейского Суда, средство правовой защиты, которое не зависит от уведомления объекта наблюдения, также могло бы стать эффективным средством правовой защиты в контексте массового перехвата данных. Точнее: в зависимости от обстоятельств такое средство правовой защиты может даже лучшим образом гарантировать надлежащую процедуру, чем система, основанная на уведомлении. Независимо от того, были ли материалы получены посредством адресного или массового перехвата, наличие оговорки о национальной безопасности может лишить требование об уведомлении какого-либо реального практического действия. Вероятность того, что требование об уведомлении будет оказывать незначительное практическое действие или не будет оказывать никакого действия, окажется выше в контексте массового перехвата данных, поскольку такое наблюдение может использоваться для целей сбора данных внешней разведки и по большей части будет направлено на сообщения лиц, находящихся за пределами территориальной юрисдикции государства. Следовательно, даже если личность объекта наблюдения известна, у властей могут отсутствовать сведения о его местонахождении.

273. Полномочия и процессуальные гарантии, которыми обладает орган, важны для определения эффективности средства правовой защиты. Соответственно, в отсутствие требования о наличии уведомления крайне важно, чтобы правовая защита осуществлялась органом, который, необязательно будучи судебным, является независимым от исполнительной власти и гарантирует справедливость производства, проводя, насколько это возможно, состязательный процесс. Решения этого органа должны быть мотивированными и обязательными в отношении, *inter alia*, прекращения незаконного перехвата и уничтожения незаконно полученных и/или хранящихся перехваченных материалов (см., *mutatis mutandis*, упомянутое выше Постановление Европейского Суда по делу «Сегерстедт-Виберг и другие против Швеции» (Segerstedt-Wiberg and Others v. Sweden), § 120; а также упомянутое выше Постановление Европейского Суда по делу «Леандер против Швеции» (Leander v. Sweden), §§ 81–83, в котором отсутствие полномочий выносить обязательные решения составляло основной недостаток предлагаемого механизма контроля).

274. В свете вышеизложенного Европейский Суд установит, соответствует ли режим массового перехвата данных Конвенции, посредством проведения общей оценки функционирования режима. В ходе такой оценки прежде всего будет рассмотрен вопрос о том, содержит ли нормативно-правовая база Швеции достаточные гарантии против злоупотреблений и применяются ли к процессу «сквозные» гарантии (см. выше § 264). При этом Европейский Суд будет учитывать фактическое функционирование системы перехвата, включая систему сдержек и противовесов при осуществлении полномочий, а также наличие или отсутствие каких-либо доказательств фактического злоупотребления (см. упомянутое выше Постановление Европейского Суда по делу «Ассоциация за европейскую интеграцию и права человека и Экимджиев против Болгарии» (Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria), § 92).

275. При анализе вопроса о том, действовали ли власти Швеции в рамках предоставленных их пределов усмотрения (см. выше § 256), Европейскому Суду потребуется принять во внимание более широкий ряд критериев, чем шесть гарантий, установленных в упомянутом выше Решении Европейского Суда по делу «Вебер и Саравия против Германии» (Weber and Saravia v. Germany). В частности, рассматривая в совокупности требования «предусмотрено законом» и «необходимость» согласно сложившемуся подходу в данной области (см. упомянутое выше Постановление Большой Палаты Европейского Суда по делу «Роман Захаров против Российской Федерации» (Roman Zakharov v. Russia), § 236; и упомянутое выше Постановление Европейского Суда по делу «Кеннеди против Соединенного Королевства» (Kennedy v. United Kingdom), § 155), Европейский Суд установит,

были ли в нормативно-правовой базе Швеции четко определены следующие элементы:

1) основания, при которых массовый перехват может быть разрешен;

2) обстоятельства, при которых сообщения отдельных лиц могут подлежать перехвату;

3) порядок выдачи разрешения;

4) порядок отбора, изучения и использования перехваченных материалов;

5) меры предосторожности при передаче материалов другим лицам;

6) ограничения продолжительности перехвата, хранения перехваченных материалов и обстоятельства, при которых такие материалы должны быть удалены или уничтожены;

7) порядок и способы проверки независимым органом соблюдения указанных выше гарантий и полномочия этого органа по устранению нарушений;

8) порядок проведения независимой *ex post facto* проверки такого соответствия и полномочия компетентного органа по устранению выявленных нарушений.

276. Несмотря на то, что меры предосторожности при передаче перехваченных материалов другим лицам являются одним из шести критериев, установленных в упомянутом выше Решении Европейского Суда по делу «Вебер и Саравия против Германии» (Weber and Saravia v. Germany), до настоящего времени Европейский Суд не давал каких-либо особых разъяснений относительно таких мер. При этом очевидно, что власти некоторых государств регулярно обмениваются материалами со своими партнерами по разведке и даже в определенных случаях предоставляют своим партнерам прямой доступ к своим собственным системам. Следовательно, по мнению Европейского Суда, передача властями государства – участника Конвенции материалов, полученных путем массового перехвата, властям иностранного государства или международным организациям должна ограничиваться теми материалами, которые были собраны и хранились в соответствии с Конвенцией, а к самой передаче необходимо применять дополнительные особые гарантии. Во-первых, обстоятельства, при которых такая передача может иметь место, должны быть четко указаны во внутригосударственном законодательстве. Во-вторых, власти передающего государства должны удостовериться в том, что в принимающем государстве существуют гарантии, позволяющие предотвратить злоупотребления и несоразмерное вмешательство при обработке данных. В частности, власти принимающего государства должны гарантировать безопасное хранение материалов и ограничить его дальнейшее раскрытие. Это необязательно означает, что защита, гарантируемая в принимающем государстве, должна быть сопоставима с защитой, предоставляемой в передающем государстве, и необязательно требует предоставления гарантии перед каждой передачей. В-третьих, необходимы повышенные гарантии, когда становится очевидно, что осуществляется передача материалов, требующих обеспечения особой конфиденциальности, например, конфиденциальных журналистских материалов. Наконец, Европейский Суд считает, что передача материалов партнерам по внешней разведке также должна подлежать независимому контролю.

277. По причинам, указанным выше в § 256, Европейский Суд не убежден в том, что получение соответствующих данных о сообщениях в порядке их массового перехвата в любом случае представляет собой меньшее вмешательство, чем получение данных о содержании. Следовательно, Европейский Суд считает, что перехват, хранение и изучение сопутствующих данных о сообщениях следует анализировать с учетом тех же гарантий, которые применяются к содержанию сообщений.

278. При этом, хотя разрешение на перехват сопутствующих данных о сообщениях, как правило, выдается одновременно с разрешением на перехват содержания сообщений, разведывательные службы после получения таких данных могут рассматривать их по-разному. С учетом различного характера сопутствующих данных о сообщениях и различных способов их использования разведывательными службами Европейский Суд полагает, что правовые положения, регулирующие их обработку, необязательно должны быть во всех отношениях идентичны правовым положениям, регулирующим обработку содержания сообщений, до тех пор, пока действуют указанные выше гарантии.

(iv) Оценка Большой Палатой Европейского Суда настоящего дела

(α) Предварительные замечания

279. Как отметила Палата Европейского Суда, стороны не оспаривали, что деятельность властей Швеции в области радиотехнической разведки основана на законодательстве Швеции (см. § 111 Постановления Палаты Европейского Суда). Кроме того, не вызывает сомнений, что оспариваемый режим радиотехнической разведки преследует законные цели в интересах национальной безопасности, защищая внешнюю политику, политику обороны и безопасности Швеции и выявляя внешние угрозы для страны. Таким образом, следуя изложенному выше подходу, остается рассмотреть вопрос о том, было ли внутригосударственное законодательство доступным и предусматривало ли оно надлежащие и эффективные меры предосторожности и гарантии для удовлетворения требований «предсказуемости» и «необходимости в демократическом обществе».

280. Массовый перехват электронных сигналов в рамках внешней разведки в Швеции регулируется несколькими законами, основными из которых являются следующие: Закон о внешней разведке и соответствующее постановление, Закон и Постановление о радиотехнической разведке, Закон о суде по вопросам внешней разведки, а также закон и Постановление об обработке персональных данных Радиотехническим центром. Соответствующие дополнительные положения, касающиеся, в частности, некоторых аспектов функционирования применимых механизмов надзора и средств правовой защиты, содержатся в Постановлении об инструкциях для Инспекции по надзору, Законе об инструкциях для парламентских омбудсменов и в Законе о надзоре со стороны канцлера юстиции (см. выше §§ 14–74).

281. Доступность указанных положений не оспаривалась. Следовательно, Европейский Суд признает, что законодательство Швеции было достаточно «доступным».

282. Обращаясь к вопросу о том, содержит ли законодательство надлежащие и эффективные меры предосторожности и гарантии для удовлетворения требований «предсказуемости» и «необходимости в демократическом обществе», Европейский Суд в подпунктах (β)–(*ι*) ниже рассмотрит каждое из восьми требований, изложенных выше в § 275.

283. В настоящем деле Европейский Суд проведет анализ одновременно в отношении перехвата содержания электронных сообщений и связанных с ними данных. Подобный подход оправдан тем фактом, который стороны не оспаривают, что в рамках действующего в Швеции режима радиотехнической разведки одни и те же правовые положения, процедуры и гарантии, касающиеся перехвата, удержания, изучения, использования и хранения электронных сигналов, в равной мере применяются как к данным о сообщениях, так и к содержанию сообщений. Следовательно, в рамках действующего в Швеции режима не возникает отдельного вопроса в связи с использованием данных о сообщениях в контексте массового перехвата данных.

(β) Основания, при которых массовый перехват может быть разрешен

284. Как отметила Палата Европейского Суда, согласно Закону о радиотехнической разведке соответствующая разведка может проводиться только для мониторинга:

1) внешних военных угроз для страны;

2) условий участия Швеции в международных миротворческих или гуманитарных миссиях или угроз для безопасности интересов Швеции при выполнении таких операций;

3) стратегических обстоятельств, связанных с международным терроризмом или другими серьезными трансграничными преступлениями, которые могут угрожать важным национальным интересам;

4) разработки и распространения оружия массового поражения, военной техники и иной подобной специальной продукции;

5) серьезных внешних угроз социальной инфраструктуре;

6) внешних конфликтов, имеющих последствия для международной безопасности;

7) операций внешней разведки против интересов Швеции, а также

8) действий или намерений иностранной державы, которые имеют существенное значение для внешней политики, политики безопасности или обороны Швеции (см. выше § 22).

285. Подготовительные материалы к Закону о радиотехнической разведке подробнее раскрывают значение указанных восьми целей (см. выше § 23). По мнению Европейского Суда, уровень детализации и используемые термины описывают область, в которой может использоваться массовый перехват данных, с достаточной ясностью, с учетом, в частности, того, что оспариваемый режим направлен на выявление неизвестных внешних угроз, характер которых может варьироваться и изменяться с течением времени.

286. Европейский Суд отмечает, что, хотя статья 4 Закона о внешней разведке исключает проведение радиотехнической разведки как направления внешней разведки для решения задач в области правоохранительной деятельности или предотвращения преступлений, одна из восьми перечисленных выше целей касается «серьезных трансграничных преступлений», включая (согласно подготовительным материалам) «незаконный оборот наркотических средств или торговля людьми такой степени тяжести, что это может угрожать важным национальным интересам» (см. выше § 23).

287. В подготовительных материалах уточняется, что цель в этом отношении состоит в изучении терроризма и других трансграничных преступлений с точки зрения внешней политики и политики безопасности Швеции, а не оперативной борьбы с преступной деятельностью (см. *ibid*). Не вызывает сомнений, что информация, полученная с помощью оспариваемого режима радиотехнической разведки, не может быть использована в уголовном производстве. Как пояснили власти Швеции, для расследования уголовных преступлений нельзя издавать распоряжения с указанием задач для радиотехнической разведки, а когда Радиотехнический центр передает разведывательные данные другим ведомствам, он оговаривает, что эти данные не могут использоваться в уголовных расследованиях. В свете вышеизложенного Европейский Суд не разделяет опасения заявителя в связи с тем, что с 1 марта 2018 г. некоторые управления полиции могут издавать распоряжения с указанием задач и что Государственной служ-

бе безопасности может быть предоставлен доступ к аналитическим материалам Радиотехнического центра (см. выше § 193, *in fine,* и § 196, *in fine*). Европейский Суд признает убедительными объяснения властей Швеции о том, что доступ может быть предоставлен только к «данным, представляющим собой результаты анализа», с тем, чтобы можно было проводить стратегическую оценку, и что запрет на использование методов радиотехнической разведки как направления внешней разведки в целях расследования уголовных преступлений применяется в полной мере (см. выше § 214).

288. В целом основания, по которым может быть разрешен массовый перехват в Швеции, четко описаны, чтобы обеспечить необходимый контроль на этапе выдачи разрешения и функционирования, а также надзор *ex post facto*.

(γ) Обстоятельства, при которых сообщения отдельных лиц могут подлежать перехвату

289. В рамках режима массового перехвата данных ряд обстоятельств, при которых сообщения могут быть перехвачены, очень широк, поскольку объектом наблюдения являются носители сообщений, а не устройства, с которых отправляются сообщения, равно как и не отправители или получатели сообщений. Ряд обстоятельств, при которых сообщения могут быть проанализированы у́же, но по сравнению с адресным перехватом эта категория всё же является относительно широкой, поскольку массовый перехват данных может использоваться для более разнообразного диапазона целей, а сообщения могут быть выбраны для анализа с учетом иных факторов, отличных от личности отправителя или получателя.

