Эффективный демократический надзор за деятельностью национальных служб безопасности

Тематический доклад

COMMISSIONER FOR HUMAN RIGHTS
COMMISSAIRE AUX DROITS DE L'HOMME
COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Эффективный демократический надзор за деятельностью национальных служб безопасности

Тематический доклад,
опубликованный Комиссаром
Совета Европы по правам человека

Совет Европы

Выводы, представленные в данной работе, являются ответственностью автора и не обязательно отражают официальную политику Совета Европы.

Комиссар по правам человека публикует доклады с целью обсуждения и анализа важных текущих проблем прав человека. Многие из них также включают рекомендации Комиссара по разрешению выявленных проблем. Выводы, содержащиеся в этих экспертных документах, не обязательно отражают позицию Комиссара.

Доклады доступны на веб-сайте Комиссара: www.commissioner.coe.int

Фото обложки: © Shutterstock

Обложка: Documents and Publications Production Department (SPDP), Council of Europe

Издано при финансовом содействии Женевского Центра демократического контроля над вооруженными силами

Перевод: Центр исследований армии, конверсии и разоружения

Макет издания на русском языке: Марк Канарский, Киев

Выражаем признательность:

Данный доклад был подготовлен независимым консультантом Айданом Уиллзом (Aidan Wills).

Содержание

КРАТКОЕ СОДЕРЖАНИЕ 5

1. Обзор влияния деятельности служб национальной безопасности на защиту прав человека в Европе 5

2. Обзор международных и европейских стандартов осуществления демократического надзора за деятельностью национальных служб безопасности 6

3. Национальная практика стран – членов совета Европы 7

4. На пути к действенному и демократическому надзору за национальными службами безопасности 9

РЕКОМЕНДАЦИИ КОМИССАРА 12

О системе надзора в целом 12

О пределах надзора за службами безопасности 12

О независимости и демократической легитимности надзорных органов 14

Об эффективности надзорных органов 15

Об оценке деятельности надзорных органов и систем 16

ГЛАВА 1. ВСТУПЛЕНИЕ 17

ГЛАВА 2. ОБЩИЙ ОБЗОР ВЛИЯНИЯ ДЕЯТЕЛЬНОСТИ НАЦИОНАЛЬНЫХ СЛУЖБ БЕЗОПАСНОСТИ НА ЗАЩИТУ ПРАВ ЧЕЛОВЕКА В ЕВРОПЕ 19

2.1. Неприкосновенность и свобода личности 20

2.2. Право на частную и семейную жизнь 22

2.3. Право на свободу слова, собраний и объединений 25

2.4. Право на справедливый суд и право на эффективную правовую защиту 27

ГЛАВА 3. ОБЩИЙ ОБЗОР МЕЖДУНАРОДНЫХ И ЕВРОПЕЙСКИХ СТАНДАРТОВ ДЕМОКРАТИЧЕСКОГО НАДЗОРА ЗА НАЦИОНАЛЬНЫМИ СЛУЖБАМИ БЕЗОПАСНОСТИ 29

3.1. Международные и региональные правовые инструменты 29

3.2. Необязательные рекомендации и принципы 33

ГЛАВА 4. НАЦИОНАЛЬНЫЕ ПРАКТИКИ В СТРАНАХ-ЧЛЕНАХ СОВЕТА ЕВРОПЫ 42

4.1. Парламентские комитеты 43

4.2 Институты независимого надзора 49

4.3 Судебные органы 55

4.4. Квази-судебные санкционирующие органы 59

4.5. Исполнительная власть 60

4.6. Меры внутреннего контроля 61

4.7. Средства массовой информации и гражданское общество 62

ГЛАВА 5. К ДЕМОКРАТИЧЕСКОМУ И ЭФФЕКТИВНОМУ НАДЗОРУ ЗА НАЦИОНАЛЬНЫМИ СЛУЖБАМИ БЕЗОПАСНОСТИ **64**

5.1. Предварительное санкционирование связанных с вмешательством мер 66

5.2. Рассмотрение жалоб 67

5.3. Доступ контролеров к информации 67

5.4. Прозрачность органов надзора 69

5.5. Оценка систем надзора 69

ССЫЛКИ **71**

СУДЕБНЫЕ ПРЕЦЕДЕНТЫ **79**

Европейский суд по правам человека 79

Национальные суды 79

КРАТКОЕ СОДЕРЖАНИЕ

Разоблачения бывшего наемного сотрудника разведки США Эдварда Сноудена снова привлекли внимание к деятельности служб безопасности стран – членов Совета Европы. Беспокойство по поводу использования широкомасштабного электронного наблюдения вновь ставит вопрос о необходимости эффективного надзора за деятельностью служб безопасности. Надзор за деятельностью спецслужб абсолютно необходим для того, чтобы эти учреждения не только способствовали защите населения, которому они призваны служить, но и соблюдали принцип верховенства права и прав человека в своей деятельности. Однако откровения Сноудена, причастность некоторых европейских служб безопасности к тайному содержанию под стражей и незаконной выдаче подозреваемых в терроризме, а также сообщения о противоправной деятельности служб безопасности в некоторых странах Совета Европы сеют серьезные сомнения в способности национальных систем надзора эффективно выполнять свою функцию.

В таком контексте тематический доклад анализирует способы повышения эффективности национальных систем надзора для лучшего соблюдения прав человека и достижения прозрачности в работе спецслужб.

Доклад сфокусирован на изучении различных способов надзора за деятельностью государственных органов, включая самостоятельные надзорные ведомства, отделы/подразделения при государственных структурах и при вооруженных силах, имеющих полномочия по сбору, анализу и передаче разведывательных данных внутри страны. Эти данные собираются для информирования политиков, военачальников, полиции, пограничных и таможенных служб об имеющихся угрозах национальной безопасности и другим ключевым национальным интересам. Несмотря на то, что некоторые службы безопасности уполномочены арестовывать и содержать граждан под стражей, настоящий доклад не затрагивает вопрос надзора за этой их деятельностью.

Комиссаром Совета Европы по правам человека сформулирован ряд рекомендаций на основе вопросов, затрагиваемых настоящим исследованием. Эти рекомендации изложены в конце данного резюме.

1. ОБЗОР ВЛИЯНИЯ ДЕЯТЕЛЬНОСТИ СЛУЖБ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ НА ЗАЩИТУ ПРАВ ЧЕЛОВЕКА В ЕВРОПЕ

Современные примеры влияния деятельности служб безопасности на права человека рассматриваются по четырем направлениям.

Во-первых, это деятельность спецслужб, которая сказывается на неприкосновенности личности, включая право на жизнь, право на свободу и личную

неприкосновенность, а также право не подвергаться пыткам или бесчеловечному, жестокому и унижающему достоинство обращению. Приводятся примеры причастности служб безопасности к выдачам и тайному содержанию под стражей лиц, подозреваемых в терроризме; к обмену информацией, ведущей к выдаче таких лиц, пыткам, нанесению ударов беспилотниками, а также к арестам и произвольному содержанию людей под стражей.

Во-вторых, это влияние деятельности служб безопасности на частную и семейную жизнь. Во многих странах это наиболее распространенный вид вмешательства служб безопасности в права человека. Довольно подробно рассматриваются массовое наблюдение и использование коммуникационных и метаданных; также уделяется внимание защищенности использования компьютерных сетей и международному обмену разведывательными данными.

В-третьих, это отражение деятельности служб безопасности на свободе выражения мнений, собраний и объединений. Рассматриваются как прямые, так и косвенные вмешательства в эти права, в том числе превентивный эффект, оказываемый возможным и фактическим наблюдением. Обсуждается также и более глубокий урон демократическим процессам, наносимый вмешательством служб безопасности в работу политиков, судей и неправительственных организаций (НПО).

Наконец, вкратце исследуется влияние деятельности служб безопасности на справедливое судебное разбирательство, включая наблюдение за общением адвокатов со своими клиентами, а также ограничение права на справедливое судебное разбирательство мерами засекречивания информации в контексте охраны государственной тайны в делах, в которых вовлечены службы безопасности.

2. ОБЗОР МЕЖДУНАРОДНЫХ И ЕВРОПЕЙСКИХ СТАНДАРТОВ ОСУЩЕСТВЛЕНИЯ ДЕМОКРАТИЧЕСКОГО НАДЗОРА ЗА ДЕЯТЕЛЬНОСТЬЮ НАЦИОНАЛЬНЫХ СЛУЖБ БЕЗОПАСНОСТИ

Международные и европейские стандарты надзора за деятельностью служб безопасности подразделяются на юридически-обязательные инструменты и необязательные принципы и рекомендации. Первая категория включает в себя положения ряда международных и региональных договоров, а также их толкование соответствующими судами или специальными договорными органами. Несмотря на то, что непосредственно к надзору применимо очень малое количество международных или региональных юридических инструментов, немалое количество положений, имеющих прямое отношение к надзору за службами безопасности, можно извлечь из правоприменительной практики Европейского суда по правам человека (далее – «Суд» или «Страсбургский суд») по статьям 3, 5, 8 и 13 Европейской конвенции о защите прав человека и основных свобод (далее – «Конвенция» или «ЕСПЧ»). Они содержат требования эффективности расследования серьезных нарушений прав человека, наличия эффективных средств правовой защиты от нарушений со стороны служб безопасности, в том числе в контексте тайного наблюдения, за-

благовременного получения разрешения на применение интрузивных (вторгающиеся в частную жизнь) методов наблюдения, а также оценку методов наблюдения *пост фактум*.

Во вторую категорию входят рекомендации, резолюции, заявления и доклады из следующих четырех источников: (i) учреждения Организации Объединенных наций (ООН), в том числе Генеральная Ассамблея и ее специально уполномоченные агентства; (ii) учреждения Совета Европы, в том числе Венецианская комиссия, Парламентская ассамблея (ПАСЕ) и ее докладчики, а также Комиссар по правам человека; (iii) Европейский Союз; и (iv) транснациональные инициативы гражданского общества. За последние 10 лет число таких документов резко возросло до такой степени, что образовалась целая отрасль принципов «мягкого права» в области надзора; по каждому из них даны ключевые или новые рекомендации, выделены существенные различия между ними.

Наиболее полными являются Сборник ООН по передовой практики по надзору за службами безопасности (UN 2010a), подготовленный бывшим Специальным докладчиком ООН по вопросам прав человека и борьбе с терроризмом, а также знаковый доклад Венецианской комиссии о демократическом надзоре за деятельностью служб безопасности. Ряд других докладов и резолюций касаются вопроса надзора за деятельностью служб безопасности в более широком контексте. Особо значимыми являются те рекомендации, которые даны уполномоченными органами ООН, Комиссаром Совета Европы по правам человека, ПАСЕ и Европейским парламентом в свете разоблачений Сноудена.

Отдельно рассматриваются Глобальные принципы национальной безопасности и Право на информацию (принципы Тсване) поскольку они содержат руководящие ориентиры в таких ключевых вопросах, как доступ к информации надзорными органами и публичный доступ к документам, находящимся в ведении служб безопасности и надзорных органах. Другие исследуемые в докладе положения содержатся в «Оттавских принципах» и в так называемых принципах Необходимости и Соразмерности.

3. НАЦИОНАЛЬНАЯ ПРАКТИКА СТРАН – ЧЛЕНОВ СОВЕТА ЕВРОПЫ

Страны – члены Совета Европы по-разному подходят к организации надзора за деятельностью своих служб безопасности. В этом разделе рассматриваются внутригосударственные подходы к надзору со стороны парламентских комитетов, независимых надзорных учреждений, включая экспертные надзорные органы, а также учреждений, имеющих более широкие полномочия, включая омбудсменов, комиссаров по защите персональных данных/информации; а также со стороны судебных и квази-судебных инстанций. Кроме того, в докладе кратко рассматривается роль политических руководителей, органов внутреннего контроля служб безопасности и неформального надзора со стороны гражданского общества и средств массовой информации. Не рассматривая национальные системы надзора в совокупности, приводятся примеры из отдельных составляющих этих систем в различных странах. Это делается для

того, чтобы подчеркнуть разницу в подходах разных стран и особо подчеркнуть передовую положительную практику.

Особо отмечается, что среди членов Совета Европы нет страны, система надзора которой согласовывалась бы со всеми международными или региональными принципами и положительной практикой, упомянутыми в докладе, как и не существует наилучшего подхода к организации системы 4 надзора за службами безопасности. Тем не менее, цель доклада – выделить отдельные подходы или методы, обладающие значительными преимуществами с точки зрения защиты прав человека.

Комитеты при Парламентах

Подробно рассматриваются полномочия и роль парламентских комитетов по надзору, которые традиционно считаются основными органами, отвечающими за надзор за деятельностью служб безопасности. Существенным признаком эффективности работы парламентских комитетов по надзору является их доступ к засекреченной информации; этот вопрос рассматривается в докладе в свете альтернативных мер защиты информации, а также в связи с деликатным вопросом доверия конфиденциальной информации самим парламентарием. В этом подразделе также рассматривается часто упускаемый из виду вопрос отношений между парламентскими комитетами и другими надзорными органами.

Независимые надзорные учреждения

Все более заметную роль в надзоре за деятельностью служб безопасности играют экспертные органы по вопросам безопасности и разведки. В докладе излагается мнение, что они имеют основополагающее значение для повышения эффективности надзора и улучшения защиты прав человека.

Надзор со стороны экспертных органов по вопросам безопасности и разведки получает все большее распространение в пространстве Совета Европы и зачастую лучше всех могут осуществлять повседневный надзор за законностью деятельности служб безопасности. Учитывая преимущества этих органов, в докладе подчеркивается необходимость повышения их легитимности в соответствии с демократическими принципами.

В большинстве стран – членов Совета Европы органы защиты персональных данных и омбудсмены играют ограниченную роль в надзоре за службами безопасности. Тем не менее, в докладе приводятся примеры, когда эти органы могут способствовать эффективности систем надзора.

Судебные органы

О судебных органах речь идет, прежде всего, в связи с выдачей ими разрешений на применение интрузивных методов наблюдения. Обращает на себя внимание тот факт, что очень немногие государства предусматривают полу-

чение разрешения суда на массовое видеонаблюдение, доступ к коммуникационным данным или использование компьютерных сетей. Эта область права отстает от развития систем наблюдения и, следовательно, применение даже традиционных интрузивных методов наблюдения не требуют санкции суда в большинстве юрисдикций. Ситуация постепенно меняется, в докладе приводятся примеры государств – членов Совета Европы, которые в настоящее время требуют судебного подтверждения необходимости массового наблюдения и доступа к собранным коммуникационным данным. Также в докладе приветствуется привлечение специалистов или общественных защитников к участию в процессах о получении разрешений на наблюдение для обеспечения лучшей защиты интересов предполагаемых объектов наблюдения.

Квази-судебные разрешительные органы

В нескольких странах – членах Совета Европы созданы квази-судебные органы по выдаче разрешений на применение интрузивных методов наблюдения. Довольно подробно описана новая бельгийская система, поскольку Бельгия является одной из немногих стран, в которой законодательство устанавливает необходимость получения особого разрешения на эксплуатацию компьютерных сетей. Преимуществом таких контролирующих органов в сравнении с судебными инстанциями может быть их подотчетность другому надзорному учреждению. Внутренний контроль Несмотря на то, что собственный контроль в службах безопасности не являлся объектом анализа в рамках настоящего доклада, тем не менее, представляется важным отметить ключевую роль самих сотрудников служб безопасности в обеспечении того, чтобы деятельность этих служб соответствовала стандартам прав человека. Внешний контроль никогда не будет эффективным, если в службе безопасности отсутствует внутренняя культура, а сотрудники не уважают права человека.

4. НА ПУТИ К ДЕЙСТВЕННОМУ И ДЕМОКРАТИЧЕСКОМУ НАДЗОРУ ЗА НАЦИОНАЛЬНЫМИ СЛУЖБАМИ БЕЗОПАСНОСТИ

Опираясь на международные стандарты и национальный опыт, в этом разделе доклада приводятся наиболее значительные цели и важнейшие принципы, способствующие эффективности надзора за деятельностью служб безопасности. Некоторые из них также указаны в качестве заголовков в кратком содержании доклада.

Демократический надзор

Важность демократического надзора объясняется тем, что службы безопасности (и, в частности, отделения, непосредственно выполняющие оперативные задачи) оказывают государственные услуги народу и от имени народа, а потому, избранные народом представители должны быть вовлечены в процесс обеспечения эффективности и законности оказываемых спецслужбами государственных услуг. Демократический характер надзора достигается, прежде

всего, действиями парламента, который принимает законы в области надзора за деятельностью служб безопасности, выделением внепарламентским надзорным учреждениям необходимых бюджетных ресурсов, контроле за работой экспертных надзорных органов, повышении эффективности работы надзорных учреждений, а также в постоянном контроле и внеплановых проверках деятельности служб безопасности.

Заблаговременное разрешение на использование интрузивных методов

Необходимость получения независимого разрешения до начала наблюдения должна распространяться на нецелевой массовый сбор информации; сбор и доступ к коммуникационным данным (в том числе, находящихся у частных операторов); и, теоретически, на использование компьютерных сетей. Сам процесс выдачи или повторной выдачи разрешения на применение интрузивных методов наблюдения также должен быть предметом проверок. Учитывая трудности, которые могут возникнуть при обращении в судебные инстанции за разрешением использования интрузивных методов, выбор может отдаваться в пользу квазисудебной модели надзора.

Рассмотрение жалоб

Полномочия большинства надзорных органов ограничены предоставлением рекомендаций службам безопасности и/или органам исполнительной власти. Однако, с учетом требований Европейской конвенции о защите прав человека о необходимости доступа к эффективному средству правовой защиты всем лицам, утверждающим что их права были нарушены службами безопасности, государства должны обеспечивать гражданам доступ также и в учреждения, способные принимать юридически обязательные решения.

Доступ к информации, связанной с международным сотрудничеством в области разведывательной деятельности

Особого внимания заслуживает вопрос о доступе к информации, относящейся к международному сотрудничеству в области разведки. В связи с международным сотрудничеством между службами безопасности и последствиями такого сотрудничества на права человека, особую важность имеет возможность надзора за обмениваемой в рамках такого сотрудничества информацией, как получаемой, так и направляемой в иностранные юрисдикции. Для надлежащего надзора за обменом информацией важно, чтобы надзирающие органы не рассматривались как «третьи лица» ни на законодательном уровне, ни на практике, а также важно, чтобы они не подпадали в зависимость от контролируемых спецслужб в рамках осуществления надзора за их деятельностью.

Ресурсы для надзорных органов

Возможности по сбору, обмену и получению информации большинства служб безопасности увеличиваются в силу технологического прогресса, увеличения бюджета их финансирования, а также ввиду использования все более сложных систем для реализации этих целей. Соответственно, ключевым условием для эффективного надзора становится необходимость обращения к независимой технической 6 экспертизе. Системы сбора и хранения разведывательной информации становятся все более сложными, а их воздействие на права человека не может быть легко оценено, не прибегая к услугам эксперта.

Оценка работы надзорных систем: кто наблюдает за наблюдателями?

Несмотря на то, что в пространстве Совета Европы налицо прогресс в установлении надзора за деятельностью служб безопасности, очень немногие страны продолжают совершенствовать свои системы, путем пересмотра их эффективности.

Для эффективности предотвращения и реагирования на нарушения прав человека в контексте деятельности служб безопасности, органы надзора за их деятельностью должны быть наделены соответствующими правовыми полномочиями, ресурсами и должны иметь соответствующую профессиональную компетенцию. Эти требования изменяются вместе с изменением характера деятельности служб безопасности. В таком контексте очень важно, чтобы эффективность систем надзора периодически подвергалась проверке. Проверки могут быть периодическими или внеплановыми, а их регламентация должна быть предусмотрена законодательством, регулирующим работу надзорных органов.

РЕКОМЕНДАЦИИ КОМИССАРА

С учетом выводов и результатов проведенных исследований в докладе Комиссар выступает со следующими рекомендациями, направленными на укрепление надзора за национальными службами безопасности и на повышение уровня защиты прав человека этими службами в своей работе.

В целях соответствия требованиям Конвенции деятельности, уставов и политики служб безопасности, а также в целях осуществления эффективного демократического надзора за их деятельностью, Комиссар призывает государства – члены Совета Европы предпринять следующие шаги.

О системе надзора в целом

1. Создать новый, либо уполномочить существующий орган (единый или несколько разных), полностью независимый от исполнительной власти и от служб безопасности, целью которого станет надзор всех аспектов законодательства, правового положения, руководства и самой деятельности служб безопасности. Под всеми упоминаемыми в документе надзорными органами подразумеваются независимые надзорные органы, которым присущи описанные в настоящих Рекомендациях характеристики.
2. Обеспечить соответствие систем надзора за деятельностью служб безопасности соответствующим минимальным требованиям, устанавливаемым правоприменительной практикой Европейского суда по правам человека, требованиям, содержащимся в Сборнике ООН по передовой практики по надзору за службами безопасности (UN 2010a), а также в Рекомендациях Венецианской комиссии.

О пределах надзора за службами безопасности

3. Обеспечить, чтобы надзор за всеми этапами сбора (независимо от применяемых методов или источников получения), обработки, хранения, распространения и уничтожения персональных данных службами безопасности осуществлялся только одним учреждением, независимым этих служб и от исполнительной власти.

4. Обеспечить, чтобы надзор за службами безопасности не ограничивался вопросом законности вмешательства служб безопасности в частную и семейную жизнь, но также распространялся и на вмешательство в свободу выражения мнений, собраний, объединений, мысли, совести и религии.

5. Уполномочить надзорные органы тщательно изучать соблюдение службами безопасности прав человека при сотрудничестве с иностранными органами, включая в рамках сотрудничества по обмену информацией, при проведении совместных операций, а также в рамках предоставления оборудования и обучения. Надзор за сотрудничеством служб безопасности с иностранными органами должен включать (но не ограничиваться нижеописанной деятельностью):

    а. изучение ведомственных директив и внутренних регламентов, применимых к международному разведывательному сотрудничеству;

    б. оценку рисков нарушения прав человека и их минимизации во время сотрудничества с иностранными службами безопасности, а также в конкретных ситуациях при проведении совместных оперативных мероприятий;

    в. контроль за передаваемыми за рубеж персональными данными, включая любые оговорки и условия передачи данных;

    г. надзор за запросами служб безопасности в адрес зарубежных партнеров с целью: (i) получения информации о каких-либо лицах; и (ii) наблюдения за какими-либо лицами;

    д. оценку соглашений о сотрудничестве в области разведки;

    е. надзор за проведением совместных операций и за реализацией программ наблюдения, осуществляемых в рамках сотрудничества с зарубежными партнерами.

6. Требовать, чтобы службы безопасности получали разрешение со стороны независимого от исполнительной власти органа, как в теории, так и на практике, на осуществление любого из нижеперечисленных видов деятельности самостоятельно, либо в сотрудничестве с частными компаниями):

    а. ведение нецелевого массового наблюдения независимо от используемых методов, технологий или видов коммуникаций, которые подлежат постановке под наблюдение;

    б. использование ключевых слов или других фильтров для извлечения данных из информации, собранной с помощью массового наблюдения, в особенности, когда использование таких фильтров способно идентифицировать лиц;

    в. сбор информации из коммуникаций/метаданных напрямую либо через третьих лиц, в том числе частных компаний;

г. сбор персональных данных, находящихся в распоряжении других государственных органов;

д. наблюдение через компьютерные сети.