290. Что касается перехвата сообщений, радиотехническая разведка, проводимая с помощью волоконно-оптических проводов, может затрагивать только сообщения, пересекающие границу Швеции. В дополнение, независимо от того, является ли источник сообщений воздушным или кабельным, сообщения между отправителем и получателем, которые находятся в Швеции, не могут быть перехвачены (см. выше § 25). Вместе с тем власти Швеции признали, что на начальных этапах перехвата не всегда можно отделить «внутренний» трафик от «иностранного», что подтверждается в отчете Комитета по радиотехнической разведке за 2011 год (см. выше §§ 77–80; см. также отчеты Инспекции по защите данных, выше в §§ 75–76).

291. Действительно, Радиотехнический центр также вправе перехватывать сигналы в ходе своей деятельности по разработке, что может привести к перехвату данных, не представляющих интерес для стандартной внешней разведки. Из отчета Комитета по радиотехнической разведке (см. выше §§ 77–80) следует, что сигналы, перехваченные в рамках деятельности Радиотехнического центра по разработке, могут быть использованы, в том числе путем «прочтения» и хранения, для технологических разработок независимо от того, относятся ли они к категориям, определенным в восьми целях внешней разведки.

292. Однако Европейский Суд отмечает, что сигналы, перехваченные в рамках деятельности Радиотехнического центра по разработке, представляют интерес для органов власти не с точки зрения данных, которые они могут содержать, а лишь с точки зрения возможностей, которые они предоставляют для анализа систем и путей передачи информации. По мнению Европейского Суда, объяснения властей Швеции о необходимости существования такого механизма (см. выше § 207) являются удовлетворительными. Приведенные примеры (необходимость отслеживать трафик между некоторыми странами для выявления носителей соответствующего трафика; необходимость выявлять тенденции, например, новые виды сигналов и защиты сигналов) представляются убедительными: органы власти должны быть в состоянии реагировать на изменения технологических и коммуникационных практик, вследствие чего может потребоваться мониторинг достаточно больших сегментов международного трафика сигналов. Интенсивность вмешательства в права лиц, предусмотренные статьей 8 Конвенции, в результате такой деятельности представляется весьма низкой с учетом того, что полученные подобным образом данные не соответствуют форме, предназначенной для сбора разведывательной информации.

293. Кроме того, не вызывает сомнений, что любая информация, которая может быть получена на основе сигналов, перехваченных в целях технологических разработок, не может использоваться в качестве разведывательной информации, кроме случаев, когда такое использование соответствует восьми целям и применимым распоряжениям с указанием задач (см. выше § 79). В дополнение к этому деятельность по разработке может осуществляться только на основании разрешения, выданного Судом по вопросам внешней разведки, и контролируется Инспекцией по надзору, в том числе на предмет соблюдения законодательства и распоряжений с указанием задач, утвержденных Судом по вопросам внешней разведки. При таких обстоятельствах Европейский Суд удостоверился в том, что нормативно-правовая база, в рамках которой осуществляется деятельность Радиотехнического центра по разработке, содержит гарантии, способные предотвратить попытки обойти правовые ограничения, связанные с основаниями использования радиотехнической разведки.

294. В свете вышеизложенного Европейский Суд признает, что в правовых положениях о массовом перехвате данных в Швеции достаточно четко указаны обстоятельства, при которых сообщения могут быть перехвачены.

(d) Порядок выдачи разрешения

295. В соответствии с законодательством Швеции на каждое задание в рамках радиотехнической разведки, проводимой Радиотехническим центром, должно быть заранее получено разрешение Суда по вопросам внешней разведки. Если указанная процедура может вызвать задержку или причинить иные неудобства, имеющие существенное значение для одной из целей радиотехнической разведки, Радиотехнический центр может сам выдать разрешение и незамедлительно уведомить об этом Суд по вопросам внешней разведки, который безотлагательно приступает к рассмотрению этого разрешения. Суд по вопросам внешней разведки при необходимости вправе изменить или отменить разрешение (см. выше §§ 30–33).

296. Отсутствуют сомнения в том, что Суд по вопросам внешней разведки отвечает критерию независимости от органов исполнительной власти. В частности, его председатель и вице-председатели являются судьями на постоянной основе, и, хотя все его члены назначаются властями Швеции, срок их полномочий составляет четыре года. Кроме того, не вызывает сомнений, что ни власти Швеции, ни парламент, ни какие-либо иные органы власти не могут вмешиваться в процесс принятия Судом по вопросам внешней разведки решений, которые имеют обязательную силу.

297. Как отметила Палата Европейского Суда, из соображений секретности Суд по вопросам внешней разведки никогда не проводит публичных слушаний, и все его решения имеют конфиденциальный характер. Вместе с тем законодательство Швеции предусматривает обязательное присутствие представителя по вопросам защиты частной жизни на заседаниях Суда по вопросам внешней разведки, за исключением рассмотрения срочных дел. Представитель по вопросам защиты частной жизни, который является судьей, бывшим судьей или адвокатом, действует независимо и в общественных интересах, но не в интересах какого-либо затронутого частного лица. Представитель имеет доступ ко всем материалам дела и может делать заявления (см. выше § 34). По мнению Европейского Суда, с учетом настоятельной необходимости в обеспечении секретности, в частности, на этапах выдачи первоначального разрешения и проведения радиотехнической разведки, описанный выше механизм содержит соответствующие гарантии против произвола и должен рассматриваться как неизбежное ограничение прозрачности процедуры выдачи разрешения.

298. Европейский Суд также отмечает, что, обращаясь за выдачей разрешения, Радиотехнический центр должен указать потребность в искомых разведывательных данных, носители сообщений, к которым необходим доступ, и селекторы или как минимум категории селекторов, которые будут использоваться. Это позволит проанализировать, совместимо ли задание с применимым законодательством, включая восемь целей, для которых может осуществляться радиотехническая разведка, и соразмерен ли сбор разведывательной информации возникающему в результате этого вмешательству в частную жизнь (см. выше §§ 30–33).

299. Важно отметить, что статья 3 Закона о радиотехнической разведке требует, чтобы селекторы были сформулированы таким образом, который ограничивал бы вмешательство в право на личную неприкосновенность, насколько это возможно (см. выше § 26), что предполагает анализ необходимости и соразмерности. Соблюдение этого требования на этапе выдачи разрешения находится в компетенции Суда по вопросам внешней разведки, решение которого, принятое в ходе производства с участием представителя по вопросам защиты частной жизни, является обязательным. Это важная гарантия, предусмотренная действующей в Швеции системой массового перехвата данных.

300. Европейский Суд также отмечает, что законодательство Швеции устанавливает форму специального предварительного разрешения на использование жестких селекторов, которая состоит в том, что Суд по вопросам внешней разведки проверяет, представляет ли применение селекторов, непосредственно связанных с конкретным физическим лицом, «исключительную важность» для разведывательной деятельности, как того требует статья 3 Закона о радиотехнической разведке. Европейский Суд не получил разъяснений относительно толкования статьи 3 Закона о радиотехнической разведке в практике Суда по вопросам внешней разведки, равно как и относительно взаимосвязи статьи 3 со статьей 5 указанного закона, где говорится, что судебное разрешение может как минимум в некоторых случаях касаться «категорий селекторов», а не отдельных селекторов. В подобном случае (то есть, если отдельные селекторы не будут утверждены Судом по вопросам внешней разведки) возникнет вопрос о наличии процедуры предварительного внутреннего разрешения, предусматривающей отдельную и объективную проверку (см. выше § 269). Однако принимая во внимание независимость Суда по вопросам внешней разведки и применимые процессуальные гарантии в рамках производств в этом Суде, стандарт «исключительной важности» на этапе выдачи разрешения может обеспечить соответствующую повышенную защиту от произвольного использования селекторов, связанных с идентифицированными лицами.

301. Системе выдачи разрешения в Швеции присущи некоторые ограничения. Например, Суд по вопросам внешней разведки может испытывать сложности при оценке соразмерности, если в ходатайстве Радиотехнического центра о выдаче разрешения указаны только категории селекторов, или если количество указанных селекторов составляет

несколько тысяч, или если они выражены в виде технических комбинаций цифр или букв.

302. Однако в целях анализа Европейского Суда на этом этапе имеет значение тот факт, что система выдачи разрешений в Швеции предлагает *ex ante* судебную проверку ходатайств о выдаче разрешений, которая является комплексной в том смысле, что цель задания, а также носители и категории подлежащих использованию селекторов проходят контроль, а также она достаточно подробно урегулирована в части секретной массовой радиотехнической разведки как направления внешней разведки. Такая проверка обеспечивает значительную защиту, в частности, от проведения незаконных или явно несоразмерных операций по массовому перехвату данных. Важно отметить, что система выдачи разрешений в Швеции также устанавливает рамки, в которых должна проводиться конкретная операция, и пределы, соблюдение которых впоследствии становится объектом применимых механизмов надзора и контроля *ex post facto*.

(ε) Порядок отбора, изучения и использования перехваченных материалов

303. Из материалов, имеющихся в распоряжении Европейского Суда, следует, что в Швеции перехват электронных сигналов по проводам автоматизирован, а перехват подобных сигналов по воздушным путям может быть как автоматизированным, так и осуществляться вручную. Автоматизированный перехват данных по воздушным путям идентичен процессу перехвата сигналов, проходящих по трансграничным проводам.

304. Что касается использования неавтоматизированного перехвата и поиска электронных сигналов по воздушным путям, власти Швеции в ходе производства по делу в Большой Палате Европейского Суда пояснили, что такой перехват в основном используется для передачи сообщений о военных действиях за границей в режиме, близком к реальному времени, и выполняется оператором, который в режиме реального времени прослушивает военные радиосигналы на выбранных радиочастотах или просматривает экран, где визуализирована энергия сигнала в электронной форме, а затем записывает соответствующие фрагменты для анализа и составления донесений. Заявитель не представил каких-либо комментариев по этому вопросу.

305. Даже если предположить, что перехват иностранных военных радиочастот в редких случаях может затронуть права, предусмотренные статьей 8 Конвенции, Европейский Суд отмечает, что к указанному аспекту режима радиотехнической разведки Швеции применяются те же процедуры и гарантии, что и к перехвату, и использованию проводных сообщений.

306. Обращаясь к порядку изучения перехваченных материалов, Европейский Суд отмечает, что, как пояснили власти Швеции, Радиотехнический центр обрабатывает данные с помощью автоматизированных и ручных средств с применением, среди прочего, криптоанализа, структурирования и перевода с одного языка на другой. Затем аналитик проводит анализ обработанных сведений в целях выявления среди них разведывательных данных. Следующим шагом является составление донесения и его распространение среди выбранных получателей данных внешней разведки (см. выше §§ 18 и 29).

307. По мнению Европейского Суда, важно, что на стадии рассмотрения Радиотехнический центр обязан уничтожать перехваченные внутренние сообщения незамедлительно после их идентификации (см. выше § 38).

308. Несмотря на то, что различие между внутренними и внешними сообщениями не может быть устойчивым и запрет перехватывать первые, очевидно, не может полностью предотвратить такой перехват на автоматическом этапе сбора сигналов, исключение внутреннего трафика из сферы применения радиотехнической разведки следует считать существенным ограничением усмотрения властей и гарантией против злоупотреблений. Указанное ограничение устанавливает пределы, в рамках которых властям разрешено действовать, и дополняет существующие механизмы выдачи предварительного разрешения, надзора и контроля важным критерием, связанным с законностью операции и защитой прав отдельных лиц. В частности, очевидно, что выбор носителей сообщений и категорий селекторов, который подлежит контролю со стороны Суда по вопросам внешней разведки (см. выше § 30), должен отражать указанное выше исключение внутренних сообщений.

309. Как уже отмечалось (см. выше § 300), практика Суда по вопросам внешней разведки, касающаяся выдачи предварительного разрешения на использование селекторов или категорий селекторов, непосредственно связанных с идентифицируемыми лицами, не была предоставлена Европейскому Суду. Вместе с тем Европейский Суд принимает во внимание утверждение властей Швеции о том, что Радиотехнический центр систематически ведет журналы и записи на протяжении всего процесса, начиная с момента сбора данных до составления окончательного донесения, передачи данных другим сторонам и уничтожения. Все поисковые запросы аналитиков фиксируются. Если поиск осуществляется в базе, содержащей персональные данные, в документах отражаются использованные селекторы, время, имя аналитика и обоснование поискового запроса, включая детальное распоряжение с указанием задач, которое служит основанием для проведения поиска. В дополнение к журналам регистрируются решения, принятые в ходе радиотехнической разведки.

310. Заявитель не оспаривал вышеизложенное, однако, по его мнению, (i) не было доказано,

что журналы заполнялись достаточно подробно и (ii) что практика ведения Радиотехническим центром учета, неустановленная на законодательном уровне, подчинялась внутренним процедурам и усмотрению Радиотехнический центр.

311. Европейский Суд считает, что обязанность вести журналы и подробный учет каждого этапа операций по массовому перехвату данных, включая все используемые селекторы, должна быть предусмотрена во внутригосударственном законодательстве. Тот факт, что в Швеции такая обязанность установлена только во внутренних инструкциях, несомненно, является недостатком. Однако с учетом, в частности, механизмов надзора, охватывающих все аспекты деятельности Радиотехнического центра, отсутствуют основания полагать, что подробные журналы и записи на практике не ведутся или что Радиотехнический центр может произвольно изменить свои внутренние инструкции и снять с себя обязательство в этом отношении. В 2010 и 2016 годах Инспекция по защите данных Швеции действительно подвергла критике один из аспектов практики Радиотехнического центра по ведению журналов. Вместе с тем эта критика затрагивала только способ отслеживания Радиотехническим центром журналов для обнаружения неоправданного использования персональных данных (см. выше § 76). Кроме того, власти Швеции пояснили, что с 1 января 2018 г. журналы, которые ранее велись отдельными «владельцами систем» в рамках Радиотехнического центра, направляются в центральное подразделение, что делает их мониторинг более эффективным. Информация об этом изменении была доведена до сведения Инспекции по защите данных Швеции, которая не требовала принятия дополнительных мер и прекратила дело.

312. Законодательство Швеции предусматривает особую защиту персональных данных, включая данные, которые могут раскрывать аспекты частной жизни или коммуникаций физических лиц. В контексте радиотехнической разведки Закон об обработке персональных данных Радиотехническим центром возлагает на Радиотехнический центр обязательство гарантировать, что сбор персональных данных осуществляется только в разрешенных целях, которые прямо предусмотрены в распоряжениях с указанием задач, и в пределах разрешения, выданного Судом по вопросам внешней разведки. Как отметила Палата Европейского Суда, обрабатываемые персональные данные также должны быть достаточными и иметь отношение к цели обработки. Не может быть обработано бóльшее количество персональных данных, чем это необходимо для соответствующей цели. Следует приложить все разумные усилия для исправления, блокировки и удаления персональных данных, которые являются неверными или неполными в отношении преследуемой цели (см. выше § 40). Сотрудники Радиотехнического центра, которые занимаются обработкой персональных данных, проходят официальную процедуру допуска, обязаны соблюдать конфиденциальность и обрабатывать персональные данные безопасным способом. Кроме того, сотрудники могут быть привлечены к уголовной ответственности в случае ненадлежащего выполнения задач, связанных с обработкой персональных данных (см. выше § 42).

313. Заявитель критиковал тот факт, что меры предосторожности, указанные в предыдущем параграфе, применяются только к перехваченным материалам, содержащим «информацию, которая прямо или косвенно затрагивает физическое лицо». На этом основании заявитель сделал вывод о том, что юридическим лицам защита не предоставляется.

314. Европейский Суд, однако, отмечает, что отсутствуют какие-либо причины полагать, что защита, гарантированная Законом об обработке персональных данных Радиотехническим центром и Постановлением об обработке персональных данных Радиотехническим центром, не применяется к содержанию сообщений, которыми обмениваются юридические лица, такие как заявитель, когда эти сообщения содержат «информацию, которая прямо или косвенно затрагивает физическое лицо». Кроме того, следует отметить, что большинство правовых требований и гарантий, предусмотренных в вышеупомянутом законодательстве, как правило, имеют значение только для физических лиц. Например, рассматриваемый закон запрещает обработку персональных данных исключительно на основании того, что известно о расе или этнической принадлежности какого-либо лица, о его или ее политических, религиозных или философских взглядах, членстве в союзе, состоянии здоровья или сексуальной жизни. Закон об обработке персональных данных Радиотехническим центром предусматривает специальное требование, ограничивающее хранение материалов, содержащих персональные данные, и применение санкций в случае ненадлежащего управления данными. Он гарантирует особый порядок мониторинга обработки персональных данных и устанавливает полномочия Инспекции по защите данных в этом отношении. Иными словами, рассматриваемый закон устанавливает еще один уровень защиты с учетом специфики персональных данных в дополнение к уже существующим гарантиям, которые применимы к информации, касающейся как физических, так и юридических лиц.

315. Подобный подход, учитывающий особую важность персональных данных, не представляется проблематичным и не означает, что сообщения юридических лиц не подлежат защите. Вопреки утверждению заявителя, в соответствующем законодательстве нет ничего, что предполагало бы, что перехваченные материалы, не содержащие персональных данных, могут использоваться в целях, несовместимых с первоначальной целью перехва-

та, утвержденной Судом по вопросам внешней разведки.

316. В целом Европейский Суд удостоверился в том, что законодательство об отборе, изучении и использовании перехваченных данных содержит надлежащие гарантии против злоупотреблений, которые могут затронуть права, предусмотренные статьей 8 Конвенции.

(ст) Меры предосторожности при передаче материалов другим лицам

317. Что касается передачи данных от Радио-технического центра другим органам власти Швеции, Европейский Суд отмечает, что сама цель радиотехнической разведки состоит в получении информации, имеющей значение для осуществления соответствующими органами власти своих задач. Круг внутригосударственных органов, которым может быть предоставлена подобная информация в Швеции, ограничен и включает в себя, прежде всего, Государственную службу безопасности и Вооруженные силы. Радиотехнический центр может предоставить указанным органам прямой доступ к данным, которые представляют собой результаты анализа в базе данных, чтобы они могли проводить оценку террористических угроз на стратегическом уровне. Это делается, в частности, в рамках Национального центра оценки террористических угроз – трехсторонней рабочей группы аналитиков Радиотехнического центра, Государственной службы безопасности и Вооруженных сил. По мнению Европейского Суда, описанный режим четко определен и, по всей вероятности, не порождает особого риска злоупотреблений.

318. Европейский Суд также отмечает, что Палата Европейского Суда выразила опасения в отношении действующего в Швеции механизма передачи данных властям иностранных государств или международным организациям, выделив три аспекта: (a) законодательство не требует учета возможного ущерба, причиненного заинтересованному лицу при принятии решения о передаче данных; (b) отсутствуют положения, требующие от государства-получателя или организации-получательницы осуществлять защиту данных посредством тех же или аналогичных гарантий, которые применяются в соответствии с законодательством Швеции; (c) возможность передавать данные, когда это необходимо для «международного сотрудничества в области обороны и безопасности», предполагает достаточно широкую свободу усмотрения. Вместе с тем Палата Европейского Суда сочла, что надзорные механизмы в достаточной мере компенсировали указанные нормативные недостатки (см. § 150 Постановления Палаты Европейского Суда).

319. В ходе производства по делу в Большой Палате Европейского Суда власти Швеции по существу оспорили наличие проблемных аспектов, подчеркнув, что международное сотрудничество ограничивается обменом информацией с доверенными иностранными партнерами и контролируется Инспекцией по надзору. Заявитель, в свою очередь, утверждал, что дискреционные полномочия, предоставленные Радиотехническому центру, были слишком широкими и что существующие механизмы надзора не компенсировали выявленные недостатки, поскольку отсутствовали правовые требования, соблюдение которых можно было бы контролировать (см. более подробное изложение позиций сторон выше в §§ 200, 201, 215 и 216).

320. Прежде всего Европейский Суд отмечает, что в настоящем деле он не рассматривает конкретный случай, например, раскрытия или использования властями иностранного государства или организацией персональных данных, переданных им властями Швеции. В Европейский Суд не поступало сведений о каких-либо случаях такого раскрытия или использования. Тем не менее, поскольку возможность передачи разведывательных данных иностранным сторонам предусмотрена в рамках существующего в Швеции режима и деятельности по массовому перехвату данных, само наличие которых может рассматриваться как вмешательство в права, гарантированные статьей 8 Конвенции, Европейский Суд, принимая во внимание жалобы заявителя, должен проверить действующий в Швеции режим передачи разведывательных данных и его функционирование на предмет их соответствия требованиям качества закона и необходимости в демократическом обществе. Жалобы заявителя касаются исключительно отправки разведывательных данных иностранным сторонам и не затрагивают получение иностранных разведывательных данных и их использование властями Швеции.

321. Не вызывает сомнений, что у государств – участников Конвенции может возникнуть необходимость в передаче иностранным службам разведывательной информации, полученной путем массового перехвата сообщений, по ряду причин, в том числе в целях предупреждения властей иностранных государств об угрозах, обращения к ним за помощью в выявлении и устранении таких угроз или в целях предоставления международным организациям возможности действовать в рамках их мандата. Международное сотрудничество имеет решающее значение для эффективности усилий властей по обнаружению и пресечению потенциальных угроз для национальной безопасности государств – участников Конвенции.

322. Европейский Суд подчеркивает, что возможность Радиотехнического центра обмени-

ваться полученной разведывательной информацией с иностранными партнерами предусмотрена законодательством Швеции, которое также устанавливает соответствующую общую цель (см. выше §§ 49 и 74). Однако следует отметить, что степень обобщенности используемых формулировок неизбежно приводит к выводу о том, что Радиотехнический центр может отправлять разведывательные данные за границу, когда считается, что это соответствует интересам Швеции.

323. Принимая во внимание непредсказуемость ситуаций, которые могут потребовать сотрудничества с иностранными партнерами по внешней разведке, становится понятным, что точные пределы обмена разведывательными данными невозможно ограничить законом, например, путем установления исчерпывающих и подробных перечней таких ситуаций или видов разведывательных данных или информации, которые могут быть переданы. Тем не менее применимое правовое регулирование и правоприменительная практика должны функционировать таким образом, чтобы ограничивать риск злоупотреблений и несоразмерного вмешательства в права, предусмотренные статьей 8 Конвенции.

324. В этом отношении Европейский Суд отмечает, что, во-первых, в той мере, в которой разведывательные данные, передаваемые иностранным службам, принимают форму информации, полученной Радиотехническим центром посредством массового перехвата данных, они заведомо являются продуктом законодательно урегулированных процедур, к которым применяются все соответствующие гарантии. К ним относятся процессуальные гарантии, в частности, разрешение Суда по вопросам внешней разведки и надзор со стороны инспекции (см. выше §§ 295–302 и ниже §§ 345–353), а также ограничения по существу, например, ограничения, касающиеся оснований для разрешения перехвата сигналов, поиск, в частности, с помощью селекторов, идентифицируемого лица, а также весь дальнейший анализ (см. выше §§ 284–288 и 303–316). Как уже отмечалось, указанные выше процедуры предполагают оценку необходимости и соразмерности, в частности, в отношении прав, предусмотренных статьей 8 Конвенции. Следовательно, внутренние гарантии, применяемые в Швеции в процессе получения разведывательных данных, которые впоследствии могут быть переданы иностранным партнерам, также ограничивают, по крайней мере в некоторой степени, риск неблагоприятных последствий, которые могут возникнуть после передачи.

325. Европейский Суд также отмечает, что механизмы надзора, предусмотренные Законом об обработке персональных данных, специально разработанные для защиты персональных данных, применяются ко всей деятельности Радиотехнического центра (см. выше § 56).

326. По мнению Европейского Суда, несмотря на вышеизложенные соображения, отсутствие в соответствующем законодательстве о радиотехнической разведке явно выраженного правового требования к Радиотехническому центру оценивать необходимость и соразмерность обмена разведывательной информацией на предмет его возможного воздействия на права, предусмотренные статьей 8 Конвенции, является существенным недостатком режима массового перехвата данных в Швеции. В результате действия такого законодательства Радиотехнический центр, по-видимому, не обязан принимать какие-либо меры даже в ситуациях, когда, например, в материалах, подлежащих передаче за границу, содержится информация, серьезно ущемляющая права на неприкосновенность частной жизни, но при этом передача такой информации не представляет какой-либо значительной ценности для разведки. Кроме того, хотя власти Швеции явно теряют контроль над переданными материалами после их отправления, у Радиотехнического центра нет каких-либо обязательств проводить анализ и определять, обеспечивает ли иностранный получатель разведывательных данных приемлемый минимальный уровень защиты (см. выше § 276).

327. Ответ властей Швеции на указанные опасения по существу состоял в том, что сотрудничество разведки с иностранными службами неизбежно осуществляется на основе общей заинтересованности в обеспечении секретности информации и что эта практическая реалия ограничивает риски злоупотребления.

328. Европейский Суд считает подобный подход недостаточным в качестве гарантии. Власти Швеции не указали на наличие каких-либо препятствий для того, чтобы четко установить во внутригосударственном законодательстве обязанность Радиотехнического центра или другого соответствующего органа сопоставлять необходимость передачи разведывательных данных за границу с необходимостью защиты права на уважение частной жизни. Для сравнения Европейский Суд отмечает, что, например, соответствующий режим в Соединенном Королевстве предусматривает обязательство принимать разумные меры для того, чтобы удостовериться в том, что власти иностранного государства обеспечивают функционирование необходимых процедур для защиты перехваченных материалов и гарантий того, что они раскрываются, копируются, распространяются и хранятся только в минимально необходимом объеме (см. статью 7.5 Кодекса практики Соединенного Королевства по перехвату сообщений, приведенную в упомянутом выше Постановлении Европейского Суда по делу «Организация Big Brother Watch и другие против Соединенного Королевства» (Big Brother Watch and Others v. United Kingdom), § 96).

329. Действительно, в 2014 году Инспекция по надзору провела общую проверку сотрудничества

Радиотехнического центра с другими государствами, а в период с 2009 по 2017 год она неоднократно проверяла другие соответствующие аспекты ее деятельности, включая обработку персональных данных и передачу отчетов (см. выше § 53). Однако поскольку функция Инспекции по надзору заключается в контроле законности, то в отсутствие явно выраженного правового обязательства Радиотехнического центра учитывать вопросы обеспечения конфиденциальности или добиваться хотя бы некоторых гарантий в этом отношении от иностранных партнеров перед отправлением им разведывательной информации представляется обоснованным полагать, как считает заявитель, что Инспекция по надзору не отслеживает возможные риски или несоразмерные последствия обмена разведывательными данными для прав, предусмотренных статьей 8 Конвенции. Власти Швеции не смогли убедить Европейский Суд в том, что это делается на практике, например, на основании конституционных или других общих положений о защите основных прав. Таким образом, в отличие от Палаты Европейского Суда, Большая Палата Европейского Суда не может согласиться с тем, что недостатки нормативно-правового регулирования в достаточной степени компенсируются надзорными элементами действующего в Швеции режима.