7. Удостовериться, что наблюдение через компьютерные сети подвергается такому же надзору, как и при других методах наблюдения, одинаково воздействующих на права человека.

8. Изучить вопрос привлечения к процессу выдачи разрешений на ведение целевого и нецелевого наблюдения независимых защитников общественных интересов для представления интересов потенциальных объектов наблюдения.

9. Изучить вопрос о том, как независимый контролирующий орган может *пост фактум* пересмотреть процедуру выдачи уполномоченным органом разрешения на ведение наблюдения.

10. Создать новый, либо наделить полномочиями существующий надзорный орган для приема и рассмотрения жалоб по всем аспектам деятельности служб безопасности. В тех случаях, когда такие органы ограничены вынесением юридически необязательных заключений и рекомендаций, государства должны обеспечить заявителям возможность обращения в иные учреждения, способные предоставить средство правовой защиты, которое будет эффективным как по закону, так и на практике.

11. Предоставить надзорному органу полномочия аннулировать разрешения на ведение наблюдений, а также приостанавливать те наблюдения, на проведение которых не требуется получения разрешений, в случаях, когда такое наблюдение будет расценено как незаконное, а также предоставить надзорному органу право требовать уничтожения любой информации, полученной с использованием таких методов.

12. Обеспечить, чтобы процедуры, в рамках которых рассматриваются нарушения, выявленные непосредственно заявителями, либо нарушения, ставшие известными иными путями, соответствовали процессуальным нормам европейского законодательства в области прав человека.

О независимости и демократической легитимности надзорных органов

13. Стараться укреплять связи между экспертными надзорными органами и парламентами, предпринимая следующие шаги:

а. предоставить соответствующему парламентскому комитету возможность назначать членов надзорных органов;

б. наделить парламент правом поручать экспертным органам проводить расследования по определенным вопросам и делам;

в. установить требование отчетности экспертных надзорных органов и их участия в слушаниях в соответствующем парламентском комитете.

Об эффективности надзорных органов

14. Обеспечить, чтобы органы надзора за службами безопасности имели полный доступ к необходимой для реализации своих полномочий информации независимо от уровня секретности. Доступ надзорных органов к информации должен быть обеспечен законом и гарантирован возможностью использования полномочий следствия, обеспечивающих такой доступ. Любые попытки ограничить доступ надзорных органов к засекреченной информации должны пресекаться и, при необходимости, наказываться.

15. Установить обязанность служб безопасности быть открытыми и сотрудничать с надзорными органами. Со своей стороны, надзорные органы несут ответственность за профессиональное осуществление своих полномочий, в том числе в вопросах сбора и использования засекреченной информации строго для решения задач, возложенных на них законом.

16. Обеспечить, чтобы доступ надзорных органов к информации не ограничивался и не обуславливался решениями третьих лиц или самих контролируемых органов безопасности. Это требования является ключевым для того, чтобы обеспечить независимость демократического надзора от наложения вето со стороны иностранных учреждений, которые передавали информацию службам безопасности. Доступ надзорных органов к информации должен распространяться на всю имеющуюся у служб безопасности соответствующую информацию, в том числе на ту, которая предоставляется иностранными службами.

17. Требовать от служб безопасности самостоятельно раскрывать контролирующим органам информацию, использование которой несет определенные риски для прав человека, а также информацию о потенциальных нарушениях прав человека деятельностью служб безопасности.

18. Обеспечить законодательную возможность привлекать обладающих специальными познаниями независимых специалистов к работе парламентских комитетов по надзору и экспертных надзорных органов. В частности, надзорные органы должны иметь возможность привлекать специалистов в области информационных и коммуникационных технологий, которые могли бы помочь таким учреждениям лучше разбираться и оценивать системы наблюдения и, как следствие, точнее оценивать их вмешательство в права человека.

19. Обеспечить достаточные кадровые и финансовые ресурсы учреждениям, надзирающим за деятельностью служб безопасности для полноценной реализации их полномочий. Полноценная реализация полномочий подразумевает необходимость прибегать к специализированным познаниям в области технологий, которые позволят органам надзора разбираться и оценивать 9 системы сбора, обработки и хранения информации. Достаточность таких ресурсов должна регулярно пересматриваться с учетом того, что увеличение бюджета служб безопасности может потребовать одновременного увеличения бюджета надзорных органов.

20. Обеспечить, чтобы все надзорные органы, имеющие доступ к засекреченной информации и персональным данным (независимо от того, засекречены они или нет) приняли меры, гарантирующие использование этой

информации исключительно в рамках полномочий надзорных органов. О прозрачности и взаимодействии с общественностью

21. Законодательно прописать обязанность органов надзора за деятельностью служб безопасности периодически отчитываться путем обнародования публичных версий своих докладов о проделанной работе и проведенных расследованиях. Эта обязанность влечет за собой необходимость выделения дополнительных ресурсов, которые позволят надзорным органам составлять содержательные отчеты без ущерба для их основных надзорных функций.

22. Обеспечить, чтобы законодательство о свободе информации распространялось также на службы безопасности и надзирающие за ними органы и, более того, решения об отказе в предоставлении информации принимались индивидуально в каждом отдельном случае, были должным образом обоснованы и проверялись независимым комиссаром по защите персональных данных/информации.

Об оценке деятельности надзорных органов и систем

23. Периодически оценивать и пересматривать правовые нормы, институциональные основы и процедуры, а также практику надзора за деятельностью служб безопасности. Следующие элементы должны быть составной частью оценки их деятельности (но не ограничиваться ими):

    а. полномочия надзорных органов, закрепленные в нормах права;

    б. вклад надзорных органов в обеспечение того, чтобы правовая основа, политика и сама деятельность служб безопасности соответствовали внутригосударственным и международным нормам в области прав человека;

    в. эффективность методов работы надзорных органов;

    г. использование новых технологий при осуществлении надзора;

    д. достаточность полномочий и средств для доступа к засекреченной информации;

    е. защита информации надзорными органами;

    ж. взаимодействие и сотрудничество между надзорными органами;

    з. отчетность и информирование общественности.

24. Оценивать соответствие целям национальной безопасности мер надзора за сбором и хранением персональных данных частными компаниями, в том числе поставщиками услуг связи, а также сотрудничество между частными компаниями и службами безопасности.

25. Пересматривать правовую основу надзора за эксплуатацией компьютерных сетей службами безопасности с точки зрения достаточности существующих механизмов для соблюдения внутригосударственного и европейского законодательства в области прав человека.

Глава 1

ВСТУПЛЕНИЕ

Непрекращающиеся разоблачения бывшего вольнонаемного сотрудника американской разведки Эдварда Сноудена вновь привлекли внимание к деятельности служб безопасности в странах-членах Совета Европы. Тревога по поводу последствий широкой электронной слежки снова породила вопросы об адекватности надзора за службами безопасности. Не требует доказательств, что надзор за службами безопасности имеет основополагающее значение для того, чтобы эти институты помогали защите людей, которым они служат (и их прав), и соблюдали закон и права человека при выполнении этой задачи. Однако разоблачения Сноудена, причастность некоторых европейских служб безопасности к тайному задержанию и выдаче подозреваемых в терроризме лиц в минувшее десятилетие и продолжающиеся обвинения в иных нарушениях в разных странах породили серьезные сомнения в способности национальных систем надзора выполнять эту роль.

Так, комиссар Совета Европы по правам человека недавно назвал демократический надзор за службами безопасности во многих европейских странах «до прискорбия неадекватным» (Commissioner for Human Rights 2015: 26).

В контексте данного доклада термин «надзор» используется в широком значении, включая проверку деятельности, принципов и правил служб безопасности до, во время и после их применения (принятия). Он включает функции, которые называют по-разному – мониторинг, проверка, рассмотрение, оценка. Термин «контроль» оставлен для функций, при которых соответствующий орган непосредственно участвует в принятии решения о том, будет ли служба безопасности заниматься той или иной деятельностью, и как именно. Надзор за службами безопасности в целом осуществляют следующие стороны: парламент; исполнительная власть; суд; специальные органы надзора; внутренние органы служб безопасности. Эти стороны вместе называют «системой надзора». В контексте данного доклада «внешний надзор» означает надзор со стороны институтов, являющихся внешними по отношению к службам безопасности и соответствующим департаментам/ министерствам/ министрам исполнительной ветви власти. В дополнение к официальным институтам надзора, которые в целом опираются на закон или даже на конституцию, гражданское общество и СМИ также играют важную роль в надзоре за службами безопасности и в мониторинг работы органов надзора.

Вывеска «служба безопасности» касается государственных органов, включая как самостоятельные ведомства, так и департаменты/подразделения других правительственных департаментов или вооруженных сил, имеющие задачу сбора, анализа и передачи информации в пределах государства для обеспечения принятия обоснованных решений политиками, военным командованием, полицейскими органами следствия и пограничными (таможенными) ведомствами касательно угроз национальной безопасности и другим фундаментальным национальным интересам. В некоторых странах-членах Совета Европы их функции могут включать также элементы правоохранительной деятельности и защиты объектов и людей. Для этого некоторые службы безопасности также имеют полномочия принуждения – ареста и задержания. Надзор за этой деятельностью должен руководствоваться теми же принципами, что применяются по отношению к персоналу правоохранительных органов – в данном докладе они детально не рассматриваются.

Соблюдение прав человека службами безопасности зависит не только от эффективного надзора, но и от правовой базы их работы. В многочисленных публикациях рассмотрено применение Европейской конвенции прав человека («Конвенция», или ЕКПЧ) к деятельности служб безопасности и сформулированы принципы, касающиеся сферы и хода их деятельности.[1] Данный доклад не будет возвращаться к этим вопросам; он не будет рассматривать, что службам безопасности разрешено делать или как нужно регулировать их работу. Вместо этого цель данного доклада – систематизировать международные стандарты и национальные подходы к надзору за службами безопасности для поиска практик и процедур, способных усилить защиту прав человека в работе служб безопасности. Это будет сделано сначала путем анализа международных правовых стандартов и принципов «мягкого права», касающихся надзора, и затем – путем рассмотрения национальных подходов к разным аспектам надзора. Наконец, в этом докладе будет рассмотрен ряд задач развития (совершенствования) системы надзора за службами безопасности. Перед тем, как приступить к оценке, в документе представлен общий обзор последствий для прав человека в некоторых областях деятельности служб безопасности на территории Совета Европы.

1. Например: ООН 2010a; Cameron 2000; Omtzigt 2015.

Глава 2

ОБЩИЙ ОБЗОР ВЛИЯНИЯ ДЕЯТЕЛЬНОСТИ НАЦИОНАЛЬНЫХ СЛУЖБ БЕЗОПАСНОСТИ НА ЗАЩИТУ ПРАВ ЧЕЛОВЕКА В ЕВРОПЕ

Давно признано, что работа служб безопасности ограничивает ряд прав человека и может подрывать демократические процессы в целом. Службы безопасности имеют ряд характеристик, создающих потенциал для нарушений прав человека, если эти службы не подлежат эффективному надзору и не опираются на эффективные законы. Среди таких характеристик – использование связанных с возможностью вмешательства полномочий, которые могут быть использованы бесконтрольно, в значительной степени в условиях секретности, и в некоторых странах рассматриваются как предоставленный правительству инструмент, который может быть использован в политических целях.

Цель этой главы – показать некоторые пути, которыми службы безопасности влияли (и продолжают влиять) на права человека в странах-членах Совета Европы; она не ставит целью дать исчерпывающий анализ того, как именно деятельность служб безопасности затрагивает права человека. Этот общий обзор приведен, чтобы лучше показать, почему службы должны подлежать строгой системе надзора. Во всей этой главе речь идет о деятельности служб безопасности. Однако иногда это нужно относить и к представителям исполнительной власти, которые направляют, определяют политику и в некоторых случаях ставят задачи службам безопасности. В разных странах Совета Европы политическая исполнительная власть имеет давнюю историю (зло)употребления служб безопасности для незаконной и антидемократической деятельности.

В данной главе будет приведен ряд наиболее ярких примеров деятельности служб безопасности, затрагивающей права человека, за минувшие 15 лет. Однако следует помнить, что нарушения прав человека службами безопасности в Европе имеют давнюю историю, многие из них происходили в эпоху, когда

службы безопасности в гораздо меньшей степени подвергались регламентации и надзору, и общественность была осведомлена о деятельности служб безопасности значительно меньше, чем сегодня. Среди ярких исторических примеров – систематические нарушения прав человека такими службами безопасности, как Stasi (в Германской Демократической Республике), Securitate (в Румынии) и STB (в Чехословакии). Нарушения прав человека ни в коем случае не сводились к деятельности служб безопасности бывшего Восточного блока. Расследования в других странах, таких, как Люксембург и Норвегия, выявили широкую незаконную слежку внутри страны, главным образом – за левыми группами и политиками.

Современные примеры влияния, которое деятельность служб безопасности может оказывать на права человека, можно разбить на четыре большие категории. Во-первых, это деятельность, влияющая на неприкосновенность личности, включая право на жизнь, право на личную свободу и безопасность, и право не подвергаться пыткам, бесчеловечному, жестокому и унизительному обращению. Во-вторых, деятельность служб безопасности влияет на право на частную и семейную жизнь. В большинстве юрисдикций это главный инструмент влияния служб безопасности на права человека. В-третьих, деятельность служб безопасности влияет на права на свободу слова, объединения и собраний. Наконец, будет коротко рассмотрено воздействие служб безопасности на право на справедливый суд и судебные процессы с участием служб безопасности.

2.1. Неприкосновенность и свобода личности

После террористических актов в США в сентябре 2001 г. («9/11») на территории Совета Европы имели место разоблачения деятельности служб безопасности в контексте борьбы с терроризмом. В целом эти разоблачения касались контртеррористической деятельности под эгидой США с участием в той или иной степени по крайней мере 25 европейских служб безопасности и правительств (Commissioner for Human Rights 2014b). Что касается причастности европейских служб безопасности к контртеррористической деятельности под эгидой США, на данный момент подтверждено или принято считать, что службы стран-частниц Совет Европы:

- размещали секретные американские тюрьмы, где подозреваемые в терроризме удерживались без связи с внешним миром и в неподобающих условиях[2];
- содействовали похищению и передаче людей на такие объекты в Европе и за пределами Европы[3];

2. Суд вынес решение против Польши в двух случаях: Al Nashiri v. Poland; Husayn (Abu Zubaydah) v. Poland. Эти решения уже окончательны, после того, как Страсбургский суд отказал в разрешении передать их в его Большую палату. Продолжаются процессы против Румынии (Al Nashiri v. Romania) и Литвы (Abu Zubaydah v. Lithuania). См. также: European Parliament 2013 и Connolly 2014.
3. См., например: El Masri v. «the former Yugoslav Republic of Macedonia» и Nasr and Ghali v. Italy. См. также: Open Society Justice Initiative 2013: 78 (Georgia), 109 (Sweden).

- организовывали и (или) принимали участие в допросах лиц, задержанных неевропейскими разведслужбами, вместе либо вместо этих служб[4].

Такие действия нарушали, в частности, Статьи 3, 5, 6, 8 и 13 Европейской конвенции прав человека. Полномасштабное исследование этих разоблачений находится за рамками данного доклада. Достаточно сказать, что институты Совета Европы (намного больше, чем национальные институты) занимались расследованием и устранением этих нарушений прав человека. В частности, можно упомянуть отчеты о расследованиях Дика Марти (Dick Marty) для Комитета по правовым вопросам и правам человека Парламентской ассамблеи Совета Европы (ПАСЕ) и знаковые решения Европейского суда по правам человека в процессах Ан-Нашири против Польши, Хусаина (Абу Зубайдаха) против Польши и Ель Масри против «Бывшей Югославской Республики Македония».

Кроме нарушений прав человека в контексте контртеррористической деятельности под эгидой США, поступали сообщения о пытках, негуманном и унизительном обращении, произвольных задержаниях и незаконном применении силы со смертельным исходом российскими силами безопасности, особенно в Чечне и Дагестане[5].

Было также много заявлений о том, что Европейские службы безопасности замешаны в нарушении права на неприменение пыток и/или не быть произвольно задержанным из-за передачи ими информации зарубежным партнерам. Хотя последствия такого информирования трудно проверить, похоже, что передавалась, в частности: информация или вопросы, заданные лицам, которых задерживали и пытали неевропейские службы безопасности[6]; информация разведслужбам США, которая могла быть использована для идентификации и выявления местонахождения людей для внесудебных убийств[7]; и информация, приведшая к выдаче людей и (или) их произвольному задержанию неевропейскими разведслужбами[8].

Кроме деятельности, касающейся международного сотрудничества разведслужб, поступали сообщения о том, что в некоторых странах Совета Европы службы безопасности продолжают участвовать в произвольных арестах и удержании людей без связи с внешним миром[9]. Именно в этой области секретность и широкая свобода действий, характерные для работы служб безопасности, представляют особую угрозу неприкосновенности личности.

---

4. См., например: Human Rights Watch 2009: 17-35; Cobain 2013: 240-242, 253, 257-258 и Open Society Justice Initiative 2013: 78 (Germany).
5. См., например: ООН 2010b: параграфы 208-214 и Nemtsova 2012.
6. Cobain 2013: Chapter 8.
7. См., например: Singh and Scholes 2014; Stark 2011; Osborne 2013.
8. См., например, продолжающийся в Великобритании процесс Абдула Хакима Бельхаджа (Abdul Hakim Belhaj): www.reprieve.org.uk/case-study/abdul-hakim-belhaj/, accessed 28 March 2015.
9. Например: Commissioner for Human Rights 2013a: § 8.

2.2. Право на частную и семейную жизнь

Службы безопасности могут сильней всего влиять на право на частную и семейную жизнь путем сбора, хранения и передачи персональных данных[10]. Праву на частную жизнь угрожает не только фактическое применение этих мер по отношению к данным лицам, но и возможность их применения или даже само существование законодательства, разрешающего их применение[11]. Право на частную жизнь, конечно, может быть законно ограничено службами безопасности, если это соответствует требованиям национального законодательства и ЕКПЧ.

В прошлом обеспокоенность влиянием на право на частную жизнь вызывало в основном использование службами безопасности целенаправленной слежки при помощи таких методов, как прослушивание личного телефона или размещение подслушивающих устройств в жилище – иными словами, меры, направленные на данного человека или организацию, обычно на основе обоснованного подозрения в участии в серьезной преступной деятельности или другой угрозе национальной безопасности. Сбор информации о человеке, включая привлечение информаторов и внедрение в группы, является еще одним аспектом работы служб безопасности, давно влияющим на право на частную жизнь. Хотя такие действия продолжаются и по-прежнему влияют на право на частную жизнь, обеспокоенность ими во многих странах Совета Европы сменяют сообщения о нецеленаправленной, массовой слежке за электронными средствами связи.

Быстрое развитие технологий дало службам безопасности в ряде стран-членов Совета Европы возможность шире контролировать средства связи при меньших трудозатратах. В Европе общественное внимание в связи с массовым перехватом службами безопасности впервые привлекли сообщения о системе «Echelon» в начале столетия (European Parliament 2001). Гораздо более серьезными стали разоблачения бывшего вольнонаемного сотрудника американской разведки Эдварда Сноудена, впервые прозвучавшие летом 2013 г. Сноуден сообщил о масштабной слежке за электронными средствами связи и Интернетом со стороны Агентства национальной безопасности США и различных служб безопасности в Европе. Сообщения о подобных программах также появились, в частности, во Франции[12].

---

10. Подтверждено Европейским судом по правам человека в отношении следующих видов деятельности: телефонная связь (Malone v. the United Kingdom [64]); электронная почта (Weber and Saravia v. Germany [77]); хранение информации в реестрах служб безопасности (Segerstedt-Wiberg and Others v. Sweden [72]); несообщение человеку о сборе информации о нем (Segerstedt-Wiberg and Others v. Sweden [99]); хранение и использование персональных данных службой безопасности (Leander v. Sweden [48]); передача и использование другими органами власти, представляющая собой отдельный акт вмешательства (Weber and Saravia v. Germany [79]); передача на уничтожение и неуведомление (Weber and Saravia v. Germany [79]); установка подслушивающих устройств (Vetter v. France [20]).
11. Weber and Saravia v. Germany [78-79]; Liberty and Others v. the United Kingdom [57].
12. Follorou and Johannès 2013; Follorou 2014; Bigo et al. 2014.

В отличие от более традиционных методов слежения, программы, о которых сообщалось, не обязательно направлены против конкретных лиц или организаций в связи с подозрением в участии в той или иной деятельности. Вместо этого широко применяется автоматический перехват (с помощью разных инструментов, а иногда – при помощи провайдеров услуг связи) огромных массивов информации, проходящей по оптоволоконным кабельным или беспроводным линиям связи, или хранящейся у третьих сторон. Собранная информация включает содержание сообщений, а также так называемые данные связи, или мета-данные, такие, как электронные адреса, IP-адреса, телефонные номера и места нахождения телефонов. Собранная информация позднее просматривается или фильтруется, используя определенные настройки или условия поиска информации, касающейся лиц (организаций), интересующих службы безопасности[13].

Разоблачения Сноудена вызвали серьезную тревогу за право на частную и семейную жизнь. Такая деятельность расследовалась Европейским парламентом (ЕП), Комитетом по правовым вопросам и правам человека ПАСЕ (докладчик Питер Омтцигт (Pieter Omtzigt)) и различными национальными органами надзора. Претензии в этой связи предъявлялись как в национальных судах[14], так и в Страсбургском суде[15].

Комментируя сообщения о массовой слежке, специальный докладчик ООН Бен Эммерсон (Ben Emmerson) заявлял, что:

> Само существование программ массовой слежки таит возможность непропорционального вмешательства в право на частную жизнь … постоянный и неизбирательный сбор государствами всех сообщений или мета-данных несовместим с существующими концепциями частной жизни. [Эти программы –] прямой и продолжающийся вызов укоренившимся нормам международного права. (ООН 2014: §§18, 59)

Верховный комиссар ООН по правам человека также выразил озабоченность оправданием такого вмешательства в право на частную жизнь, заявив:

> Будет недостаточно, если меры будут направлены на поиск нескольких иголок в стогу сена; правильный критерий – воздействие мер на стог сена, соответствующее возможному вреду; а именно, являются ли меры необходимыми и пропорциональными. (Управление Верховного комиссара ООН по правам человека 2014: §25)

Наконец, комиссар Совета Европы по правам человека назвал такую массовую слежку «серьезной угрозой праву на частную жизнь» (Commissioner for Human Rights 2013b).

Право на частную жизнь затрагивает не только перехват содержимого сообщений, но и сбор, хранение и использование так называемых данных связи, или

13. Общий обзор см. в: Venice Commission 2015: §§ 48-51; Bigo et al. 2013; Omtzigt 2015.
14. См., например, Privacy International in the UK: www.privacyinternational.org/?q=legal-actions, accessed 28 March 2015.
15. Big Brother Watch and Others v. the United Kingdom.

мета-данных[16]. Хотя данные связи могут собирать и хранить непосредственно службы безопасности, в большинстве стран частные провайдеры услуг связи по закону обязаны хранить данные связи клиентов определенный период.

В апреле 2014 г. Судебная палата Европейского союза заключила, что директива о хранении данных ЕС, которая позволяла хранение данных связи провайдерами услуг связи для правоохранительной деятельности, несовместима с правом на частную жизнь[17]. Комментируя связь данных связи с частной жизнью, палата заключила, что:

> Данные [связи], взятые в целом, могут позволить сделать очень точные выводы о частной жизни людей, чьи данные сберегаются, такие, как привычки повседневной жизни, постоянное или временное место жительства, ежедневные или иные перемещения, занятия, социальные отношения этих людей и их социальное окружение[18].

Во многих странах-членах Совета Европы массовая неизбирательная слежка служб безопасности либо не регламентируется каким-то общедоступным законом, либо регламентируется настолько туманно, что закон предусматривает мало ограничений и вносит мало ясности в эти меры.

Это проблематично с позиций прав человека, поскольку усложняет понимание частными лицами и организациями правовой основы и оснований для возможного перехвата их сообщений или оспаривание такой слежки как незаконной (Commissioner for Human Rights 2014a: 109-110).

Незаконное проникновение в компьютерные сети (в просторечии – хакерство) – еще одна сфера деятельности служб безопасности, таящая серьезный риск для прав человека. Хакерство охватывает такие разные методы, как внедрение вирусов или «троянов» в информационные системы для извлечения информации; использование камер и микрофонов компьютеров и переносных устройств для фиксации деятельности пользователей; проникновение в электронные устройства для манипуляций с содержанием отправленных ими (им) сообщений[19]. Эта сторона деятельности остается относительно новой, детально не регламентированной в законодательстве о службах безопасности и не рассмотренной в публичных отчетах о работе служб безопасности. Тем не менее ясно, что такая деятельность представляет серьезную угрозу для права на частную и семейную жизнь. Хакерство потенциально более бесцеремонно, чем перехват содержания сообщений и (или) мета-данных, не в последнюю очередь – потому, что оно дает доступ к информации, которой человек предпочел бы никогда ни с кем не делиться. В обращении к Трибуналу по полномочиям следствия (*Investigatory Powers Tribunal*) Великобритании организация Privacy International передает угрозу частной жизни следующим образом:

---

16. Подробнее см.: Commissioner for Human Rights 2014a: 115-117.
17. Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources and Others, см. в частности [29] [57] [58] и [65].
18. Там же, [27].
19. Общий обзор см. в: Omtzigt 2015: §§ 66-69; Gallagher and Greenwald 2014; BBC News 2015.

> Современный эквивалент вторжения в чей-то дом, поиска в его шкафах, дневниках и письмах и установки устройств для постоянной слежки в будущем и, при использовании мобильных устройств, получение хронологической информации, включая все места, где он был в прошлом году … если мобильное устройство заражено, постоянная слежка нигде не оставит человека в покое. (Privacy International 2014: §§ 4-6, 11-18)

Если взять в качестве примера использование микрофона и камеры смартфона для фиксации текущих контактов и окружения человека, это, безусловно, более бесцеремонно, чем размещение подслушивающих устройств в доме или машине и (или) персональная слежка за таким человеком. Хакерство также может привести к возникновению в системе слабых мест, чем могут воспользоваться третьи стороны, например, организованные преступные группы.

Наряду с озабоченностью тем, что межгосударственный обмен разведывательной информацией может привести к пыткам и произвольному задержанию человека, передача персональных данных службами безопасности за рубеж часто влечет последствия для права на частную жизнь. Это право затрагивается каждый раз при передаче персональных данных. Особая обеспокоенность возникает, когда иностранные службы безопасности, которым передается информация, не имеют аналогичных стандартов защиты данных и (или) строгих юридических требований, ограничивающих использование персональных данных в тех или иных целях. Хотя многие службы безопасности сопровождают переданную информацию оговорками (требованиями касательно порядка использования информации), они не могут полностью нивелировать возможные нарушения получателем права на частную жизнь. Следующий вопрос – преднамеренное или случайное использование межгосударственного обмена разведывательной информацией, чтобы обойти ограничения, обычно действующие в отношении сбора информации. В то время как службы безопасности обычно должны получить санкцию, например, на перехват переговоров человека в своей стране, если та же информация была получена зарубежным партнером и затем передана, она может не подпадать под такие ограничения.

Эти риски возрастают в условиях обмена разведывательной информацией, предусматривающих автоматическую передачу электронных данных и (или) наличие встроенных систем сбора и хранения информации в интересах нескольких государств[20].

2.3. Право на свободу слова, собраний и объединений

Деятельность служб безопасности влияет на право на свободу слова, собраний и объединений, то есть права, призванные защитить взаимоотношения с другими людьми.

20. Общий обзор см. в: Venice Commission 2015: § 78.

Препятствование этим правам может иметь далеко идущие последствия для процессов, присущих функционированию демократии и верховенства права, включая свободную прессу, деятельность политических партий, профсоюзов, религиозных организаций и правозащитников.

Препятствование этим правам может быть прямым или опосредованным. Службы безопасности иногда прямо препятствуют праву на свободу слова, например, вынуждая СМИ менять свою редакторскую политику (Human Rights Watch 2014a: 25), требуя не допустить публикации информации[21], настаивая, чтобы организации удалили переданную в эфир информацию[22], вынуждая организации удалять информацию, которая может (в дальнейшем) быть опубликована (Borger 2013), и изымая информация у журналистов[23]. Такие меры иногда могут представлять собой законное ограничение прав человека; однако они также предпринимаются в нарушение ЕКПЧ.

Столь же важно использование полномочий (например, служб безопасности России), позволяющих службам безопасности выносить предупреждения лицам, поведение которых (включая публикации или выступления) считается нежелательным, но еще не достигло порога уголовного преступления[24].

Непрямое препятствование правам на свободу слова, объединения и собраний в первую очередь происходит из-за слежки, включая как целенаправленные, так и неизбирательное мероприятия, и (все больше) хакерство служб безопасности. Мониторинг службами безопасности (возможный или фактический) переписки, высказываний и разговоров человека может ограничивать осуществление этих прав, поскольку он влияет на желание человека участвовать в таком общении и может формировать содержание такого общения. Реагируя на сообщения о массовой слежке в интернете, Верховный комиссар ООН по правам человека заметил, что под угрозой оказывается все эти права, потому что это права, которыми все чаще пользуются при помощи цифровых СМИ (Управление Верховного комиссара ООН по правам человека 2014). В этой связи, существует прочная связь между правом на частную и семейную жизнь и свободой слова, объединения и собраний. Частная жизнь позволяет людям реализовать другие свои права без незаконного вмешательства (Генеральная Ассамблея ООН 2013).

Ограничительный эффект (потенциальной) слежки возникает не только из-за перехвата содержания сообщений или переговоров, но и, как недавно признала Судебная палата Европейского союза, из-за законов, разрешающих хранение данных связи/мета-данных[25].

---

21. Sunday Times v. the United Kingdom (No. 2).
22. Например: Le Monde 2013.
23. См., например, дело Девида Миранды (David Miranda) в Великобритании: www.bbc.co.uk/news/uk-23782782, accessed 28 March 2015.
24. См., например, дискуссию Венецианской комиссии о таких полномочиях в России: Venice Commission 2012: §§ 48-61.
25. Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources and Others [28].

Европейский суд по правам человека признал, что не только фактическое ведение слежки влияет на право на свободу слова (и, по аналогии, объединений и собраний), но и само существование законодательства, разрешающего такие меры, представляет собой вмешательство[26]. Кроме сбора информации, Суд признал, что обработка персональных данных касается не только права на уважение к частной и семейной жизни, но и права на свободу мысли, совести и религии, слова, собраний и объединений, если такие данные обрабатывают в связи с политической позицией человека или его участием в тех или иных группах[27].

В некоторых странах Совета Европы правящая партия или руководители правительства/государства продолжают использовать службы безопасности в качестве инструмента. Такое вмешательство принимает разные формы. В наиболее грубой форме оно включает запугивание (и даже физические нападения) со стороны служб безопасности в отношении людей (организаций), которые считаются критически настроенными к правительству, а также прямое вмешательство в политические процессы (Commissioner for Human Rights 2013a: §39). Чаще службы безопасности подслушивают оппозиционных политиков, НПО и судей (по требованию политической исполнительной власти или по своей собственной инициативе), чтобы получить компрометирующую информацию для очернения и (или) запугивания лиц, считающихся оппонентами. Такие обвинения звучали, например, в «Бывшей Югославской Республике Македония» и Сербии (Balkan Insight 2015a). Деятельность подобного характера подрывает демократические процессы и верховенство права. Наконец, были случаи, когда службы безопасности вели несанкционированную слежку за членами исполнительной власти (Higgins 2013). Это особенно проблематично, учитывая, что демократическое правление требует, чтобы службы безопасности находились под гражданским контролем и не становились государством в государстве.

Особенно тревожит влияние слежки служб безопасности за СМИ, чьи функции включают информирование о политике и практике безопасности правительств. Слежка может подрывать конфиденциальность журналистских источников и, соответственно, способность журналистов раскрывать «грехи» правительства[28]. Такая работа особенно важна, учитывая, что во многих странах официальные органы надзора были неэффективны при фиксации и реагировании на нарушения прав человека службами безопасности.

2.4. Право на справедливый суд и право на эффективную правовую защиту

Деятельность служб безопасности может вредить праву на справедливый суд и праву на эффективную правовую защиту разными путями. Во-первых, людям часто очень трудно подать гражданский иск против служб безопасности, даже если они знают, что их права могли быть нарушены. Дело в том, что правитель-

26. Weber and Saravia v. Germany [144].
27. Segerstedt-Wiberg and Others v. Sweden [107].
28. Weber and Saravia v. Germany [143] [145]; см. также: European Parliament 2014: §§ 86-87.

ства и службы безопасности могут ссылаться на аргумент государственной тайны, чтобы не допустить заслушивания претензий, или придерживаться тактики «не подтверждать и не отрицать» (в отношении своих агентов и деятельности), чтобы выхолостить судопроизводство.

Во-вторых, если и удается подать иск, судебная процедура может быть существенно изменена для защиты секретной информации. Такие изменения процедуры могут усложнить или сделать невозможным справедливый суд. Например, участников и их законных представителей могут не допустить к участию в процессе или его части, что осложняет им ознакомление и тем более защиту в делах против них. Также могут быть ограничены или отсутствовать права на разъяснение приговора и очень ограничиваться права апелляции.

В-третьих, перехват переписки между адвокатами и их клиентами, как это было недавно выявлено в Великобритании, может нарушать равенство сторон и право на справедливый суд, особенно если в процессе участвуют службы безопасности (Travis and Bowcott 2015).

В-четвертых, передача информации иностранным органам безопасности и правоохранительным органам может нести риск для права на справедливый суд. Что касается информации, передаваемой иностранным органам, существует риск ее использования (вопреки предупреждениям о надежности или запрете использования в судебном процессе) в уголовных и других процессах.

Информация, полученная от иностранных органов, которая могла быть получена с нарушением прав человека или является ненадежной по другим причинам, в некоторых странах может использоваться в судебных процессах, что делает их несправедливыми.

Наконец, некоторые страны приняли законы, дающие сотрудникам служб безопасности фактический иммунитет от расследования и (или) гражданских исков. В Турции, например, сотрудников служб безопасности нельзя преследовать в судебном порядке без разрешения премьер-министра и министра внутренних дел[29]. Такие положения могут способствовать безнаказанности нарушений прав человека.

29. Turkey 2014; Human Rights Watch 2014b.

Глава 3

ОБЩИЙ ОБЗОР МЕЖДУНАРОДНЫХ И ЕВРОПЕЙСКИХ СТАНДАРТОВ ДЕМОКРАТИЧЕСКОГО НАДЗОРА ЗА НАЦИОНАЛЬНЫМИ СЛУЖБАМИ БЕЗОПАСНОСТИ

Международные и европейские стандарты надзора за службами безопасности в целом можно разделить на обязательные правовые инструменты («твердое право») и необязательные принципы или рекомендации («мягкое право»). К последней категории относится ряд международных и региональных договоров, а также их толкование соответствующими судебными или договорными органами. Последняя категория включает рекомендации, резолюции, декларации и отчеты из четырех источников: (i) институты ООН; (ii) институты Совета Европы; (iii) Европейский Союз; (iv) международные инициативы гражданского общества.

3.1. Международные и региональные правовые инструменты

Не существует международных договоров, прямо касающихся надзора за службами безопасности. Однако Международный пакт о гражданских и политических правах (МПГПП)[30], Конвенция ООН против пыток (UNCAT) и ЕКПЧ включают статьи, касающиеся обязательств государств по надзору за службами безопасности.

Все страны-участниц Совета Европы связаны этими договорами.

30. International Covenant on Civil and Political Rights, 16 December 1966 (entry into force 23 March 1976).

Конкретные требования надзора согласно Статье 8 ЕКПЧ (Право на уважение к частной и семейной жизни)

Статья 8 ЕКПЧ толкуется как предполагающая ряд требований к надзору за службами безопасности. Применяя Статью 8, Страсбургский суд определил критерии (минимальных) требований надзора с тем, чтобы мероприятия служб безопасности, ограничивающие право на частную и семейную жизнь, соответствовали ЕКПЧ. Суд также изложил факторы, которые могут оцениваться на индивидуальной основе при принятии решения, обеспечивает ли данная система надзора достаточную защиту. Эта судебная практика была выработана главным образом на основе исков, поданных в связи с целенаправленными и неизбирательными мерами слежки, хранением персональных данных службами безопасности и попытками отдельных лиц проверить, хранят ли службы безопасности их персональные данные.

Обсуждаемые тут принципы, тем не менее, можно применить к надзору за другими мероприятиями, затрагивающими Статью 8 Конвенции. Стоит отметить, что они могут распространяться на хакерство в ситуациях, когда эти мероприятия затрагивают право на частную жизнь. Хотя они не рассматриваются в данном документе, следует отметить, что деятельность служб безопасности должна соответствовать и другим требованиям, изложенным в Статье 8(2) и практике ее применения, не касающимся непосредственно надзора (Venice Commission 2007, 2015).

Суд отметил критическую важность внешнего надзора для защиты от злоупотреблений и произвольного применения связанных с вмешательством мероприятий. Он подчеркнул, что внешний надзор за мероприятиями слежки может проводиться до осуществления этих мероприятий, во время их осуществления или после их завершения[31]. Последние этапы часто объединяют в один этап, отличный от санкционирования связанных с вмешательством мероприятий[32].

Что касается санкционирования мер слежки, то Суд четко выразил предпочтение санкционированию слежки судебным органом, но не назвал это требованием соблюдения Статьи 8[33]. Органы, призванные санкционировать связанные с вмешательством мероприятия, должны быть независимы от соответствующих служб и от исполнительной власти[34]. Суд дал понять, что эти меры предосторожности в разной степени касаются санкционирования целенаправленной и неизбирательной слежки[35]. Оценивая, обеспечивает ли данный орган или система достаточную защиту на этапе санкционирования, Суд может принимать во внимание их полномочия и компетенцию[36], а также количество санкций, выдаваемых ежегодно[37].

---

31. Klass and Others v. Germany [54].
32. Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria [84]. См. также: Cameron 2013: 170-171.
33. Klass and Others v. Germany [54] [56]; Kennedy v. the United Kingdom [167].
34. Dumitru Popescu v. Romania [72][73]; Klass and Others v. Germany [56].
35. Liberty and Others v. the United Kingdom [64].
36. Klass and Others v. Germany [56].
37. Lordachi and Others v. Moldova [51].

Европейский суд по правам человека также принял решение о правилах последующего надзора, указав, что Статья 8 может быть нарушена, если в последующем рассмотрении мер слежки, хранения и уничтожения персональных данных службами безопасности не участвовал действительно независимый орган[38]. Должна существовать четкая правовая база, определяющая, как осуществляется такой надзор[39]. Наконец, Суд определил ряд дополнительных характеристик органов надзора, связанных с оценкой, обеспечивают ли меры надзора достаточную защиту. Среди них – имеет ли контролер доступ ко всем соответствующим документам (включая секретные материалы); издаются ли публичные отчеты (с соответствующими ограничениями для секретных материалов); и имеет ли орган надзора полномочия аннулировать санкцию/ордер на слежку и требовать уничтожения полученных материалов[40].

Отдельно от Суда, в решении 2014 г., обязательном для 28 стран-членов Совета Европы, являющихся также членами ЕС, Большая судебная палата ЕС указала, что для доступа государственных органов к данным связи требуется:

Предварительное рассмотрение судом или независимым административным органом, решение которого направлено на ограничение доступа к данным и их использования строго тем, что необходимо для выполнения поставленной задачи, которое проводится после обоснованного запроса этих органов, поданного в рамках процедур предотвращения, выявления или уголовного производства[41].

Следует отметить, что это решение было принято в конкретных условиях оценки законности директивы ЕС о хранении данных, требовавшей хранения данных в основном для правоохранительных целей. Кроме того, национальная безопасность и деятельность служб безопасности в значительной степени выходят за рамки законодательства ЕС. Тем не менее, решение Судебной палаты Европейского союза четко указывает, что требуется предварительное независимое утверждение запросов на доступ к данным связи, чтобы осуществление таких полномочий соответствовало праву на частную жизнь. Почти наверняка будет применяться такое же обоснование, как и при рассмотрении подобных мер, в т.ч. в связи со службами безопасности, согласно Статье 8 ЕКПЧ.

Расследование нарушений прав человека и обеспечение эффективной правовой защиты

Государства обязаны обеспечить возможность обращения людей за эффективной правовой защитой при нарушении их прав (Article 13 ECHR; Article 2(3) ICCPR; Articles 13 and 14 UNCAT). Это очевидно касается надзора за

38. Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria [85] [87].
39. Lordachi and Others v. Moldova [49].
40. Kennedy v. the United Kingdom [166] [167].
41. Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources and Others [62].

службами безопасности, поскольку один или несколько институтов, ответственных за надзор, должны расследовать обвинения в нарушении прав человека и обеспечивать эффективную правовую защиту жертв. Важность обеспечения эффективной правовой защиты подтвердил Комитет ООН по правам человека, заявив, что не расследование заявлений о нарушениях прав человека само по себе может быть нарушением МПГПП (Комитет по правам человека ООН 2004: § 15).

В свете обвинений в пытках, UNCAT устанавливает более детальные требования, включая «систематическое рассмотрение правил, инструкций, методов и практик допроса, а также правил содержания под стражей и обращения с лицами, подвергнутыми любой форме ареста, задержания или заключения», и проведение незамедлительного расследования обвинений в пытках[42].

В странах, где службам безопасности разрешено допрашивать и (или) задерживать людей (или они делают это без правовых оснований), эти обязательства вряд ли будут действенными.

Не считается хорошей практикой, когда службы безопасности имеют полномочия ареста, допроса и задержания, и применение этих полномочий не должно разрешаться, если службы не имеют правоохранительных функций. В любых обстоятельствах, в которых службы пользуются такими полномочиями, считается важным, чтобы они подлежали тем же стандартам, что применяются по отношению к правоохранительным органам, выполняющим те же функции[43].

Статья 13 ЕКПЧ и практика ее применения налагают такие же требования на расследование и устранение нарушений прав человека службами безопасности. Кроме того, Суд заключил, что если у человека есть аргументированная претензия к службам безопасности (или любому другому государственному органу) в связи с нарушением Статьи 3 или 5, соответствующую статью следует читать вместе со Статьей 13, чтобы требовать эффективного официального расследования[44]. Это требует серьезных попыток выяснить, что произошло, принятия всех обоснованных мер для сохранения улик, разрешения жертве фактически участвовать в расследовании и независимости любого расследования от исполнительной власти[45].

Суд давно признал, что концепция эффективной правовой защиты не может иметь такое же содержание при проведении тайных мероприятий, связанных с вмешательством, потому что эффективность таких мер зависит от их сохранения в тайне. Ввиду этого Суд согласился, что если тайные меры слежки продолжаются или лицу не может быть сообщено о них на других законных

42. Конвенция ООН против пыток и других жестоких, бесчеловечных или унижающих достоинство видов обращения и наказания, 10 декабря 1984 г. (введена в действие 26 июня 1987 г.), Статьи 11-12.
43. ООН 2010a: практические методы 27-28; International Commission of Jurists 2009: 89.
44. Assenov and Others v. Bulgaria [102]; El Masri v. «the former Yugoslav Republic of Macedonia» [182] [242].
45. Assenov and Others v. Bulgaria [102-103]; El Masri v. «the former Yugoslav Republic of Macedonia» [182-184].

основаниях, правовая защита должна быть настолько действенной, насколько это возможно в данных обстоятельствах[46]. Однако Суд заключил, что тот факт, что человека нельзя информировать, следят ли за ним, не должен препятствовать возможности подать жалобу в орган надзора. Такой орган должен быть способен провести расследование, чтобы гарантировать проведение всех мероприятий в соответствии с законом, не информируя жалобщика[47]. Как только человеку станет известно о мероприятиях, вследствие юридического требования информировать его или иным образом, он должен иметь право обратиться в орган, способный обеспечить эффективную правовую защиту. Суд подчеркнул, что такая правовая защита должна осуществляться не только по закону, но и на практике[48].

По аналогии с требованиями надзора за мерами слежки (описанными выше), нет требования, чтобы орган, ответственный за расследование жалоб и обеспечение правовой защиты, был судебным органом. Тем не такие органы должны иметь достаточные полномочия и процедурные гарантии для обеспечения эффективности правовой защиты[49]. В частности, от того, имеет ли орган полномочия вводить юридически обязательные меры правовой защиты (а не рекомендации), зависит оценка его эффективности в контексте Статьи 13[50]. Полномочия давать распоряжения об уничтожении файлов или стирании собранной информации являются важным сопутствующим обстоятельством[51]. При оценке наличия эффективной правовой защиты можно принимать во внимание совокупность имеющихся мер правовой защиты[52], которые могут предоставлять разные органы.

3.2. Необязательные рекомендации и принципы

Существует растущий массив актов международного и европейского мягкого права, касающихся надзора за службами безопасности. Хотя обязательных принципов «твердого права», касающихся надзора, относительно немного, необязательные предложения и рекомендации формируют детальную основу для систем разработки, усиления и оценки надзора за службами безопасности. Многие документы, рассмотренные в данном разделе, имеют значительный вес, учитывая, что они были выпущены серьезными международными институтами и основаны на существующих хороших практиках, а не «мечтах». В этом разделе рассмотрен ряд ключевых положений и инноваций каждого набора принципов.

---

46. Klass and Others v. Germany [69].
47. Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria [100].
48. Segerstedt-Wiberg and Others v. Sweden [117]. См. также: Venice Commission 2007: § 129.
49. Klass and Others v. Germany [67]; Segerstedt-Wiberg and Others v. Sweden [117]; Leander v. Sweden [83].
50. Leander v. Sweden [82].
51. Segerstedt-Wiberg and Others v. Sweden [120]; Kennedy v. the United Kingdom [167].
52. Klass and Others v. Germany [72]; Leander v. Sweden [77].