330. В целом отсутствие в Законе о радиотехнической разведке или в другом соответствующем законодательстве требования учитывать заинтересованность соответствующего лица в обеспечении неприкосновенности частной жизни при принятии решения об обмене разведывательными данными является существенным недостатком действующего в Швеции режима, который следует принимать во внимание при оценке Европейским Судом совместимости такого режима со статьей 8 Конвенции.

(ζ) Ограничения продолжительности перехвата, хранения перехваченных материалов и обстоятельства, при которых такие материалы должны быть удалены или уничтожены

331. Решение о продолжительности операций по массовому перехвату данных, разумеется, должны принимать внутригосударственные органы власти. Однако при этом должны быть предусмотрены достаточные гарантии, такие как четкое указание во внутригосударственном законодательстве на период, после которого срок действия разрешения на перехват данных истекает, условия, при которых срок действия разрешения может быть продлен, и обстоятельства, при которых оно должно быть отменено (см. упомянутое выше Постановление Большой Палаты Европейского Суда по делу «Роман Захаров против Российской Федерации» (Roman Zakharov v. Russia), § 250).

332. В соответствии со статьей 5(a) Закона о радиотехнической разведке разрешение может быть выдано на срок, не превышающий шести месяцев. Этот срок может быть продлен каждый раз на шесть месяцев после повторной полной проверки соответствующих условий выдачи разрешения Судом по вопросам внешней разведки. Следовательно, как отметила Палата Европейского Суда, в законодательстве Швеции четко определены период, по истечении которого срок действия разрешения истекает, и условия, при которых он может быть продлен.

333. Однако, что также было отмечено Палатой Европейского Суда, отсутствуют положения, которые бы обязывали Радиотехнический центр, органы власти, уполномоченные издавать детальные распоряжения с указанием задач, или Суд по вопросам внешней разведки отменять задание по проведению радиотехнической разведки, если условия для его выполнения перестали существовать или сами меры более не требуются.

334. В ходе производства по делу в Большой Палате Европейского Суда заявитель утверждал, что отсутствие положений об отмене разрешений, когда необходимость в них отпадает, создает возможности для чрезмерного и ненадлежащего наблюдения в течение нескольких месяцев до тех пор, пока срок действия разрешения не истечет сам по себе. По мнению заявителя, указанный недостаток является существенным с учетом огромного объема информации, которая может быть получена посредством массового перехвата за этот период. Власти Швеции утверждали, что операция по перехвату данных прекращается в случаях, когда в ней пропадает необходимость или когда распоряжение с указанием задач отменено либо если такая операция не соответствует разрешению.

335. По мнению Европейского Суда, прямо выраженное положение о прекращении массового перехвата данных, когда необходимость в нем отпадает, было бы более четким, чем существующие в Швеции механизмы, согласно которым разрешения, по всей видимости, могут отменяться, а могут и не отменяться при наступлении обстоятельств, требующих такой отмены, в период до истечения шестимесячного срока их действия.

336. Однако, как считает Европейский Суд, значение этого недостатка не следует переоценивать по двум основным причинам. Во-первых, законодательство Швеции предусматривает соответствующие механизмы, в частности, возможность запрашивающего органа отменить распоряжение с указанием задач и надзор со стороны Инспекции по надзору. Оба механизма могут привести к отмене операции по массовому перехвату данных, когда условия для нее перестают существовать или когда необходимость в ней отпадает. Во-вторых, в контексте радиотехнической разведки как направления внешней разведки введение правового требования отменять разрешение, когда необходимость в нем отпадает, скорее всего, в силу своего

характера в значительной степени зависит от внутренних оперативных оценок, предполагающих секретность. Соответственно, в особом контексте массового перехвата данных для целей внешней разведки наличие надзорных механизмов, предполагающих доступ ко всей внутренней информации, как правило, следует считать обеспечивающим аналогичные законодательные гарантии против злоупотреблений, связанных с продолжительностью операций по перехвату данных.

337. По изложенным выше соображениям Европейский Суд считает, что законодательство Швеции удовлетворяет требованиям, касающимся продолжительности массового перехвата сообщений.

338. В §§ 145 и 146 своего Постановления Палата Европейского Суда сделала следующие выводы относительно обстоятельств, при которых перехваченные данные должны быть удалены и уничтожены:

> «145. Вопреки утверждению заявителя, несколько положений регулируют ситуации, когда перехваченные данные должны быть уничтожены. Так, разведывательные данные должны быть уничтожены немедленно, если они: 1) касаются конкретного физического лица и были признаны не имеющими значения для целей радиотехнической разведки; 2) защищены конституционными положениями об обеспечении конфиденциальности в целях защиты анонимных авторов и средств массовой информации; 3) содержат информацию, которой обмениваются подозреваемый и его или ее адвокат и на которую вследствие этого распространяется адвокатская тайна, или 4) содержат информацию, предоставленную в религиозном контексте исповеди или индивидуального консультирования, кроме случаев, когда имеются исключительные причины для изучения такой информации… Кроме того, если были перехвачены сообщения между отправителем и получателем, которые находятся в Швеции, несмотря на запрет перехвата таких сообщений, они должны быть уничтожены, как только их внутренний характер станет очевидным… Наконец, если временное разрешение, выданное Радиотехническим центром, было отменено Судом по вопросам внешней разведки, все разведывательные данные, собранные на основании этого разрешения, должны быть немедленно уничтожены…
>
> 146. Хотя Радиотехнический центр вправе хранить базы данных исходных материалов, содержащих персональные данные, в течение периода до одного года, следует помнить о том, что под исходными материалами понимается необработанная информация. Иными словами, такая информация подлежит обработке вручную. Европейский Суд признает необходимость хранения Радиотехническим центром исходных материалов перед их обработкой вручную. При этом Европейский Суд подчеркивает важность удаления этих данных, как только становится очевидным, что они не имеют значения для задач радиотехнической разведки».

339. Большая Палата Европейского Суда в целом поддерживает этот анализ, но считает важным отметить, что у нее недостаточно информации о некоторых аспектах практического применения правил об уничтожении перехваченных материалов.

340. Разумеется, надзорные полномочия Инспекции по надзору охватывают мониторинг практики Радиотехнического центра по уничтожению перехваченных материалов, и указанный аспект ее деятельности уже был предметом проверок (см. выше § 53). Это важная гарантия надлежащего применения существующих правил.

341. Между тем в ходе производства по делу в Большой Палате Европейского Суда заявитель указал, что ограничения срока хранения перехваченных материалов и требования, упомянутые Палатой Европейского Суда в отношении их уничтожения, не применялись к материалам, не содержащим персональных данных. Власти Швеции не прокомментировали отдельно этот вопрос.

342. По мнению Европейского Суда, хотя особые требования в отношении уничтожения материалов, содержащих персональные данные, явно обоснованы, также должна существовать общая правовая норма, регулирующая уничтожение других материалов, полученных путем массового перехвата сообщений, хранение которых может затрагивать, например, право на уважение корреспонденции, предусмотренное статьей 8 Конвенции, в том числе юридических лиц, таких как заявитель. Как минимум, что также подчеркнула Палата Европейского Суда, необходимо наличие правового требования об удалении перехваченных данных, утративших актуальность для целей радиотехнической разведки. Власти Швеции не доказали, что нормативно-правовая база Швеции охватывает этот аспект. Тем не менее отмечая, что лишь в очень ограниченном количестве случаев может произойти так, что ни одно из особых правил уничтожения перехваченных материалов, указанных в предыдущих параграфах, не будет применяться, Европейский Суд признает этот аспект процессуальным недостатком нормативно-правовой базы.

343. Наконец, Европейский Суд не располагает достаточной информацией о том, каким образом необходимость хранить или уничтожать материалы, содержащие персональные данные, оценивается на практике, а также о том, всегда ли необработанные перехваченные материалы хранятся в течение максимального срока продолжительностью в один год или необходимость дальнейшего хранения регулярно пересматривается, как это и должно быть. В результате представляется затруднительным сделать исчерпывающие выводы, охватывающие все аспекты хранения и удаления перехваченных материалов. В контексте своего анализа проверки *ex post facto* в рамках действующей в Швеции системы массового перехвата данных Европейский Суд вернется к вопросу о том, какие выводы можно сделать с учетом отсутствия у него достаточной

информации по вышеуказанному вопросу и иным аспектам функционирования шведской системы.

344. Таким образом, для целей настоящего этапа анализа, хотя Европейский Суд в предыдущем параграфе отметил процессуальный недостаток, который необходимо устранить, он считает, что в целом обстоятельства, при которых перехваченные материалы подлежат уничтожению, четко определены в законодательстве Швеции.

(η) Надзор

345. В соответствии с законодательством Швеции задача осуществления надзора за деятельностью внешней разведки в целом и радиотехнической разведки в частности возложена в основном на Инспекцию по надзору. Дополнительные надзорные функции, хотя и с меньшими полномочиями, выполняет Инспекция по защите данных.

346. Отмечая, что совет Инспекции по надзору возглавляют постоянные судьи или бывшие судьи и что его члены, назначаемые властями Швеции на срок не менее четырех лет, избираются из кандидатов, предложенных партийными группами в парламенте, Европейский Суд удостоверился в том, что она осуществляет свои функции в качестве независимого надзорного механизма.

347. Инспекция наделена широкими полномочиями, охватывающими все виды деятельности по радиотехнической разведке, от начала до конца. Среди прочего ей поручено предоставлять Радиотехническому центру доступ к носителям сообщений после проверки того, что запрашиваемый доступ соответствует разрешению, выданному Судом по вопросам внешней разведки (статья 19(a) главы 6 Закона об электронной коммуникации). Инспекция рассматривает прочие аспекты деятельности Радиотехнического центра, включая перехват, анализ, использование и уничтожение материалов. Важно отметить, что она вправе изучать используемые селекторы (статья 10 Закона о радио-технической разведке) и имеет доступ ко всем соответствующим документам Радиотехнического центра (см. выше §§ 50–53).

348. Таким образом, представляется, что Инспекция по надзору имеет полномочия и инструменты, необходимые для оценки не только соблюдения формальных требований законодательства Швеции, но и для изучения аспектов соразмерности вмешательства в индивидуальные права, которое может быть связано с деятельностью по радиотехнической разведке. В связи с этим следует отметить, что в ходе своих проверок Инспекция по надзору также подробно изучала, в частности, используемые селекторы (см. выше § 53).

349. Заявитель отметил, что некоторые акты, изданные Инспекцией по надзору, имеют форму заключений и рекомендаций, а не юридически обязательных решений. По-видимому, он полагал, что это существенно ослабляло ее реальное влияние работы.

350. Европейский Суд отмечает, что согласно статье 10 Закона о радиотехнической разведке при обнаружении доказательств ненадлежащего сбора сигналов Инспекция по надзору вправе принять юридически обязательное решение о прекращении сбора данных или об уничтожении записей или документов, содержащих собранные данные. Что касается некоторых других вопросов, таких как потенциальная гражданско-правовая ответственность властей в отношении лица или организации либо наличие указаний на возможное совершение уголовного преступления, Инспекция по надзору обязана уведомлять компетентные органы, которые наделены полномочиями принимать юридически обязательные решения. Европейский Суд считает описанный механизм удовлетворительным. Хотя законодательство Швеции, по-видимому, действительно не предусматривает юридической возможности для исполнения рекомендаций Инспекции по надзору, направленных на развитие или корректировку деятельности радиотехнического центра, Европейский Суд отмечает, что согласно заключениям Государственного ревизионного управления, которое проводило проверку деятельности этой Инспекции в 2015 году, Радиотехнический центр внедрил практики обработки ее заключений. Более того, ее предложения рассматривались серьезно и приводили к необходимым изменениям, если этого требовала ситуация. Меры, определенные Инспекцией по надзору, были приняты, за исключением одного случая, когда Радиотехнический центр передал дело властям Швеции (см. выше § 54).

351. Имеющаяся у Европейского Суда информация о проверках, проведенных Инспекцией по надзору, подтверждает, что она не только теоретически, но и на практике активно проверяет деятельность Радиотехнического центра как на общей систематической основе, так и целевым образом. В частности, за восемь лет Инспекция по надзору провела 102 проверки, включая подробное изучение использованных селекторов, процедур уничтожения разведывательных данных, передачи отчетов, сотрудничества с другими государствами и международными организациями, обработки персональных данных, а также проверку общего соблюдения законодательства, директив и разрешений, относящихся к деятельности по радиотехнической разведке. В результате этих проверок было подготовлено несколько заключений и предложений для Радиотехнического центра, одно заключение было направлено властям Швеции. В качестве иллюстрации влияния работы Инспекции по надзору можно привести тот факт, что, когда, например, в 2011 году она предложила внести некоторые изменения во внутренние правила Радиотехнического центра, касающиеся унич-

тожения данных, это было сделано в том же году (см. выше § 53).

352. Наконец, Инспекция по надзору издает ежегодные отчеты, которые доступны для всеобщего ознакомления, а ее деятельность подлежит проверке со стороны Государственного ревизионного управления (см. выше §§ 53 и 54).

353. При таких обстоятельствах отсутствуют основания сомневаться в том, что законодательство и правоприменительная практика Швеции обеспечивают эффективный надзор за деятельностью в области радиотехнической разведки в Швеции. Европейский Суд считает, что функции Инспекции в сочетании с судебной процедурой получения предварительного разрешения в Суде по вопросам внешней разведки формируют эффективную защиту от злоупотреблений на важнейших этапах процесса радиотехнической разведки: до и в процессе перехвата, в ходе анализа, использования и уничтожения полученной информации.

(θ) Проверка ex post facto

354. Стороны, по-видимому, не оспаривают, что предусмотренная Законом о радиотехнической разведке теоретическая возможность уведомлять физических лиц о применении непосредственно связанных с ними селекторов никогда не использовалась на практике по соображениям секретности (см. выше §§ 58, 59, 75, *in fine,* и 80).

355. По мнению Европейского Суда, очевидно, что уведомление затронутых лиц в контексте действующей в Швеции системы радиотехнической разведки как направления внешней разведки, если это вообще технически возможно, может иметь далеко идущие последствия, которые трудно предвидеть заранее. Как отмечалось выше (см. выше § 272), в контексте массового перехвата данных эффективным средством правовой защиты могло бы стать такое средство правовой защиты, которое не зависит от уведомления объекта перехвата. Соответственно, Европейский Суд признает законным подход властей государства-ответчика в этом отношении. В то же время отсутствие функционирующего механизма уведомления должно компенсироваться эффективностью средств правовой защиты, которые должны быть доступны лицам, подозревающим, что их сообщения могли подвергнуться перехвату и анализу.

356. В связи с этим Европейский Суд отмечает, что Закон о радиотехнической разведке предусматривает проверку *ex post facto* по инициативе физических или юридических лиц без необходимости доказывать, что они могли подвергнуться массовому перехвату данных. В порядке реагирования на обращение любого лица, независимо от его гражданства и места жительства, Инспекция по надзору должна расследовать, были ли сообщения такого лица перехвачены посредством радиотехнической разведки, и, если это так, проверить, соответствовали ли перехват и обработка информации закону. Как уже отмечалось (см. выше § 350), Инспекция по надзору вправе принять решение о прекращении операции по радиотехнической разведке или об уничтожении разведывательных данных.

357. Заявитель отметил, что у лица отсутствует возможность получить информацию о том, действительно ли его сообщения были перехвачены, или в целом получить мотивированные решения. В соответствии с применимым законодательством Швеции Инспекция по надзору информирует заявителя только о проведении расследования (см. выше § 61).

358. Из материалов, имеющихся в распоряжении Европейского Суда (см., в частности, выше §§ 61 и 203), следует, что Инспекция по надзору регулярно рассматривает обращения отдельных лиц.

359. Тем не менее, хотя Инспекция по надзору действительно является независимым органом, Европейский Суд отмечает, что, принимая во внимание обязанность этого органа по надзору и мониторингу за деятельностью Радиотехнического центра, что предполагает принятие или санкционирование оперативных решений, в частности, касающихся доступа к носителям сигналов, использования селекторов, анализа, использования и уничтожения перехваченных материалов (см. выше §§ 50–53), дополнительная функция Инспекции по проведению проверки *ex post facto* на основании обращения отдельных лиц может привести к ситуациям, когда ей придется оценивать свою собственную деятельность по надзору за операциями Радиотехнического центра по массовому перехвату данных. В условиях секретности, которые служат правомерной характеристикой соответствующих процедур, и в отсутствие правового обязательства Инспекции по надзору объяснять причины заинтересованному лицу могут возникнуть сомнения относительно того, обеспечивает ли рассмотрение Инспекцией по надзору индивидуальных жалоб в таких ситуациях надлежащие гарантии объективности и тщательности. Нельзя исключать, что ее двоякое положение может вызвать конфликт интересов и, следовательно, соблазн пропустить упущение или проступок, чтобы избежать критики или иных последствий.

360. В этом отношении Европейский Суд принимает во внимание тот факт, что деятельность самой Инспекции по надзору подлежит проверке (см. выше § 54), что в принципе можно считать соответствующей гарантией. Однако он отмечает, что власти Швеции не представили какой-либо информации, которая свидетельствовала бы о том, что проведенные до сих пор проверки охватывали расследования, проводимые Инспекцией по надзору по обращениям лиц, запрашивающих информацию о том, были ли их

сообщения перехвачены Радиотехническим центром. По-видимому, у Государственного ревизионного управления, которое отвечает за проверку значительного числа административных органов в различных секторах, отсутствует правовое обязательство проводить такие специальные проверки и делать это на регулярной основе. В указанных обстоятельствах и с учетом структурного недостатка, отмеченного в предыдущем параграфе, Европейский Суд не убежден в том, что потенциальная возможность проверки рассмотрения Инспекцией по надзору жалоб отдельных лиц со стороны Государственного ревизионного управления является достаточной.

361. Кроме того, по мнению Европейского Суда, система проверки *ex post facto*, которая не дает обоснованных решений в ответ на жалобы, поданные отдельными лицами, или как минимум решений, содержащих причины, доступ к которым мог бы быть предоставлен специальному советнику, прошедшему официальную процедуру допуска, слишком сильно зависит от инициативы и настойчивости назначенных должностных лиц, неподконтрольных общественности. Что касается действующей в Швеции системы, Европейский Суд отмечает, что заявителю не сообщается каких-либо подробностей относительно содержания и результатов расследования, проводимого Инспекцией по надзору, и, следовательно, ей, по-видимому, предоставлены широкие дискреционные полномочия. Мотивированное решение имеет неоспоримое преимущество, поскольку предлагает общедоступные рекомендации по толкованию применимых правовых норм, по ограничениям, которые необходимо соблюдать, и по способу согласования публичных интересов и прав отдельных лиц в особом контексте массового перехвата сообщений. Как отметил Европейский Суд в упомянутом выше Постановлении по делу «Кеннеди против Соединенного Королевства» (Kennedy v. United Kingdom) (§ 167), публикация подобных правовых позиций повышала тщательность проверок в этой области. Изложенные соображения приводят Европейский Суд к выводу, что упомянутые выше особенности действующей в Швеции системы не содержат достаточных оснований для уверенности общественности в том, что нарушения при их наличии будут выявлены и устранены.

362. Действительно, отдельные лица могут обращаться к парламентским омбудсменам и канцлеру юстиции, которые могут проверить действия властей на предмет, *inter alia*, законности и возможного посягательства на основные права и свободы. Канцлер юстиции и омбудсмены вправе возбуждать уголовное или дисциплинарное производство (см. выше §§ 66–68). Хотя указанные механизмы подачи жалоб являются значимыми, Европейский Суд отмечает, что они, по всей видимости, редко используются в контексте массового перехвата сообщений (см. выше § 67, *in fine*). В любом случае Европейский Суд полагает, что судебная процедура в независимом органе, который, насколько это возможно, проводит состязательный процесс, приводящий к принятию обоснованных и юридически обязательных решений, является важным элементом эффективной проверки *ex post facto*. Однако ни канцлер юстиции, ни омбудсмены не соответствуют этим требованиям.

363. Наконец, Европейский Суд согласен с заявителем в том, что доступное в Соединенном Королевстве средство правовой защиты в виде процедуры в Следственном трибунале (см. упомянутое выше Постановление Европейского Суда по делу «Организация Big Brother Watch и другие против Соединенного Королевства» (Big Brother Watch and Others v. United Kingdom), §§ 413–415) иллюстрирует возможность согласовывать законные интересы в обеспечении безопасности и необходимость обеспечения надежной проверки *ex post facto* в отношении деятельности по массовому перехвату данных.

364. В целом двоякое положение Инспекции по надзору и отсутствие у представителей общественности возможности получить мотивированные решения в той или иной форме в ответ на обращения или жалобы в связи с массовым перехватом сообщений – элементы, которые не соответствуют требованиям эффективной проверки *ex post facto*, – следует рассматривать как недостаток действующего в Швеции режима, который Европейскому Суду необходимо принимать во внимание при оценке его совместимости со статьей 8 Конвенции. По мнению Европейского Суда, вышеупомянутый недостаток имеет особое значение, принимая во внимание то обстоятельство, что Европейский Суд не располагает достаточной информацией о практике Суда по вопросам внешней разведки в части вынесения предварительного разрешения на использование жестких селекторов или категорий селекторов (см. выше § 300) и в отношении порядка практического применения правовых требований по уничтожению перехваченных материалов (см. выше § 343). Это, несомненно, усиливает неуверенность заинтересованных лиц относительно возможности произвола или злоупотреблений в отношении них.

(i) Вывод

365. Европейский Суд убежден в том, что массовый перехват данных имеет важное значение для государств – участников Конвенции при выявлении угроз для их национальной безопасности. Это было признано, в частности, Венецианской комиссией (см. выше § 86). В современных условиях, по-видимому, какие-либо альтернативы или их сочетание будут недостаточными для того,

чтобы заменить возможности массового перехвата данных.

366. Европейский Суд также напоминает, что в его задачу входит не установление идеальной модели радиотехнической разведки, а, скорее, проверка существующих правовых и практических механизмов, которые концептуально и функционально отличаются в разных государствах – участниках Конвенции, на предмет их соответствия Конвенции. В рамках этой задачи существующая в Швеции модель радиотехнической разведки и предлагаемые ею гарантии защиты от злоупотреблений должны рассматриваться как единое целое.

367. Проверка существующей в Швеции системы массового перехвата данных в настоящем деле показала, что такая система основана на детально прописанных правовых нормах, имеет четко ограниченные пределы и предоставляет соответствующие гарантии. Основания, на которых может быть разрешен массовый перехват данных в Швеции, четко определены, обстоятельства, при которых сообщения могут быть перехвачены и изучены, изложены с достаточной ясностью, продолжительность перехвата данных регулируется и контролируется законом, а процедуры отбора, изучения и использования перехваченных материалов сопровождаются надлежащими гарантиями от злоупотреблений. Одинаковые меры защиты в равной степени применяются к содержанию перехваченных сообщений и к данным о сообщениях.

368. Важно отметить, что предусмотренная в Швеции процедура получения предварительного судебного разрешения и надзор со стороны независимого органа в принципе призваны гарантировать практическое применение требований внутригосударственного законодательства и стандартов Конвенции и ограничивать риск несоразмерных последствий, затрагивающих права, предусмотренные статьей 8 Конвенции. В частности, следует отметить, что в Швеции пределы каждой задачи по массовому перехвату данных, а также ее законность и соразмерность в целом являются предметом производства по выдаче предварительного судебного разрешения в Суде по вопросам внешней разведки, в заседаниях которого принимает участие представитель по вопросам защиты частной жизни, защищающий общественные интересы.

369. Европейский Суд выявил три недостатка существующего в Швеции режима массового перехвата данных: отсутствие четкой нормы об уничтожении перехваченных материалов, не содержащих персональные данные (см. выше § 342); отсутствие в Законе о радиотехнической разведке или в ином соответствующем законодательстве требования о том, чтобы при принятии решения о передаче разведывательных материалов иностранным партнерам учитывались интересы отдельных лиц в обеспечении защиты частной жизни (см. выше §§ 326–330); отсутствие эффективной проверки *ex post facto* (см. выше §§ 359–364).

370. Что касается первого из указанных недостатков, то вероятность того, что он приведет к неблагоприятным последствиям для прав, предусмотренных статьей 8 Конвенции, ограничивается наличием в законодательстве Швеции четких норм об уничтожении перехваченных материалов в ряде обстоятельств и, прежде всего, когда они содержат персональные данные.

371. Однако Европейский Суд считает, что второй недостаток потенциально может привести к достаточно серьезным неблагоприятным последствиям для затронутых физических лиц или организаций. Как отмечалось выше, указанный недостаток позволяет механически передавать за границу информацию, серьезно ущемляющую право на неприкосновенность частной жизни или право на уважение корреспонденции, даже если ее значение для разведывательной деятельности невелико. Следовательно, подобная передача данных может создавать явно несоразмерные риски для прав, предусмотренных статьей 8 Конвенции. Кроме того, на Радиотехнический центр не возлагается каких-либо обязательств анализировать и устанавливать, обеспечивает ли иностранный получатель разведывательных данных приемлемый минимальный уровень гарантий.

372. Наконец, двоякое положение Инспекции по надзору и отсутствие у представителей общественности возможности получить мотивированные решения в той или иной форме в ответ на обращения или жалобы в связи с массовым перехватом сообщений ослабляют механизм контроля *ex post facto* в такой степени, что это создает риски для соблюдения основных прав затронутых лиц. Кроме того, отсутствие эффективной проверки на последнем этапе процесса перехвата данных не согласуется с позицией Европейского Суда, согласно которой степень вмешательства в права отдельных лиц, предусмотренные статьей 8 Конвенции, возрастает по мере продвижения процесса (см. выше §§ 239 и 245) и не соответствует требованию наличия «сквозных» гарантий (см. выше § 264).