3.2.1. Специальные органы ООН и Верховный комиссар по правам человека

В 2009 г. Совет по правам человека ООН поручил специальному докладчику по защите и поддержке прав человека при борьбе с терроризмом подготовить «подборку оптимальных практических методов, применяемых в отношении законодательной и институциональной основы специальных служб, и мер, касающихся надзора за их деятельностью» (Совет по правам человека ООН 2009; ООН 2010a). Он был разработан в ходе консультаций со многими сторонами, включая бывших руководителей разведок, правозащитников, с учетом мнения правительств многих стран. Эти принципы позднее были одобрены Европейским парламентом и Парламентской ассамблеей Совета Европы.

Подборка ООН включает содержательные рекомендации по надзору, включая признание важности специального надзора (в данном докладе он именуется экспертным надзором), в дополнение к парламентскому, судебному, исполнительному и внутреннему надзору и контролю. В подборке также подчеркивается важность существования органа надзора, чьи обязанности включают проверку использования персональных данных разведывательными ведомствами и получение жалоб по таким вопросам (ООН 2010a: практические методы 25-26).

Не менее важны рекомендации о необходимости сосредоточиться на всесторонней деятельности служб, причем надзор должен охватывать (как минимум):

- соответствие закону;
- эффективность и действенность их деятельности;
- их финансы; и
- их административные практики. (ООН 2010a: практический метод 6)

Наконец, рекомендации, чтобы орган надзора мог контролировать сотрудничество с иностранными разведслужбами и службами безопасности (включая договора о сотрудничестве), важны, принимая во внимание бурное развитие сотрудничества и последствия такого сотрудничества для прав человека (Born, Leigh and Wills, публикация готовится).

В 2014 г. специальный докладчик ООН по правам человека и борьбе с терроризмом предложил рекомендации по надзору за массовой слежкой, включавшие следующее.

- Независимый орган надзора должен получить право санкционировать слежку (в т.ч. массовую слежку), принимая во внимание не только национальное законодательство, но и требования необходимости и пропорциональности международного правозащитного права.
- Необходимость доступа отдельных лиц к эффективной правовой защите в случаях возможных нарушений прав на частную жизнь в интернете. Подчеркивается, что органы, ответственные за рассмотрение таких жалоб, могут иметь разные формы, лишь бы они имели доступ ко всей соответствующей информации, необходимые ресур-

сы и могли давать распоряжения об обязательных мерах правовой защиты (ООН 2014: §§ 48-50 and 61). Такое подтверждение того, что значение имеет содержание, а не форма органов надзора, важно для выработки принципов применения в отношении стран с разными конституционными (правовыми) системами – что совпадает и с подходом, принятым в подборке ООН.

Рекомендации специального докладчика ООН по свободе слова 2013 г. идут дальше, призывая к тому, чтобы слежка за линиями связи происходила только под надзором судебного органа (ООН 2013: § 81). Это больше, чем требования ЕКПЧ, выработанные на основе прецедентного права (см. выше). Франк Ла Рю (Frank La Rue) также рекомендовал, чтобы предоставление данных связи государственным ведомствам, включая службы безопасности, частными компаниями отслеживал независимый орган надзора или суд (ООН 2013: § 86).

Верховный Комиссар ООН по правам человека в 2014 г. опубликовал доклад, в котором предлагалось, чтобы процесс санкционирования включал «позиции защиты общественных интересов». Речь идет об адвокатах, назначенных, чтобы представлять интересы будущего объекта слежки (Управление Верховного Комиссара ООН по правам человека 2014: § 38).

Генеральная Ассамблея ООН

Генеральная Ассамблея ООН в 2014 г. отреагировала на разоблачения Сноудена, призвав государства, в частности:

учредить новые или продолжать использовать уже имеющиеся независимые, эффективные, обеспеченные надлежащими ресурсами и беспристрастные внутренние механизмы судебного, административного и/или парламентского надзора, способные обеспечивать в соответствующих случаях прозрачность и подотчетность в отношении слежения государств за сообщениями, их перехвата и сбора личных данных; предоставлять лицам, чье право на неприкосновенность личной жизни было нарушено в результате незаконного или произвольного слежения, доступ к эффективным средствам правовой защиты в соответствии с международно-правовыми обязательствами в области прав человека. (Генеральная Ассамблея ООН 2014: § 4)

3.2.2. Венецианская комиссия Совета Европы

Венецианская комиссия Совета Европы сыграла ведущую роль в обеспечении демократического контроля над службами безопасности. Доклад Венецианской комиссии 1998 г. о службах внутренней безопасности был первым документом, подготовленным международной организацией на эту тему (Venice Commission 1998). Во всестороннем докладе 2007 г. Венецианская комиссия представила полный анализ разных форм и моделей надзора. Доклад включает подробный анализ внутреннего, парламентского, судебного и экспертного надзора.

Венецианская комиссия выявила необходимость эффективных мер внутреннего контроля в службах безопасности, включая контроль нижнего звена ру-

ководства, процедуры обязательного утверждения запросов на разрешение связанных с вмешательством мер на уровне руководства и обучение правам человека и демократическим ценностям (Venice Commission 2007: §§ 131-133). Касательно парламентского надзора, Венецианская комиссия рекомендует, чтобы: членов комитета выбирал парламент (а не исполнительная власть), были представлены разные партии, и обеспечивалась поддержка достаточно квалифицированным персоналом (там же, §§ 21, 24). Что касается судебного надзора, то Венецианская комиссия рекомендует специальную подготовку по вопросам безопасности и изучение возможности назначения специальных адвокатов, представляющих интересы будущих объектов слежки в контексте процедур разрешения (там же, §§ 28, 31). Среди рекомендаций органам экспертного надзора – назначать их членов и принимать их отчеты парламентом (а не исполнительной властью), и избегать контроля правительства за отчетами (там же, § 34).

Также рекомендовано отделить функции рассмотрения жалоб от функций более широкого надзора (там же, § 247). Наконец, в докладе содержится важное напоминание о том, что механизмы надзора должны существовать не только на бумаге – они должны реализовываться и анализироваться (там же, § 260). Указания о том, как проводить анализ, не предлагаются.

В 2015 г. Венецианская комиссия обновила свой доклад в свете разоблачений Сноудена (Venice Commission 2015). Доклад содержит детальные рекомендации ограничений и механизмов надзора, которые могут быть адаптированы для использования при неизбирательной слежке и использовании мета-данных. Венецианская комиссия подчеркнула особую необходимость введения ограничений на двух этапах.

- Когда выбирают настройки, чтобы определить информацию, отбираемую из материалов, собранных при массовой слежке. Хотя это может разрешить судебный орган, согласно рекомендации, с этой задачей лучше всего может справиться гибридный внешний орган, состоящий из экспертов и судей, потому что это включает не только правовую оценку, но и (внешне) политические и технические соображения.
- Когда аналитики принимают решение о том, нужно ли хранить информацию, собранную путем неизбирательной слежки и отобранную при помощи настроек – процесс минимизации.

Венецианская комиссия рекомендует, чтобы за этой функцией в последующем следил внешний орган. (Venice Commission 2015: §§ 46-48, 120-121)

Парламентская ассамблея Совета Европы (ПАСЕ)

ПАСЕ также предложила принципы надзора за службами безопасности, в форме резолюций, рекомендаций и отчетов комитетов. Их можно сформулировать на основе работы Комитета по правовым вопросам и правам человека над тайными задержаниями, выдачами, массовой слежкой и государственной тайной. Будучи собранием парламентариев из 47 стран Европы, ПАСЕ естественно сосредоточилась в своих рекомендациях на необходимости усиления

парламентского надзора, порекомендовав, в частности, всем парламентам создать специальные комитеты для надзора за службами безопасности[53].

Ассамблея проявила особый интерес к доступу к информации для специальных и постоянных парламентских комитетов, подтвердив необходимость доступа парламентских комитетов ко всей информации, касающейся выполнения их функции, а также четких следственных полномочий для получения таких материалов (ПАСЕ 2013: § 9). В недавнем проекте резолюции Комитет по правовым вопросам и правам человека подчеркнул необходимость наличия механизмов надзора для доступа (и права рассмотрения) к информации, касающейся международного сотрудничества между службами безопасности (разведслужбами) безотносительно к принципу контроля со стороны источника[54]. Это особенно важно, учитывая объем информации, получаемой и передаваемой зарубежным партнерам[55].

Ассамблея также рекомендовала странам-участницам разработать состязательные процедуры для арбитража в связи со спорами, касающимися публикации информации парламентскими комитетами (и расследования судебными органами дел, касающихся служб безопасности) (ПАСЕ 2011: § 13). Этот специфический аспект прозрачности органов надзора не был охвачен другими принципами и представляет собой ценное дополнение, поскольку часто возникают затруднения с тем, что может публиковать комитет по надзору и как должны разрешаться любые споры с исполнительной властью. Может быть, самой инновационной рекомендацией Ассамблеи было ее предложение 2005 г., чтобы Комитет министров принял кодекс этики для служб безопасности аналогично Европейскому кодексу полицейской этики (ПАСЕ 2005: § 10.i.e). Хотя эта рекомендация не реализована, она остается важным пожеланием, к которому стоит вернуться.

Бывший член ПАСЕ Дик Марти воспользовался своим окончательным докладом, чтобы поддержать принципы, изложенные в вышеупомянутой подборке ООН (ООН 2010a) и в докладе Венецианской комиссии о демократическом надзоре за службами безопасности 2007 г. (Marty 2011: §§ 48-49). Марти также рекомендовал предоставить органам надзора четкие следственные полномочия, которые позволили бы им проверять деятельности служб безопасности, даже если правительство выступает против такой проверки. Кроме того, он подчеркнул часто упоминаемую важность надлежащего ресурсного обеспечения органов надзора и их полной независимости от исполнительной власти (Marty 2011: § 55).

Комиссар по правам человека

Комиссар по правам человека также давал рекомендации, касающиеся надзора за службами безопасности, в ответ на разоблачения массовой слежки.

Он подчеркивал важность формирования культуры уважения прав человека и верховенства права в службах безопасности для создания эффективной систе-

53. ПАСЕ 2011: § 13; ПАСЕ 2005: § 10.i.b.
54. В соответствии с данным принципом, служба, от которой исходит информация, имеет право определять, кому передавать эту информацию.
55. Omtzigt 2015; LAHRC 2015: § 17.2.

мы демократического надзора (Commissioner for Human Rights 2014a: 22). Это связано с необходимостью сосредоточиться на внутреннем управлении и контроле, как подчеркнула Венецианская комиссия. Комиссар также использовал свои визиты в разные страны для дачи рекомендаций, включая заявления о том, что правовая база для надзора за службами безопасности должна охватывать новые технологии слежки (Commissioner for Human Rights 2014c: 71-72). Это особенно актуальная рекомендация, поскольку одна из причин, почему некоторые органы надзора стремились разрешить проблемы, созданные массовой слежкой и хакерством, заключается в том, что они не имеют техники для надзора за деятельностью служб безопасности с применением новых технологий.

Генеральный секретарь

Усилия институтов Совета Европы дополнил бывший Генеральный секретарь Совета Европы Терри Дэвис (Terry Davis), который также дал рекомендации по надзору в 2006 г. Это произошло после сообщений о тайных задержаниях и выдачах в Европе. Дэвис отметил недостаточность проверки деятельности иностранных служб (на территории стран-членов Совета Европы) органами надзора[56]. Хотя он не вдавался в детали, как это нужно делать, эта сторона надзора ранее не была охвачена другими рекомендациями и принципами.

3.2.3. Европарламент Европейского Союза

В своем докладе о массовой слежке 2014 г. (European Parliament 2014: §§ 74-79) комитет Европарламента по гражданским свободам, правосудию и внутренним делам (Комитет LIBE) предложил рекомендации по надзору на национальном уровне (European Parliament 2007). Комитет призвал, по его выражению, к «содержательному надзору», проводимому парламентским и (или) экспертным органом надзора. Такое признание экспертного надзора подтверждает сдвиг в направлении более плюралистического понимания надзора – не только парламентского и судебного. Учитывая проблемы, сопровождающие надзор за массовой слежкой за электронными средствами связи, комитет подчеркнул необходимость предоставления контролерам достаточных технических возможностей, знаний и ресурсов. В этой связи участники призвали предоставить органам надзора полномочия посещать объекты для расследования.

Комитет Европарламента по гражданским свободам, правосудию и внутренним делам также рекомендовал, чтобы органы надзора обращались к общественности в форме отчетов. Это особенно важно, потом что контролеры призваны играть ключевую роль в разъяснении работы служб общественности и, где это необходимо, укреплении общественного доверия. Наконец, что касается надзора за слежкой, парламентарии подчеркнули, в частности, необходимость как предварительного, так и последующего надзора; это соответствует подходу Суда (European Parliament 2014).

56. Council of Europe 2006a: § 101(iv); Council of Europe 2006b: §§ 46 and 68.

Обобщая все это, Комитет по гражданским свободам, правосудию и внутренним делам призвал создать группу высокого уровня для разработки в ЕС минимальных стандартов надзора на основе принципов и лучших практик, предложенных ООН и Советом Европы (European Parliament 2014: § 77). На момент написания новых сообщений на этот счет не было.

«Рабочая группа по Статье 29»

Также под эгидой Европейского Союза, «Рабочая группа по Статье 29» в составе представителей национальных комиссий по защите данных в 2014 г. приняла декларацию европейских ценностей защиты персональных данных в контексте слежения силами национальной безопасности. Декларация содержит призыв к независимому и эффективному надзору за слежкой, включая реальное участие национальных органов защиты данных (DPA) (European Data Protection Authorities 2014: § 8). Ранее Рабочая группа рекомендовала, чтобы в государствах, где за использованием защиты данных службами безопасности надзирает национальный орган защиты данных, отличный от органа надзора, были «регулярные контакты между этим органом и национальным органом защиты данных для обеспечения единообразного и согласованного применения принципов защиты данных» (Article 29 2014a: § 8). Это важно, поскольку во многих странах-членах Совета Европы органы защиты данных не допускаются к надзору за службами безопасности (см. ниже), и поэтому их опыт защиты не используется в сфере, в которой защита данных весьма сложна.

Какой бы орган ни отвечал за надзор за использование персональных данных, «Рабочая группа по Статье 29» подчеркнула необходимость разрешения им обоим изучать вопросы по собственной инициативе и реагировать на жалобы, а также иметь полномочия реализовывать свои решения (Article 29 2014a: § 8, Recommendation B2). Наконец, «Рабочая группа по Статье 29» рекомендовала систематизировать и хранить персональные данные так, чтобы это упрощало независимый надзор (Article 29 2014b: § 11). Тем самым признается, что эффективный надзор зависит не только от полномочий и ресурсов органов надзора, но и от того, как такие институты, как службы безопасности, могут содействовать надзору и подотчетности при ведении данных.

3.2.4. Инициативы гражданского общества

Инициативы гражданского общества привели к разработке ряда важных наборов международных принципов, касающихся надзора за службами безопасности.

Принципы Цване

Глобальные принципы национальной безопасности и права на информацию (Принципы Цване, Global Principles on National Security and the Right to Information, Tshwane Principles) были разработаны в 2013 г. при участии более чем 500 экспертов со всего мира, включая многочисленных специалистов

сферы безопасности, под эгидой Правовой инициативы открытого общества (*Open Society Justice Initiative*, Open Society Foundations 2013). Принципы Цване содержат подробные указания о доступе к информации для органов, надзирающих за сферой безопасности, включая службы безопасности. Начиная с принципа, что контролеры должны иметь доступ ко всей информации, необходимой для выполнения их законных обязанностей, принципы содержат подробные указания о: видах информации (материалов), к которым контролеры должны иметь доступ; следственных полномочиях, финансовых и людских ресурсах, необходимых для обеспечения такого доступа и надлежащего использования информации; и мерах защиты информации, подлежащей надзору (Open Society Foundations 2013: Principles 32, 33, 35). Принципы Цване также содержат подробные указания об отчетности и сфере деятельности органов надзора, включая потребность в публичных версиях докладов и механизмы обеспечения публичного доступа к процедуре рассмотрения жалоб (Open Society Foundations 2013: Principle 34).

Принципы Цване наиболее известны благодаря их детальным рекомендациям о публичном доступе к информации органов власти, включая службы безопасности и их органы надзора. Особенно важны для неформального надзора за службами безопасности, в частности, со стороны СМИ и НПО, следующие указания.

- Органы власти должны предоставлять информацию по запросу, с ограниченными исключениями, регламентированными законом и необходимыми для предотвращения конкретного, подлежащего определению вреда законным интересам, в т.ч. национальной безопасности.
- Нельзя вводить ограничения на право на информацию, исходя из соображений национальной безопасности, если правительства не могут подтвердить, что ограничения определены законом и необходимы в демократическом обществе для защиты законных интересов национальной безопасности.
- Недостаточно, чтобы орган власти просто считал, что существует риск вреда; власть должна указать конкретные, основательные причины в подтверждение своей позиции.
- Лицо или организация, запрашивающие информацию, имеют право на быстрое и недорогое рассмотрение независимым органом отказа в предоставлении информации или вопросов, связанных с запросом. (Open Society Foundations 2013: Principles 1-5, 26)

Хотя Принципы Цване – продукт гражданского общества, можно сказать, что они имеют немалый вес в Европе, поскольку они были поддержаны в резолюции ПАСЕ, и Европарламент также высоко оценил эти принципы[57].

57. ПАСЕ 2013: §§ 7-8; European Parliament 2014, § 77.

Оттавские принципы

Оттавские принципы борьбы с терроризмом и прав человека (Ottawa Principles on Anti-terrorism and Human Rights*)* были разработаны группой экспертов по правам человека и борьбе с терроризмом в 2006 г.

Эти принципы призывают к плюралистическому подходу к надзору за службами безопасности, включая меры внутреннего контроля в службах безопасности; исполнительную власть; независимый орган надзора; законодательную власть; судебную проверку; институты прав человека, защиты данных, свободы информации и аудита; и гражданское общество (Ottawa Principles 2006: 9.1.1).

Особенно полезно перечисление в Оттавских принципах задач системы надзора, среди которых – обеспечение правомерности; эффективности; прозрачности; легитимности и подотчетности деятельности служб безопасности (Ottawa Principles 2006: 9.1.2).

Оттавские принципы рассматривают независимый орган рассмотрения (т.е. экспертный непарламентский институт) в качестве центрального элемента системы надзора. Они предписывают, чтобы такой орган как минимум рассматривал правомерность (законность) деятельности служб безопасности и имел полномочия рассмотрения жалоб (Ottawa Principles 2006: 9.3). Как и во многих других рекомендациях, эти принципы также подчеркивают необходимость наличия у контролеров надлежащих ресурсов, доступа к информации и следственных полномочий, а также выхода публичных отчетов (Ottawa Principles 2006: 9.1.5, 9.3.3.b, d).

Принципы необходимости и пропорциональности

Международные принципы применения прав человека при наблюдении за линиями связи (*International Principles on the Application of Human Rights to Communications Surveillance*) 2013 г., разработанные ведущими экспертами в области частной жизни и безопасности и поддержанные более чем 400 НПО и научными учреждениями, дают рекомендации по применению существующих международных правовых стандартов к цифровому наблюдению. Важным дополнением к лексикону международных принципов надзора за службами безопасности является призыв предоставить независимому органу надзора право «оценивать, публикует ли государство полную и точную информацию об использовании и масштабе методов и полномочий наблюдения за линиями связи в соответствии с его обязательствами прозрачности … и публиковать периодические доклады и другую информацию, касающуюся наблюдения за линиями связи»[58]. Тем самым признано, что органы надзора должны играть важную роль в обеспечении большей прозрачности служб безопасности, что важно для формирования (восстановления) доверия к службам безопасности.

58. https://en.necessaryandproportionate.org/text, Principle 10.

Глава 4

НАЦИОНАЛЬНЫЕ ПРАКТИКИ В СТРАНАХ-ЧЛЕНАХ СОВЕТА ЕВРОПЫ

Страны-члены Совета Европы практикуют разные подходы к структуре и осуществлению надзора за своими службами безопасности. В этой главе будут рассмотрены национальные подходы к надзору со стороны: (i) парламентских комитетов; (ii) институтов независимого надзора, включая органы экспертного надзора за безопасностью (разведкой) и институты, имеющие более широкую юрисдикцию, такие, как омбудсмены и уполномоченные по вопросам данных (информации); и (iii) судебных органов, включая квази-судебные органы. Меньше внимания будет уделено роли политической исполнительной власти и механизмов внутреннего контроля служб безопасности. Эта глава заканчивается рядом примеров, показывающих роль неформальных контролеров: гражданского общества и СМИ.

О рассмотрении жалоб, касающихся служб безопасности, речь идет в нескольких главах, поскольку страны-члены Совета Европы наделили этими функциями разные органы надзора. Хотя в надзоре за службами безопасности важны специальные запросы, в этом документе рассматриваются только постоянные органы надзора, работающие на регулярной основе. Вместо рассмотрения целостных национальных систем надзора, взяты примеры из систем разных стран. Это сделано с тем, чтобы подчеркнуть разницу в подходах и хороших практиках.

Ни в одной из стран-членов Совета Европы система надзора не соответствует всем международно и регионально признанным принципам и хорошим практикам, рассмотренным в Главе 5. Также следует подчеркнуть, что не существует одного, лучшего подхода к организации системы надзора за службами безопасности. Разные конституционные нормы, правовые и политические системы, исторические ситуации обусловливают разные подходы на территории Совета Европы. Соответственно нужно с осторожностью подходить к огульному заимствованию или копированию опыта других стран. Вместе с тем нет сомнения, что существуют модели и практики, которые можно считать более эффективными для защиты прав человека при деятельности служб безопасности. Эти примеры будут рассмотрены в данной главе.

4.1. Парламентские комитеты

В большинстве стран-членов Совета Европы либо создан парламентский комитет (подкомитет) по надзору за службами безопасности (как в Италии, Германии, Польше), либо эти функции поручены комитету с более широкими полномочиями, например, внутренних дел, национальной безопасности или обороны (как в Грузии и Черногории). Многие парламентские комитеты также могут иметь законодательные функции, но они находятся за рамками данного доклада.

На территории Совета Европы наблюдается тенденция поручать парламентский надзор за службами безопасности одному комитету, занимающемуся исключительно надзором за службами безопасности. В некоторых государствах создано несколько комитетов по надзору, каждый их которых отвечает за конкретную службу безопасности. Например, в парламенте Румынии имеются отдельные комитеты по надзору за службой внутренней безопасности и за службой зарубежной разведки, а также комитет обороны, чьи обязанности включают определенные аспекты работы обеих служб. Так же обстоит ситуация в Словакии, где имеются отдельные комитеты по надзору за Словацкой информационной службой и за Бюро национальной безопасности. Такое разделение труда может обеспечить более высокий уровень специализации и сосредоточение опыта членов комитетов.

С другой стороны, недостатки такого подхода включают риск того, что некоторые вопросы (например, обмена информация между двумя службами безопасности/разведслужбами) могут находиться на стыке полномочий двух или нескольких комитетов (Venice Commission 2007: § 154), и ресурсы может быть выгодней концентрировать на развитии одного комитета.

Полномочия и сфера надзора

В большинстве стран-членов Совета Европы полномочия комитетов парламентского надзора сформулированы нечетко, в результате чего комитет может надзирать (отслеживать, проверять) только данные службы безопасности. Например, во Франции парламентская делегация по вопросам разведки (*Délégation Parlementaire au Renseignement*) имеет задачу надзора за «общей деятельностью и методами» разных разведслужб и служб безопасности. В Германии орган парламентского контроля (*Parlamentarische Kontrollgremium*) имеет задачу надзора за «деятельностью» служб безопасности и разведслужб[59].

Большинство комитетов парламентского надзора занимаются различными вопросами, включая политику, финансы и руководство службами, а также некоторые аспекты проведенных операций (Wills and Vermeulen 2011: 92-95, 102-110, 115-116). Проверка соблюдения закона – постоянная задача, стоящая во всех этих областях. Однако некоторые парламентские комитеты, например, комитет парламентского контроля над разведывательными операциями

59. France 2007: Section 1.

литовского Сейма, имеют специальные полномочия проверять соблюдение службами безопасности конституционных прав и свобод (в дополнение к другим вопросам)[60].

Хотя «глубина» надзора разных парламентских комитетов разная, природа этих органов такова, что большинство из них не в состоянии осуществлять регулярный, детальный надзор за оперативной деятельностью, включая сбор, обмен и использование персональных данных. Такой мониторинг все больше осуществляют непарламентские независимые органы надзора.

Главная причина в том, что такого рода проверка занимает очень много времени, весьма специфична и требует ресурсов. Поэтому некоторые страны-члены Совета Европы предпочитают дополнять парламентский надзор более детальной постоянной проверкой оперативной деятельности и особенно использования и обращения с персональными данными (см. ниже).

Что касается временных аспектов надзора, парламентские комитеты европейских стран осуществляют надзор почти исключительно постфактум, рассматривая то, что уже произошло. Не имеется аналога американской практики – предварительно информировать избранных членов комитетов Конгресса по разведке о конкретных операциях или программах. С точки зрения прав человека и подотчетности нежелательно привлекать органы надзора заранее, учитывая, что им, возможно, придется рассматривать эту деятельность и в последующем – при этом может возникнуть конфликт интересов.

Рассмотрение жалоб

Некоторые парламентские комитеты по надзору (например, в Польше, Венгрии и Словакии) также обязаны рассматривать жалобы на службы безопасности[61]. Однако они вряд ли способны обеспечить эффективную правовую защиту, как того требует ЕКПЧ, потому что они, как правило, не могут давать обязательных для выполнения распоряжений. Могут также возникать вопросы, способны ли политические органы обеспечить непредвзятое расследование жалоб на нарушения прав человека. Существует явный риск того, что рассмотрение жалоб может быть политизировано и что жалобщики не смогут добиться удовлетворения из-за стремления правящих партий выгородить коллег в политическом руководстве.

Отношения с органами экспертного надзора

Парламентские комитеты по надзору также могут играть важную роль в мониторинге работы органов экспертного надзора (см. ниже); иными словами, в надзоре за контролерами. Эта роль может включать: постановку органам экспертного надзора задач рассмотрения вопросов, на изучение которых у

60. Lithuania 2002: Article 23.
61. Подробнее см.: Forcese 2012: 189-190.

парламентских комитетов может не хватать времени, ресурсов или знаний[62]; оценку их эффективности; назначение членов этих органов; обеспечение наличия у них должных полномочий и ресурсов; проведение слушаний их отчетов и реализация (или обеспечение реализации исполнительной властью) рекомендаций, предложенных этими органами. В Норвегии, например, эту роль выполняет Постоянный комитет Стортинга по контролю и конституционным вопросам (*Kontroll- og konstitusjonskomité*)[63], а в Нидерландах – комитет по разведке и безопасности второй палаты, специальный парламентский комитет в составе руководителей политический партий в палате (Verhoeven 2011: 254-255).

Доступ парламентских комитетов по надзору к секретной информации

Все парламентские комитеты по надзору имеют определенный доступ к секретной информации, и в большинстве случаев их доступ шире, чем у любого другого члена парламента (Wills and Vermeulen 2011: 117-121). Хотя потребности любого органа надзора в точной информации определяет его мандат, хорошая практика парламентских комитетов по надзору предусматривает доступ ко всей информации, которую они считают относящейся к выполнению их функций, а ограничения (если они есть) должны быть определены как можно уже. Совместный постоянный комитет по осуществлению парламентского контроля за румынской разведслужбой (внутренняя служба безопасности) в Румынии и Комитет национальной безопасности Латвии являются примерами комитетов по надзору, имеющих неограниченный доступ к информации[64]. Кроме того, полезно, когда доступ парламентских комитетов по надзору к информации подкреплен обязанностью предварительного предоставления со стороны служб безопасности и (или) исполнительной власти.

Особенно важны для защиты прав человека требования предварительного предоставления информации о деятельности, влияющей на право на частную жизнь. Прекрасным примером в этом отношении является Германия, где федеральное правительство обязано каждые шесть месяцев передавать контрольному органу Бундестага список выполненных мероприятий слежки, запросов информации у частных компаний, тревожных оповещений в рамках Шенгенского соглашения, введенных в полицейскую информационную систему, и персональных данных, переданных иностранным органам[65].

---

62. Например, после разоблачений Сноудена парламент Нидерландов потребовал, чтобы голландский комитет по надзору за службами разведки и безопасности (CTIVD) рассмотрел, в частности, массовый сбор данных голландскими службами и его последствия для прав человека: CTIVD 2014: 1.
63. Подробнее: Norway 2014: 5.
64. См. Wills and Vermeulen 2011: 128-129. В Румынии имеются ограничения на информацию о будущих и текущих операциях.
65. Germany 2001a: Section 14(1); Germany 1990b: Sections 8(a)(g), 17(3), 18(1)(a). См. также: With and Kathmann 2011: 219-220.

В некоторых странах-членах Совета Европы имеются опасения в отношении предоставления допуска парламентариям, включая членов комитетов парламентского надзора, к особо деликатной информации, особенно информации об операциях служб безопасности.

Такие опасения наиболее распространены в поставторитарных странах и странах, в парламентах которых представлены сепаратистские политические партии. Чтобы развеять эти опасения, разработаны разные механизмы, самым распространенным из которых является требование проверки предлагаемых членов комитетов парламентского надзора и получения допуска перед тем, как занять место в комитете.

Эта практика неоднозначна, по ряду причин. Во-первых, службам безопасности, возможно, придется проверять своих будущих контролеров, что ставит эти службы (а значит, и исполнительную власть) в положение, при котором они де-факто получают право ветировать членов комитетов парламентского надзора. Такая ситуация может быть использована, например, чтобы не допустить назначения потенциально критически настроенного члена парламента в комитет по надзору. Во-вторых, возникает более широкий вопрос разделения властей из-за того, что исполнительная власть получает возможность влиять или ограничивать работу членов парламента, избранных избирателями, через процедуру допуска. Если необходима проверка членов парламента, хорошей практикой может считаться рекомендательный характер доклада служб безопасности о проверке, тогда как окончательное решение о назначении парламентария в комитет по надзору принимает парламент.

Например, в Венгрии парламентский комитет по национальной безопасности принимает окончательное решение, займет ли член парламента место в комитете, независимо от результатов проверки (Földváry 2011: 231). Наконец, процедура проверки неизбежно требует, чтобы службы безопасности стремились получить деликатные персональные данные ото всех и обо всех членах парламент. Могут возникнуть вопросы о том, как в последующем может быть использована такая информация, особенно в ситуациях, когда службы безопасности или политическая исполнительная власть недовольны подходом того или иного члена комитета по надзору.

В разных странах-членах Совета Европы существуют альтернативы проверке. В Германии и Испании утверждены мероприятия отбора членов комитетов парламентского надзора, призванные обеспечить назначение и доступ к секретной информации только парламентариев, способных заручиться поддержкой (доверием) законодательного органа. В обеих странах предполагаемый член парламентского комитета по надзору должен получить поддержку квалифицированного большинства законодательного органа для назначения в комитет[66]. После получения такой поддержки уже нет требования допуска.

В других странах опасения о защите информации пытались разрешить, требуя, чтобы парламентские комитеты по надзору могли получать доступ только

66. Sánchez Ferro 2011: 269; With and Kathmann 2011: 219.

к некоторым категориям секретной информации, если они проголосуют за это квалифицированным большинством. Например, члены комитета безопасности республики в итальянском парламенте могут большинством в две трети проголосовать за отмену любых ограничений государственной тайны, которые в ином случае не разрешали бы их доступ к оперативной информации при расследовании нарушений со стороны офицеров разведки (Italy 2007: Article 31(9)). Аналогичным образом, комитет по национальной безопасности парламента Венгрии (члены которого тоже должны иметь допуск), как правило, не имеют доступа к наиболее критичной информации об оперативных методах, но могут проголосовать большинством в две трети за отмену этого ограничения для того или иного расследования (Hungary 1995: Section 16(2)). Хотя такие меры могут не позволить ненадежным членам комитета самостоятельно «выуживать» информацию, существует реальный риск того, что правящие партии могут использовать свои позиции в комитетах по надзору, чтобы блокировать доступ к наиболее важным видам информации и таким образом помешать расследованию деятельности.

Преимущества и недостатки парламентского надзора

Главные преимущества парламентского надзора за службами безопасности можно обобщить следующим образом. Во-первых, будучи избранными представителями, контролеры пользуются демократической легитимностью, проверяя службы безопасности от имени тех, кто их избрал.

Во-вторых, парламенты имеют рычаги утверждения бюджета законодателями и, иногда, полномочия по распределению бюджета, которыми можно воспользоваться для того, чтобы исполнительная власть и службы безопасности изменили свою политику или практики, нарушающие права человека.

Наконец, парламентарии в целом имеют наилучшие позиции для надзора за ролью исполнительной власти в управлении и контроле служб безопасности, потому что в большинстве стран-членов Совета Европы парламент имеет конституционную обязанность и право привлекать исполнителей к ответственности.

Есть и ряд недостатков, связанных с парламентским надзором[67].

Главный недостаток заключается в том, что члены парламентских комитетов могут одновременно иметь много обязанностей, и им может быть трудно уделять достаточно внимания надзору за службами безопасности. Это влияет на способность комитетов парламентского надзора осуществлять глубокую проверку деятельности служб безопасности, что особенно необходимо для надзора за законностью оперативной деятельности. Вторая, связанная с ним черта парламентского надзора – то, что в большинстве случаев парламентарии не имеют знаний о службах безопасности. Это усугубляется недостатком времени и, во многих странах, коротким пребыванием в комитете, что не позволяет набраться опыта.

67. Подробнее см.: Wills and Vermeulen 2011: 88-89; и Farson 2012: 38-40.

Этот недостаток усугубляется тем, что службы безопасности расширяют использование сложных технологий, которые нужно ясно понимать для полной оценки последствий для прав человека.

Наиболее существенный недостаток парламентского надзора, с точки зрения защиты прав человека – то, что проверке служб безопасности может повредить политизация комитетов надзора[68]. Парламентарии не всегда подходят для решения задач непредвзятой проверки соблюдения закона службами безопасности. Партийно-политические соображения могут побудить парламентских контролеров либо защитить службы безопасности и политической исполнительной власти от критической проверки, либо осуществлять надзор так, чтобы причинить максимальный политический ущерб оппонентам, вместо обеспечения законности (и эффективности) деятельности служб безопасности. Даже если комитеты по надзору возглавляют члены оппозиции, правящие партии потенциально могут использовать большинство в комитетах по надзору, чтобы ограничить проверку тех аспектов деятельности служб безопасности, которые могут быть политически невыгодны. Это особенно проблематично в странах, где службы безопасности по-прежнему используют и рассматривают как инструменты правящих политических партий (фигур).

Оценка соблюдения закона – не та сфера надзора, которая должна служить партийной политике, и даже поиск политического компромисса в таких комитетах может повредить эффективной защите прав человека[69].

Другие причастные парламентские комитеты

Хотя в этой главе рассматриваются комитеты по надзору как таковые, следует отметить, что в некоторых странах созданы комитеты (подкомитеты) с узкими полномочиями для надзора за отдельными сторонами деятельности служб безопасности. Среди примеров – комитет по тайным фондам испанских Кортесов и конфиденциальный комитет немецкого Бундестага, которые оба отвечают за проверку бюджета (финансирования) служб безопасности[70]. Хотя может казаться, что такой бюджетный надзор прямо не связан с защитой прав человека, существует важная взаимосвязь, поскольку финансовые практики часто указывают на правомерность программ или операций в целом.

Деятельность, нарушающая права человека, часто оставляет финансовые следы, анализ которых может раскрыть информацию о такой деятельности.

Помимо этих комитетов с узкими полномочиями, во многих парламентах есть и другие комитеты, чьи полномочия охватывают разные аспекты политики или деятельности служб безопасности. Хорошим примером служит работа совместного комитета по правам человека британского парламента. Комитет, в частности, рассматривал политику службы безопасности в контексте бо-

68. См., например: Marty 2011: § 45.
69. Commissioner for Human Rights 2013a: §12; Управление Верховного комиссара ООН по правам человека 2014: § 38.
70. Подробнее см.: Wills 2012a: 163-164; Sánchez Ferro 2011: 271.

лее широкого тематического изучения или законодательной проверки таких аспектов, как борьба с терроризмом, использование закрытых материалов в судах и обязательства касательно прав человека в отношениях с иностранными государствами с неудовлетворительным состоянием прав человека[71]. Главное ограничение надзора этих «общих» комитетов состоит в том, что во многих случаях они не имеют таких прав доступа к информации, как специализированные комитеты по надзору, а кроме того, им может не хватать знаний комитетов надзора в области безопасности.

4.2 Институты независимого надзора

Органы экспертного надзора за безопасностью/разведкой

Органы экспертного надзора – это непарламентские органы, создаваемые специально для надзора за службами безопасности. Признавая ценность постоянного экспертного внепартийного надзора, все больше стран-членов Совета Европы создают органы экспертного надзора в сфере безопасности/ разведки. Такие органы обычно уполномочены в первую очередь рассматривать законность деятельности и политики служб безопасности, включая соблюдение ими правозащитного права. Например, так обстоит ситуация в Норвегии, Нидерландах и Португалии[72]. Однако есть и исключения из этого правила, например, постоянный комитет по надзору за разведслужбами (1-й комитет) в Бельгии, имеющий очень широкие полномочия, охватывающие, в том числе, эффективность деятельности служб безопасности и координацию между службами безопасности[73]. В отличие от их парламентских коллег, органы экспертного надзора в основном или полностью сосредоточены на службах безопасности, а не на руководстве исполнительной власти этими службами.

В отличие от парламентских комитетов по надзору, экспертные органы работают на (практически) постоянной основе. Это в целом означает, что они способны обеспечить более полную и глубокую проверку, чем их парламентские коллеги.

Постоянный и непрерывный надзор особенно важен для мониторинга законности работы служб безопасности, поскольку это обычно сложная, забирающая много времени и кропотливая работа. Там, где органы экспертного надзора существуют, они в основном занимаются повседневной проверкой служб безопасности и являются главным элементом внешнего надзора за службами безопасности, например, в Нидерландах, Бельгии, Хорватии, Норвегии, Швеции и Португалии[74].

---

71. См.: www.parliament.uk/business/committees/committees-a-z/joint-select/human-rights-committee/, accessed 28 March 2015.
72. Portugal 2004: Article 9(1); Norway 1995: s2; Netherlands 2002: Article 64(2).
73. Belgium 1991: Article 33; см. также: http://comiteri.be/images/pdf/engels/w.toezicht%20-%20l.control.pdf; Committee I's website: http://comiteri.be/, both accessed 28 March 2015.
74. Portugal: www.cfsirp.pt/; подробнее см.: www.ennir.be/portugal/intelligence-review-portugal-0, both accessed 28 March 2015.

Состав

Органы экспертного надзора обычно имеют от одного до пяти членов, среди которых всегда есть люди с юридическими (судебными) знаниями. Во многих случаях их члены – бывшие судьи, бывшие прокуроры и бывшие политики. Этих людей обычно проверяют и дают им наивысший уровень допуска. Одно из важных преимуществ подхода органа экспертного надзора состоит в том, что контролеров могут (в теории, хотя не всегда на практике) выбирать исходя из их знаний и опыта. В парламентских комитетах по надзору обычно иначе.

Устав или принятая практика могут требовать, чтобы в комитет входили люди с определенными знаниями и опытом. Например, в Нидерландах комитет по надзору за службами разведки и безопасности (CTIVD) выработал практику включения в свой состав бывшего высокопоставленного сотрудника правоохранительных органов и двух членов с юридической подготовкой[75]. Признавая политический характер деятельности надзора и разведки, некоторые экспертные органы, например, комитет по надзору за службами разведки, наблюдения и безопасности (*EOS-Utvalget*) в Норвегии, включают бывших парламентариев и министров, наряду с правоведами. В Хорватии принят особенно передовой подход – их Совет по гражданскому надзору за службами безопасности и разведки должен включать членов, имеющих научную подготовку в политологии, праве и электронике[76]. Среди членов этого органа были видные фигуры гражданского общества и правозащитники. Включение в процесс надзора людей с разным опытом обеспечивает представительство соперничающих критических позиций, что, в свою очередь, может способствовать доверию общества к органам надзора[77].

Экспертные органы может назначать парламент (например, норвежский комитет EOS-Utvalget и Совет по надзору за системами информации Португальской Республики), исполнительная власть (например, уполномоченный по разведслужбам Великобритании и Комиссия по безопасности и защите информации Швеции) или оба вместе (как голландский CTIVD). Поскольку члены органов экспертного надзора не заседают в парламенте, иногда считают, что этим институтам не хватает демократической легитимности. Чтобы развеять такие опасения и убедить общественность в независимости органов экспертного надзора от исполнительной власти, может быть целесообразно задействовать парламент при выборе и назначении их членов. Такую связь с законодательным органом можно еще более укрепить их отчетностью непосредственно перед соответствующим комитетом парламента, как это происходит в Бельгии, где работу 1-го комитета контролирует комитет палаты представителей.

---

75. CTIVD website: www.ctivd.nl/?English, accessed 28 March 2015.
76. Croatia 2006: Article 110(2); подробнее см.: Cvrtila 2012.
77. См., например, комментарии бывшего руководителя британской разведслужбы SIS: (Norton-Taylor 2015).

Сфера их деятельности

Органы экспертного надзора, как правило, имеют право проверять законность деятельности служб безопасности, включая сбор и использование персональных данных службами безопасности.

Полная оценка соблюдения прав человека требует проверки:

- разрешения на сбор данных;
- самого процесса сбора (включая соблюдение всех ордеров);
- повторного разрешения мероприятий;
- хранения, использования и передачи данных службами безопасности;
- требований, касающихся минимизации и (или) удаления полученных данных (особенно путем неизбирательного наблюдения); и
- соблюдения всех требований уведомления людей о наблюдении за ними (если такие требования применимы).

Примерами органов экспертного надзора, полномочия которых охватывают широкий спектр деятельности служб безопасности, связанной с персональными данными, являются немецкая комиссия G10, голландская CTIVD и Комиссия по безопасности и защите информации Швеции (SIN)[78]. Некоторые органы экспертного надзора, напротив, имеют более узкие полномочия, сосредотачиваясь на отдельных аспектах сбора и использования данных. Например, в Великобритании уполномоченный по перехвату линий связи и уполномоченный по разведслужбам занимаются в основном процессом разрешения. Инспекция военной разведки Швеции следит за перехватом международных линий связи, а также качеством и минимизацией данных, собранных в ходе такого перехвата[79].

Доступ к информации и следственные полномочия

В разных странах-членах Совета Европы закон требует, чтобы органы экспертного надзора имели полные права доступа к информации, которую они могут считать входящей в их полномочия, независимо от источников такой информации[80].

Учитывая объем информации, получаемой от иностранных органов, важно, чтобы доступ органов надзора не ограничивался информацией, генерируемой службами безопасности, за которыми они надзирают – что означало бы, что они не могут рассматривать информацию, поступившую из-за рубежа.

Поскольку службы больше, чем раньше, сотрудничают с иностранными партнерами и хранят больше информации, поступившей от зарубежных служб, это закрыло бы некоторые операции или сферы деятельности для независимой про-

78. Germany 2001a: Section 15(5); Cameron 2011: 280.
79. Bigo et al. 2013: 61; Cameron 2011: 281.
80. Например, UK 2000: Sections 58(1)(2) and 60(1); Netherlands 2002: Section 73(1); Norway 1995: Section 4.

верки. Признавая это, некоторые органы надзора давали понять, что правило «третьей стороны» (иначе, принцип контроля источника) к ним не применимо, потому что они имеют гарантированный законом доступ к информации, хранящейся у служб/исполнительной власти, за которыми они надзирают[81].

Доступ к информации может быть подкреплен следственными полномочиями, включая полномочия затребовать в суд людей и документы и право досматривать помещения без уведомления. Хотя эти полномочия используют редко, они усиливают позицию органа надзора, когда служба безопасности противится изучению определенных вопросов[82]. В Бельгии 1-й комитет имеет даже специальную службу расследований, следователи которой могут применять полицейские полномочия, чтобы обеспечить сотрудничество должностных лиц службы безопасности (Belgium 1991: Articles 45, 49).

Другим мощным инструментом надзора является право прямого доступа к системам и базам данных разведслужб, как правило – в офисах в помещениях служб безопасности. Такое право имеют норвежский комитет EOS-Utvalget и голландский CTIVD[83]. Этот инструмент дает контролерам право доступа и непосредственной проверки всех файлов, систем и корреспонденции, касающейся расследования, что усложняет службе безопасности утаивание чего-то от проверки. Ясно, что такие инструменты следует использовать добросовестно и в полном соответствии с законным мандатом органа надзора.

Дополнительным инструментом/полномочием, ставшим особенно актуальным, является право привлекать независимых экспертов (прошедших проверку безопасности) для консультаций по техническим вопросам.

С усложнением технологий безопасности и разведки нужен более высокий уровень технических знаний для понимания и анализа систем, применяемых для сбора, обработки и хранения информации (включая персональные данные). Последствия такой технологии для прав человека нельзя оценить полностью без использования таких знаний. Признавая важность этого, некоторые органы надзора получили законное право привлекать технических специалистов для консультаций на постоянной основе[84].

Рассмотрение жалоб

Некоторые страны-члены Совета Европы уполномочили органы экспертного надзора рассматривать жалобы на деятельность служб безопасности, включая заявления о незаконном наблюдении и (или) использовании персональных данных. Среди примеров – 1-й комитет в Бельгии, шведский SIN и норвежский комитет EOS-Utvalget. По сравнению с рассмотрением жалоб не связанными с без-

81. Например: Norway 2014: 1; Laethem 2011: 199; Wills and Vermeulen 2011: 125.
82. Netherlands 2002: Article 74; Belgium 1991: Article 48(2); общий обзор следственных полномочий в некоторых европейских странах см. в Wills and Vermeulen 2011: 134-135.
83. Verhoeven 2011: 257; Norway 2014: 5.
84. Norway 2012, Norway 2013 and Norway 2014; см. также: With and Kathmann 2011: 221; Cameron 2011.