373. Европейский Суд удостоверился в том, что основные характеристики существующего в Швеции режима массового перехвата данных соответствуют требованиям Конвенции в части качества закона, и, следовательно, считает, что функционирование этого режима на момент рассмотрения дела Палатой Европейского Суда в большинстве аспектов находилось в пределах того, что «необходимо в демократическом обществе». Однако, по его мнению, недостатки, описанные в предыдущих параграфах, не в должной мере компенсируются имеющимися гарантиями, и, таким образом, действующий в Швеции режим массового перехвата данных выходит за пре-

делы усмотрения, предоставленные властям государства-ответчика в этом отношении. Европейский Суд напоминает, что режим массового перехвата имеет значительный потенциал для злоупотреблений, которые отрицательно скажутся на праве лиц на уважение их частной жизни (см. выше § 261). Таким образом, принимая во внимание принцип верховенства права, который прямо указан в Преамбуле к Конвенции и воплощен в объекте и цели статьи 8 Конвенции (см. упомянутое выше Постановление Большой Палаты Европейского Суда по делу «Роман Захаров против Российской Федерации» (Roman Zakharov v. Russia), § 228), Европейский Суд считает, что действующий в Швеции режим массового перехвата данных, рассматриваемый в целом, не содержит достаточных «сквозных» гарантий, чтобы обеспечивать надлежащую и эффективную защиту от произвола и риска злоупотреблений.

(d) Вывод в соответствии со статьей 8 Конвенции

374. Принимая во внимание сделанный выше вывод относительно законности и обоснованности оспариваемого режима массового перехвата данных, Европейский Суд считает, что в настоящем деле имело место нарушение статьи 8 Конвенции.

III. ПРЕДПОЛАГАЕМОЕ НАРУШЕНИЕ СТАТЬИ 13 КОНВЕНЦИИ

375. Заявитель жаловался на то, что средства правовой защиты, доступные в рамках действующего в Швеции режима массового перехвата данных, были недостаточными и не соответствовали требованиям статьи 13 Конвенции, которая гласит:

> «Каждый, чьи права и свободы, признанные в настоящей Конвенции, нарушены, имеет право на эффективное средство правовой защиты в государственном органе, даже если это нарушение было совершено лицами, действовавшими в официальном качестве».

376. Палата Европейского Суда постановила, что не возникает отдельного вопроса в соответствии с указанным положением Конвенции (см. § 184 Постановления Палаты Европейского Суда).

377. Большая Палата Европейского Суда приходит к такому же выводу с учетом установления факта нарушения статьи 8 Конвенции.

IV. ПРИМЕНЕНИЕ СТАТЬИ 41 КОНВЕНЦИИ

378. Статья 41 Конвенции гласит:

> «Если Суд объявляет, что имело место нарушение Конвенции или Протоколов к ней, а внутреннее право Высокой Договаривающейся Стороны допускает возможность лишь частичного устранения последствий этого нарушения, Суд, в случае необходимости, присуждает справедливую компенсацию потерпевшей стороне».

A. Ущерб

379. Заявитель отметил, что установление факта нарушения будет являться достаточной компенсацией. Власти Швеции согласились с этим.

380. Соответственно, Европейский Суд не присуждает какой-либо компенсации по данному основанию.

B. Расходы и издержки

381. Заявитель требовал выплатить ему 544 734 шведских крон в качестве компенсации за 217 часов юридической работы в рамках производства в Палате Европейского Суда и за 190 часов юридической работы в ходе производства в Большой Палате Европейского Суда (всего 407 часов) по часовой ставке, равной 1 302–1 380 шведских крон.

382. Заявитель также требовал компенсации расходов на проезд и проживание трех его представителей в связи с их участием в слушании по делу в Большой Палате Европейского Суда 10 июля 2019 г. Указанные расходы составляли 8 669 шведских крон за авиабилеты и 8 231 шведскую крону за размещение в отеле (всего 16 900 шведских крон). Заявитель предоставил копии соответствующих счетов.

383. Следовательно, общая сумма компенсации, требуемая заявителем, составила 561 634 шведских крон (что эквивалентно примерно 52 625 евро).

384. Власти Швеции не возражали против требований заявителя, но сочли, что, если будет установлено нарушение только одной из статей Конвенции, указанных в жалобе, компенсация должна быть соответственно уменьшена.

385. В соответствии с прецедентной практикой Европейского Суда заявитель имеет право на возмещение судебных расходов и издержек только в той части, в которой было доказано, что они были действительно понесены, являлись необходимыми и разумными по размеру. В настоящем деле, принимая во внимание предоставленные ему материалы, вышеизложенные критерии и отмечая в дополнение, что нарушение Конвенции было установлено в связи с основной жалобой заявителя, в соответствии со статьей 8 Конвенции, Европейский Суд считает разумным присудить заявителю 52 625 евро в качестве возмещения всех судебных расходов и издержек.

C. Процентная ставка при просрочке платежей

386. Европейский Суд полагает, что процентная ставка при просрочке платежей должна определяться исходя из предельной кредитной ставки

Европейского центрального банка плюс три процентных пункта.

На основании изложенного Большая Палата Европейского Суда:

1) *отклонила* единогласно предварительное возражение властей государства-ответчика относительно статуса жертвы заявителя;

2) *постановила* 15 голосами «за» при двух – «против», что имело место нарушение требований статьи 8 Конвенции;

3) *постановила* единогласно, что отсутствует необходимость отдельно рассматривать жалобу заявителя в соответствии со статьей 13 Конвенции;

4) *постановила* единогласно, что:

(a) власти государства-ответчика обязаны в течение трех месяцев выплатить заявителю 52 625 евро, а также любой налог, который может быть начислен на указанную сумму, в качестве компенсации судебных расходов и издержек; данная сумма подлежит переводу в валюту государства-ответчика по курсу, действующему на день выплаты;

(b) с даты истечения указанного трехмесячного срока и до момента выплаты на указанную сумму должны начисляться простые проценты, размер которых определяется предельной кредитной ставкой Европейского центрального банка, действующей в период неуплаты, плюс три процентных пункта.

Совершено на английском и французском языках, вынесено на слушании 25 мая 2021 г. в соответствии с пунктами 2 и 3 правила 77 Регламента Европейского Суда.

Сёрен ПРЕБЕНСЕН	Роберт СПАНО
Заместитель Секретаря	Председатель
Большой Палаты Суда	Большой Палаты Суда

В соответствии с пунктом 2 статьи 45 Конвенции и пунктом 2 правила 74 Регламента Европейского Суда к настоящему Постановлению прилагаются следующие отдельные мнения судей:

(a) совместное совпадающее мнение судей Пауля Лемменса, Фариса Вехабовича и Марко Бошняка;

(b) совпадающее мнение судьи Пауло Пинто де Альбукерке;

(c) совместная декларация о голосовании судей Йона Фридрика Кьёльбро и Эрика Веннерстрёма.

СОВМЕСТНОЕ СОВПАДАЮЩЕЕ МНЕНИЕ СУДЕЙ ПАУЛЯ ЛЕММЕНСА, ФАРИСА ВЕХАБОВИЧА И МАРКО БОШНЯКА

В настоящем деле мы голосовали совместно с большинством судей по всем пунктам резолютивной части. Как и в связанном деле «Организация Big Brother Watch и другие против Соединенного Королевства» (Big Brother Watch and Others v. United Kingdom) (жалобы №№ 58170/13, 62322/14 и 24969/15), мы полагаем, что настоящее Постановление должно идти значительно дальше в подтверждении важности защиты частной жизни и корреспонденции, в частности, посредством введения более строгих минимальных гарантий, а также путем более строгого применения таких гарантий к оспариваемому режиму массового перехвата данных. Доводы, приведенные в нашем совпадающем мнении по упомянутому делу, в значительной степени применимы и в настоящем деле. Во избежание излишнего повторения мы предлагаем обратиться к указанному отдельному мнению. В той мере, в которой некоторые его параграфы не имеют отношения к настоящему делу ввиду различий в нормативно-правовой базе двух режимов массового перехвата данных, их следует просто игнорировать как не относящиеся к делу.

СОВПАДАЮЩЕЕ МНЕНИЕ СУДЬИ ПАУЛО ПИНТО ДЕ АЛЬБУКЕРКЕ

1. Я голосовал совместно с большинством судей, но совсем по иным причинам. Нормативно-правовая база Швеции во многих отношениях вызывает вопросы, которые большинство судей проигнорировали либо важность которых они преуменьшили. Внутригосударственная правоприменительная практика еще более проблематична. Фактически внутригосударственная правоприменительная практика еще менее ясна, чем практика Соединенного Королевства. Однако Европейский Суд по правам человека (далее – Европейский Суд) разрешил дело, не осознавая важные аспекты такой практики, в частности, актуальную практику ведения журналов и подробной документации по каждому этапу процесса массового перехвата данных. На удивление власти Швеции были освобождены от обязанности представлять доказательства своих утверждений, поскольку Европейский Суд просто исходил из действительности утверждений властей Швеции[1]. Еще более озадачивает тот факт, что Европейский Суд даже не имел доступа к соответствующей прецедентной практике компетентного суда Швеции в области массового перехвата данных, игнорируя, например, фактическое толкование статьи 3 Закона о радиотехнической

[1] См. § 311 настоящего Постановления: «отсутствуют основания полагать, что подробные журналы и записи на практике не ведутся или что Радиотехнический центр может произвольно изменить свои внутренние инструкции и снять с себя обязательство в этом отношении».

разведке Судом по вопросам внешней разведки[1]. Как и в Постановлении по делу «Организация Big Brother Watch и другие против Соединенного Королевства» (Big Brother Watch and Others v. United Kingdom) (жалобы №№ 58170/13, 62322/14 и 24969/15), пристрастная методология Европейского Суда в совокупности с размытыми формулировками привела к несовершенному режиму гарантий в настоящем деле[2].

Правовые цели массового перехвата данных

2. Первым крупным недостатком действующего в Швеции режима является отсутствие предсказуемости относительно правовых целей массового перехвата данных, как они изложены в Законе о радиотехнической разведке. Цель, связанная с внешними военными угрозами для страны, может включать в себя «не только неминуемые угрозы, такие как угроза вторжения, но и явления, которые в долгосрочной перспективе могут перерасти в угрозы безопасности»[3]. Это в высшей степени неопределенная цель как в части временного, так и пространственного измерения, которая позволяет составлять профили иностранцев, членов меньшинств и законно действующих организаций, которые могут рассматриваться как потенциальные угрозы в долгосрочной перспективе.

3. Цель, связанная со фундаментальным изучением международного терроризма или других серьезных трансграничных преступлений, которые могут угрожать важным национальным интересам, включая «незаконный оборот наркотических средств или торговлю людьми такой степени тяжести, что это может угрожать важным национальным интересам»[4], не определяет в достаточной степени серьезные трансграничные преступления. Понятие «серьезные преступления» в международном праве охватывает преступления, которые наказываются лишением свободы на срок четыре года или более[5]. Таким образом, чтобы считаться предсказуемым, понятие серьезных преступлений, которые могут повлечь за собой применение режима массового перехвата данных, должно быть связано с перечнем конкретных серьезных преступлений или в целом с преступлениями, наказуемыми лишением свободы на срок четыре года или более. Не так обстоит дело в Швеции.

4. Цель, связанная с разработкой или распространением оружия массового поражения, военной техники и другой подобной специальной продукции, может включать в себя «среди прочего, деятельность, имеющую отношение к обязательствам Швеции в части нераспространения и экспортного контроля оружия массового поражения, даже в тех случаях, когда такая деятельность не является преступлением или не противоречит международным конвенциям»[6]. По информации, официально предоставленной властями Швеции[7], к «подобной специальной продукции» относятся боеприпасы, военная и гражданская продукция двойного назначения и даже техническое содействие, как предусмотрено в Законе № 1064(2000) «О контроле продукции двойного назначения и техническом содействии». Однако контролируемые виды деятельности («среди прочего») не определены в достаточной степени. Охватывает ли указанная цель экономический и торговый шпионаж в интересах шведской оружейной, аэрокосмической, электронной, нефтехимической и другой обрабатывающей промышленности?

5. Цель, связанная с серьезными внешними угрозами социальной инфраструктуре, «включает, среди прочего, серьезные угрозы, связанные с информационными технологиями, которые исходят из-за границы. Серьезный характер угроз означает, например, что они должны быть направлены на жизненно важные общественные системы энерго- и водоснабжения, связи или финансовых услуг»[8]. Ни виды угроз («среди прочего»), ни системы социальной инфраструктуры, которые могут находиться под угрозой («например»), не разграничены в достаточной степени. Означает ли эта цель, например, что всеобщая забастовка в соседней стране, которая в итоге может нарушить функционирование и дестабилизировать шведскую систему распределения энергии или нефти, может оправдать наблюдение за профсоюзами, участвовавшими в забастовке, и их членами? Что если предполагаемая «угроза» направлена против систем общественного транспорта и спорта Швеции? Оправдывает ли массовый приезд иностранных футбольных фанатов на футбольный чемпионат в Швеции наблюдение за всеми футбольны-

[1] См. § 300 настоящего Постановления: «Европейский Суд не получил разъяснений относительно толкования статьи 3 Закона о радиотехнической разведке в практике Суда по вопросам внешней разведки…». Я вернусь к этому пункту ниже.

[2] Критика *pro autoritate* подхода Европейского Суда к режиму массового перехвата данных изложена в моем мнении, приложенном к упомянутому выше Постановлению по делу «Организация Big Brother Watch и другие против Соединенного Королевства» (Big Brother Watch and Others v. United Kingdom).

[3] См. § 23 настоящего Постановления.

[4] *Ibid*.

[5] В пункте «b» статьи 2 Конвенции ООН против транснациональной организованной преступности «серьезное преступление» определено как преступление, наказуемое лишением свободы на максимальный срок не менее четырех лет или более строгой мерой наказания. Тот же подход принят в Пояснительном докладе к Рекомендации Комитета Министров Совета Европы государствам-членам № Rec(2005)10 (см. § 20 Пояснительного доклада).

[6] См. § 23 настоящего Постановления.

[7] См.: https://www.loc.gov/law/help/foreign-intelligence-gathering/sweden.php#Signal

[8] См. § 23 настоящего Постановления.

ми фанатами из стран, участвующих в чемпионате?

6. Цель, связанная с действиями или намерениями иностранной державы, которые имеют существенное значение для внешней политики, политики безопасности или обороны Швеции, формулируется очень широко. Уточняется «недостаточность того, чтобы явление представляло общий интерес, напротив, разведывательные данные должны оказывать непосредственное воздействие на действия или позицию Швеции по различным вопросам внешней политики, политики безопасности или обороны»[1]. Тем не менее этого уточнения недостаточно, поскольку оно не разграничивает порог существенности и конкретные затронутые предметные области. Беспокойство вызывает и тот факт, что даже «намерения» иностранной державы могут оправдать инициирование действий по наблюдению, что открывает возможности для мониторинга «инородных» философских и религиозных *Weltanschauungen*[2]. Мониторинг «причин»[3] этнических, религиозных и политических конфликтов, который охватывается целью, связанной с внешними конфликтами, имеющими последствия для международной безопасности, является частью той же актуализированной оруэлловской политики контроля мыслей[4].

7. Цель, связанная с «деятельностью по разработке»[5], – это настоящая правовая черная дыра, которая позволяет перехватывать и анализировать сообщения, не попадающие под восемь целей внешней разведки[6]. Это карт-бланш на мониторинг «больших сегментов международного трафика сигналов»[7]. Доводы властей Швеции о том, что такие данные не ведут к составлению каких-либо разведывательных донесений, но имеют важное значение для мониторинга «постоянных изменений в сферах международной радиотехнической обстановки, технического прогресса и радиотехнической защиты»[8], равносильны заявлению о том, что все интернет-коммуникации должны подлежать проверке, чтобы Радиотехнический центр мог идти в ногу с постоянно меняющейся интернет-средой, техническими разработками и защитой Интернета. Это, очевидно, абсурд, но фактически власти Швеции утверждают именно так. Бесцельный (то есть выходящий за пределы восьми установленных законом целей) сбор такого неограниченного количества данных *per se* составляет несоразмерное вмешательство в статьи 8 и 10 Европейской конвенции по защите прав человека и основных свобод (далее – Конвенция).

8. Наконец, также вызывает озабоченность тот факт, что постоянно расширяющиеся полномочия правоохранительных органов (таких как Государственная служба безопасности и Национальное оперативное отделение Главного полицейского управления) выдавать поручения на проведение радиотехнической разведки и получать доступ к собранным данным или разведывательным донесениям ставят под угрозу принцип категоричности, лежащий в основе режима массового перехвата данных в Швеции, то есть принцип, согласно которому данные должны собираться и обрабатываться для одной или нескольких законных целей и не могут использоваться способом, несовместимым с такими целями, в частности, они не могут использоваться правоохранительными органами в целях уголовного производства. Фактически Инспекция по надзору недавно предупредила, что правоохранительные органы не смогут отделять информацию, полученную от Радиотехнического центра, от своей правоохранительной деятельности[9].

Разрешение массового перехвата данных

9. Законодательство Швеции поручает суду санкционировать массовое наблюдение. Но Суд по вопросам внешней разведки не относится к обычным судам. В этом заключается второй серьезный недостаток действующей в Швеции системы. В состав Суда по вопросам внешней разведки входят один председатель, один или два вице-председателя и от двух до шести непрофессиональных

---

[1] *Ibid*.

[2] *Weltanschauungen* (нем.) – мировоззрение, взгляды (*примеч. переводчика*).

[3] См. § 23 настоящего Постановления.

[4] Аналогичным образом, Комитет ООН по правам человека в § 36 Заключительных замечаний по седьмому докладу относительно Швеции от 28 апреля 2016 г., CCPR/C/SWE/CO/7, выразил озабоченность по поводу «ограниченной прозрачности в том, что касается объема надзорных полномочий и гарантий при их применении». Я хотел бы отметить, что Специальный докладчик ООН по вопросам поощрения и защиты прав человека и основных свобод в условиях борьбы с терроризмом в § 43 своего доклада от 22 февраля 2016 г., A/HRC/31/65, выразил мнение о том, что «эффективные стратегии не должны быть основаны на предвзятых или неправильных представлениях о группах, наиболее подверженных радикализации или насильственному экстремизму, но должны развиваться на основе фактических данных, чтобы обеспечить правильное понимание национальных и местных проблем, влияющих на процесс радикализации».

[5] См. § 24 настоящего Постановления.

[6] Как отмечается в отчете Комитета по радиотехнической разведке (см. § 79 настоящего Постановления).

[7] См. § 292 настоящего Постановления.

[8] Доводы властей Швеции, представленные на слушании в Большой Палате Европейского Суда 10 июля 2019 г.

[9] См. ссылку на позицию Инспекции по надзору в комментариях заявителя, представленных в Большой Палате Европейского Суда 3 мая 2019 г., с. 24, которые власти Швеции не оспаривали.

членов, в основном бывших политиков[1], которые назначаются властями Швеции на четырехлетний срок. Период их назначения может быть продлен, что укрепляет их политическую связь с властями Швеции. Даже представитель по вопросам защиты частной жизни, который должен действовать в общественных интересах, но не в интересах какого-либо затронутого частного лица, назначается властями Швеции, и срок его полномочий может быть продлен. Кроме того, можно обойтись без его вмешательства. Если вопрос настолько срочен, что задержка может серьезно поставить под угрозу цель обращения, заседание может быть проведено и решение может быть вынесено в отсутствие представителя по вопросам защиты частной жизни и без предоставления ему иной возможности дать свои комментарии. В высшей степени политизированный статус членов Суда по вопросам внешней разведки согласуется с тем, что он никогда не проводил публичных слушаний, а его решения являются окончательными и конфиденциальными[2]. С учетом указанных характеристик Суд по вопросам внешней разведки скорее напоминает политический орган, а не по-настоящему независимый судебный орган[3].

10. Надзор Суда по вопросам внешней разведки охватывает оценку конкретных «носителей» (носителей сигналов), к которым Радиотехнический центр будет иметь доступ, «селекторов» (поисковых запросов) и категорий селекторов, которые будут использоваться для автоматического сбора данных, а также срока действия разрешения на наблюдение. Однако отсутствует требование об аннулировании разрешения, если необходимость в сборе сообщений отпадает[4], или об уничтожении в течение определенного срока перехваченных материалов, не содержащих персональных данных[5]. Также отсутствует требование о том, чтобы Суд по вопросам внешней разведки проверял наличие разумных подозрений в отношении какого-либо лица, ставшего объектом наблюдения. Жесткие селекторы, непосредственно относящиеся к конкретному лицу, действительно могут использоваться только в случае их «исключительной важности» для разведывательной деятельности[6], но это ограничение применяется лишь к автоматизированному сбору данных, а не к селекторам, используемым для поиска в собранном массиве данных. Это означает, что законодательство допускает большую степень усмотрения Радиотехнического центра при сборе и поиске сообщений и связанных с ними данных, особенно если разрешение Суда по вопросам внешней разведки относится к категориям селекторов[7]. Проблема отсутствия конкретности в отношении селекторов представляется еще более серьезной относительно селекторов, используемых для сопутствующих данных о сообщениях[8].

11. Кроме того, отсутствуют какие-либо доказательства того, что Суд по вопросам внешней разведки может и на практике оценивает необходимость защиты конфиденциальных сообщений, в том числе в ситуациях, когда существует обоснованная вероятность того, что такие сообщения будут пере-

[1] См. Доклад Венецианской комиссии «О демократическом контроле над органами радиотехнической разведки» от 2015 года, с. 33.

[2] Я не понимаю, почему большинство судей упрекают Инспекцию по надзору (которая не является судом) за вынесение непубличных решений, но готово согласиться с тем, что Суд по вопросам внешней разведки (который является судом) не выносит публичных решений (см. для сравнения см. §§ 297 и 372 настоящего Постановления).

[3] Венецианская комиссия сочла его «гибридным органом» (см. упомянутый выше Доклад Венецианской комиссии, с. 33). Именно поэтому Комитет ООН по правам человека просил власти Швеции обеспечить «создание эффективных и независимых механизмов контроля за обменом разведывательной информацией, содержащей персональные данные» (см. § 37 упомянутых выше Заключительных замечаний Комитета ООН по правам человека). Это не единичный случай в Европе. Агентство Европейского союза по основным правам выявило следующие недостатки в государствах – членах ЕС: «По результатам также были выявлены ограничения полной независимости, когда некоторые надзорные органы в значительной степени зависят от органов исполнительной власти: законодательство не наделяет их полномочиями принимать обязательные решения, у них ограниченный штат сотрудников и бюджет, либо их офисы расположены в правительственных зданиях» (Агентство Европейского союза по основным правам «Наблюдение за разведывательными службами: гарантии основных прав и средства правовой защиты в Европейском союзе», том II: «Перспективы области и законодательные изменения», 2017, с. 11).

[4] Большинство судей упускают важность этого недостатка, путая «наличие надзорных механизмов» с предоставлением конкретной материально-правовой гарантии, которая обязывает прекращать излишний перехват данных (см. § 336 настоящего Постановления).

[5] Большинство судей считают нормы об уничтожении перехваченных материалов, содержащих персональные данные, достаточно четкими «в целом», игнорируя упущения в части регулирования материалов, не содержащих персональные данные (см. § 344 настоящего Постановления).

[6] Меня озадачивает тот факт, что большинство судей готовы согласиться с тем, что «стандарт исключительной важности» для санкционирования жестких селекторов «может обеспечивать соответствующую повышенную защиту» в отсутствие у них какого-либо представления о том, как Суд по вопросам внешней разведки применяет указанный стандарт (см. § 300 настоящего Постановления). Это равносильно карт-бланшу для Суда по вопросам внешней разведки и властей Швеции.

[7] Большинство судей справедливо признают это, допуская, что «может быть затруднительно» оценить аспект соразмерности, когда в обращении Радиотехнического центра о выдаче разрешения указаны только категории селекторов (см. § 301 настоящего Постановления). Именно поэтому массовый перехват данных на основе категорий селекторов недопустим (см. мое отдельное мнение, приложенное к упомянутому выше делу «Организация Big Brother Watch и другие против Соединенного Королевства» (Big Brother Watch and Others v. United Kingdom).

[8] Как указано в отчете Комитета по радиотехнической разведке (см. § 78 настоящего Постановления) и признано властями Швеции (см. § 220 настоящего Постановления).

хвачены в качестве «прилова» при запрашиваемом перехвате данных. Конфиденциальные сообщения, например, связанные с источниками средств массовой информации и адвокатской тайной, защищены только тем, что в случае их перехвата они должны быть уничтожены. Вызывает беспокойство тот факт, что не защищаются даже сообщения в религиозном контексте исповеди или индивидуального консультирования, поскольку они могут быть перехвачены и изучены в исключительных случаях.

Надзор за исполнением разрешений на перехват данных

12. Суд по вопросам внешней разведки не осуществляет надзор за исполнением разрешения на массовый перехват данных и даже за предполагаемым последующим использованием перехваченных сообщений. Эта задача поручена Инспекции по надзору. Как и в случае с Судом по вопросам внешней разведки, состав Инспекции по надзору определяется властями Швеции, которые назначают ее членов на четырехлетний срок с возможностью продления их полномочий. При этом председатель и вице-председатель являются судьями на постоянной основе или бывшими судьями, а другие четыре члена инспекции избираются из числа бывших политиков, предложенных партийными группами, представленными в парламенте[1]. Инспекция работает неполный рабочий день[2] при содействии «небольшого секретариата»[3].

13. Инспекция по надзору не имеет полномочий устанавливать посредством обязательного решения, является ли разрешение Суда по вопросам внешней разведки законным, или отдавать распоряжения об исправлении практики Радиотехнического центра или о реформировании ее внутренних правил, как и полномочий предоставлять компенсацию. Однако Инспекция по надзору может принять решение о прекращении операции или об уничтожении перехваченных материалов, если они не соответствуют предоставленному разрешению. Инспекция по надзору не вправе принимать какие-либо обязательные решения, касающиеся нарушений Конвенции, Конституции Швеции или Закона об обработке персональных данных Радиотехническим центром. Вместо этого она может обратиться в Инспекцию по защите данных.

14. Инспекция по защите данных выполняет общую надзорную функцию в отношении защиты персональных данных. При осуществлении своей функции она имеет доступ к персональным данным, обрабатываемым Радиотехническим центром, и к соответствующей документации, а также к помещениям, где она хранится. Инспекция по защите данных не вправе самостоятельно принимать какие-либо обязательные решения в отношении Радиотехнического центра и не обязана принимать какие-либо меры после получения сообщения от Инспекции по надзору. Если же она решит принять меры, то единственное, что она может сделать, – это довести свою позицию до сведения Радиотехнического центра или обратиться в Административный суд для уничтожения незаконно обработанных персональных данных. Однако на сегодняшний момент она никогда не пользовалась указанным полномочием[4].

15. Наконец, что касается внутреннего надзора, в состав Совета по защите конфиденциальности Радиотехнического центра, которому поручено проводить мониторинг мер, принимаемых для защиты личной неприкосновенности, также входят члены, назначаемые властями Швеции. Этот орган представляется неэффективным, о чем свидетельствует тот факт, что в 2010 и 2016 годах Инспекция по защите данных безуспешно критиковала Радиотехнический центр за неспособность проводить надлежащий мониторинг журналов, используемых для обнаружения неправомерного использования персональных данных[5]. Заявленного введения в 2018 году центральной функции мониторинга и отслеживания журналов, как утверждали власти Швеции, недостаточно. Фактически у Радиотехнического центра отсутствует обязательство вести журналы и подробную документацию о каждом этапе массового перехвата данных, включая перехват, последующее использование и передачу данных. Это означает, что любая практика ведения документации, если таковая имеет место, в сущности зависит от внутренних процедур и усмотрения.

Средства правовой защиты

16. Отсутствие действительно независимого разрешения и надзора за внедрением мер по массовому перехвату данных усугубляется чисто виртуальным характером средств защиты, доступных объекту перехвата[6]. Закон предусматривает уве-

[1] Венецианская комиссия сочла Инспекцию по надзору «гибридным органом», как и Суд по вопросам внешней разведки (см. упомянутый выше Доклад Венецианской комиссии, с. 33).

[2] Как признали власти Швеции на слушании в Большой Палате Европейского Суда 10 июля 2019 г.

[3] Как описано в упомянутом выше Докладе Венецианской комиссии, с. 33.

[4] См. § 57 настоящего Постановления.

[5] См. § 76 настоящего Постановления.

[6] Агентство Европейского союза по основным правам подчеркивало, что эффективность средств правовой защиты зависит от способности принимать юридически обязательные решения, которые как минимум должны предусматривать право отдавать распоряжение о прекращении наблюдения, уничтожении незаконно собранных данных и выплате надлежащей компенсации (см. упомянутый выше доклад Агентства Европейского союза по основным правам «Наблюдение за разведывательными службами», с. 114).

домление объекта перехвата о массовом перехвате данных в случаях, когда использовались селекторы, напрямую связанные с конкретным лицом, и соображения секретности не имеют преимущественной силы. Гарантия распространяется только на физических лиц, а не на юридических лиц, каковым является заявитель. В любом случае указанный закон существует только на бумаге[1].

17. В дополнение, по обращению физического или юридического лица Инспекция по надзору может провести расследование на предмет соответствия закону перехвата и обработки перехваченных материалов, и такие расследования проводились. Удивительно, но во всех 132 делах, расследованных инспекцией, она ни разу не приняла решение в пользу заявителя[2]. Простая причина этого заключается в том, что Инспекция по надзору является *iudex in causa sua*[3], поскольку ей поручено проверять свою собственную надзорную деятельность даже без необходимости информировать заявителя о своих выводах или объяснять какие-либо причины своих решений[4]. Методы работы Инспекции по надзору недалеки от мрачного процесса, описанного Францем Кафкой.

18. Кроме того, частные лица вправе обращаться в Радиотехнический центр с запросом о раскрытии и об исправлении обрабатываемых персональных данных, а решения Радиотехнического центра о раскрытии информации могут быть обжалованы в Административном суде. Однако внутригосударственные нормы о секретности могут воспрепятствовать доступу частного лица к данной информации[5], не говоря уже о *de facto* полномочиях Административного суда проверять собственную оценку секретности, проведенную Радиотехническим центром. О такой «Уловке-22»[6] свидетельствует тот факт, что этой возможностью ни разу не пользовались[7]. В любом случае указанный правовой механизм недоступен юридическим лицам, таким как заявитель.

19. Наконец, ни парламентские омбудсмены, ни канцлер юстиции не проводят какого-либо эффективного надзора, поскольку они не уполномочены принимать юридически обязательных решений по прекращению перехвата данных или уничтожению перехваченных материалов. Фактически они никогда не считали необходимым действовать в пределах своих полномочий, например, путем возбуждения уголовного или дисциплинарного производства в отношении должностных лиц Радиотехнического центра[8] или в случае канцлера юстиции путем присуждения компенсации.

Передача перехваченных данных иностранным разведывательным службам

20. Что касается передачи перехваченных данных иностранным третьим сторонам, единственная гарантия, предусмотренная законом, состоит в том, что такая передача должна отвечать национальным интересам. Отсутствует требование учитывать права на частную жизнь или гарантировать, что власти государства-получателя предоставляют гарантии, аналогичные тем, что применимы в Швеции. Если полномочия органа, осуществляющего перехват данных, сформулированы в законодательстве столь широко, а надзор сводится к проверке того, что орган действует в рамках своих законодательных полномочий, то подобный надзор достаточно ограничен[9].

---

[1] См. §§ 60 и 80 настоящего Постановления. Действительно, Комитет ООН по правам человека просил власти Швеции гарантировать, «что затронутые лица имеют надлежащий доступ к эффективным средствам правовой защиты в случае злоупотреблений» (см. § 37 упомянутых выше Заключительных замечаний Комитета ООН по правам человека).

[2] См. § 61 настоящего Постановления. В § 218 настоящего Постановления большинство судей ссылаются на 141 проверку по обращениям отдельных лиц, ни одна из которых не выявила «ненадлежащего сбора сигналов». Неясно, что большинство судей пытались продемонстрировать этим. С одной стороны, они признают, что о решениях можно уведомлять «специального советника, прошедшего официальную процедуру допуска», но, с другой стороны, они требуют, чтобы решение было «общедоступным», и критикуют «отсутствие у представителей общественности возможности получить мотивированные решения в той или иной форме в ответ на обращения» (см. для сравнения §§ 361 и 372 настоящего Постановления).

[3] Так в тексте. Вероятно, имеется *в виду judex in causa sua* (лат.) – судья в своем деле (*примеч. переводчика*).

[4] Это не имеет ничего общего со стандартом Европейского союза, изложенным в упомянутом выше докладе Агентства Европейского союза по основным правам «Наблюдение за разведывательными службами», с. 14: «Государства – члены ЕС должны гарантировать, что судебные и внесудебные органы, предоставляющие средства правовой защиты, обладают полномочиями и компетенцией для эффективной оценки и принятия решений по жалобам отдельных лиц, связанным с наблюдением… В частности, такие органы должны иметь доступ к помещениям разведывательных служб и собранным данным, иметь право выносить обязательные решения и информировать заявителей о результатах своего расследования. Лицам должна быть предоставлена возможность обжаловать решение этого органа».

[5] Как признала сама Палата Европейского Суда (см. § 175 Постановления Палаты Европейского Суда).

[6] «Уловка-22» (англ. Catch 22) – ситуация, возникающая в результате логического парадокса между взаимоисключающими правилами (*примеч. переводчика*).

[7] См. § 64 настоящего Постановления.

[8] См. §§ 66–68 настоящего Постановления.

[9] Законодательство Швеции очень далеко от универсального стандарта, описанного Организацией Объединенных Наций в Подборке надлежащих практик в сфере создания нормативной и институциональной базы и мероприятий, направленных на обеспечение соблюдения разведывательными службами прав человека в контексте борьбы с терроризмом, в том числе в сфере надзора за разведывательными службами от 17 мая 2010 г. (A/HRC/14/46): «Практика 31.

21. Доводы властей Швеции о том, что международное сотрудничество обусловлено соблюдением властями государства-получателя законодательства Швеции, не находит подтверждения в законодательстве какого-либо государства. Фактически власти Швеции ссылались только на «общие руководящие принципы Радиотехнического центра»[1]. На практике Радиотехнический центр обязан только уведомлять Инспекцию по надзору о принципах, регулирующих ее сотрудничество с иностранными разведывательными службами, и о том, в какие страны и каким организациям он передает данные, а также предоставлять общую информацию о своих операциях. Поскольку ни один надзорный орган не имеет полномочий осуществлять фактический контроль над тем, используется ли сотрудничество с иностранной разведкой для обхода законодательства Швеции и защищают ли власти государств-получателей данные с помощью тех же или аналогичных гарантий, что предусмотрены законодательством Швеции, мониторинг деятельности Радиотехнического центра по международному сотрудничеству со стороны Инспекции по надзору, на который ссылаются власти Швеции, не имеет значения[2].

22. Позиция властей еще менее приемлема, поскольку она несовместима с международными обязательствами Швеции не только с точки зрения ее обязательств перед Европейским союзом[3], но и перед Советом Европы. В дополнение к Конвенции статья 2 Дополнительного протокола к Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных, касающегося надзорных органов и трансграничной передачи данных (ETS № 181), ратифицированного Швецией, гласит, что стороны должны гарантировать надлежащий уровень защиты персональных данных при передаче их в третьи страны и что исключения допустимы только при наличии законных преобладающих интересов. В Пояснительном докладе к указанному Дополнительному протоколу уточняется, что исключения следует толковать ограничительно, «чтобы исключение не стало правилом» (§ 31). Как раз это и произошло в Швеции.

Вывод

23. В целом надзорные органы Швеции либо не отвечают требованию достаточной независимости, либо не осуществляют эффективный контроль, либо и то, и другое. Суд по вопросам внешней разведки с его скрытым производством и не подлежащими обжалованию секретными решениями, не является судом, отправляющим правосудие от имени народа и подотчетным ему. Это секретная комиссия политических ставленников, осуществляющая ограниченный диктат, который не может быть обжалован. Она служит одной-единственной цели: скрыть недостатки выбора Радиотехнического центра, то есть фактически выбора политики наблюдения, сделанного властями, создавая у шведов обманчивое впечатление, будто в г. Стокгольме есть суд, который защищает право на частную жизнь.

24. Не лучше обстоит дело с Инспекцией по надзору. При получении запроса расследовать, соответствовали ли перехват и обработка сообщений законодательству, она принимает решения *in causa sua*, даже без обязательства информировать заявителя о своих выводах или объяснять причины своих решений. С заявителем обращаются как с объектом в руках всемогущего кафкианского государства, лишенным права на частную жизнь, а не как с лицом, наделенным правами в отношениях с властями и против них.

25. Шведский неизбирательный подход к международному обмену перехваченными данными с разведывательными службами представляет бóльшую опасность для гражданских прав и демократического управления, чем адресный подход.

26. Вместо увеличения количества надзорных органов с виртуальными полномочиями целесообразнее было бы учредить полностью независимый суд, состоящий из старших судей, наделенных полномочиями осуществлять эффективный сквозной контроль процесса перехвата данных, то есть выдавать разрешение и осуществлять регулярный надзор за внедрением адресных, основанных на конкретных подозрениях мер по массовому перехвату данных, а также прекращать незаконный сбор и хранение перехваченных данных и иметь

Обмен разведывательной информацией между разведывательными службами одного государства или с органами иностранного государства основан на внутригосударственном законодательстве, определяющем четкие параметры такого обмена, в том числе условия, которые должны быть соблюдены для обмена информацией, органы, с которыми такой обмен возможен, и гарантии, применимые к обмену разведывательными данными». См. также Практики 32–35.

[1] См. § 216 настоящего Постановления.

[2] См. также § 36 упомянутых выше Заключительных замечаний Комитета ООН по правам человека, где комитет выразил особую озабоченность в связи с «отсутствием достаточных гарантий против произвольного вмешательства в право на частную жизнь в связи с обменом данными с другими разведывательными службами».

[3] См. упомянутый выше доклад Агентства Европейского союза по основным правам «Наблюдение за разведывательными службами», с. 13: «Государства – члены ЕС должны определить правила международного обмена разведывательными данными. Такие правила должны подлежать проверке надзорными органами, которые должны оценивать, соблюдаются ли при передаче и получении разведывательной информации основные права и предусмотрены ли они надлежащие гарантии… Государства – члены ЕС должны обеспечивать, чтобы нормативно-правовая база, регулирующая сотрудничество в сфере разведки, четко определяла объем полномочий надзорных органов в сфере сотрудничества разведывательных служб».

необходимый доступ к секретным документам для выполнения этой задачи[1].

27. Доводы о практической невозможности внедрить указанный стандарт следует безоговорочно исключить: рассматриваемая проблема является вопросом не практической эффективности, а верховенства права. Именно право устанавливает границы эффективных государственных служб, а не наоборот. Но это можно понять, только поднявшись, как «Странник» Каспара Давида Фридриха, над морем тумана, обволакивающего рассуждения властей Швеции.

[1] См. мое отдельное мнение, приложенное к упомянутому выше Постановлению Европейского Суда по делу «Организация Big Brother Watch и другие против Соединенного Королевства» (Big Brother Watch and Others v. United Kingdom), в котором обсуждаются требования к совместимому с Конвенцией режиму массового перехвата данных.

СОВМЕСТНАЯ ДЕКЛАРАЦИЯ О ГОЛОСОВАНИИ СУДЕЙ ЙОНА ФРИДРИКА КЬЁЛЬБРО И ЭРИКА ВЕННЕРСТРЁМА

1. Мы голосовали против установления нарушения статьи 8 Конвенции и, следовательно, хотели бы дистанцироваться от аргументации и выводов Большой Палаты Европейского Суда относительно обмена разведывательной информацией (см. §§ 317–330 настоящего Постановления) и проверки *ex post facto* (см. §§ 354–364 настоящего Постановления).

2. Принимая во внимание характер вопроса, разрешенного Европейским Судом, значимость его Постановления, значительное большинство голосов в пользу установления нарушения статьи 8 Конвенции, а также учитывая аргументацию в принятом единогласно Постановлении Палаты Европейского Суда, мы отказываемся от подробного изложения наших правовых доводов в настоящем деле и ограничимся декларацией о голосовании.