опасностью органами, например, омбудсменами, преимущество заключается в том, что люди, рассматривающие жалобы, вероятно, лучше знакомы с ситуацией в силу других своих функций надзора, что может помочь в рассмотрении жалоб.

Такие органы также имеют (должны иметь) доступ к наиболее деликатной информации, а также процедуры и опыт работы с ней. Это упрощает оперативное рассмотрение жалоб и может, таким образом, дать существенное преимущество по сравнению с более общими органами рассмотрения жалоб, такими, как омбудсмены (Forcese 2012: 186). С точки зрения защиты прав человека, следует отметить, что органы экспертного надзора вообще-то не имеют полномочий выносить юридически обязывающих определений после рассмотрения жалобы. Как правило, они могут только давать рекомендации и представления службам и политической исполнительной власти, но не могут распорядиться о выплате или компенсации либо удалении (корректировке) персональных данных[85]. Так, в Швеции SIN может сделать вывод о том, что, например, персональные данные жалобщика обрабатывались не в соответствии с законом. Однако SIN затем должен сообщить о данном человеке министру юстиции, который принимает решение о необходимости выплаты компенсации, и, при необходимости, дело нужно передать в орган защиты данных, который распорядится об удалении персональных данных (Cameron 2011: 284).

Вынесения необязательных рекомендаций недостаточно для эффективной правовой защиты жалобщика. Требование удалить или скорректировать персональные данные и (или) выплатить компенсацию является самым распространенным и необходимым средством правовой защиты в связи со сбором и использованием службами безопасности персональных данных. Учитывая, что большинство органов экспертного надзора не могут принимать обязывающих решений, людям, чьи права были нарушены службами безопасности, приходится одновременно или впоследствии обращаться к какому-то органу, который может обеспечить такую правовую защиту. Решая, обеспечивается ли эффективная правовая защита, имеет смысл всесторонне рассмотреть систему надзора.

Омбудсмены

Полномочия омбудсменов в разных странах Европы существенно разнятся, и большинство из них не играют заметной роли в надзоре за службами безопасности. Во многих странах омбудсмен имеет возможность расследовать жалобы на службы безопасности, но они редко делают это на практике. Омбудсмены, однако, могут сыграть ценную роль как при рассмотрении жалоб, касающихся служб безопасности, так и расследуя действия служб безопасности по собственной инициативе. Это особенно касается государств, не имеющих органов экспертного надзора за безопасностью/разведкой или сильных парламентских комитетов по надзору.

Достойным внимания примером омбудсмена, играющего активную роль в надзоре за службами безопасности, является сербский защитник граждан. Его офис расследует жалобы, касающиеся служб безопасности, действует упреж-

85. Обсуждение этого вопроса см. в: Forcese 2012: 192-193; Hernes 2008: 81-82.

дающе, по собственной инициативе начиная расследования деятельности служб безопасности, и успешно оспаривал законы о службе безопасности в конституционном суде[86]. Сербия показала, что предоставление омбудсмену прав оспаривать неконституционные законы полезно для защиты прав человека. При таком оспаривании омбудсмен может иметь гораздо более выгодную позицию, чем частные лица или НПО. В Нидерландах омбудсмен тоже рассматривает жалобы, касающиеся безопасности и разведслужб, но жалобщики могут обращаться к омбудсмену только после подачи жалобы в соответствующее министерство и не получив удовлетворительного ответа.

Как и у многих органов экспертного надзора за безопасностью/разведкой, один из недостатков модели омбудсмена заключается в том, что большинство из этих институтов может лишь давать рекомендации. Этого недостаточно, когда права человека нарушены, и человек ждет эффективной правовой защиты.

Органы защиты данных и комиссии по вопросам информации

Органы защиты данных и комиссии по вопросам информации – это независимые органы надзора, ответственные за проверку соблюдения государственными органами (а в некоторых случаях – и частными организациями) законодательства о защите данных и (или) о свободе доступа к информации. Эти функции часто выполняет один орган.

Рамки, в которых органы защиты данных надзирают за использованием персональных данных службами безопасности, зависят от того, охватывает ли законодательство о защите данных службы безопасности, распространяется ли мандат органов защиты данных на службы безопасности, ограничения права людей на доступ к персональным данным, хранимым службами безопасности, и ограничения доступа органов защиты данных к секретной информации. Недавнее исследование Рабочей группы ЕС по Статье 29 показало, что в очень немногих европейских странах органы защиты данных полностью надзирают за использованием персональных данных службами безопасности и что очень часто они совершенно не допущены к этой сфере. Тем не менее некоторые из этих институтов имеют полномочия и активно надзирают за использованием службами безопасности персональных данных и (или) запросами о доступе к информации, хранимой службами безопасности (Article 29 2014a: §§ 9-10).

Функции органов защиты данных могут включать проверку рассмотрения и принятия решений по индивидуальным запросам о доступе к персональным данным, хранимым службами безопасности. Они могут также по собственной инициативе вести расследование и проверку работы служб безопасности с данными. Например, в Германии федеральный уполномоченный по защите данных изучает соблюдение службами безопасности закона о защите данных, за исключением данных, собранных в ходе наблюдения (которыми занимается другой орган – Комиссия G10), эти вопросы охватывают ее двухлетние отчеты

86. См., например: Protector of Citizens of the Republic of Serbia 2010; Protector of Citizens of the Republic of Serbia 2014: 14-15, 207-211.

(With and Kathmann 2011:227). Словенская и сербская комиссии по вопросам информации имеют схожую роль надзора[87].

Во многих европейских странах службы безопасности полностью исключены из сферы действия законодательства о свободе информации/доступе к информации (Jacobsen 2013: 9-10). Это означает, что граждане не могут требовать доступа к конкретным документам, а уполномоченные по информации не имеют полномочий рекомендовать или требовать раскрытия информации. Швейцария является примером страны, где служба безопасности не исключена из сферы действия закона о свободе информации. В ходе процесса, инициированного журналистом, пытавшимся получить доступ к резюме отчетов разведслужбы, федеральный административный трибунал недавно подтвердил, что даже секретная информация может подлежать раскрытию[88]. Федеральный уполномоченный по защите данных и информации надзирает за рассмотрение запросов граждан об информации. Так же обстоит дело в Словении, где уполномоченный по информации проверяет обоснованность неразглашения информации службами безопасности и может распорядиться рассекретить информацию в соответствующих обстоятельствах (Jacobsen 2012: 17).

Наконец, и словенский, и сербский уполномоченные по информации использовали свои полномочия, чтобы оспорить законы о хранении данных и наблюдении в своих конституционных судах. Это – яркие примеры способности независимых органов надзора проводить проверки не только соблюдения прав человека в практике служб безопасности, но и правовой базы деятельности этих служб.

4.3 Судебные органы

Хотя суды могут проверять и рассматривать действия служб безопасности и их последствия во многих ситуациях, в этом разделе мы сосредоточимся на роли судебных органы в санкционировании связанных с вмешательством мер наблюдения службами безопасности и в рассмотрении жалоб на (возможную) деятельность служб безопасности.

Жалобы на службы безопасности

Что касается жалоб на службы безопасности, в большинстве стран-членов Совета Европы частные лица теоретически имеют возможность возбудить дело для получения правовой защиты. Дело можно возбудить непосредственно, когда лицо пытается оспорить арест, допрос или задержание (в тех немногих странах, где службам безопасности разрешены эти полномочия). Однако, как отмечено выше (см. раздел 2.4 о праве на справедливый суд), часто возникают существенные препятствия для судопроизводства против служб безопасности.

87. Slovenian Information Commissioner: www.ip-rs.si/?id=195, accessed 28 March 2015; Serbian Information Commissioner: www.poverenik.rs/index.php, accessed 28 March 2015; см. также: Petrović 2012: 21-23.
88. Stoll 2014; Goumaz 2014.

Использование судов, чтобы оспорить наблюдение службы безопасности или использование данных, еще сложнее, потому что в большинстве случаев человек не знает о таком нарушении своих прав (Venice Commission 2007: § 243). Дело обычно можно возбудить, только если человек узнает о таких мерах на основании каких-то требований об уведомлении, случайно, от информатора или в ходе другого судебного процесса. Иногда имеются прямые ограничения на оспаривание людьми тайного наблюдения в обычных судах до того, как их специально уведомят о слежке (Germany 2001a: Section 13).

В Великобритании создан специальный судебный орган, Трибунал следственных полномочий (*Investigatory Powers Tribunal*, *IPT*), для рассмотрения жалоб о наблюдении и всех связанных с правами человека претензий к службе безопасности[89]. Он имеет исключительные полномочия рассматривать такие претензии. Преимуществом этой модели является то, что она позволяет расследовать иски в связи с (предполагаемым) наблюдением, даже если это наблюдение продолжается, и он может давать обязательные распоряжения, если мероприятия окажутся незаконными. В 2015 г. Трибунал вынес свое первое решение против служб безопасности и разведки, придя к выводу, что некоторые аспекты межгосударственного обмена разведывательной информацией нарушали Статьи 8 и 10 Европейской конвенции прав человека, потому что они «не соответствовали закону»[90]. Несмотря на этот успех, в модели этого трибунала существуют серьезные недостатки, и ее резко критиковали[91]. А именно, жалобщиков можно не информировать о слушаниях, они не имеют автоматического права присутствовать на слушаниях или быть представленными адвокатом, по их выбору, причины решения могут не поясняться, и решения IPT нельзя обжаловать или изменить в суде.

Санкционирование связанных с вмешательством мер

В большинстве стран-членов Совета Европы требуется, чтобы их службы безопасности получили ордер суда на проведение мероприятий для сбора информации, считающихся особенно бесцеремонными в аспекте права на частную и семейную жизнь.

Среди исключений из чисто судебной модели санкционирования – Великобритания и Нидерланды (санкционирует исполнительная власть), Польша (согласие судьи и независимого Генерального прокурора, не принадлежащего к исполнительной власти) (Poland 2002: Article 27), Бельгия и Германия (разные формы квази-судебных санкций), и Румыния (санкция специальных прокуроров)[92].

Хотя виды мероприятий, требующих внешней санкции, бывают разными, обычно они включают целенаправленный перехват связи (если лицо/организация, чьи линии связи планируется перехватывать, известна с самого начала),

89. UK 2000: Sections 65-67; веб-сайт IPT см.: www.ipt-uk.com/, accessed 28 March 2015.
90. Liberty & Others vs. the Security Service, SIS, GCHQ.
91. См., например: JUSTICE 2011: 133-153; Leigh 2012: 438-439.
92. Romania 1991: Article 13. Следует отметить критику судом этого подхода к выдаче санкций, как не полностью независимого от исполнительной власти: Dumitru Popescu v. Romania [69-73].

поиск и арест имущества и установку записывающих устройств в жилищах. В то же время в большинстве стран судебной санкции не требуется, например, для сбора информации при помощи людей, неизбирательной массовой слежки, использования компьютерных сетей, поиска по уже существующим банкам данных, собранных путем массовой слежки, получения данных, собранных другими правительственными ведомствами, и доступа к данным, хранимым частными компаниями. Заметным исключением является Сербия, где служба безопасности сейчас должна получить санкцию суда не только на тайное наблюдение или запись любой формы переговоров, но и на получение данных связи и на осуществление поиска в данных, уже полученных с использованием связанных с вмешательством полномочий (Serbia 2014: Articles 13 and 15). Этот подход служит полезным примером в свете нынешних дебатов о том, как лучше контролировать доступ служб безопасности к данным, собранным путем, например, массового сбора, а также доступ к данным связи.

Разоблачения Сноудена подняли вопросы о рамках судебных санкций на неизбирательную массовую слежку за кабельными и беспроводными линиями связи. Хотя общедоступная информация об этом ограничена, законы большинства стран-членов Совета Европы прямо не требуют санкции суда на такие меры (если они разрешены национальным законодательством и находятся в пределах возможностей службы безопасности). Однако в Швеции имеется специальный суд, дающий разрешение на неизбирательный массовый перехват кабельных и беспроводных международных линий связи (т.е. не считающихся полностью внутренними). Суд военной разведки в составе двух судей и шести заседателей выдает радиослужбе министерства обороны (FRA) ордера на использование конкретных настроек (потоков для поиска) в тех или иных международных кабелях[93].

Хотя точные модальности применения и рассмотрения судебных ордеров в разных странах различаются, в большинстве случаев эту роль выполняет старший судья, специально назначенный согласно закона или выбранный по предусмотренной законом процедуре. Например, в Боснии и Герцеговине такой судья является председателем суда Боснии и Герцеговины или назначенным им судьей. В Венгрии это судья, назначенный председателем столичного суда, а в Чехии – судья, возглавляющий коллегию судей высшего суда в соответствующем географическом регионе[94]. Хорватия предусматривает дополнительное ограничение при выдаче повторной санкции (продлении санкции) на связанные с вмешательством мероприятия: это должна делать коллегия в составе трех судей, а не один судья, в случае первичной санкции (Croatia 2006: Articles 36 and 37(2)).

Обычно судьи принимают решение о разрешении на основе письменных заявлений, но в некоторых странах предусмотрены слушания по заявлениям, по которым возникают сложные вопросы или судьи хотят задать вопросы представителю службы безопасности. Заседания всегда проводятся постфактум, и в большинстве стран будущий объект связанных с вмешательством мер никак не представлен. Инновационный подход принят в Норвегии, где интересы буду-

93. Cameron 2011: 281; Bigo et al. 2013: 61; Pond 2013.
94. Bosnia and Herzegovina 2004: Article 77; Hungary 1995: Section 58; Czech Republic 1994 § 9(1).

щего объекта мер наблюдения со стороны полиции безопасности представляет допущенный службами безопасности адвокат, который может оспорить основания для ордера, приведенные службой безопасности[95]. Это делается на основе письменных представлений. Суд военной разведки Швеции (см. выше), согласно сообщениям, использует подобную систему для выдачи ордеров на перехват международных линий связи (Pond 2013). За пределами Европы, группа изучения технологий разведки и связи при президенте США призвала к учреждению должности адвоката по защите интересов общественности «для представления интересов тех, чьи права на частную жизнь или гражданские свободы могут быть под угрозой»[96]. Участие такого лица в процессе санкционирования связанных с вмешательством мероприятий обеспечивает лучшую защиту прав человека, ибо это позволяет санкционирующему органу выслушать разные взгляды, включая толкование положений закона, что помогает обеспечить критический анализ обоснования, предложенного службами безопасности.

Санкция суда часто считается лучшей защитой прав человека, прежде всего – потому, что судей обычно считают независимыми, непредвзятыми и менее зависящими от политических соображений, окружающих деятельность служб безопасности, что может повлиять на решения министра о разрешении.

Судей также считают способными лучше оценить правовые критерии, в частности, необходимости и пропорциональности, что весьма важно, когда запрашиваемые мероприятия могут иметь существенные последствия для прав человека.

Санкция суда, однако – не панацея, гарантирующая соблюдение прав человека при разрешении и применении связанных с вмешательством мер службами безопасности (Venice Commission 2012: § 35). У санкций суда есть ряд потенциальных недостатков. Во-первых, эффективность санкции суда как средства защиты прав человека в значительной степени зависит от независимости конкретных судей. В странах, где судьи не независимы, маловероятно, что они будут очень критично подходить к запросам служб безопасности об использовании связанных с вмешательством мероприятий.

Во-вторых, знания столь же необходимы для эффективности санкции суда (Venice Commission 2007: §§ 205-206). Судьи, чей опыт в вопросах безопасности ограничен (и даже опытные судьи), могут быть не склонны критиковать оценки национальной безопасности чиновниками службы безопасности, обращающимися за ордером (Cameron 2008: 45). Иногда это дополняет склонность некоторых судей почтительно относиться к исполнительной власти в вопросах национальной безопасности. В-третьих, также выражались опасения, что во многих странах санкция суда равнозначна штампованию решений, принятых службами безопасности, и очень мало запросов на ордера отклоняются (Управление Верховного Комиссара ООН по правам человека 2014: § 38). Наконец, в тесной связи с проблемой «штампования», фактом является то, что судей обычно нельзя привлечь к ответственности за ордера, выданные ими службам безопасности. Чтобы сберечь независимость суда и разделение

95. Norway 1981: Section 100a; Norway 2014: 8.
96. Review Group on Intelligence and Communications Technologies 2013: 203-204 and Recommendation 28.

полномочий, процедура выдачи ордеров обычно не подлежит последующей проверке органом надзора (Cameron 2011: 285).

Напротив, министра или квази-судебный орган, дающий санкцию, легче привлечь к ответственности в парламенте или независимым органом надзора за принятые ими решения, и эта возможность может иметь благотворный эффект на принятие решений (Borger 2014).

4.4. Квази-судебные санкционирующие органы

На территории Совета Европы есть несколько государств, где связанные с вмешательством мероприятия должны быть санкционированы квази-судебным органом. В Бельгии недавно был принят новых подход к разрешению (и надзору) за осуществлением некоторых мероприятий, связанных с вмешательством.

Административная комиссия (*SIM Commission*)[97] в составе трех допущенных службой безопасности мировых судей (действующих не в качестве судей), назначенная исполнительной властью, дает «обязательный для исполнения совет» службам безопасности, когда те обращаются с просьбой о применении «исключительных мер» (самых крайних из трех категорий мер)[98]. Эти исключительные меры включают наблюдение и обыск частного жилища; проникновение в электронные системы; перехват связи; использование агентов, в т.ч. путем создания ложных учетных записей. В разведоперациях с участием людей, например, при использовании информаторов или внедрении в организации, не принято запрашивать разрешение независимого органа, и в связи с этим бельгийское законодательство признает последствия разведопераций с участием людей для прав человека.

Что важнее, бельгийское законодательство признает последствия хакерства для прав человека и требует, чтобы такие мероприятия санкционировал внешний орган. Есть и другая категория менее бесцеремонных «специфических мер» (включая идентификацию пользователя услуг связи и доступа к данным электронной связи), которые могут быть разрешены руководителем соответствующей службы безопасности. Однако они должны сначала уведомить комиссию SIM, а службы также должны ежемесячно отчитываться о применении таких мер[99].

Сложная бельгийская система санкционирования связанных с вмешательством мер также предусматривает текущий надзор за применением мер, разрешенных Комиссией SIM, для оценки их законности (включая, в частности, их пропорциональность). Комиссия имеет полномочия приостановить применение связанных с вмешательством мер или, в случае менее бесцеремонных мероприятий, санкционированных директором службы, может распорядиться о запрете использования собранных данных. Комиссия SIM, со своей стороны, должна информировать орган экспертного надзора (1-й комитет – см. выше) о выдаче или отказе разрешений и их продления.

---

97. Ее полное название: La commission administrative chargée de la surveillance des méthodes spécifiques et exceptionnelles de recueil de données par les services de renseignement et de sécurité.
98. Belgium 2010: Articles 18 (2)(3)(9)(10), 43(1).
99. Belgium 1998: Articles 18 (2) (3).

1-й комитет рассматривает все разрешения и проведение мероприятий службами безопасности. Этот орган экспертного надзора может фактически отменить решение Комиссии SIN разрешить, отказать в разрешении или приостановить меры[100].

Такой надзор санкционирующего органа обеспечивает дополнительную защиту прав человека.

Немецкий подход к санкционированию связанных с вмешательством мер также заслуживает рассмотрения.

Такие меры может в первую очередь разредить назначенный правительством министр, который затем обращается за разрешением в орган под названием Комиссия G10 (иногда – задним числом). Это касается не только целенаправленного наблюдения, но и неизбирательного наблюдения с применением настроек или условий поиска, законность (включая пропорциональность) которых оценивает Комиссия G10. Что касается неизбирательного наблюдения, то Комиссия G10 также проверяет минимальность данных, полученных путем наблюдения[101]. Комиссия G10, назначенная парламентским комитетом по надзору, может считаться квази-судебной, поскольку ее возглавляет лицо, имеющее право на судебную должность (но действующее не в качестве судьи); три других члена могут быть или не быть депутатами Бундестага[102].

Необходимость разрешения и от члена исполнительной власти, и от независимых органов, включая судей[103] или квази-судебный орган, дает значительные преимущества с точки зрения прав человека. Она гарантирует двойную «проверку» вне службы безопасности и потенциально гарантирует, что в процессе задействованы качества и исполнительной, и судебной санкции.

4.5. Исполнительная власть

Политическая исполнительная власть является потребителем, постановщиком задач, контролером и надзирателем за службами безопасности. Ее нельзя считать совершенно сторонним надзирателем, поскольку исполнительные органы участвуют в процессе разведки – они ставят задачи, выдают разрешения, определяют политику и приоритеты служб безопасности (Venice Commission 2007: § 129). Во всех странах-членах Совета Европы за службы безопасности отвечают один или несколько представителей исполнительной власти. В целом службы безопасности принадлежат к ряду министерств – обороны, юстиции, внутренних дел, но могут подчиняться и премьер-министру (например, в Турции), президен-

100. Подробный анализ проверки этих мероприятий 1-м комитетом см. в: Belgian Standing Intelligence Agencies Review Committee 2012: 143-169; Belgium 1998: Articles 43(3) (3)(4)(5).
101. Germany 2001a: Section 10(1); With and Kathmann 2011: 221-223; Venice Commission 2015: §§ 124-125.
102. Germany 2001a: Section 15.
103. Канада является примером страны, не входящей в Совет Европы, где также применен двухуровневый подход к выдаче разрешений – заместителя министра и судьи федерального суда. См.: Canada 1984: § 21(1).

ту (например, в Румынии) или могут находиться под совместным руководством президента и премьер-министра (например, в Хорватии). Контроль и надзор исполнительной власти может осуществлять и коллективный орган, например, совет национальной безопасности, как в Хорватии и Сербии. В Хорватии, например, Совету национальной безопасности помогает офис Совета национальной безопасности, отвечающий, в частности, за мониторинг законности деятельности служб безопасности (Croatia 2006: Article 107(1)). Это дополняет надзор за законностью со стороны внешнего органа экспертного надзора (см. выше).

Обязанности исполнительной власти включают также составление указаний, дополнительных правил, общей политики и приоритетов служб безопасности. Эти функции включают выдачу указаний о том, как учитывать права человека и обеспечивать надлежащий учет прав человека в политике и приоритетах. Например, британское правительство давало службам безопасности и разведслужбам указания по обмену информацией о лицах, содержащихся в предварительном заключении или допрашиваемых иностранными службами безопасности (UK 2010). На исполнительную власть возложена основная обязанность обеспечить работу служб безопасности с соблюдением прав человека.

Ввиду этого внешние органы надзора могут стремиться к тому, чтобы министры использовали свои полномочия, например, чтобы составлять кодексы этики или правила обмена информацией с зарубежными партнерами.

Наконец, в некоторых странах-членах Совета Европы министры также отвечают за разрешение использования мер наблюдения[104] и определение ключевых слов (параметров поиска), которые службы безопасности могут использовать при поиске в так называемых данных связи (Bigo et al. 2013: 74). Там, где министры имеют такую роль, важно, чтобы у них был доступ к советникам, способным помочь им оценить права человека и более широкие правовые последствия любых предлагаемых мер.

4.6. Меры внутреннего контроля

Хотя данный доклад в первую очередь касается внешнего надзора, руководители служб безопасности и их персонал играют ведущую роль в обеспечении законности их деятельности и соблюдении прав человека. Именно сотрудники служб безопасности, а не внешние контролеры, присутствуют при принятии многих решений, имеющих важные последствия для прав человека. Поэтому наибольшее значение имеют ценности, этика и юридические знания персонала служб безопасности. Для этого руководители служб безопасности должны применять жесткие критерии проверки при отборе и набирать только людей с соответствующими качествами. Они также должны организовывать постоянную подготовку, в т.ч. по вопросам прав человека (Venice Commission 2007: § 132) и роли внешних органов надзора. Важно, чтобы внешние органы надзора проверяли эту внутреннюю политику и практику служб безопасности.

104. Например: UK 2000: Sections 7 and 8; Netherlands 2002: Article 19 (за исключением почты, что должно быть разрешено судом, согласно Статье 23).

В конце концов, эффективные системы внешнего надзора мало значат, если службы безопасности не стремятся работать, уважая права человека и способствуя надзору и подотчетности (Venice Commission 2007: §§ 130, 134). Аналогично, для того, чтобы внешний надзор способствовал соблюдению прав человека и подотчетности в службах безопасности, нужно желание сотрудничать с органами надзора и учитывать их рекомендации.

Все службы безопасности вводят внутренние процедуры разрешения определенных мер, рассмотрения своей деятельности, надлежащего учета деятельности и отчетности о проблемах[105]. В большинстве случаев эти процедуры вводит высшее руководство, но их может требовать и закон. Например, в Германии службы безопасности обязаны обеспечивать применение мер наблюдения под надзором сотрудника, имеющего право занимать должность в суде[106].

Некоторые страны-члены Совета Европы, например, Италия, Босния и Герцеговина, Сербия, также законодательно ввели в службах безопасности посты генеральных инспекторов.

Функции этих внутренних инспекторов включают оценку законности деятельности служб[107]. Хотя эта функция надзора может быть полезна для предупреждения руководителей служб и законодательной власти обо всех проблемах, внутренние генеральные инспектора не могут заменить строгую внешнюю проверку.

4.7. Средства массовой информации и гражданское общество

Роль СМИ в освещении вопросов безопасности на территории Совета Европы весьма разнится и зависит, в частности, от владельцев ЗМИ, законов о защите источников журналистской информации и людских и финансовых ресурсов медийных организаций. СМИ часто опережают официальную «линию» надзора, раскрывая и расследуя такие вопросы, как тайные выдачи и задержания, раньше постоянных органов надзора (Priest 2005). Во многих случаях работа журналистов приводила к расследованиям постоянных и специальных органов надзора.

Журналисты играют особенно важную роль в раскрытии незаконной деятельности служб безопасности в ситуациях, когда официальные системы надзора не могут обнаружить либо пресечь практику нарушения прав человека (ПАСЕ 2011: § 8). Они также могут быть рупором для сотрудников служб безопасности, желающих донести до общественности опасения о незаконности, если у них нет возможности добиться рассмотрения этих опасений по предписанным каналам, нет доверия к таким каналам, или если нет другого разрешенного внешнего канала для разоблачений.

Неправительственные организации (НПО) также участвуют в мониторинге и предании гласности работы органов надзора. НПО на западе Балкан были особенно активны в этом отношении, а ряд НПО специализируется в вопросах верховен-

105. Общий обзор см. в: Born and Leigh 2005: 46-49.

106. Germany 2001a: Section 11(1).

107. Bosnia and Herzegovina 2004: Article 33(1); Petrović 2012: 14-15.

ства права в сфере безопасности. Например, после принятия закона о парламентском надзоре за сферой безопасности и обороны в 2010 г. Черногорский Institut Alternativa проводил ежегодные исследования реализации закона, обращая первоочередное внимание на эффективность работы комитета, которому поручен надзор за сферой безопасности[108]. Важно, чтобы НПО (и СМИ) интересовались не только службами безопасности, но и институтами, которые надзирают за ними.

НПО также играют важную роль в привлечении к ответственности и участии в судебных процессах, касающихся служб безопасности, в Европейском суде по правам человека и национальных судах. Такие организации, как Open Society Justice Initiative, Reprieve и польский Хельсинский фонд прав человека, участвовали в подаче исков, касающихся прав человека, в связи с участием европейских государств в тайных задержаниях и выдачах под руководством США. Несколько НПО, включая Privacy International, Big Brother Watch и Liberty, активно участвовали в возбуждении дел против правительств в национальных и международных судах в связи с законами и практикой слежки. Одним из примеров является дело Liberty и др. против Великобритании (в котором Страсбургский суд выявил несоответствие Конвенции ранее существовавшей британской правовой базы, использовавшейся при массовом перехвате международных линий связи). Роль НПО остается жизненно важной в контексте непрекращающихся проблем массовой слежки, межгосударственного обмена разведывательной информацией и хакерства служб безопасности.

НПО также могут быть полезны, организуя кампании за расследование деятельности служб безопасности и предлагая свои знания для таких расследований, а также внося представления, когда парламент принимает или изменяет законы о службах безопасности. В минувшее десятилетие эти организации привлекали внимание к вероятным недостаткам в процессах надзора и отчетности и выступали за более строгое, независимое специальное расследование деятельности служб безопасности (Townsend 2014).

Способность СМИ и НПО осуществлять неформальный надзор за службами безопасности в значительной степени зависит от наличия среды, в которой они могут спорить с правительствами по деликатным вопросам, не боясь запугивания или расплаты.

В некоторых странах-членах Совета Европы ситуация иная. Существование и сфера действия законов о свободе информации также влияет на способность СМИ и НПО заниматься этими вопросами. Хотя во многих странах-членах Совета Европы службы безопасности не охвачены этими законами, некоторые национальные законы позволяют частным лицам (организациям) запрашивать информацию у служб безопасности или о службах безопасности и требовать, чтобы службы обосновывали (под внешним надзором) решения не предоставлять информацию. Такие подходы к свободе информации позволяют организациям гражданского общества и СМИ получать информацию, которая может помочь им в их работе, без риска для национальной безопасности.

108. См.: http://institut-alternativa.org/?lang=en, accessed 28 March 2015.

Глава 5

К ДЕМОКРАТИЧЕСКОМУ И ЭФФЕКТИВНОМУ НАДЗОРУ ЗА НАЦИОНАЛЬНЫМИ СЛУЖБАМИ БЕЗОПАСНОСТИ

Исходя из международных принципов и национальных практик, рассмотренных в данном документе, очевидно, что системы надзора могут быть устроены очень по-разному, преследуя при этом схожие цели. При планировании и оценке систем надзора полезно сосредоточиться на сути, а не на форме надзора. Это позволяет достигать одинаковых целей, допуская разные конституционные и правовые системы, а также разные национальные традиции. Цель этой, последней главы – показать ряд важных принципов и задач, вытекающих из предыдущего анализа.

Главный принцип, который можно вывести из рассмотренных выше международных принципов и практики разных государств, состоит в том, что все аспекты деятельности, политики, финансирования, администрации и правил служб безопасности должны подлежать проверке как минимум одной организацией, являющейся внешней и независимой от служб безопасности и исполнительной власти. Международные принципы и практика многих стран-членов Совета Европы показывают, что такая внешняя проверка должна быть предварительной (там, где это возможно), текущей, и последующей.

Широкие задачи систем надзора должны включать ответственность служб безопасности и (при необходимости) политической исполнительной власти и содействие повышению:

- эффективности служб безопасности при исполнении их законных полномочий, включая участие в предупреждении угроз правам человека, в частности, вследствие терроризма, шпионажа и кибер-преступности;
- эффективности, финансовой законности и экономности служб безопасности; и
- соответствию правил, стратегий и операций законности и правам человека.

Третья задача является предметом данного доклада и конечной задачей для всех остальных задач, рассмотренных в этой главе. Стоит напомнить, что, хотя данный доклад касается внешнего надзора за службами безопасности, внутренние проверки и меры контроля в этих службах исключительно важны для решения вышеупомянутых задач.

Демократический надзор важен, потому что службы безопасности (и соответствующие исполнительные ведомства) предоставляют публичные услуги обществу и от имени общества, и поэтому избранные представители должны участвовать в обеспечении эффективного, действенного и законного предоставления этих услуг. Соответственно, «демократический» аспект надзора обеспечивается в первую очередь участием парламента. Опыт стран-членов Совета Европы показывает, что парламентарии вносят свой вклад:

- обеспечивая всесторонний надзор за службами безопасности в национальном законодательстве;
- выделяя необходимые бюджетные ресурсы непарламентским институтам надзора;
- надзирая за работой органов экспертного надзора;
- рассматривая эффективность институтов надзора (включая свои собственные комитеты);
- и проводя текущие проверки и специальные расследования деятельности служб безопасности.

Парламентский надзор за службами безопасности остается важным в любой демократической стране, но, как показывают международные принципы и практика государств, растет понимание того, что права человека и верховенство права лучше всего защищены, когда надзор парламентариев дополнен экспертным надзором. Органы экспертного надзора в целом имеют лучшие возможности осуществлять текущую, детальную и политически нейтральную проверку, необходимую для защиты прав человека. Этот вид надзора особенно необходим при проверке действий служб безопасности, влияющих на права на частную жизнь, свободу слова, собраний и объединения.

Такая деятельность включает сбор, использование, хранение, передачу (в т.ч. национальным правоохранительным ведомствам и зарубежным органам) и удаление персональных данных. Поскольку органы экспертного надзора играют все большую роль в надзоре за службами безопасности, важно обеспечить принятие мер для того, чтобы эти институты имели определенную демократическую легитимность. Соответственно, в разных странах-членах Совета Европы имеются парламентские комитеты, которые следят за работой экспертов-контролеров, назначают (и увольняют) сотрудников и получают их отчеты.

5.1. Предварительное санкционирование связанных с вмешательством мер

Касательно предварительного санкционирования сбора информации, права человека лучше всего защищены, если орган, независимый от служб безопасности и политической исполнительной власти, должен санкционировать связанные с вмешательством мероприятия. Растет понимание того, что внешнее санкционирование должно охватывать:

- неизбирательный массовый сбор информации;
- использование ключевых слов или настроек для извлечения данных из информации, собранной путем массового перехвата, особенно если они касаются людей, чью личность можно установить;
- сбор и доступ к данным связи (в т.ч. в частном секторе);
- проникновение в компьютерные сети.

Как показано выше, последствия такой деятельности для прав человека слишком значительны, чтобы ее разрешала только исполнительная власть или (еще хуже) службы безопасности, присвоившее себе это право. Внешнюю санкцию на эти меры должен давать судебный или квази-судебный орган, либо совместно один из этих органов и исполнительная власть.

Привлечение разного опыта для участия в процессе санкционирования связанных с вмешательством мероприятий может обеспечить лучшую защиту, чем санкция политического или судебного органа. Процесс санкционирования безусловно должен включать правовую и правозащитную оценку предлагаемых мер, но может быть полезно также рассмотреть все политические риски, связанные с предлагаемыми мерами. Соответственно, двухуровневый процесс санкционирования, объединяющий санкцию (квази-)судебного органа и санкцию министра, может предложить наиболее надежную модель предварительной проверки.

Как и в любом элементе процесса сбора информации, процесс санкционирования или подтверждения связанных с вмешательством мероприятий тоже требует проверки. Учитывая трудности, которые могут возникать при попытках оценить решения суда о санкционировании связанных с вмешательством мер, можно рассмотреть квази-судебные модели. Квази-судебное санкционирование, более распространенное на территории Совета Европы, включает судебный опыт без судебного статуса санкционирующего органа. Как показывает практика разных государств, работу таких органов может проверять другой орган надзора без возникновения опасений, связанных с возможной последующей проверкой решений суда.

Защиту прав человека путем процесса санкционирования также можно улучшить, привлекая адвокатов, которые представляют интересы будущего объекта (а в случае массовой слежки – побочных жертв) наблюдения и других возможных форм бесцеремонного вмешательства, например, хакерства. Эта третья сторона может обжаловать предложенное службой безопасности на-

блюдение, и их участие снижает риск того, что процесс санкционирования превратится в простое «штампование».

5.2. Рассмотрение жалоб

Все страны-члены Совета Европы должны обеспечивать, чтобы их системы надзора включали определенный независимый орган, которому можно направлять жалобы на службы безопасности. Независимо от того, идет ли речь об органе экспертного надзора за безопасностью/разведкой или не связанном с безопасностью органе надзора, таком, как омбудсмен, жалобы должен рассматривать орган, имеющий необходимый доступ и следственные полномочия для тщательного расследования. Большинство органов надзора могут только давать рекомендации службам безопасности и (или) исполнительной власти. Поскольку ЕКПЧ требует, чтобы лица, считающие (или знающие), что их права были незаконно нарушены службами безопасности, имели доступ к институту, способному предоставить эффективную правовую защиту, государство должно обеспечить этим людям также доступ к институту, способному давать юридически обязательные распоряжения. Полномочия такого органа должны включать не только предоставление компенсации жертвам любых нарушений, но и полномочия отменять соответствующие ордера и давать распоряжения об удалении незаконно собранных персональных данных.

5.3. Доступ контролеров к информации

Доступ контролеров к информации имеет огромное значение и упоминается почти во всех международных принципах, касающихся надзора. Контролеры, в частности, не могут давать полную и надежную оценку законности операций, программ и политики, если они не имеют доступа ко всей соответствующей информации. Хотя это не самоцель, доступ ко всей информации, касающейся расследования (и более широкие полномочия данного органа надзора), является предварительным условием эффективной проверки.

Право органов надзора на доступ к информации должно дополняться обязанностью служб безопасности и их персонала быть открытыми и сотрудничать с контролерами, а также требованием, чтобы данные категории информации раскрывались автоматически. Использование таких следственных полномочий, как вызов в суд, обыск и конфискация, также укрепляет позицию контролеров в случаях, когда информацию не предоставляют добровольно.

Предоставление контролерам доступа к информации не означает, что органы надзора должны постоянно иметь неограниченный доступ к любой информации – основанием для доступа всегда должен быть мандат и текущая деятельность данного органа надзора.

Исходя из того, что лучшей практикой считается, когда по крайней мере один внешний орган надзора имеет полномочия надзирать за каждой областью деятельности служб безопасности, по крайней мере один внешний контролер должен иметь неограниченный доступ к информации, касающейся каждой

области. Соответственно, важная задача при планировании и совершенствовании системы надзора – обеспечить, чтобы доступ контролеров к информации был гарантирован законом и обеспечен соответствующими следственными инструментами для облегчения такого доступа.

Основополагающий принцип эффективного надзора заключается в том, что органы надзора (а не службы безопасности или исполнительная власть, являющиеся объектом проверки) должны определять, какая информация касается их работы. В случае спора на эту тему должны иметься механизмы их оперативного разрешения.

Важным дополнением к обеспечению доступа контролеров ко всей релевантной информации является необходимость реализации мер обеспечения, чтобы обрабатываемая контролерами информация была защищена и использовалась только в целях надзора. Если органы надзора имеют процедуры, исключающие злоупотребление деликатной информацией, нет оснований не верить их членам больше, чем сотрудникам исполнительной власти или служб безопасности.

Доступ к информации на основании и в связи с международным сотрудничеством разведок заслуживает особого рассмотрения. Учитывая широкое международное сотрудничество служб безопасности (и возможный эффект такого сотрудничества на права человека), важно, чтобы контролеры могли проверять информацию о таком сотрудничестве, включая информацию, полученную от зарубежных органов или предоставленную им. Чтобы обеспечить надлежащую проверку этой деятельности, важно, чтобы контролеров в силу закона или на практике не считали «третьей стороной» и не применяли к ним принцип контроля источника. Демократический надзор весьма затруднен, если зарубежные органы фактически имеют право вето (поскольку службы безопасности должны запрашивать разрешение иностранных партнеров перед тем, как контролеры смогут просмотреть такую информацию) на то, что может проверять орган надзора.

Еще одна задача – обеспечить контролеров необходимыми финансовыми и людскими ресурсами, гарантирующими их эффективность. Многие службы безопасности наращивают свои возможности (благодаря техническому прогрессу и растущим бюджетам) собирать, передавать и получать информацию и используют для этого все более сложные системы. Ресурсы большинства контролеров не выросли соразмерно таким изменениям. Сейчас общепризнано, что использование независимых технических знаний неотъемлемо от эффективного надзора.

Системы сбора и хранения информации усложнились, и последствия этого для прав человека трудно оценить без специальных знаний. Поэтому законы должны разрешать контролерам нанимать технических специалистов, и должны предоставляться ресурсы, позволяющие им делать это.

5.4. Прозрачность органов надзора

Органы надзора проверяют службы безопасности от имени населения. Важными задачами при этом является предоставление общественности гарантий (в обоснованных случаях), что службы безопасности осуществляют свои функции в соответствии с законом, и сообщение (если это необходимо) о том, что сделано неправильно. Органы надзора могут делать это, только если они своей отчетностью и другими формами информирования показывают, что службы безопасности находятся под строгим надзором и что все случаи нарушений прав человека (или других нарушений) рассматриваются. Вторая задача в этой связи – информировать общественность о роли служб безопасности в демократической стране. Это особенно важно для обществ, в которых службы безопасности в прошлом нарушали права человека и (или) не пользуются доверием общества. Для этого важно, чтобы органы парламентского и экспертного надзора максимально привлекали общественность. Они должны быть обязаны издавать публичные версии своих регулярных или специальных отчетов, соблюдая соответствующие меры для сохранения некоторых деталей в секрете по соображениям национальной безопасности и защиты частной жизни.

5.5. Оценка систем надзора

На территории Совета Европы достигнут существенный прогресс в организации внешнего надзора за службами безопасности, но очень немногие страны пошли дальше, проводя анализ эффективности отдельных органов надзора, не говоря уже о системах надзора[109]. Законодательно создав органы надзора, во многих случаях 10-20 лет назад, большинство стран не пересматривало их организации или делало это только после громких скандалов или провалов разведки. Поэтому очень трудно выяснить, в частности: занимаются ли системы надзора наиболее актуальными аспектами деятельности служб безопасности; эффективно ли они способствуют лучшему соблюдению прав человека в политике, операциях и правилах служб безопасности; используют ли эффективные методы и проводят ли достаточно строгие расследования; пользуются ли они доверием общества; предоставляют ли они точные и полезные отчеты.

Как показано выше, для того, чтобы системы надзора эффективно предупреждали и реагировали на опасения за права человека в работе или в связи с работой служб безопасности, им нужен соответствующий юридический мандат и полномочия, ресурсы и знания. Эти требования растут с развитием характера, масштабов и технологий, применяемых в работе служб безопасности.

109. Среди исключений – Бельгия и Нидерланды: Sénat et Chambre des Représentants de Belgique, «Evaluation du fonctionnement des Comités permanent de contrôle des services de police et de renseignements», Rapport fait au nom des commissions spéciales chargées du suivi parlementaire des Comités permanent de contrôle des services de police de renseignements par MM. Foret and De Crem, 16 fйvrier 1996. 437/1 – 95/96 Chambre, 1-258/1 Sénat; Fijnaut 2012.

Поэтому важно, чтобы системы надзора периодически оценивались на предмет наличия или отсутствия необходимых характеристик.

Связанный с этим вопрос – можно ли считать, что органы надзора (и, более широко, системы надзора) эффективно исполняют свои функции – вне зависимости от адекватности их правового мандата, полномочия и ресурсов. Он включает оценку эффективности обеспечения соответствия политики, операций и практик служб безопасности правам человека, а также рассмотрения и реагирования на жалобы, способствующего возмещению ущерба и организационному совершенствованию. Оценка таких вопросов требует глубокого анализа функциональности методов и подходов работы контролеров. Поэтому прежде чем приступать к официальной оценке, следует посмотреть, как можно оценить эффективности надзора, и в частности, как можно оценить способность системы надзора защитить права человека[110]. Это темы для дальнейшего обсуждения и потенциальной работы на европейском уровне.

Парламенты и министры могут играть важную роль в этом отношении, обеспечивая включение положений об оценке в законодательство о службах безопасности и надзоре за ними[111]. Как вариант, исполнительная власть, парламент или органы надзора могут формировать такие оценки на временной основе, как это недавно было сделано в Нидерландах. Альтернативная, или дополнительная модель принята в Великобритании, где имеется независимый рецензент законодательства о терроризме (*Independent Reviewer of Terrorism Legislation*)[112]. Хотя его бюро занимается законодательством о борьбе с терроризмом более широко, этот чиновник рассматривает адекватность положений закона, касающихся надзора, и уполномочен давать соответствующие рекомендации.

110. Подробнее см.: Wills 2012b: 471-499.
111. Наилучший пример в этом отношении мы имеем за пределами территории Совета Европы: Canada 1984: § 56; Canada 1990.
112. См.: https://terrorismlegislationreviewer.independent.gov.uk/, accessed 28 March 2015.

Ссылки

Article 29 Working Party (2014a), Opinion 04/2014 on surveillance of electronic communications for intelligence and national security purposes, 819/14/EN WP 215, 10 April 2014.

Article 29 Working Party (2014b), Joint Statement of the Article 29 Working Party, adopted 26 November 2014.

Balkan Insight (2015a), «Serbian ombudsman complains of threats», 21 January 2015: www.balkaninsight.com/en/article/serbian-ombudsman-threaten-aftermilitary-secret-service-revelation, accessed 28 March 2015.

Balkan Insight (2015b), «Macedonia PM accused of large-scale wire-tapping», 9 February 2015: www.balkaninsight.com/en/article/eavesdropping-bombshell-explodes-in-macedonia, accessed 28 March 2015.

BBC News (2015), «Sim card firm links GCHQ and NSA to hack attacks», 25 February 2015: www.bbc.co.uk/news/technology-31619907, accessed 28 March 2015.

Belgian Standing Intelligence Agencies Review Committee (2011), Annual report 2010-2011, Intersentia, Brussels. Available at: www.comiteri.be/images/pdf/publicaties/activity_report_2010-2011.pdf, accessed 28 March 2015.

Belgium (1991), Act governing review of the police and intelligence services and of the Coordination Unit for Threat Assessment 1991. Available at: http://comiteri.be/images/pdf/engels/w.toezicht%20-%20l.control.pdf, accessed 28 March 2015.

Belgium (1998), Law on the Intelligence and Security Services 1998.

Belgium (2010), Law on the Intelligence and Security Services 1998, (as modifed by the law on collection of data by the intelligence and security services of 14 February 2010).

Bigo D. et al. (2013), «National programmes for mass surveillance of personal data in EU Member States and their compatibility with EU law», European Parliament, Brussels.

Bigo D. et al. (2014), «France's surveillance: justice, freedom and security in the EU», openDemocracy.net, 14 May 2014.

Borger J. (2013), «NSA files: why the Guardian in London destroyed hard drives of leaked files», The Guardian, 20 August 2013.

Borger J. (2014), «Ministers should assess UK surveillance warrants, says Philip Hammond», The Guardian, 23 October 2014.

Born H. and Leigh I. (2005), Making intelligence accountable, Parliament of Norway, Oslo.

Born H., Leigh I. and Wills A. (forthcoming), Making international intelligence cooperation accountable, Parliament of Norway, Oslo.

Bosnia and Herzegovina (2004), Law on the intelligence and security agency of Bosnia and Herzegovina 2004.

Cameron I. (2000), National security and the European Convention on Human Rights, Martinus Nijhof Publishers, The Hague.

Cameron I. (2008), «National Security and the European Convention on Human Rights – Trends and Patterns», speech to the Stockholm International Symposium on National Security and the European Convention on Human Rights, 4-5 December 2008.

Cameron I. (2011), «Parliamentary and specialised oversight of security and intelligence agencies in Sweden», in Wills A. and Vermeulen M. (eds) (2011), «Parliamentary oversight of security and intelligence agencies in the European Union», European Parliament, Brussels.

Cameron I. (2013), «Foreseeability and safeguards in the area of security: some comments on ECHR case law», in Regards sur le contrôle, Laethem W. (Van) and Vanderborght J. (eds) (2013), Intersentia, Antwerp.

Canada (1984), Canadian Security Intelligence Service Act 1984.

Canada (1990), «In fux but not in crisis», Canada Special Committee on the Review of the CSIS Act and the Security Act (NCJ 131163), Ottawa, Canada. Cobain I. (2013), Cruel Britannia: a secret history of torture, Portobello Books, London.

Commissioner for Human Rights, Council of Europe (2013a), «Human rights and the security sector: report of the round-table with human rights defenders, organised by the Office of the Council of Europe Commissioner for Human Rights, Kyiv, 30-31 May (2013)», CommDH(2013)17.

Commissioner for Human Rights, Council of Europe (2013b), «Human rights at risk when secret surveillance spreads», Human Rights Comment, 24 October 2013.

Commissioner for Human Rights, Council of Europe (2014a), The rule of law on the internet and in the wider digital world, Issue Paper, Council of Europe, Strasbourg.

Commissioner for Human Rights, Council of Europe (2014b), Statement of 12 December 2014: www.facebook.com/permalink.php?story_fbid=377981239044459&id=118705514972034, accessed 28 March 2015.

Commissioner for Human Rights, Council of Europe (2014c), «Report by Nils Muižnieks, Council of Europe Commissioner for Human Rights, following his visit to the Netherlands, from 20 to 22 May 2014», CommDH(2014)18, 14 October 2014.

Commissioner for Human Rights, Council of Europe (2015), «4th quarterly activity report 2014», CommDH(2015)3.

Connolly K. (2014), «Romanian ex-spy chief acknowledges CIA had 'black prisons' in country», The Guardian, 14 December 2014.

Council of Europe (2006a), «Secretary General's report under Article 52 ECHR on the question of secret detention and transport of detainees suspected of terrorist acts,

notably by or at the instigation of foreign agencies», SG/Inf (2006)5, 28 February 2006.

Council of Europe (2006b), «Secretary General's supplementary report», SG/Inf (2006)13, 14 June 2006.

Croatia (2006), Act on the Security Intelligence System of the Republic of Croatia, 30 June 2006.

CTIVD (2014), «Review report on the processing of telecommunications data by GISS and DISS», No. 38, 5 February 2014.

Cvrtila V. (2012), «Intelligence governance in Croatia», DCAF. Available at: www.dcaf.ch/content/download/104961/1617969/version/2/fle/croatia_eng1.pdf, accessed 28 March 2015.

Czech Republic (1994), Act on the Security Information Service, Act No. 154 of July 7, 1994.

European Data Protection Authorities (2014), Joint Statement of the European Data Protection Authorities Assembled in the Article 29 Working Party, adopted 26 November 2014, 14/EN WP227.

European Parliament (2001), «Report on the existence of a global system for the interception of private and commercial communications (ECHELON interception system)», Temporary Committee on the ECHELON Interception System, 11 July 2001, A5-0264/2001.

European Parliament (2007), «Resolution on the alleged use of European countries by the CIA for the transportation and illegal detention of prisoners», 14 February 2007, P6_TA(2007)0032.

European Parliament (2013), «Resolution of 10 October 2013 on alleged transportation and illegal detention of prisoners in European countries by the CIA», P7_TA(2013)0418.

European Parliament (2014), «Report on the US NSA surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs», A7-0139/2014, 21 February 2014.

Farson S. (2012), «Establishing effective intelligence oversight systems» in Born H. and Wills A. (eds) (2012) Overseeing intelligence service: a toolkit, DCAF, Geneva.

Fijnaut C. (2012), «Het toezicht op de inlichtingen- en veiligheidsdiensten: de noodzaak van krachtiger samenspel, De vertrekpunten en uitkomsten van een gespreksronde», The Hague.

Földváry G. (2011), «Parliamentary and specialised oversight of security and intelligence agencies in Hungary», Annex A in Wills A. and Vermeulen M. (2011), Parliamentary oversight of security agencies in the European Union, European Parliament, Brussels.

Follorou J. (2014), «Espionnage: comment Orange et les services secrets coopèrent», Le Monde, 20 March 2014.

Follorou J. and Johannès F. (2013), «Révélations sur le Big Brother français», Le Monde, 4 July 2013.

Forcese C. (2012), «Handling complaints about intelligence services», in Born H. and Wills A. (eds), Overseeing intelligence services: a toolkit, DCAF, Geneva.

France (2007), Loi n° 2007-1443 du 9 octobre 2007 portant création d'une délégation parlementaire au renseignement.

Gallagher R. and Greenwald G. (2014), «How the NSA plans to infect 'millions' of computers with malware», The Intercept, 3 December 2014: https://frstlook.org/theintercept/2014/03/12/nsa-plans-infect-millions-computers-malware/, accessed 28 March 2015.

Germany (2001a), Act restricting the Privacy of Correspondence, Posts and Telecommunications (G10 Act), Federal Law Gazette I, p. 1254, revised 2298, last amended by Article 2 of the Act of June 6 2013, Federal Law Gazette I, p. 1482.

Germany (1990b), Act on the Protection of the Constitution (BVerfSchG), Federal Law Gazette I, p. 2954, last amended by Article 6 of the Act of June 6, 2013, Federal Law Gazette I, p. 1602.

Germany (1978), Parliamentary Control Panel Act (PKGrG), Federal Law Gazette I, p. 453, last amended by the Act of July 29, 2009, Federal Law Gazette I, p. 2346.

Goumaz M. (2014), «Statut spécial voulu par les espions», Le Temps, 1 July 2014.

Hernes H. (2008), «Effective Remedy with Regard to Secret Surveillance and Security Files», speech to the Stockholm International Symposium on National Security and the European Convention Human Rights, 4-5 December 2008.

Higgins A. (2013), «Luxembourg's prime minister resigns», New York Times, 12 July 2013.

Human Rights Watch (2009), Cruel Britannia, British complicity in the torture and ill-treatment of terror suspects in Pakistan, November 2009.

Human Rights Watch (2014a), Rights in retreat: abuses in Crimea, Human Rights Watch, New York.

Human Rights Watch (2014b), «Turkey: spy agency law opens door to abuse», April 2014: www.hrw.org/news/2014/04/29/turkey-spy-agency-law-opens-door-abuse, accessed 28 March 2014.

Hungary (1995), Act CXXV of 1995 on the National Security Services, section 16(2).

International Commission of Jurists (2009), Assessing damage, urging action: report of the Eminent Jurists Panel on terrorism, counter-terrorism and human rights, ICJ, Geneva.

Italy (2007), Law 127/2007 (as amended 1 August 2012).

Jacobsen A. (2012), «Regional consultation on national security and the right to information», www.right2info.org/resources/publications/national-security-page/european-questionnaires/slovenia-rosana-lemut-strle, accessed 28 March 2015.

Jacobsen A. (2013), «National security and the right to information in Europe», April 2013: www.right2info.org/resources/publications/national-security-expert-papers/jacobsen_nat-sec-and-rti-in-europe, accessed 28 March 2015.

JUSTICE (2011), Freedom from suspicion: surveillance reform for a digital age, Justice, London.

Laethem W. (Van) (2011), «Parliamentary and specialised oversight of security and intelligence agencies in Belgium», in Wills A. and Vermeulen M. (2011), «Parliamentary oversight of security and intelligence agencies in the European Union», European Parliament, Brussels.

LAHRC (2015), Draft Resolution adopted by LAHRC on 26 January 2015.

Le Monde (2013), «La DCRI accusée d'avoir illégalement forcé la suppression d'un article de Wikipédia», 6 April 2013.

Leigh I. (2012), «A view from across the Channel: intelligence oversight in the UK», in Laethem W. (Van) and Vanderborght J. (2012) (eds), Regards sur le contrôle, Intersertia, Antwerp.

Lithuania (2002), Law on Operational Activities 2002 (as amended).

Marty D. (2011), «Abuse of state secrecy and national security: obstacles to parliamentary and judicial scrutiny of human rights violations», Report for the Committee on Legal Affairs and Human Rights, Doc. 12714, 16 September 2011.

Nemtsova A. (2012), «Putin's secret war,» Foreign Policy, June 2012.

Netherlands (2002), Intelligence and Security Services Act 2002. Available at: www.ctivd.nl/?download=WIV%202002%20Engels.pdf, accessed 28 March 2015.

Norton-Taylor R. (2015), «Britain needs independent scrutiny of intelligence, says former head of MI6», The Guardian, 17 March 2015.

Norway (1981), Criminal Procedure Act, Act of 22 May 1981 No. 25 (as amended).

Norway (1995), Act relating to the Oversight of Intelligence, Surveillance and Security Services Act No. 7 of 3 February 1995. Available at: http://eos-utvalget.no/english_1/legal_framework/content_3/text_ 1401199215164/1401199215664/lovengelsk.pdf, accessed 28 March 2015.

Norway (2012), EOS-Utvalget Committee, Annual Report 2011.

Norway (2013), EOS-Utvalget Committee, Annual Report 2012.

Norway (2014), EOS-Utvalget Committee, Annual Report 2013.

Omtzigt, P. (2015), «Mass surveillance», PACE Committee on Legal Affairs and Human Rights, 26 January 2015, [AS/Jur (2015) 01].

Open Society Foundations (2013), Global Principles on National Security and the Right to Information (Tshwane Principles), adopted on 12 June 2013 in Tshwane, South Africa: www.opensocietyfoundations.org/sites/default/files/global-principles-national-security-10232013.pdf, accessed 28 March 2015.

Open Society Justice Initiative (2013), Globalizing torture: CIA secret detention and extraordinary rendition, OSF, New York.

Osborne L. (2013), «Germany denies phone data sent to NSA used in drone attacks», The Guardian, 12 August 2013.

Ottawa Principles on Anti-terrorism and Human Rights, adopted in 2006 in Ottawa, Canada: http://aix1.uottawa.ca/~cforcese/hrat/principles.pdf, accessed 28 March 2015.

Petrović P. (2012), «Serbia», Strengthening intelligence oversight in the Western Balkans series, DCAF, Geneva. Available at: www.dcaf.ch/content/download/104944/1617879/version/2/fle/serbia_eng1.pdf, accessed 28 March 2015.

Poland (2002), Act of 24 May 2002. Internal Security Agency and Foreign Intelligence Agency.

Pond E. (2013), «What the NSA can learn from Sweden», World Policy Blog, 9 August 2013, www.worldpolicy.org/blog/2013/08/09/what-nsa-can-learn-sweden, accessed 28 March 2015.

Portugal (2004), Intelligence Systems of the Portuguese Republic, Framework Law 4/2004.

Priest D. (2005), «CIA holds suspects in secret prisons», Washington Post, 2 November 2005.

Privacy International (2014), Statement of Grounds submitted to the Investigatory Powers Tribunal, 8 May 2014: www.privacyinternational.org/sites/default/files/PI%20Hacking%20Case%20Grounds.pdf, accessed 28 March 2015.

Protector of Citizens of the Republic of Serbia (2010), «Report on a preventive control visit by the Protector of Citizens to the Security-Information Agency», (Belgrade, 2010). Available at: www.ombudsman.org.rs/ attachments/088_Report%20on%20the%20Preventive%20Control%20Visit.pdf, accessed 28 March 2015.

Protector of Citizens of the Republic of Serbia (2014), Annual Report for 2013. Available at: www. ombudsman.rs/attachments/2013%20Annual%20Report%20of%20the%20Protector%20of%20Citizens.pdf, accessed 28 March 2015.

Review Group on Intelligence and Communications Technologies (2013), «Liberty and security in a changing world», 13 December 2013: www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_fnal_report.pdf, accessed 28 March 2015.

Romania (1991), Law on the National Security of Romania, No. 51/July 29 1991.

Sánchez Ferro S. (2011), «Parliamentary and specialised oversight of security and intelligence agencies in spain», Annex A in Wills A. and Vermeulen M. (2011), «Parliamentary oversight of security agencies in the European Union», European Parliament, Brussels.

Serbia (2014), The Law on Security Information Agency Official Gazette of the Republic of Serbia (as amended in 2014), Official Gazette Nos. 42/2002, 111/2009,65/2014 – US, 66/2014.

Singh A. and Scholes J. (2014), «Denmark, the CIA, and the killing of Anwar al-Awlaki», 30 April 2014: www.opensocietyfoundations.org/voices/denmark-cia-and-killinganwar-al-awlaki, accessed 28 March 2015.

Stark H. (2011), «Germany limits information exchange with US intelligence», Der Spiegel, 17 May 2011.

Stoll M. (2014), «Des documents du SRC peuvent aussi etre publics», Oefentlichkeitsgesetz.ch, 15 December 2014: www.oefentlichkeitsgesetz.ch/francais/2014/12/des-documents-du-src-peuvent-aussi-etre-publics/#more-3569, accessed 28 March 2015.

Townsend M. (2014), «UK rights groups reject official inquiry into post-September 11 rendition», The Observer, 8 November 2014.

Travis A. and Bowcott O. (2015), «UK admits unlawfully monitoring legally privileged communications», The Guardian, 18 February 2015.

Turkey (2014), Law Amending the Law on State Intelligence Services and the National Intelligence Agency, No. 6532, April 2014.

UK (2000), Regulation of Investigatory Powers Act (RIPA) 2000.

UK (2010), «Consolidated guidance to intelligence officers and service personnel on the detention and interviewing of detainees overseas, and on the passing and receipt of intelligence relating to detainees», Cabinet Office, London, July 2010.

Venice Commission (1998), «Internal security services in Europe», 7 March 1998, CDL-INF (98) 6.

Venice Commission (2007), «Report on the democratic oversight of the security services», 11 June 2007, CDL-AD(2007)016.

Venice Commission (2012), «Revised draft opinion on the federal law on the Federal Security Service (FSB) of the Russian Federation», Opinion no. 661/2011.

Venice Commission (2015), «Update of the 2007 Report on the democratic oversight of the security services and report on the democratic oversight of signals intelligence agencies», adopted at the 102nd plenary session (Venice, 20-21 March 2015, CDL-AD(2015)006.

Verhoeven N. (2011), «Parliamentary and specialised oversight of security and intelligence agencies in Germany», in Wills A. and Vermeulen M. (2011), «Parliamentary oversight of security agencies in the European Union», European Parliament, Brussels.

Wills A. (2012a), «Financial oversight of intelligence services,» in Born H. and Wills A. (eds) (2012), Overseeing intelligence services: a toolkit, DCAF, Geneva.

Wills A. (2012b), «Who's watching the overseers? Ad hoc evaluations of intelligence oversight and control bodies», in Laethem W. (Van) and Vanderborght J. (eds), Regards sur le contrôle, Intersertia, Antwerp.

Wills A. and Vermeulen M. (2011), «Parliamentary oversight of security and intelligence agencies in the European Union», European Parliament, Brussels.

With H. (De) and Kathmann E. (2011), «Parliamentary and specialised oversight of security and intelligence agencies in Germany», in Wills A. and Vermeulen M. (2011), «Parliamentary oversight of security agencies in the European Union», European Parliament, Brussels.

Генеральная Ассамблея ООН (2013), Резолюция 68/167, 18 декабря 2013 г., A/RES/68/167.

Генеральная Ассамблея ООН (2014), Резолюция 69/166, A/RES/69/166, 18 декабря 2014 г.

Комитет по правам человека ООН (2004), Замечание общего порядка № 31, UN Doc.CCPR/C/21/Rev.1/Add.13 (2004).

ООН (1987), Конвенция ООН против пыток и других жестоких, бесчеловечных или унижающих достоинство видов обращения и наказания, 10 декабря 1984 г. (введена в действие 26 июня 1987 г.).

ООН (2010a), «Подборка оптимальных практических методов, применяемых в отношении законодательной и институциональной основы и мер, которые обеспечивают соблюдение прав человека специальными службами в условиях борьбы с терроризмом, в том числе касающихся надзора за их деятельностью», Специальный докладчик по вопросу о поощрении и защите прав человека и основных свобод в условиях борьбы с терроризмом, 17 мая 2010 г., A/HRC/14/46.

ООН (2010b), «Совместное исследование о глобальной практике в связи с тайным содержанием под стражей в условиях борьбы с терроризмом», Специальный докладчик по вопросу о поощрении и защите прав человека и основных свобод в условиях борьбы с терроризмом, A/HRC/13/42, 19 февраля 2010 г.

ООН (2013), «Доклад Специального докладчика по вопросу о поощрении и защите права на свободу мнений и их свободное выражение Франка Ла Рю», 17 апреля 2013 г., A/HRC/23/40.

ООН (2014), «Доклад Специального докладчика по вопросу о поощрении и защите прав человека и основных свобод в условиях борьбы с терроризмом», 23 сентября 2014 г., A/69/397.

ПАСЕ (2005), Парламентская ассамблея Совета Европы, Рекомендация 1713 (2005), 23 июня 2005 г.

ПАСЕ (2011), Парламентская ассамблея Совета Европы, Резолюция 1838 (2011), 6 октября 2011 г.

ПАСЕ (2013), Парламентская ассамблея Совета Европы, Резолюция 1954 (2013), 2 октября 2013 г.

Совет по правам человека ООН (2009), Резолюция 10/15, 10-я сессия, 26 марта 2009 г.

Управление Верховного Комиссара ООН по правам человека (2014), «Право на неприкосновенность личной жизни в цифровой век», 30 июня 2014 г., A/HRC/27/37, UN High Commissioner for Human Rights. Available at: www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/ A.HRC.27.37_en.pdf, accessed 28 March 2015.

Судебные прецеденты

Европейский суд по правам человека

Abu Zubaydah v. Lithuania, Application No. 46454/11, communicated on 14 December 2012.

Al Nashiri v. Poland, Application No. 28761/11, 24 July 2014.

Al Nashiri v. Romania, Application No. 33234/12, communicated on 18 September 2012.

Assenov and Others v. Bulgaria, Application No. 90/1997/874/1086, 28 October 1998.

Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria, Application No. 62540/00, 28 June 2007.

Big Brother Watch and Others v. the United Kingdom, Application No. 58170/13, lodged on 4 September 2013 (challenging PRISM and TEMPORA).

Dumitru Popescu v. Romania, Application No. 71525/01, 26 April 2007.

El Masri v. «the former Yugoslav Republic of Macedonia», Application No. 39630/09, 13 December 2012.

Husayn (Abu Zubaydah) v. Poland, Application No. 7511/13, 24 July 2014.

Iordachi and Others v. Moldova, Application No. 25198/02, 10 February 2009.

Kennedy v. the United Kingdom, Application No. 26839/05, 18 May 2010.

Klass and Others v. Germany, Application No. 5029/71, 6 September 1978.

Leander v. Sweden, Application No. 9248/81, 26 March 1987.

Liberty and Others v. the United Kingdom, Application No. 58243/00, 1 July 2008.

Malone v. the United Kingdom, Application No. 8691/79, 2 August 1984.

Nasr and Ghali v. Italy, Application No. 44883/09, communicated on 22 November 2011.

Segerstedt-Wiberg and Others v. Sweden, Application No. 62332/00, 6 June 2006.

Sunday Times v. the United Kingdom (No. 2), Application No. 13166/87, 26 November 1991.

Vetter v. France, Application No. 59842/00, 31 May 2005.

Weber and Saravia v. Germany, Application No. 54934/00, decision on admissibility of 29 June 2006.

Национальные суды

Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources and Others, Joined Cases C-293/12 and C-594/12, 14 April 2014.

Liberty & Others vs. the Security Service, SIS, GCHQ, IPT/13/77/H, 6 February 2015.

Эффективный демократический надзор за деятельностью национальных служб безопасности

Координаторы проекта:
Иден Коул (Женевский Центр демократического
контроля над вооруженными силами),
Валентин Бадрак (Центр исследований армии, конверсии и разоружения)

напечатано: Адеф Украина

Тираж: 1000 экз.

Разоблачения массовой слежки за электронными линиями связи вольнонаемным сотрудником американской разведки Эдвардом Сноуденом вызвали серьезные опасения в нарушении права на частную и семейную жизнь, свободы слова и свободы объединений. Нынешним разоблачениям предшествовали другие, касающиеся участия некоторых служб безопасности в серьезных нарушениях прав человека на протяжении предыдущих десяти лет. Все это вызывает вопрос об адекватности правового регулирования и надзора за деятельностью служб безопасности на территории Совета Европы.

Данный доклад в первую очередь рассматривает роль национальных институтов, ответственных за санкционирование, мониторинг, проверку и рассмотрение деятельности служб безопасности и, в меньшей степени, исполнительных органов, ответственных за службы безопасности. В частности, были рассмотрены примеры следующих институтов надзора разных европейских государств: парламентские комитеты, судебные и квази-судебные органы, органы экспертного надзора за разведкой и безопасностью, уполномоченные по данным и информации, институты омбудсменов и исполнительной власти, и механизмы внутреннего контроля служб безопасности.

Наряду с анализом национальных практик надзора, в данном докладе также рассмотрен растущий массив международных принципов «твердого» и «мягкого» права, касающихся надзора за службами безопасности. Особое внимание уделено актуальности Европейской конвенции прав человека и ее прецедентному праву в этой области. В публикации целенаправленно рассмотрен надзор за деятельностью, вызывающей в настоящее время опасения за права человека, включая сотрудничество со службами безопасности и разведки других государств, неизбирательную массовую слежку за электронными линиями связи и проникновение в компьютерные сети (хакерство).

В докладе содержится ряд рекомендаций, как можно усилить надзор за службами безопасности для обеспечения лучшей защиты прав человека в данной сфере деятельности государства. Признавая, что единственной «идеальной» модели или системы надзора не существует, рекомендации предлагают принципы, которые могут быть реализованы в любой политической или конституционной системе.

www.commissioner.coe.int

RUS

www.coe.int

Совет Европы является ведущей организацией на континенте в области прав человека. Он включает в себя 47 стран, 28 из которых являются членами Европейского Союза. Все страны-члены Совета Европы подписали Европейскую конвенцию о правах человека – международный договор, призванный защищать права человека, демократию и верховенство права. За применением Конвенции в государствах-членах следит Европейский суд по правам человека.

COMMISSIONER FOR HUMAN RIGHTS
COMMISSAIRE AUX DROITS DE L'HOMME

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE