# ПРОСЛУШИВАНИЕ ТЕЛЕФОНОВ В МЕЖДУНАРОДНОМ ПРАВЕ И ЗАКОНОДАТЕЛЬСТВЕ ОДИННАДЦАТИ ЕВРОПЕЙСКИХ СТРАН

# 12(49)

**ХАРЬКОВСКАЯ ПРАВОЗАЩИТНАЯ ГРУППА**

**ХАРЬКОВ**

**1999**

В специальном выпуске №49 информационно-аналитического бюллетеня "Права людини" дан обзор законодательства одиннадцати европейских стран о прослушивании телефонных переговоров. Описаны решения Европейского Суда по правам человека, относящиеся к прослушиванию. Рассмотрен ряд международных и национальных проектов по контролю за информацией в электронных средствах коммуникаций. Приводится текст нового немецкого закона о телекоммуникациях.

---

## Содержание

---

## От составителя

Среди многих средств, используемых государственными спецслужбами, прослушивание телефонных разговоров[1] весьма специфично. С одной стороны, это ценное, даже необходимое средство борьбы с преступностью. С другой стороны, не будучи таким явным ограничением прав человека, как, например, конфискация имущества, прослушивание телефонных разговоров государством представляет собой не меньшую угрозу свободе человека. В худшем случае прослушивание телефонов означает, что не подотчетные общественности государственные спецслужбы получают секретный доступ к частным разговорам с целью нахождения какого-либо компромата или же просто с целью выявления и запугивания инакомыслящих. Люди, прожившие десятки лет в тоталитарных советских государствах и зафиксировавшие тем или иным образом свою нелояльность этому строю, хорошо помнят ощущение полной незащищенности и необходимость

скрывать свои действия и свои отношения с другими людьми от всевидящего глаза и всеслышащего уха служб безопасности.

После бархатных революций в Центральной и Восточной Европе и распада СССР ситуация изменилась. Новые парламенты и правительства постсоветских стран заявили о приверженности идеям демократии и прав человека. Почти все эти страны стали членами Совета Европы. Обязавшись выполнять Европейскую Конвенцию прав человека, они должны изменить законодательство и практику так, чтобы они соответствовали нормам европейского права, в том числе и в отношении действий спецслужб, условия работы которых неизбежно связаны с опасностью нарушения права на неприкосновенность личной жизни, защищаемое 8 статьей Конвенции. Эта коллизия объективно обусловлена. Рост организованной преступности, терроризма, наркобизнеса требует неординарных действий спецслужб по пресечению и раскрытию преступлений, а для этого необходимы все более совершенные методы и средства получения информации. Поэтому понятно желание спецслужб получить установленные законом дополнительные возможности. В то же время исторический опыт убеждает, что во всех без исключения странах отсутствие реального надзора за действиями спецслужб неизбежно приводит к злоупотреблениям, к слежке за деятелями оппозиции, профсоюзов, журналистами, активистами движения за права человека, просто нешаблонно мыслящими людьми.

В настоящем издании предпринята попытка рассмотрения законодательства ряда европейских стран о прослушивании и его соответствия нормам международного права. Вначале дано определение перехвата телефонных разговоров согласно международному праву, затем описаны относящиеся к нему решения Европейского Суда по правам человека (обзор ограничен решениями, принятыми до начала 1996 г.) и сформулированы стандарты, которым должно соответствовать национальное законодательство, чтобы соблюдалась статья 8 Европейской Конвенции прав человека. После этого дается сравнение основных положений международного права и национального законодательства, регулирующего прослушивание телефонных разговоров в одиннадцати европейских странах (Великобритании, Германии, Финляндии, Франции, Швейцарии, Швеции, Венгрии, Польше, Румынии, Российской Федерации и Украине). Рассмотрение соответствующих законов каждой из этих стран имеет целью дать ответ на следующие вопросы: какое законное основание имеет государственная власть для перехвата телекоммуникаций? какова процедура, разрешающая принятие таких мер? каковы процедуры контроля за соответствием закону практики прослушивания? и насколько процедуры, принятые в каждой из стран, сравнимы со стандартами, установленными Европейским Судом по правам человека? Обсуждение проблемы заключает статья профессора Денниса Телльборга (Швеция) о путях развития законодательства о прослушивании телефонов.

В последующей части книги приводится информация о международных и национальных проектах, ставящих целью контроль за информацией в электронных средствах коммуникаций: о межконтинентальной системе Echelon, проекте Европейского Союза ENFOPOL, законе США о содействии правоохранительным органам в области коммуникаций, российской СОРМ и др.

В Приложении дан перевод немецкого закона о телекоммуникациях, одного из немногих национальных законов, регулирующих развитие современных электронных коммуникаций.

Б(льшая часть книги является обзором западных источников, некоторые разделы написаны составителем. Книга является одним из плановых результатов работы

Харьковской правозащитной группы в международном Проекте "Службы безопасности в условиях конституционной демократии". Без информационной и консультативной поддержки Проекта книга просто не состоялась бы. Мы приносим глубокую благодарность всем участникам Проекта, помогавшим в работе над книгой, и прежде всего профессору Кейт Мартин и профессору Анджею Жеплинскому. Мы сердечно благодарим также вице-президента Академии правовых наук Украины профессора Юрия Михайловича Грошевого за ценные замечания и редактора бюллетеня российской правозащитной сети "Права человека в России" Сергея Смирнова за возможность использовать подготовленные им материалы.

Е.Е.Захаров

## Прослушивание телефонов в международном праве

Право на конфиденциальность корреспонденции было принято в международном праве с 1948. Всеобщая декларация ООН по правам человека и Европейская Конвенция по защите прав и основных свобод человека прямо указывают на конфиденциальность личной корреспонденции. Ст.12 Всеобщей декларации гласит:

Никто не может подвергаться произвольному вмешательству в его личную и семейную жизнь, произвольным посягательствам на неприкосновенность его жилища, тайну его корреспонденции или на его честь и репутацию. Каждый человек имеет право на защиту закона от такого вмешательства или таких посягательств.

Многие международные соглашения по правам человека ссылаются на конфиденциальность корреспонденции как на право. Международный пакт о гражданских и политических правах, Конвенция ООН о трудящихся-мигрантах, Конвенция ООН о правах ребенка оперируют одними и теми же понятиями. На региональном уровне эти права наполняются большей силой.

Так, ст.8(1) Европейской Конвенции ясно устанавливает, что "каждый человек имеет право на уважение его личной и семейной жизни, его жилища и тайны его корреспонденции".

Однако указанные документы не рассматривают это право как абсолютное. Ст.12 Всеобщей декларации ООН защищает от того, что называется неясным термином "произвольное вмешательство", каковое, по-видимому, противопоставляется вмешательству согласно закону с ясно сформулированной целью. Европейская Конвенция определяет пределы этого права гораздо более четко. Ст.8(2) гласит:

Не допускается вмешательство государственных органов в осуществление этого права, за исключением случаев, когда это предусмотрено законом и необходимо в демократическом обществе в интересах государственной безопасности, общественного порядка или экономического благосостояния страны, для поддержания порядка и предотвращения преступлений, защиты здоровья и морали, или защиты прав и свобод других лиц.

Итак, согласно Европейской Конвенции по защите прав человека, все лица имеют право на конфиденциальность корреспонденции, но это право можно ограничить "в соответствии с законом" и если это "необходимо в демократическом обществе".

## ЕВРОПЕЙСКИЙ СУД ПО ПРАВАМ ЧЕЛОВЕКА[2]

Европейский Суд по правам человека значительно сузил круг этих весьма абстрактных исключений, рассмотрев ряд конкретных судебных дел, связанных именно с прослушиванием телефонных разговоров и предполагаемым нарушением ст.8 Конвенции.

Процесс Класса и др. против Федеративной Республики Германии[3] был первым делом, рассмотренным Европейским судом по правам человека по вопросу о возможном нарушении прав человека посредством прослушивания телефонных разговоров. В этом деле, рассмотренном в 1978 г., Класс и др. утверждали, что Дополнение G-10 от 1968 г. к Германскому Основному Закону, которое разрешало прослушивание телефонных разговоров (см. обсуждение в части, касающейся Германии), фактически противоречит ст.8 Конвенции. Класс и др. признали, что у них нет оснований полагать, что их телефоны прослушивались. Скорее, они действовали из принципа и "не признавали Дополнение к закону на том основании, что в нем не содержалось четкого требования уведомлять лиц, чьи разговоры должны прослушиваться, после того, как прослушивание закончилось, и что в Дополнении не предусматривалась возможность оспорить в суде применение этих мер" (Класс, примечание)[4]. В сущности, заявители не оспаривали права демократического государства применять такие меры для своей защиты, но утверждали, что Дополнение G-10 "не содержит достаточных предохранительных мер против возможных злоупотреблений" (Класс, 47). Германское правительство ответило, что, во-первых, поскольку заявители не утверждали, что их телефоны прослушивались, то их нельзя рассматривать как "жертв нарушения их прав" согласно ст.25(1) Конвенции;[5] и, во-вторых, что статья 8(2) Конвенции "не требует судебного контроля секретного прослушивания и что система надзора, согласно Дополнению G-10, на самом деле эффективно защищает права личности" (Класс, 54).

Относительно вопроса, связанного со ст.25(1), Суд в своем решении выделил секретность надзора. Суд постановил, что если лицо не знает о нарушении своих прав, то нарушение все равно существует. По мнению суда "недопустимо", что "право гарантированное конвенцией, может быть нейтрализовано тем, что лицо не знает о нарушении своих прав". Тогда, добавил Суд, "ст.8 как бы отменяется" (Класс, 36). Следовательно, постановил Суд, "лицо может, при определенных условиях, считать себя жертвой нарушения, состоящего лишь в том, что существуют секретные меры или закон, допускающий такие меры, даже в случае, когда такие меры к нему не применялись" (Класс, 34). Поскольку любое лицо может быть потенциальной жертвой нарушения ст.8 Конвенции, не зная об этом, каждое лицо в качестве жертвы может обжаловать такой порядок в суде.

При обсуждении ст.8 Суд принял, что телефонные разговоры включаются в понятия "частная жизнь" и "корреспонденция", несмотря на то, что термин "прослушивание телефонных разговоров" не включен явно в Конвенцию. Суть решения, по мнению Суда, была в том, является ли прослушивание телефонных разговоров, определяемое в Дополнении G-10 "оправданным в терминах ст.8(2)". Суд заявил:

Так как эта статья указывает исключения из права, гарантированного Конвенцией, они должны трактоваться в узком смысле. Право на секретное наблюдение за гражданами характерно для полицейских государств, а в демократических государствах, согласно Конвенции, такое наблюдение может быть терпимо только в случае крайней необходимости для сохранения демократических институтов (Класс, 42).

Перед рассмотрением заявления о недостаточном предупреждении злоупотреблений Суд заметил, что вследствие "развития терроризма в Европе" и "весьма серьезной угрозы", перед которой стоят европейские демократические страны, "государство должно иметь право защищаться от таких угроз и устанавливать секретное наблюдение за подрывными

элементами, действующими в пределах его юрисдикции", поэтому Суд признал, что "существование определенного законодательства, регулирующего скрытый надзор за почтой и связью, является, ввиду исключительных условий, необходимым в демократическом обществе" (Класс, 48). Однако Суд резко ограничил применение наблюдения, ясно заявив, что:

Это не означает, что страны-участницы Конвенции пользуются неограниченным дискреционным правом вести скрытое наблюдение за лицами, подпадающими под их юрисдикцию.

С целью борьбы против шпионажа и терроризма [странам-участницам Конвенции нельзя] применять всякие меры, которые они посчитают нужными… Суд должен быть убежден, что при применении любой системы наблюдения должны существовать адекватные и эффективные гарантии против злоупотреблений. (Класс, 49).

Таким образом, Суд усилил ст.8(2) Конвенции и уточнил ее смысл: во-первых, всякое наблюдение должно вестись "на основании закона"; во-вторых, оно применяется в случае "необходимости защиты демократических институтов" и, в-третьих, всякая система наблюдения должна включать "адекватные и эффективные гарантии против злоупотреблений".

Суд согласился, что Дополнение G-10 фактически "соответствовало закону", и что прослушивание телефонных разговоров согласно нему может применяться только "при необходимости защиты демократических институтов". После этого Суд перешел к рассмотрению вопроса о том, содержатся ли в этом Дополнении меры по предупреждению злоупотреблений. Ниже, обсуждая германский закон, мы разберем этот вопрос детально, а сейчас рассмотрим ряд необходимых следствий из решения Суда по делу Класса.

Во-первых, прослушивание телефонных разговоров позволяется только в тех случаях, когда существуют фактические свидетельства того, что данное лицо замешано в серьезном преступлении. "Так называемое пробное или общее наблюдение не разрешается рассматриваемым законом" (Класс, 51.1). Во-вторых, "приказ о наблюдении может быть отдан только тогда, когда получено заявление в письменном виде, мотивирующее причины установления наблюдения, и такое заявление подается только главой или заместителем главы определенной службы" (Класс, 51.2). В-третьих, "существует административная процедура, гарантирующая, что наблюдение не может быть установлено произвольно и без должных причин" (Класс, 51.3). В-четвертых, "соответствующий министр в своей практической деятельности, исключая не терпящие отлагательства случаи, должен получить предварительное разрешение органов, ответственных за надзор" (Класс, 51.4). В-пятых, "перечислены определенные обстоятельства, при которых можно устанавливать наблюдение и обрабатывать информацию, полученную в процессе наблюдения" (Класс, 52). В-шестых, Суд отчетливо заявил о предпочтительности судебного контроля над процессом прослушивания, однако заметил, что в рассмотренном случае контрольный орган функционирует удовлетворительно. И, наконец, относительно аргументов, выдвинутых Классом и созаявителями, Суд отметил, что тот факт, что лицо не уведомили об окончании прослушивания телефонных разговоров, сам по себе не противоречит ст.8, именно неуведомление обеспечивает эффективность вмешательства" (Класс, 58). Таким образом, Суд постановил, что Дополнение G-10 не является нарушением ст.8.

В деле Класса Суд впервые дал подробное описание того, что можно назвать идеальной процедурой прослушивания телефонных разговоров, согласованной со ст.8 Конвенции. Шесть лет спустя в деле Малоуна против Соединенного Королевства[6], Суд снова рассмотрел систему телефонного надзора в конкретной стране, Великобритании. Однако в деле Малоуна речь не шла о гарантиях против злоупотреблений. В этом деле Суд сосредоточил свое внимание на значении термина "на основании закона".

Малоун, торговец антиквариатом, был обвинен в торговле краденым. Позднее он был оправдан по всем пунктам обвинения. Во время судебного процесса стало ясно, что один из телефонных разговоров Малоуна был тайно записан полицией. Обвинение признало, что телефон Малоуна прослушивался в этом единственном случае. Малоун подал иск - и проиграл в английском суде по двум различным, но взаимосвязанным причинам: закон не давал ему права на тайну переговоров, а поскольку в Англии всякий волен делать что ему угодно, то ничто не мешает полицейскому офицеру прослушивать переговоры. Даже выносивший постановление судья указал, что "прослушивание телефонов вопиет о законодательном регулировании". Мистер Малоун проявил необычайную настойчивость и подал на Соединенное Королевство жалобу в Европейский Суд по правам человека. В Страсбурге Малоун утверждал, что его разговоры прослушивались несколько лет после его оправдания и что его телефон был поставлен "на счетчик" (что означает не саму запись разговора, а сбор государством информации о том, с кем и как долго абонент разговаривал по телефону)..

Суд начал обсуждение с подробного описания правил прослушивания телефонных разговоров в Англии и Уэльсе. В то время, когда прослушивался телефон Малоуна и позднее, эти правила были основаны на трех официальных докладах: Доклад Биркетта (1957), "Перехват сообщений в Великобритании" известный под названием "Белая книга" (1980) и Доклад лорда Диплока. Согласно этим докладам, в Англии и Уэльсе существовала практика, состоящая в том, что, когда следователям нужно было прослушивать чей-либо телефон, они делали это "по ордеру, подписанному Государственным Секретарем". Хотя было отмечено, что согласно Телеграфному Акту от 1868 г. разглашение любым государственным служащим какой-либо информации или перехват сообщения "вопреки своему долгу" есть преступление, было развито сильное давление на Суд, чтобы он нашел парламентский акт, который бы явно давал государству такие полномочия.

Желая найти законодательную основу, Суд рассмотрел Почтовый Акт от 1969 г. Согласно разделу 80 этого Акта:

Требование предпринять необходимые действия для информирования должностных лиц, находящихся на службе Короны, относительно содержания переданных или передаваемых сообщений по почтовым и телекоммуникационным каналам, предоставляемым Почтовой Службой, может быть предъявлено Почтовой Службе для тех же целей, и тем же способом, что и при принятии настоящего Акта, причем на главу Почтовой Службы может быть возложена обязанность информирования указанных лиц [полицейских следователей] относительно сообщений, переданных или передаваемых посредством указанной службы". (Малоун, 29)

Иными словами, возможно некоторое упорядочение процедур, в ходе которых глава Почтовой Службы может предпринять "необходимые меры" для сбора информации. Суд далее процитировал параграф 1(1) документа 5 Телеграфного Акта от 1969 г., который гласит:

При обвинении лица… в незаконном разглашении содержания сообщений… оправдательным обстоятельством для него является доказательство того, что он действовал, подчиняясь ордеру, подписанному Государственным Секретарем. (Малоун, 30)

Перед Судом встал вопрос: может ли мешанина из государственных докладов и обрывков парламентских актов отвечать смыслу выражения ст.8(2) Конвенции "на основании закона"? На этот вопрос Суд уверенно ответил отрицательно.

Это заключение Суд предварил рядом аргументов, поясняющих понятие "на основании закона". Во-первых, Суд заявил, что "рассматриваемое действие должно иметь определенные основания в национальном законодательстве". Во-вторых, "термин "закон" должен интерпретироваться не только как писаный закон, но и как неписаный". В-третьих, "закон должен быть доступен". В-четвертых, он должен быть понятен, то есть, "сформулирован достаточно точно, чтобы граждане могли регулировать свое поведение" (Малоун, 66). Вдобавок Суд ясно заявил, что "его мнение о значении выражения "на основании закона" не просто относится к тому, что в национальном законодательстве существует такой закон, но и подразумевает, какого качества этот закон" (Малоун, 67).

Рассматривая дело Малоуна, Суд задался двумя вопросами: утверждает ли закон, что Почтовая Служба может перехватывать, в целях полицейского расследования, телефонные разговоры только по ордеру, подписанному Государственным Секретарем? и "в какой мере закон определяет обстоятельства, при которых такой ордер может быть подписан и применен"? (Малоун, 70). По первому вопросу Суд установил, что хотя Доклад Биркетта и "Белая Книга" ясно описывают процедуру для установления прослушивания телефонных разговоров, "закон Англии и Уэльса... не устанавливает явным образом, при каких условиях может быть выдан ордер" (Малоун, 71). Фактически, заметил Суд, Почтовый Акт от 1969 г. однозначно утверждает, что полицейские власти могут ходатайствовать перед главой Почтовой Службы об установлении телефонного прослушивания. Что касается второго условия, то Суд установил, что, в отличие от правительственной интерпретации, раздел 80 Почтового Акта фактически не содержит оснований для процедур, изложенных в Докладе Биркетта и в "Белой Книге". Конкретно, закон не указывает предполагаемые преступления, когда дозволено вести прослушивание телефонных разговоров, не устанавливает, какие сведения должны быть включены в ордер, не указывает срок действия ордера и даже не указывает, какие именно "лица, находящиеся на службе Короны", уполномочены предъявлять ордер. Суд отметил, что законоприменительная практика в Англии и Уэльсе в большой степени основана на правительственных докладах, и, следовательно, является потенциально недоступной и изменяемой без предварительных сообщений и общественного обсуждения. В итоге Суд решил, что:

закон Англии и Уэльса не указывает достаточно ясно пределы и способ применения соответствующих полномочий органов государственной власти. Таким образом, минимальный уровень правовой защиты граждан, которая должна быть обеспечена в соответствии с принципом верховенства права в демократическом обществе, отсутствует. (Малоун, 79)

Решив, что законоприменительная практика в Англии и Уэльсе не опирается на национальное законодательство, Суд не нашел нужным применять еще и критерий "качества закона".

Суд завершил рассмотрение дела Малоуна кратким обсуждением полицейской практики прослушивания телефонных разговоров и признал, что эта практика "противоречит гарантиям, содержащимся в ст.8" (Малоун, 84). Поскольку Суд признал, что законоприменительная практика в Англии и Уэльсе не находится "в согласии с законом", то тем самым эта практика является незаконной.

Шесть лет спустя Суд рассмотрел еще два дела о возможном нарушении ст.8 по причине прослушивания телефонных разговоров. Хотя дела Ювига против Франции[7] и Крюслена против Франции[8] слегка различаются, Суд в один и тот же день принял по ним одинаковые решения относительно соответствующего французского закона.

Ювиг и его жена владели овощным киоском. В 1973 г. они были обвинены в финансовых махинациях. В мае 1974 г. в их доме был произведен обыск согласно ордеру. Согласно французским правилам был выдан другой ордер на телефонное прослушивание в течение 4-5 августа 1974 г. Прослушивание не дало полиции никакой нужной информации и не стало основанием для их последующего обвинения. Крюслен, с другой стороны, был осужден за бандитизм. В ходе судебного процесса над Крюсленом запись телефонного разговора, который он вел с неким лицом, чей телефон прослушивался согласно ордеру, выданному по совсем иным причинам, оказался существенным элементом обвинения. И Крюслен, и второй участник телефонного разговора обратились в суд, заявляя, что прослушивание являлось нарушением ст.8 Конвенции.

Суд применил к делам Ювига и Крюслена тот же стандарт, состоящий из двух частей, что и в деле Малоуна, чтобы определить, производилось ли прослушивание "на основании закона". Чтобы выяснить, имелось ли нарушение ст.8, нужно было установить, имеет ли французская законодательная практика основу в национальном законодательстве, и является ли закон, составляющий эту основу, доступным и понятным; во-вторых, нужно было выяснить, применимо ли здесь еще нечеткое понятие "качество закона".

Ст.81 Французского Уголовного Кодекса от 1958 г. наделяет судью, проводящего расследование, правом "принимать все меры расследования, которые он полагает полезными для установления истины". Судья может предпринять эти меры сам или выдать ордер старшему полицейскому офицеру, передав ему указанные полномочия. В ст.151 указывается, что "в ордере должно быть указано расследуемое преступление, стоять дата и печать судьи" (Ювиг, 15). Сам по себе этот закон, казалось бы, не должен был пройти строгую проверку, примененную в деле Малоуна. Однако, признавая, что "закон, основанный на прецедентах, традиционно играет важную роль в странах европейского континента до такой степени, что целые разделы законодательства основаны на предыдущих решениях судов" (Ювиг, 28), и что французские суды давно считают, что вышеуказанный закон предполагает прослушивание телефонных разговоров, а также то, что суды точно определили надлежащую процедуру в огромном количестве решений по подобным делам, Суд нашел французские нормы "имеющими основания в национальном законодательстве" и доступными.

При рассмотрении вопроса "качества" закона, Суд, напротив, решил, что мешанина законов и решений Верховного Суда не обладает нужным качеством. Суд признал положительной чертой то, что во французской системе имеется множество предохранительных механизмов против злоупотреблений, включая независимый орган судебного контроля, право на апелляцию, запрет прерывания разговора, конфиденциальность общения адвоката и клиента, однако, в конечном счете, Суд признал, что положения французского закона не обеспечивают защиту от злоупотреблений. Суд перечислил шесть отдельных проблем, относительно которых во французской системе не

удается достичь полного или хотя бы частичного соответствия судебных решений и положений закона:

1. Состав преступлений, при расследовании которых разрешено устанавливать прослушивание.

2. Пределы длительности прослушивания.

3. Подробные правила составления отчетов по перехваченным разговорам.

4. Гарантии получения судьей записей разговоров без исправлений и купюр.

5. Обстоятельства, при которых записи могут или должны быть уничтожены.

6. Правила уничтожения записей или их расшифровок в случае оправдания обвиняемого судом(Ювиг, 34)

Суд подытожил, что французские правила имеют основания в национальном законодательстве, но не содержат достаточных гарантий против возможных злоупотреблений.

В 1994 г. Суд по правам человека рассмотрел еще одно дело, касающееся предполагаемого нарушения ст.8 в части прослушивания телефонных разговоров, дело А. против Франции.[9] В этом деле заявительница А. предполагала, что ее телефон прослушивался в нарушение статьи 8 Конвенции. Третья сторона, господин Герлинг, пришел в полицейский участок и заявил, что готовится преступление. Герлинг предложил офицеру полиции записать его телефонный разговор с А., в котором они якобы будут обсуждать готовящееся преступление. Офицер согласился и записал разговор между Герлингом и А. - с явного согласия Герлинга, но без ордера. А. была обвинена в преступлении и позже оправдана.

А. утверждала, что офицер полиции прослушивал ее телефон, не имея ордера, в нарушение французской законоприменительной практики и ст.8 Конвенции. Правительство возражало, что, поскольку Герлинг дал согласие на запись разговора, в котором он сам участвовал, то нарушения не было. Рассмотрев это дело, Суд решил, что, хотя запись телефонного разговора одним из его участников не является противозаконным, однако участие в этом офицера полиции фактически означает действия государственного органа. А поскольку во Франции нет закона, позволяющего государственному органу прослушивать разговор по требованию одного из говорящих, то Суд признал это действие нарушением ст.8: оно не было произведено "на основании закона".

В заключение отметим, что Европейский Суд по правам человека затратил много усилий по определению неприкосновенности личной корреспонденции согласно ст.8 Европейской Конвенции по правам человека. Что еще более важно, Суд уточнил обстоятельства, при которых государству дозволено нарушить эту неприкосновенность. Суд сделал это, определив ряд требований к правилам прослушивания телефонных разговоров в странах-участницах Конвенции.

## Стандарты Европейского Суда по перехвату телефонных сообщений[10]

Для того, чтобы перехват телефонного сообщения не считался нарушением статьи 8 Европейской Конвенции по защите прав и основных свобод человека, он должен осуществляться:

"На основании закона"

Какое-либо слежение должно производиться в соответствии с действующим национальным законом (Малоун), удовлетворяющим следующим требованиям:

"доступность" - согласно писаному или неписаному закону "гражданин должен иметь возможность убедиться, что прослушивание соответствует законодательным нормам, которые использованы в данном конкретном случае" (Малоун);

"предсказуемость" - гражданин должен быть способен (если необходимо - с помощью адвоката) предвидеть последствия какого-либо возможного действия (Малоун);

"качество" - закон должен иметь адекватные и эффективные заслоны возможным злоупотреблениям (Класс).

В частности, это означает, что закон должен указывать:

- список преступлений, совершение которых может привести к прослушиванию;

- ограничиваться случаями, когда фактические основания подозревать лицо в совершении тяжкого преступления уже выявлены другими средствами (Класс);

- санкционировать прослушивание только на основании мотивированного письменного заявления определенного высокого должностного лица (Класс);

- разрешать проведение прослушивания только после получения санкции органа или должностного лица, не принадлежащего к исполнительной власти, желательно, судьи (Класс);

- устанавливать ограничение на длительность прослушивания: должен быть указан период, в течение которого санкция на прослушивание действительна (Ювиг, Крюслен);

- определять правила, касающиеся отчетов, содержащих материалы перехваченных сообщений (Ювиг, Крюслен);

- предусматривать меры предосторожности против обмена этими материалами между различными государственными органами (Ювиг, Крюслен);

- определять обстоятельства, при которых записи можно или нужно уничтожить (Ювиг);

- устанавливать, что должно делать с копиями или переписанными материалами, если обвиняемое лицо будет оправдано (Ювиг).

"Как необходимый в демократическом обществе"

"только в такой мере, которая необходима для безопасности

демократических институтов" (Класс);

"при исключительных условиях, необходимых в демократическом обществе в интересах национальной безопасности и/или предупреждения беспорядков или преступления (Класс).

Определение корреспонденции

Телефонные разговоры подлежат защите согласно Конвенции как "корреспонденция" (Класс);

практика "хронометража" также подпадает под определение "корреспонденции" (Малоун).

Определение жертвы

Любое лицо в стране, где действуют положения о тайном прослушивании телефонов, может требовать признания себя жертвой без какой-либо обязанности давать доказательства или даже на основании голословного утверждения, что слежение действительно велось.

Перевод с английского Дарьи Рублинецкой

## Обзор законодательства одиннадцати европейских стран о прослушивании телефонных разговоров

## ВЕЛИКОБРИТАНИЯ[11]

Наличие в Великобритании королевской (т.е. государственной) монополии на доставку почты означало, что подозрительные письма или посылки могли безнаказанно вскрываться: существовал даже специальный чиновник, известный под именем "секретчика", чьей обязанностью было выявлять и вскрывать все способное угрожать государственной безопасности. Это полномочие никогда не имело законодательной основы; в чем его изначальные правовые источники, никогда не объяснялось. Впрочем, если бы кто-то настаивал, то государство могло бы оправдать эту практику ссылкой на известную британскому конституционному законодательству Королевскую Прерогативу: ту долю исполнительных полномочий, которую суды признают источником юридических норм и которая напоминает о днях, когда монарх осуществлял законы единолично. Защиту государства или национальной безопасности суды как раз и признают одной из таких неотменимых прерогатив.

Это обстоятельство весьма важно как с практической, так и с идеологической точки зрения. Практической - потому, что когда возникла телефонная связь, то сложившуюся практику почтовых перехватов просто перенесли на новую почву. С идеологической и символической - потому, что установки, на основании которых действовало государство, не претерпели изменений. Идее, что человек имеет право на тайну переговоров, придается мало значения; явное предпочтение оказано государственным интересам, которые поначалу ограничивались "безопасностью", а теперь включают и борьбу с преступностью.

Поскольку источником права на перехват сообщений была объявлена Королевская Прерогатива, то никогда не возникала и необходимость представить законное обоснование Парламенту или отчитаться перед ним и общественностью в том, как работает соответствующая система. Все делалось в тайне; например, хотя записи телефонных переговоров хранились во множестве, их ни разу не предавали огласке. Так

же точно не оглашались ни критерии выбора прослушиваемых переговоров, ни продолжительность перехвата.

Практика прослушиваний любопытна тем, что полученная здесь информация никогда не использовалась как доказательство против лиц, обвиняемых в уголовном преступлении. Информация использовалась, либо чтобы установить местонахождение объекта и помочь наблюдению за ним, либо как "подсказка", чтобы продвинуть расследование, например, тайно разместить полицейских в месте, в котором, как показало прослушивание, намечено совершить ограбление. В результате, суды не имели случая вынести основанный на законно полученных данных прослушивания приговор, ибо прямо ни одного из обвиняемых эта практика не затронула. Кроме того, поскольку английский закон не признает права на тайну переговоров, то не было и возможности жаловаться, что прослушивание нарушает какой-либо защищенный законом интерес, - даже если человек был в состоянии доказать самый факт прослушивания.

Хотя Европейская Конвенция по правам человека на время рассмотрения дела Малоуна не входила в собственное законодательство Соединенного Королевства (она вошла в него только в конце 1998 года), британское правительство неизменно считалось, пускай и в минимальной степени, с неприятными решениями Страсбургского Суда. После того, как Суд по правам человека нашел, что процедура, принятая в Великобритании, нарушает ст.8 Конвенции, Британский парламент в 1985 г. принял Акт о прослушивании переговоров (далее - Акт).

Поскольку Суд постановил, что старая процедура "не соответствовала закону", ибо она была основана не на актах парламента, а на ряде правительственных докладов, парламент решил ничего не менять по существу, а узаконить старую процедуру. Статья 1 Акта гласит, что перехват сообщения в ходе его передачи является незаконным за исключением тех случаев, когда один из участников разговора согласился на прослушивание или дан приказ о прослушивании Государственным Секретарем.

Ордер на прослушивание телефонных разговоров выдается Государственным Секретарем по запросам Министерства Внутренних Дел, Министерства Иностранных Дел и Дел Содружества и Министерств по управлению Шотландией и Северной Ирландией (раздел 1.2.a). Согласно статье 2, ордер может быть дан только "в интересах национальной безопасности, для охраны экономического благосостояния Соединенного Королевства, для предотвращения или расследования тяжких преступлений". Большинство ордеров выдаются именно на последнем основании, и почти всегда запрашивает его полиция. К первому и второму обычно обращаются различные службы безопасности и разведка. "Экономическое благосостояние", как правило, связывают с внешними угрозами жизненным интересам британской экономики. В качестве примеров можно упомянуть крупномасштабные валютные спекуляции, изъятие денег из банков или попытки повлиять на цену жизненно важного сырья, такого, как, например, нефть. Однако ордера такого рода ограничены сбором информации о действиях и лицах за пределами Соединенного Королевства: для получения информации внутри страны использовать их нельзя. "Национальная безопасность" в Акте не определяется, т.е. есть ли угроза национальной безопасности, определяет чиновник.

"Тяжкое преступление" (статья 10.3) определяется весьма широко. Сюда включается всякое правонарушение, которое "связано с применением насилия, приводит к существенному денежному урону, либо совершается большой группой лиц, руководствующихся общей целью". Последнее содержит чрезвычайно широкое, почти безграничное по объему понятие, которое в общем законодательстве известно как

"сообщничество". В дополнение к этому есть отдельная категория - любое правонарушение, за которое лицо старше 21 года, не привлекавшееся ранее к уголовной ответственности, должно быть приговорено к трем и более годам заключения. В последние годы сроки заключения в Англии заметно удлинились, и впервые совершившие правонарушение лица приговариваются к тюрьме за такие преступления, за которые еще десять лет назад был бы вынесен не связанный с лишением свободы приговор. Таким образом, эта категория существенно расширилась - а вместе с ней и перечень тех правонарушений и обстоятельств, при которых законом разрешается прослушивание.

Ордер может выдаваться только в тех случаях, когда "получение информации другим путем чрезмерно сложно". Определяя, необходимо ли прослушивание, министр должен решить, может ли данная информация "быть получена другими способами" (статья 2.3). Это условие гораздо менее жесткое, нежели применявшееся ранее: в "Белой книге" требовалось, чтобы прежде были применены и не дали результата иные методы расследования, либо они были заведомо бесполезны.

Согласно статье 2 "ордер должен указывать, какие именно сообщения подлежат перехвату и кому должны передаваться соответствующие материалы", а согласно статье 3 ордер выдается на прослушивание одного телефона "который, вероятно, используется определенным лицом или организацией". Это значит, что будут прослушаны разговоры гораздо большего числа людей, нежели то показывают статистические данные о числе выданных ордеров. Политическая, промышленная, религиозная (и, конечно, преступная) организация может быть так или иначе связана с большим количеством лиц. Все сделанные в данное место звонки будут записаны даже и тогда, когда эти люди лично не подпадают под условия Акта. И тысячи звонивших в данное место никогда не узнают, что их разговор подслушан - поскольку Акт не предусматривает рассекречивание записей спустя определенное время. Обычно срок действия ордера - 2 месяца, но он может многократно продлеваться на один месяц, а в некоторых случаях - даже на шесть (статья 4). В экстренных случаях ордер может быть выдан заместителем Государственного Секретаря на срок не более двух рабочих дней. Только Государственный Секретарь может продлить ордер (статья 4) или внести изменения в уже выданный ордер (статья 5). Кроме того, согласно статье 6, Государственный Секретарь отвечает за то, чтобы прослушивание "сводилось к минимуму, необходимому для раскрытия преступления, чтобы число лиц, которые знакомятся с материалами, объем копируемого материала и число копий было минимальным" (статья 6.2). Статья 6.3 предусматривает уничтожение всех копий, как только "в них отпала необходимость".

Следует отметить, что Акт затрагивает лишь прослушивание в "кабельной" телефонной сети. Этот акт намеренно не касается использования "жучков" и других форм электронного слежения и вмешательства в личную жизнь. Серьезно устарел он и после новых технологических достижений в телекоммуникации, появления беспроводных и сотовых телефонов. По мнению английских судей, эти средства коммуникации не подпадают под действие Акта. С другой стороны, в соответствии со статьей 9 продолжает действовать запрет на использование любых материалов, которые свидетельствовали бы о прослушивании телефонов. Поэтому информация, полученная с помощью "жучков" (например, запись разговора, сделанная скрытым в комнате устройством) или материалы, полученные прослушиванием беспроводных телефонов, в качестве улик использовать уже можно. Впрочем, хотя на первый взгляд сотовые сети не подпадают под действие Акта, Министерство внутренних дел сочло, что они составляют часть общей мобильной телефонной сети, и потому предписанные в Акте процедуры должны выполняться.

Вопрос об области применимости Акта находится в состоянии неопределенности. В 1997 г. Европейский Суд по правам человека, рассматривая иск Халфорда против Соединенного Королевства, постановил, что неспособность Акта регулировать перехват разговоров во внутренних телефонных сетях, - например, перехват работодателем разговоров подчиненного в офисной телефонной сети - является отступлением от статьи 8 Европейской Конвенции о правах человека. Найти на это юридический ответ правительству только предстоит.

Акт также предусматривает создание Трибунала, возглавляемого лицом, уполномоченным занимать пост судьи, и Комиссара по надзору за соответствием действий правительства Акту. Заданием Трибунала является рассмотрение жалоб от любых лиц, которые "полагают, что сообщения, направляемые к ним или от них, прослушиваются" (статья 7.2). Рассмотрев заявление, Трибунал должен информировать заявителя и Премьер-министра о результатах разбирательства. Трибунал имеет право прекратить любое прослушивание, если оно производится без ордера; отдать распоряжение об уничтожении перехваченной информации; и/или выдать денежную компенсацию заявителю, если признает это целесообразным (статьи 7.4 и 7.5). Однако в полномочия Трибунала входит только проверка выполнения условий выдачи ордера на прослушивание согласно Акту. Самое главное - несанкционированное и потому противозаконное прослушивание полицией и охранными агентствами - оставлено под надзором самой же полиции. Не удивительно, что полицейские и другие чиновники за такое правонарушение ни разу не преследовались. Трибунал не имеет также полномочий для расследования подобных случаев по запросу третьей стороны, которая сама не затронута соответствующим ордером. Поэтому, если установлено, что ордер был дан на прослушивание разговоров А, то жалоба со стороны Б, что его разговор с А прослушивался, Трибуналом рассмотрена не будет: непричастная и ни о чем не осведомленная третья сторона лишена какой-либо защиты. На усмотрение Трибунала оставлено только решать, правильно ли выписан санкционированный министром ордер. Поскольку ордера тщательно готовятся специальными гражданскими служащими, то Трибуналу, естественно, выпадает совсем немного работы. Хотя на работу системы прослушиваний за время ее существования поступило свыше 500 жалоб, ни одна из них не имела успеха. Больше того, Акт отказывает лицам, чья жалоба не удовлетворена, в праве обжаловать его решение в каком-либо суде (статья 7.6). Это один из немногих имеющихся ныне случаев, когда британское законодательство исключает обжалование.

Комиссар, с другой стороны, обязан рассматривать ордера, выданные Государственным Секретарем, а также помогать Трибуналу (статья 8). Акт наделяет Комиссара высшей властью в исполнении этих обязанностей. В отличие от Трибунала, который может лишь реагировать на чьи-то жалобы, Комиссар обладает правом сам инициировать расследование и (так же, как и Трибунал) имеет доступ ко всем секретным материалам. Однако это совместительская должность, и с момента учреждения ее последовательно занимали лица, одновременно служившие старшими судьями и работавшие практически в одиночку, беря несколько недель отпуска на судебной службе. Они в состоянии проследить лишь за частью, причем не обязательно репрезентативой, одобренных ордеров. Наконец, Комиссар должен представлять отчет Премьер-министру о каждом нарушении Акта, а также представлять ежегодный доклад парламенту, характеризующий деятельность правительства в рамках Акта за предыдущий год. Вместе с тем, материалы, разглашение которых премьер-министр сочтет вредным с точки зрения предотвращения преступлений, защиты экономического благополучия или национальной безопасности, из обнародуемой версии отчета могут изыматься. Не имея доступа к необходимым подробностям, Парламенту весьма трудно надзирать за работой системы перехватов. Комиссар осуществляет надзор не от имени Парламента: он принадлежит к органам

исполнительной, а не законодательной власти. Трибунал также назначается правительством. Поэтому объективность надзора с их стороны может быть поставлена под сомнение.

Еще более сомнительной является статья 9 об исключении улик. Эта статья гласит, что в любом судебном процессе (за исключением процесса, проводимого Трибуналом) "нельзя задавать никаких вопросов при перекрестном допросе свидетеля, из которых можно заключить, что ордер был выдан или должен быть выдан какой-либо стороне, участвующей в деле". Единственным исключением является случай, когда суд решает, что следует закрыть дело в связи с неправильно оформленным ордером. Таким образом, не только оба надзорных органа назначаются правительством и являются фактически его частью, но и даже в суде гражданам не разрешается задавать вопросы, которые могут раскрыть перехват правительством их корреспонденции. С точки зрения этих ограничений Трибунал сможет рассмотреть очень мало дел.

Представляется маловероятным, что текущая практика в Великобритании сможет пройти критическое рассмотрение Европейским Судом по правам человека. Действительно, в отличие от дела Малоуна, процедура основана уже на парламентском законе и, следовательно, имеет основу в национальном законодательстве. Следовательно, процедура доступна. Она относительно предсказуема, хотя термин "тяжкое преступление" не имеет четкого определения. Рассматриваемый Акт почти наверняка не удовлетворяет стандарту "качества закона", прежде всего потому, что главное требование Суда, - независимый надзор - в Акте не учтено. Рассмотрев дело Класса, Суд однозначно установил, что:

Поскольку индивидууму будут, несомненно, препятствовать в защите его прав, и он не будет допущен ни к каким судебным рассмотрениям, важно, чтобы в самой процедуре содержались адекватные гарантии прав индивидуума (Класс, 55).

Это замечание приобретает особую важность в Великобритании в свете статьи 9 Акта, ибо из него следует, что согласно британскому закону скрытое прослушивание телефонных разговоров гораздо легче осуществить, чем согласно германскому закону.

В деле Класса Суд выразил предпочтение судебному надзору перед правительственным. Это не имеет места ни в Германии, ни в Великобритании, тем не менее германский закон был признан Судом как не нарушающий Конвенцию. Конкретно Суд заявил:

Парламентская комиссия и Комиссия G-10 независимы от органов, осуществляющих наблюдение; они наделены достаточной властью и компетенцией, чтобы обеспечить эффективный и постоянный контроль. Кроме того, их демократический характер гарантируется сбалансированным членством парламентской комиссии. В ней представлена оппозиция и, следовательно, последняя может участвовать в надзоре над мерами, осуществляемыми Министром, который к тому же ответственен перед Бундестагом. Эти два надзорных органа могут в данном случае рассматриваться как достаточно независимые для ведения объективного надзора. (Класс, 56).

Этого нельзя сказать о Трибунале и Комиссаре в Объединенном Королевстве. Они назначаются правительством и не обязаны "отражать демократический характер" и представлять оппозицию. И никто из них не обязан рассматривать ордера в конкретных делах.

## ГЕРМАНИЯ[12]

Германия является единственной страной, действующие нормы которой о прослушивании телефонных разговоров были одобрены Европейским Судом по правам человека. Основные положения этих норм имеют конституционную природу. До введения Дополнения G-10[13] ст.10 Германского Основного Закона воспринималась как гарантия абсолютной неприкосновенности телефонных разговоров и почтовых отправлений. До 1968 г. Германские службы безопасности и органы криминального расследования не имели законных оснований для перехвата телефонных разговоров. Однако в связи с разгулом терроризма в середине 60-х годов Бундестаг принял решение дополнить Основной Закон и перечислить обстоятельства, при которых органы национальной безопасности и другие спецслужбы получили возможность перехватывать телефонные разговоры и почтовые отправления.

24 июня 1968 г. Бундестаг принял поправку к ст.10 Основного Закона, где, в частности, отмечается: "Право [на неприкосновенность] корреспонденции может быть ограничено на основании закона... Судебные иски [при применении секретных мер для защиты национальных интересов] должны заменяться рассмотрением дел в органах, назначенных парламентом". Результатом второй части Дополнения было создание Комитета G-10 - своеобразной высшей надзорной комиссии, единственной обязанностью которой было обеспечение соблюдения норм Конституции и соответствующего закона при тайном перехвате личных сообщений. В соответствии с требованиями этой поправки Бундестаг принял закон от 13 августа 1968 г. об ограничении конфиденциальности почтовых и электронных отправлений; этот закон описывает правила, которым должны следовать германские власти при установлении прослушивания телефонных разговоров и просмотра почтовых отправлений.

Закон начинается декларацией целей: "защитить от надвигающихся угроз свободу и демократический порядок, целостность и безопасность Федерации и составляющих ее земель" (ст.1.1). Ст.2.1 четко определяет, какие предполагаемые преступления оправдывают прослушивание телефонов. Перечислены следующие преступления:

1. Преступления против мира и государственная измена.

2. Подрыв демократического строя и законности.

3. Шпионаж или угроза международной безопасности.

4. Преступления против национальной обороноспособности.

5. Преступления против войск НАТО в Германии или войск трех союзных государств в Западном Берлине.

6. Преступления, учтенные в разделе 129a Уголовного Кодекса. (Убийство, геноцид, похищение людей с целью выкупа, захват заложников, уничтожение имущества путем поджога или взрывов в транспортных средствах и отравление).

7. Преступления, учтенные в разделе 92.1(8) Акта об Иностранцах. (Секретная организация и деятельность групп, состоящих в основном из иностранцев; имеется в виду деятельность, которая, будучи открытой, была бы запрещена).

Свидетельства, полученные посредством перехвата, "допустимы только в тех случаях, когда другие способы установления фактов невозможны или чрезмерно усложнены" (ст.2.2). Более того, ордер на перехват может быть выдан только по отношению к тем

лицам, которые, согласно установленным фактам, "получают или передают расследуемую информацию с целью выйти из-под подозрения" (ст.2.2). Ст.3 отмечает, что перехват информации также допустим в случае возможности вооруженного нападения на Германию. Однако, если вышеуказанное условие неприменимо, то собранные свидетельства не могут использоваться "во вред лицам, бывшим под наблюдением" (ст.3.2).

Процедуры, установленные законом от 1968 г. также очень точны. Перехват разрешен только после внесения запроса Федеральным Бюро по защите Конституции, властями Земель, ответственными за защиту Конституции, военной контрразведкой в делах, касающихся вооруженных сил, и Федеральной Информационной Службой в делах против нее. Закон гласит, что запрос должен быть внесен в письменной форме, объяснять причины, оправдывающие надзор и определять его длительность; этот запрос передается высшим властям Земель или министру, назначенному Канцлером. Более того, запрос должен "содержать доказательства того, что другими методами нужную информацию добыть невозможно или чрезмерно сложно" (ст.4.3). После подачи запроса власти Земель или Федеральный Министр могут выдать ордер, разрешающий прослушивание. Ордер выдается на срок не более трех месяцев, и в нем указывается имя лица, чьи разговоры разрешено прослушивать.

Главной гарантией надзора является создание Комитета G-10. Комитет, возглавляется лицом, имеющим право занимать судебные должности, и включает в себя двух экспертов. Члены Комитета назначаются парламентской комиссией, состоящей из пяти депутатов нижней палаты Парламента с обязательным представительством оппозиции. Важно также то, что Министр ежемесячно информирует Комитет обо всех разрешенных им ограничительных мерах до того, как их начинают применять. Комитет имеет право отменить приказ Министра, после чего перехват немедленно прекращается, если, по причине срочности, он был начат до получения разрешения. Наконец, граждане имеют право подать жалобу в Комитет, если они считают, что их разговоры прослушиваются незаконно. Решения Комитета не подлежат обжалованию в суде. Согласно статье 9 закона назначенный министр обязан раз в два года докладывать парламентской группе об общей ситуации с применением этого закона. Комитет G-10 имеет юрисдикцию над всеми частями разведки, а также полицией всех земель Германии.

После окончания прослушивания, согласно статье 5.5, "сторона, чей телефон прослушивался, должна быть уведомлена о факте прослушивания, если это не ставит под угрозу цель расследования". А ст.7.4 обязует уничтожать всю ненужную в дальнейшем документацию. Уничтожение документации должно быть подтверждено письменным актом.

Как упоминалось выше, Европейский Суд по правам человека признал, рассмотрев дело Класса, что немецкий закон удовлетворяет требованиям ст.8(2) Конвенции. Немецкий закон действительно имеет основу в национальном законодательстве, доступен и понятен, в том смысле, как этого требует Суд. Что касается качества закона, то в нем четко определены предполагаемые преступления, при которых разрешается прослушивание телефонных разговоров. Законоприменительная практика ограничена сбором вспомогательной информации о преступлении, когда уже известны другие факты или когда сбор информации иным образом невозможен или труден. Существуют четкие правила подачи письменного запроса на применение прослушивания, указана его максимальная продолжительность и четко описаны правила уничтожения тайно собранных материалов. Суд отметил, что ордер не выдается судебными инстанциями, но признал, что наличие надзора Комитета G-10 обеспечивает надежную замену судебного

контроля. Обзор прецедентов Суда относительно норм "качества закона" показывает, что недостает только мер предосторожности в отношении обмена собранной информацией между государственными органами и определения процедуры составления итоговых докладов касательно собранной информации. Однако эти требования к качеству закона были выработаны после рассмотрения дела Класса и к оценке немецкого закона отношения не имеют.

Наконец, как гласит ст.1 закона, всю процедуру можно применять только как "необходимую для демократического общества", и Суд определил в деле Класса, что это включает защиту демократических институтов и национальной безопасности.

## ФИНЛЯНДИЯ[14]

ПРЕДИСТОРИЯ ПРОБЛЕМЫ

В Финляндии традиционно считалось, что правомочия полиции восходят к правомочиям монарха. Главной обязанностью монарха считалось обеспечение общественного порядка и безопасности.

Требование об "охране общественного порядка и безопасности" долгое время, вплоть до начала 1970-х годов, принимались финской юриспруденцией как безусловная данность. Это требование вытекало из "природы государства", что, в свою очередь, вело к доктрине, позволявшей полиции при охране общественного порядка и безопасности прибегать ко всем необходимым мерам. Согласно такой доктрине, ни одно лицо не имеет прав, ограничивающих полномочия властей по охране общественного порядка и безопасности. Таким образом, законодательной основой для данных полиции полномочий стали главным образом постановления и обычное право.

В 1966 г. появился Акт о полиции (Poliisilaki /18.2. 1966/84/). Когда он готовился, ему придавали организационное значение, но постепенно юридическая реформа изменила первоначальные планы. Акцент переместился на полномочия полиции. Реформу стали рассматривать как "нечто такое, что поставило бы на первый план ответственность и юридические обязательства, которые несет полиция, применяя против граждан силу, и что, следовательно, гарантировало бы гражданам максимально возможную защиту от произвола" (Poliisih orgahisaatiokomitean, mietihto, Komiteanmietinto 1958:15 /Отчет Полицейского организационного комитета/ с.8). К тому времени, когда дела в области юридической реформы дошли до парламентских процедур, ее главный акцент уже делался на регулировании полномочий полиции. Принятие в 1966 г. Акта о полиции создало условия, чтобы финская юриспруденция сменила подходы к полномочиям полиции.

Впрочем, Акт о полиции был непоследовательным и содержал множество туманно сформулированных и дающих полиции широкие полномочия положений. Все полномочия, касающиеся слежки, наблюдения и получения информации о том или ином лице, как правило, отсутствовали в законодательстве. Все действия полиции в этих сферах основывались на так называемом обычном праве. В 1972 г. даже финский Парламент отметил отсутствие этих полномочий в парламентских документах по уголовному праву и положениях о слежке и прослушивании. Законодательный Комитет указал, что важно как можно скорее разработать эти полномочия в деталях. В 1980-х годах Государственный Совет создал специальный Парламентский Комитет по делам полиции, и тот представил подробный отчет. (Parlamentaarisen poliisikomitean mietinto,Komiteanmietinto 1986:16 /Отчет Парламентского Комитета по делам полиции/). За отправную точку Комитет принял, что функции и полномочия полиции должны оговариваться законом.

Полицейские власти увесистый отчет приняли не особенно благожелательно: он оказался слишком либеральным. В порядке противодействия специальная рабочая группа, состоявшая главным образом из полицейского начальства, составила собственный отчет относительно необходимых юридических реформ (Poliisilakituoruhman mietinto Komiteanmietinto 1989:25 / Отчет Рабочей группы по Акту о полиции/), однако последний ни к какой реформе прямо не вел. Изъян этого "контротчета" состоял в том, что почти все его составители принадлежали к полицейскому чиновничеству. По-видимому, они руководствовались своими узко понятыми профессиональными интересами. Как следствие, политическая воля провести на основе этих отчетов какую-либо юридическую реформу отсутствовала. В итоге в 1995 г. был принят новый Акт о полиции (Poliisilaki /493/95/), глава 3 которого регулирует сбор информации.

Кроме Акта о полиции сбор информации о лице предусмотрен Актом о принудительных мерах /402/95/, глава 5а которого регулирует перехват телекоммуникаций, установление сопутствующих звонку обстоятельств и слежку с помощью технических средств. Главное различие между мерами, которые предписывают эти Акты, состоит в их применении. Если имеет место так называемая "превентивная деятельность полиции", то сбор информации осуществляется в согласии с Актом о полиции. Полиция исполняет свою обязанность обеспечить правовой и общественный порядок или обеспечить порядок и безопасность. Чтобы применить меры, установленные Актом о принудительных мерах, глава 5а, должна быть "причина подозревать, что совершено преступление". Когда такая причина появляется, то относящиеся к сбору информации правила Акта о полиции уже неприменимы. Найти тонкую границу между превентивной деятельностью полиции и расследованием преступления отнюдь не просто.

## СБОР ИНФОРМАЦИИ О ЛИЦЕ СОГЛАСНО АКТУ О ПОЛИЦИИ

Статья 28 Акта о полиции определяет используемые в Акте понятия. "Технический контроль" означает визуальное или акустическое слежение за публикой, водителями транспортных средств или пешеходами, осуществляемое с помощью технического средства, а также автоматическую запись звука или образа. "Надзор" означает постоянный или многократный сбор информации об определенном лице или его действиях. "Технический надзор" - это постоянное или многократное прослушивание определенного лица с помощью технического средства и запись голоса (перехват), наблюдение и запись (техническое наблюдение) и надзор за транспортным средством (техническая слежка).

Согласно статье 29 Акта о полиции, полиция имеет право подвергнуть "техническому контролю" общественное место или общественную дорогу с целью поддержать общественный порядок и безопасность, предотвратить правонарушение, опознать лицо, подозреваемое в правонарушении, а также отследить определенные объекты, взятые под охрану. При этом полиция должна дать какое-то предупреждение о наличии технического контроля, например, посредством дорожного знака. Согласно статье 30 Акта о полиции, офицер полиции может установить "надзор" над отдельным лицом в месте ином, нежели его жилище, с целью предотвратить правонарушение в случае, если поведение этого лица или иные сведения дают основание подозревать, что это лицо совершит правонарушение. Надзор за пределами жилища может устанавливаться также над лицом, которое на разумных основаниях можно подозревать в сообщничестве преступлениям, максимальное наказание за которые превышает заключение сроком в шесть месяцев.

Полиция может установить "технический надзор" за пределами жилища над лицом или его транспортным средством в случае, если обоснованно предполагается, что полученная информация способна помочь в предотвращении преступления. При том же условии

технический надзор может устанавливаться над лицом, находящимся в гостиничном номере или в подобном помещении. Однако прослушивающее или наблюдающее устройство не должно располагаться в помещении или транспортном средстве, где находится объект наблюдения. Надзор допустим только тогда, когда из поведения лица или иных данных явствует, что это лицо может совершить правонарушение, максимальный срок наказания за которое составляет по крайней мере 4 года заключения, либо правонарушение, связанное с наркотиками. Техническое наблюдение и техническая слежка используются, если поведение лица или иные сведения показывают, что это лицо может совершить правонарушение, за которое положено максимальное наказание большее, чем шестимесячный срок заключения, либо это лицо является сообщником в таком правонарушении. Согласно статье 31 Акта о полиции технический надзор над лицом может быть установлен в пределах его жилища в следующих случаях:

1. Полиции необходимо провести те или иные мероприятия, и они будут эффективными только в случае надзора в пределах жилища (надзор тогда устанавливается непосредственно перед мероприятиями и во время их проведения);

2. Необходимо предотвратить опасность для жизни или здоровья лица, проводящего мероприятия, или лица, подвергающегося опасности и нуждающегося в защите.

Решение о техническом надзоре принимается старшим полицейским или полицейским, который назначен старшим следователем. Об этой мере необходимо немедленно уведомить старшего полицейского. Теоретически полицейский, принимающий решение о техническом надзоре, предписанном в пункте 1 статьи 31 Акта о полиции, должен сообщить об этой мере поднадзорному лицу. Однако если такое извещение способно повредить сбору информации или досудебному расследованию правонарушения, то извещения не требуется. Никакого извещения не требуется, если надзор или технический надзор устанавливается согласно пункту 3 статьи 31 Акта о полиции или на основании прежде полученной с помощью надзора информации. В принципе, весьма маловероятно, чтобы полиция известила лицо о мерах надзора, поскольку это будет "вредить сбору информации или досудебному расследованию правонарушения". Статья 34 подробно определяет, как можно воспользоваться собранной информацией. Статьи 35 и 36 регулируют получение информации от иных властей и частных организаций и лиц.

## СБОР ИНФОРМАЦИИ О ЛИЦЕ СОГЛАСНО АКТУ О ПРИНУДИТЕЛЬНЫХ МЕРАХ

Статья 1 главы 5 Акта о принудительных мерах определяет основные используемые в Акте понятия. "Перехват телекоммуникаций" означает тайный перехват или запись сообщений с целью выяснить их содержание. Эта мера применима для того, чтобы отследить сообщение, посланное или полученное с дальнего расстояния через телекоммуникационную сеть. Телекоммуникацией может быть телефонный звонок, пересылка данных и т.п., включая все виды электронной коммуникации. "Установлением сопутствующих звонку обстоятельств" является получение тайных идентификационных сведений о субъектах общения, которые были посланы или получены с помощью прибора, подключенного к телекоммуникационной сети, и временное отключение данного прибора. Идентификационные данные о субъектах общения - это такая информация, которая делает возможным идентификацию участвующих в телекоммуникации сторон. Такой информацией могут быть, например, сведения о местонахождении телекоммуникационных терминалов, о полном телефонном номере, о времени и месте коммуникации и ее продолжительности. "Технический надзор" означает тайный перехват или запись с помощью технических средств разговора или словесного сообщения, которые не предназначены для сведения посторонних лиц и в которых перехватчик не

принимает участия ("перехват"). Прослушивание является одной из форм технического надзора. Технический надзор может быть также установлен в форме постоянного или многократного фотографирования или тайного надзора за определенным лицом или местом, где, предположительно, подозреваемый будет что-то говорить, с помощью бинокля, камеры, видеокамеры или иного подобного средства ("техническое наблюдение"). "Техническая слежка" означает надзор за транспортным средством или имуществом с помощью радиопередатчика или иного подобного прибора.

Согласно статье 1а главы 7 Акта о принудительных мерах все перечисленные принудительные меры могут применяться, если только их применение может быть сочтено оправданным, с учетом того, насколько тяжко расследуемое преступление, насколько важно его расследовать и насколько нарушаются права подозреваемого либо других лиц. Это названо принципом пропорциональности.

Перехват телекоммуникаций допускается, когда есть основания подозревать кого-то в государственной измене, измене или убийстве, непредумышленном убийстве, взятии заложников, грабеже при отягчающих обстоятельствах, профессиональной скупке краденого, угоне самолета, диверсии против воздушного судна, фальшивомонетничестве при отягчающих обстоятельствах, преступлении, связанном с наркотиками, преступлении при отягчающих обстоятельствах, вымогательстве при отягчающих обстоятельствах или дурном влиянии при отягчающих обстоятельствах, либо в преступной попытке совершить названные правонарушения. В этих случаях проводящие досудебное расследование органы могут получить санкцию на перехват или запись сообщений, отправляемых подозреваемым с принадлежащего ему устройства, которое им предположительно используется, или же предназначенных для подозреваемого сообщений, приходящих к нему через это устройство. Необходимо, чтобы полученная благодаря такому перехвату информация предположительно имела чрезвычайную важность для расследования (Акт о принудительных мерах, глава 5а, статья 2).

Установление сопутствующих звонку обстоятельств допустимо, когда есть причины подозревать кого-то в правонарушении, за которое предписано наказание не менее четырех месяцев заключения, либо в правонарушении, совершенном через терминал против системы автоматической обработки информации, либо в правонарушении, связанном с наркотиками, либо в преступной попытке совершить вышеназванные правонарушения. В перечисленных случаях осуществляющие досудебное расследование органы могут получить санкцию снять информацию о сопутствующих звонку обстоятельствах с принадлежащего подозреваемому или предположительно используемого им коммуникационного устройства. Также возможно временно такого рода устройство отключить.

Необходимо, чтобы полученная благодаря идентификации или временному отключению информация предположительно имела исключительную важность для расследования. Если истец согласен, то проводящие досудебное расследование органы имеют право получать информацию через коммуникационный прибор, находящийся во владении истца или им используемый, чтобы раскрыть правонарушение, совершенное против системы автоматической обработки информации, которая соединена с общей телекоммуникационной сетью (Акт о принудительных мерах, глава 5а, статья 3).

Согласно статье 4 главы 5 Акта технический надзор возможен, если есть причины подозревать кого-то в правонарушении, максимальное наказание за которое - не менее четырех лет заключения, или в правонарушении, связанном с наркотиками, или в преступной попытке совершить названные правонарушения. Необходимо, чтобы

полученная информация предположительно имела исключительную важность для расследования. Техническое наблюдение допустимо, когда есть причины подозревать кого-то в правонарушении, максимальное наказание за которое - по крайней мере, шесть месяцев заключения. В этом случае также необходимо, чтобы полученная информация предположительно имела исключительную важность для расследования. Техническая слежка может быть применена к лицу, подозреваемому в правонарушении, связанном с наркотиками. Техническая слежка может быть обращена на используемое подозреваемым транспортное средство или на товары, с которыми связано правонарушение. Перехват или техническое наблюдение могут быть направлены на подозреваемого только тогда, когда он находится в общественном месте, в транспортном средстве, которое находится в общественном месте, или в гостиничном номере либо подобном помещении. Перехватывающее или наблюдающее устройство не должно быть расположено в помещении, где находится подозреваемый, или в используемом им транспортном средстве.

Для перехвата телекоммуникаций или установления сопутствующих звонку обстоятельств необходима санкция. Ее дает суд. Соответствующий запрос рассматривается судом безотлагательно и в присутствии подавшего его лица или определенного этим лицом служащего. Решение выносится без слушания подозреваемого или лица, владеющего коммуникационным прибором. Решение обжалованию не подлежит. В экстраординарных случаях решение может приниматься задним числом; делается это в предельно короткие сроки. Санкция на перехват телекоммуникаций и установление сопутствующих разговору обстоятельств может единовременно даваться не более, чем на один месяц. В санкции необходимо указать, к какому лицу и какому коммуникационному устройству применяется данная мера. Кроме того, суд, выдавая санкцию, имеет право наложить и другие условия и ограничения.

Решение о перехвате, наблюдении и технической слежке может приниматься Главным Следователем. Решение о перехвате должно быть в течение 24 часов доведено до сведения офицера полиции, возглавляющего Национальное Управление полиции, заместителя этого офицера, либо шефа Охранно-ревизионного управления, либо Следственного отдела Национальной таможенной коллегии, либо главы таможенного округа. Единовременно перехват может длиться не более одного месяца. В случае технического надзора санкция должна точно указывать подвергающиеся ему лица, места, а также транспортные средства и имущество. Кроме того, могут налагаться дополнительные условия и ограничения. Обо всех принудительных мерах, оговоренных в Акте о принудительных мерах, глава 5а, должен быть подан отчет.

В некоторых случаях перехват телекоммуникаций запрещен. Перехвату не могут подвергаться беседы подозреваемого с его адвокатом и беседы подозреваемого с его священником. Этот запрет абсолютен. Некоторые другие лица частично защищены от перехвата. Ближайшие родственники подозреваемого, его врач и фармацевт, акушерка, их помощники и лица, имеющие право на охрану своих информантов (т.е. журналисты) защищены от перехвата законом, кроме случаев, когда досудебное следствие подозревает правонарушение, за которое полагается наказание в виде заключения сроком на шесть лет или более суровое наказание, либо попытку совершить такое правонарушение или соучастие в нем. Если в процессе применения принудительных мер обнаружится, что имел место разговор с перечисленными выше лицами, то действия полиции прерываются и запись или заметки, если таковые есть, немедленно уничтожаются (Акт о принудительных мерах, глава 5а, статья 10).

Когда цель принудительных мер достигнута или истек срок выданной санкции, старший следователь должен прекратить использование принудительных мер. Сообщение об этом передается лицу, которое выдало санкцию, либо лицу, принявшему решение о таких мерах. Если дело передано на рассмотрение общественному прокурору или закрыто, то о принимавшихся принудительных мерах необходимо сообщить подозреваемому.

В случае, когда среди полученной благодаря перехвату информации имеются сведения, которые не имеют отношения к расследуемому правонарушению, то, даже если они имеют отношение к какому-то другому правонарушению, запись после ознакомления с ней уничтожается или эти сведения не включаются в отчет. Вместе с тем, если эти сведения затрагивают находящееся в расследовании правонарушение и если оно может расследоваться с применением принудительных мер того же типа, что и принятые, то запись может быть сохранена, а соответствующая информация внесена в картотеку организации, проводящей досудебное расследование. Если полученная информация необходима, чтобы предотвратить преступления, предусмотренные статьей 19 главы 16 Уголовного кодекса (в число этих преступлений входят государственная измена, убийство, непреднамеренное убийство, взятие заложников, грабеж при отягчающих обстоятельствах, профессиональная скупка краденого, угон самолета, диверсия против воздушного судна, фальшивомонетничество при отягчающих обстоятельствах, правонарушение, связанное с наркотиками, и совершенное при отягчающих обстоятельствах, вымогательство при отягчающих обстоятельствах, дурное влияние при отягчающих обстоятельствах либо преступная попытка совершить названные правонарушения), то запись также может быть сохранена, а информация включена в картотеку. Записи, которые не следует уничтожать, хранятся пять лет со дня, когда по делу было принято окончательное решение или дело было закрыто.

## ВОЗМОЖНОСТИ КОНТРОЛЯ

Министерство внутренних дел осуществляет надзор за принятием описанных в настоящем отчете принудительных мер. Ежегодно Министерство внутренних дел представляет Омбудсмену отчет о применении перехвата телекоммуникаций и установлении сопутствующих разговорам обстоятельств.

Омбудсмен осуществляет парламентский надзор над полицейскими процедурами. Он проводит инспектирование различных властей, включая полицию. Ежегодно Омбудсмен дает Парламенту отчет о своей деятельности. Следует отметить, что действия полиции в Финляндии нельзя обжаловать в суде. Лицо может подать административную жалобу, однако этот путь защиты своих прав считается не особенно эффективным. Другой альтернативой является обращение к Омбудсмену или к Канцлеру Юстиции. Применение такого метода, как превентивный надзор, контролируется исключительно полицией. Нет возможности предварительно проконтролировать принятие этой меры через суд, как это обстоит в случае с мерами, предписанными в Акте о принудительных мерах, глава 5а. Вследствие отсутствия отчетности и надзора, такого характера ситуация способна легко породить труднопреодолимые сложности.

## ПРАКТИКА

Согласно сведениям от Министерства внутренних дел, в 1995 г. полиция прибегала к перехвату только трижды. В качестве причины такого скупого обращения к этому методу назывался недостаток технических средств. Установление сопутствующих звонку обстоятельств осуществлялось 439 раз. Эти меры принимались преимущественно при расследовании тяжких преступлений, в частности правонарушений, связанных с

наркотиками, грабежей при отягчающих обстоятельствах, фальшивомонетничества при отягчающих обстоятельствах. Приблизительная продолжительность перехватов составляла от 15 до 31 дня. Установление сопутствующих звонкам обстоятельств длилось в среднем 94 дня и колебалось от одного часа до более чем пятисот дней. Эта мера, как правило, применялась к телекоммуникационному устройству в собственности подозреваемого. В трех случаях из четырех санкции выдавались на установление сопутствующих звонку обстоятельств применительно к мобильным телефонам (См. отчет Омбудсмена, 1996, с. 46.).

Те же меры, что описаны в настоящем отчете, могут применяться также Таможней и Министерством обороны. Согласно отчету Омбудсмена Парламенту, оба ведомства известили его, что в 1996 году к таким мерам не прибегали (см. Отчет Омбудсмена, 1996, с. 48).

Из той информации, какая доступна независимому исследователю, можно заключить, что главной областью, где используется установление сопутствующих звонку обстоятельств, является расследование преступлений, связанных с наркотиками. Заметное место занимают также случаи грабежа при отягчающих обстоятельствах и мошенничества при отягчающих обстоятельствах. После того, как установление сопутствующих звонку обстоятельств стало более распространенным, число наиболее тяжких насильственных преступлений уменьшилось. Использование перехвата по-настоящему только начнется, когда полиция достигнет достаточного уровня технической оснащенности. На основании скудных сведений нельзя предвидеть, каким образом полиция станет использовать эти возможности. Из-за недостатка сведений о данном предмете довольно трудно проследить за применением технического надзора. Полиция отчитывается о таких мероприятиях без особой охоты.

## ЗАКЛЮЧИТЕЛЬНЫЕ ЗАМЕЧАНИЯ

В целом с точки зрения правил Европейского Суда по правам человека положение в Финляндии, как нам представляется, вполне удовлетворительное. Процедура имеет основу в национальном законодательстве, доступна и понятна. Четко указан перечень преступлений, при которых разрешено применять перехват, сам этот перечень неширок. Существуют ясные правила получения ордера на прослушивание, при этом используется судебная процедура контроля. Указана максимальная продолжительность прослушивания, она сама по себе совсем невелика. Четко описаны правила уничтожения собранных материалов, предусмотрено извещение лица о том, что его телефон прослушивался. Независимый надзор за деятельностью полиции осуществляет Омбудсмен, который отчитывается перед Парламентом, сообщая при этом о количестве перехватов и тех преступлениях, при которых он осуществлялся. Некоторые проблемы с "качеством закона" связаны с Актом о полиции.

Определения в Акте о полиции очень расплывчаты, что может породить трудноразрешимые проблемы в связи с основными правами личности, а также с правильным исполнением закона. Особая сложность в том, что отсутствует определение сообщничества. Кроме того, согласно Акту о принудительных мерах, глава 5а, статья 10, на перехват сообщений наложены специфические ограничения, которые должны быть подробнее объяснены в дальнейшем. В своей превентивной деятельности полиция может нарушать ограничения, что, без сомнения, ведет к нежелательному нарушению права личности на частную жизнь.

Кроме того, применение технического надзора в большей мере, чем перехват и установление сопутствующих звонку обстоятельств, свободно от правового контроля. Решение о техническом надзоре принимается полицией, а не независимым судом. В результате эта мера по сути находится вне надежного правового контроля, что совершенно неприемлемо.

## ФРАНЦИЯ[15]

После того, как Европейский Суд по правам человека нашел, что французские нормы нарушают Конвенцию, французский парламент принял Закон №91-646 от 10 июля 1991 г. о неприкосновенности корреспонденции, передаваемой средствами телекоммуникаций. Закон начинается утверждением, что "неприкосновенность корреспонденции, передаваемой по телекоммуникациям, должна гарантироваться законом", за исключением случаев, упомянутых в ст.1 указанного закона. Затем закон описывает двухстороннюю систему установления прослушивания телефонных разговоров.

В разделе I сказано, что прослушивание телефонных разговоров ведется по указанию судебной власти в ходе криминального расследования. Эта процедура описана как дополнение к Книге 1 Уголовного Кодекса. Закон указывает, что только в криминальных расследованиях таких преступлений, по которым наказание состоит в тюремном заключении на срок два года и более, "судья, ответственный за расследование, имеет право, в случае необходимости, разрешить прослушивание и запись телекоммуникационных сообщений". Эта операция контролируется судьей или подчиненными ему офицерами судебной полиции. Решение судьи выносится в письменной форме и не подлежит обжалованию (ст.2.100). В его решении должна указываться конкретная линия, которая будет прослушиваться, вид предполагаемого преступления и максимальная длительность прослушивания, которая не может превышать четырех месяцев (ст.100-1 и 100-2). Дополнительные гарантии против злоупотреблений включают в себя требования записи разговоров на электронных носителях по минутам и хранение записей на бумаге в запечатанном виде. Судья, ведущий расследование, или подчиненные ему офицеры судебной полиции должны переписать необходимые для дела записи на бумагу, после чего электронные носители подлежат уничтожению (ст.100-5 и 100-6). Наконец, запрещено прослушивать телефоны в жилищах или служебных помещениях адвокатов, если об этом не будет извещен президент Ассоциации юристов Франции (ст.100-7).

В отличие от норм, действующих во время рассмотрения Европейским Судом дел Ювига и Крюслена, этот закон как будто удовлетворяет требованиям Суда. Прежняя процедура была признана Судом доступной и понятной, так что новая процедура тем более удовлетворяет этим требованиям. В делах Ювига и Крюслена Суд признал приемлемым во французском законе право судьи, ведущего расследование, принимать решения по выдаче ордеров на прослушивание телефонных разговоров, и эта практика действует и доныне. Новый закон, однако, исправил недостатки прежней процедуры. Ситуации, в которых разрешено прослушивание телефонных разговоров, определены, быть может, не так четко, как в немецком законе, но они "предсказуемы" (быть может, с помощью адвоката), что и требовалось в решении Суда. Ордер теперь должен включать данные о лице, над которым устанавливается наблюдение, и о преступлении, в котором лицо подозревается. Был введен и предельный срок прослушивания, равно как и уточнена процедура составления итогового доклада. Были предприняты меры для обеспечения секретности полученных материалов, указаны обстоятельства, при которых полученная информация уничтожается. Ясно, что эта сторона французской законоприменительной практики даже превосходит требования, установленные Судом.

В разделе II закона рассматривается перехват информации с целью обеспечения национальной безопасности. "В качестве исключения", гласит начало ст.3, телекоммуникации могут прослушиваться:

в целях сбора информации, имеющей ценность для национальной безопасности, информационной защиты научного и экономического потенциала Франции, для предотвращения терроризма, организованной преступности и правонарушений, а также создания и деятельности… частной милиции и групп боевиков.

При таких обстоятельствах министр обороны, министр внутренних дел и министр таможенной службы должны обратиться к Премьер-министру с письменным запросом, содержащим основания для прослушивания. Только Премьер-министр или два его специально назначенных помощника могут разрешить прослушивание телефонных разговоров, причем это разрешение должно выдаваться в письменной форме и содержать основания для прослушивания (ст.4). С тем, чтобы оградить этот процесс от возможных злоупотреблений, на действия Премьер-министра налагается ряд ограничений. Во-первых, Премьер-министр обязан ежегодно планировать "максимальное число одновременных прослушиваний и разделить это число на квоты для отдельных министров" (ст.5). Он может разрешить прослушивание телефонных разговоров только на срок до четырех месяцев (ст.6). На бумагу информация может переноситься только в случаях, относящихся к угрозе национальной безопасности, перечисленных в ст.3 (ст.7). Записи на электронном носителе должны уничтожаться в течение шести дней, после того, как была произведена запись (ст.9). И, наконец, записи на бумаге "должны быть уничтожены после того, как в них уже нет необходимости" (ст.12).

Более того, закон требует организовать Комиссию по контролю за телефонным прослушиванием в интересах национальной безопасности(ст.13). Подобно Комитету G-10 в Германии, Комиссия является независимым административным органом, возглавляемым лицом, которое назначается Президентом из списка кандидатов, составленного вице-президентом и председателем Верховного Суда. Один заместитель главы Комиссии назначается Президентом Национальной Ассамблеи, а другой - Президентом Сената. Членам правительства запрещено присутствовать на заседаниях Комиссии. Согласно ст.14 этого закона, председатель Комиссии должен быть извещен Премьер-министром за 48 часов до начала прослушивания в интересах национальной безопасности, как было объяснено выше. В случае, если председатель сомневается в законности постановления Премьер-министра, он собирает Комиссию, которая имеет право отменить распоряжение и прекратить прослушивание. Всегда, когда Комиссия (по собственному решению или по жалобе лица, чьи разговоры прослушиваются) полагает, что прослушивание противоречит закону, она должна безотлагательно информировать об этом прокурора (ст.17). Наконец, Комиссия должна публиковать ежегодный доклад о деятельности Премьер-министра в таких делах в течение предыдущего года.

Хотя процедура расследования уголовных преступлений с помощью прослушивания телефонных разговоров, несомненно, соответствует требованиям Суда по правам человека, нормы, связанные с прослушиванием в интересах национальной безопасности, пожалуй, не удовлетворяют этим требованиям. Действительно, прослушивание производится на основании национального закона, доступного и понятного. Дан исчерпывающий перечень преступлений, при которых оно разрешено; установлена максимальная длительность прослушивания; описаны правила составления итоговых отчетов, обмена информацией между органами власти, а также уничтожения записей. И, хотя решение о прослушивании телефонных разговоров принимает орган исполнительной власти, существование независимой Комиссии по надзору, состоящей из членов обеих

палат парламента, и возглавляемой лицом, выбранным из списка, который составлен с участием главы Верховного Суда, является адекватной заменой судебного надзора, как и Комиссия G-10. Проблема связана со ст.3, которая гласит, что "телекоммуникации могут прослушиваться в целях поиска информации". Использование термина "поиск информации", в сочетании с тем фактом, что нет запрета на предварительное пробное прослушивание или указания, что сначала, если возможно, должны применяться другие методы сбора информации, является слабым местом закона. В деле Класса Суд ясно указал, что прослушивание телефонных разговоров разрешается только "если установление фактов иным способом невозможно или чрезмерно сложно". Дополнение G-10 было расценено как адекватная гарантия от злоупотреблений прежде всего потому, что "так называемое пробное или общее наблюдение не разрешается" (Класс, 51). Нельзя быть уверенным, что это условие соблюдается во французском законе.

## ШВЕЙЦАРИЯ[16]

Регулирование прослушивания телефонных разговоров в Швейцарии весьма своеобразно, как и все в этой необычной стране. До середины 60-х годов полиция или ведущий дело суд могли дать указание о прослушивании телефонных разговоров и не подвергаться никакому последующему контролю. В 1965 г. Национальный Канцлер Губер впервые потребовал сузить круг органов, которые имеют право дать указание о перехвате телефонных разговоров. Он предложил создать институт, который бы "предметно рассматривал" дела и гарантировал законность и оправданность перехватов. В 1970-х годах вопросом о прослушивании телефонов занимался в парламенте главным образом Национальный Канцлер социал-демократ Андрес Гервиг. После сомнительных прослушиваний, объектом которых стал его коллега в парламенте, председатель социал-демократической партии Губахер, Гервиг потребовал обеспечить более надежную защиту для членов парламента. В 1973 г. он выступил с новой парламентской инициативой: перехват почты и телекоммуникаций и использование электронных средств надзора должны были допускаться при расследовании лишь немногих оговоренных правонарушений; должен был вводиться независимый судебный контроль; предлагалось создать парламентскую контрольную комиссию, имеющую доступ ко всем необходимым досье.

Федеральный прокурор категорически возражал против этих требований. Он заявил, что контроль постороннего судьи помешает прокурору действовать оперативно. Парламентский контроль поставит под вопрос соблюдение секретности. Кроме того, доступ парламентской комиссии к полицейским каталогам помешает федеральному прокурору и федеральной полиции вести превентивный надзор в случаях, связанных с государственной безопасностью.

Правое большинство парламента поддержало федерального прокурора и отказало ввести парламентский контроль, равно как и строгий перечень преступлений, допускающих перехват. Поддержано было только требование Гервига и левого меньшинства о судебном контроле. В итоге после длительных парламентских дебатов (см. Kreis, Georg (ed.): Staatsschutz in der Schweiz. Die Entwicklung von 1935 - 1990, Berne (Haupt) 1993, pp. 548 ss.) в 1979 году были приняты законы о надзоре за телекоммуникациями, действующие и сегодня. Их сердцевину составляет статья 179 Уголовного кодекса, "официальные меры надзора". Хотя вообще вторжение в тайну почтовых и телекоммуникационных отправлений считается правонарушением, однако, эта новая статья предусматривает исключения. Нарушение тайны почтовых и телекоммуникационных сообщений не подвергается преследованию, если оно осуществлено при исполнении законных полномочий и если обладающий соответствующим правом судья дал на это разрешение.

Требования к такому надзору и порядок его применения должны были определяться в соответствующих криминально-процессуальных документах:

- федеральном криминально-процессуальном кодексе - для случаев, которые подлежат федеральной юрисдикции. Это, например, большинство государственных преступлений, торговля оружием и взрывчатыми веществами, боеприпасами, подделка денег. Контрабанда и сбыт наркотиков подпадают под юрисдикцию кантонов, но сложные случаи, когда провоз наркотиков осуществлялся из кантона в кантон, либо они попали в страну из-за границы, расследуются федеральным прокурором;

- военном криминальном процессуальном кодексе - для случаев, подпадающих под военный уголовный кодекс и расследующихся органами военной юстиции;

- криминальных процессуальных кодексах 26-ти кантонов - для всех остальных правонарушений.

Разрешение на прослушивание телефонных разговоров может быть дано, когда, во-первых, совершено тяжкое преступление или необходимо его предотвратить, и, во-вторых, когда без перехвата телефонных сообщений расследование натолкнется на серьезные трудности либо иные меры расследования оказались безуспешными.

Уголовный кодекс определяет обычные преступления как такие правонарушения, которые наказываются штрафом, тогда как тяжкие преступления караются тюремным заключением. Телефонный надзор допустим при расследовании 183 преступлений, которые перечисляются в Уголовном кодексе. Сюда же добавляются тяжкие преступления, указанные в законе о наркотиках, законе об оружии и т.д.

Согласно Федеральному криминальному процессуальному кодексу, являющемуся основой для военного и 26-ти кантональных процессуальных кодексов, перехват применяется против лица, подозреваемого в совершении правонарушения или участии в нем. Телефоны третьих лиц могут прослушиваться, если "имеется обоснованное подозрение, что подозреваемый может этим телефоном воспользоваться", либо что это третье лицо станет передавать подозреваемому информацию или получать информацию от него.

Важнейшим результатом нововведений 1979 года стало то, что юридический контроль начал осуществляться через разделение полномочий между властями, принимающими решение о перехвате, и властями, его санкционирующими. Указание о перехвате дается прокурором либо ведущим данное дело судьей. На федеральном уровне большая часть указаний дается федеральным прокурором. Федеральным главным судьей ордер дается только в случаях, когда расследование уже официально открыто. Разрешение на перехват должно даваться председателем федеральной или кантональной обвинительной палаты, либо, если данный кантон не имеет такой палаты, другим высокопоставленным судьей, которому специально даны такие полномочия. Правонарушения против военного уголовного кодекса рассматриваются соответствующими органами военной юстиции, где имеется такое же разделение полномочий. Разрешение на перехват дается на шесть месяцев, но может быть продлено давшим его судьей.

В 1983 году Федеральный Суд принял решение о последующем обязательном извещении поднадзорного лица о том, что его телефон прослушивался, для кантональных дел. Федеральный прокурор ввел в практику последующее извещение поднадзорного лица и для остальных дел.

На практике большая часть перехватов осуществлялась специальным подразделением национальной телефонной компании ("Телекома"), которое записывало разговоры, проводило первичный отсев важной информации и передавало записи либо стенограммы полиции либо предписавшему перехват судье. Долгое время такая мера оставалась исключительной, однако, в последние пять лет прямой перехват применяется, по-видимому, чаще.

С тех пор, как в 1997 г. "Телеком" был приватизирован (новое название - "Швейцком") и возникли другие частные телекоммуникационные компании, была создана новая федеральная служба перехвата телекоммуникацией. Она выполняет те же функции, что и прежняя специальная служба "Телекома", и поддерживает тесные связи с различными телефонными компаниями, которые должны гарантировать, что их линии и системы мобильной связи открыты для надзора со стороны полиции. Новая система пока основывается только на правительственном постановлении.[17] Новый закон о почтовом и телефонном надзоре, проект которого разрабатывался и обсуждался с конца 1989 г., даст ей настоящую законодательную основу.

Реформа законов о надзоре над телекоммуникациями является результатом процесса модернизации законодательства, который охватывает весь аппарат полиции и уголовной юстиции. Этот процесс был инициирован так называемым "каталожным скандалом". В ноябре 1989 г. опубликовала свой отчет чрезвычайная парламентская следственная комиссия Федерального Департамента юстиции и полиции.[18] Обнаружилось, что на тот момент Федеральная полиция (т.е. политическая полиция) вела досье приблизительно на 900 000 лиц и организаций, многие из которых десятилетиями находились под надзором только потому, что вели деятельность в левых политических организациях, профсоюзах или оппозиционных общественных организациях. Отчет этой комиссии вызвал широкий общественный протест: люди требовали права доступа к своему досье и упразднения политической полиции. Хотя под давлением общественности правительство волей-неволей открыло ограниченный и контролируемый доступ к досье, по мере затухания протестов его политика становилась все консервативнее и жестче.

Парламентская следственная комиссия была создана в связи с делом Ганса В.Коппа, цюрихского адвоката. Его жена Элизабет Копп, министр юстиции Швейцарии, вынуждена была в 1989 г. уйти в отставку, потому что она предупредила мужа о предстоящем расследовании отмывки денег, которую проводила корпорация Шакарчи Трейдинг. Ганс Копп состоял одним из членов административного совета этой компании. Указание прослушивать телефон Ганса Коппа было дано, чтобы расследовать предполагаемое разглашение служебной тайны. Подозревался неизвестный служащий федеральной администрации, а Коппа считали просто третьим лицом. По решению суда само подозрение было достаточным основанием, чтобы дать указание о надзоре. Поскольку же Копп как адвокат был носителем профессиональных тайн, то вся имеющая к ним отношение информация должна была рассматриваться под контролем магистрата, а не специальной службы телекоммуникационной сети. Копп пытался обжаловать действия администрации, но безуспешно. Тогда он обратился в Европейский Суд по правам человека. Весной 1998 г. Суд вынес решение в пользу Коппа. Хотя парламентский контроль правомерности и обоснованности перехвата телефонных разговоров законом не предусмотрен, парламент в некоторой степени осуществляет такой контроль путем создания специальных комиссий. Несмотря на то, что чрезвычайная парламентская следственная комиссия выявила неожиданно большое число случаев наблюдения, ее выводы были достаточно дружелюбными.[19] Число выданных в 1980-е годы ордеров было признано "сравнительно небольшим": от 40 до 80 ордеров в год. "Такие цифры показывают, что законные полномочия использовались с большой осторожностью. Во

всех случаях выполнены строгие юридические формальности". В то же время, комиссия обнаружила, что последующее извещение лица, ордер на прослушивание которого был выдан, имело место только в 10% случаев.

В ноябре 1992 года постоянная Комиссия по административному контролю при Национальном Совете заявила, что процедура выдачи разрешений не обеспечивает реального контроля правомерности и обоснованности выдаваемых ордеров на перехват.[20] Выдавая санкции, председатель федеральной обвинительной палаты пользовался простым готовым формуляром. Не было ни обоснований, ни простого пояснения причин. С тех пор, как был введен судебный контроль, ни один исходящий от федерального прокурора ордер на прослушивание не оказался отклоненным. Уже в 1991 году Следственная комиссия по делам государственной безопасности при местном парламенте Цюриха[21] сделала примерно такие же выводы, когда рассматривала так называемое "дело о взрывах". В весьма многочисленных случаях расследование так и не было официально завершено - ни передачей дела в суд, ни составлением официального акта. Председатель обвинительной палаты продлевал разрешение на перехват разговоров подозреваемого в течение нескольких лет, но ни перехват, ни другие следственные меры не принесли никакого результата, который позволил бы подкрепить обвинение. Таким образом, судебный контроль формально осуществлялся, но фактически его не было. Так же обстоит дело, видимо, и по сей день. В ноябре 1996 г. в журнале "Фэктс" был напечатан закрытый правительственный отчет о защите общественной безопасности. Федеральный прокурор возбудил расследование по делу о разглашении служебной тайны. Подозревался в этом деле неизвестный работник федеральной администрации, а журнал и его редакция фигурировали как третья сторона. Спустя всего полгода и несмотря на ограниченное количество выдаваемых на прослушивание ордеров, председатель обвинительной палаты не мог вспомнить, подписывал ли он ордер на прослушивание телефонов и перехват факсимильных сообщений журнальной редакции или на прослушивание телефонов, принадлежащих отдельным журналистам.

Уголовное законодательство и процессуальный кодекс определяют перехват почты и телефонных переговоров как меры, принимаемые с целью расследовать преступные действия либо предотвратить правонарушения, которые иначе были бы совершены в ближайшем будущем. Однако большая продолжительность перехватов и регулярное возобновление ордеров свидетельствуют об ином: меры надзора, юридически обоснованные интересами следствия, оказываются средством постоянной упреждающей слежки. Даже парламентская следственная комиссия Федерального Департамента юстиции и полиции, нарисовавшая столь дружелюбную картинку проводимого федеральным прокурором телефонного надзора, указала на чрезвычайную длительность прослушиваний. В отчете комиссии цитируется записка заместителя федеральной полиции: "По данным нашего расследования, X ведет себя странно, что, вероятно, должно подкрепить наши подозрения, но не дает и едва ли даст достаточные улики для обвинения. Тем не менее, есть опасность, что в любой момент он совершит преступление... Таким образом, мотивировка мер, которые к нему применяются, за многие годы сильно изменилась, превращаясь в соображения превентивного надзора. Сегодня телефонное прослушивание лишь во вторую очередь служит раскрытию уголовных преступлений; первая его функция состоит в предотвращении преступлений и выяснении, с какими третьими лицами вступает в контакты поднадзорное лицо".[22]

Надзор за господином X, длившийся более полутора лет, комиссия рассматривала как одно изолированное дело. Однако особый комиссар по делам о рассекречивании "старых" картотек государственной безопасности в своем итоговом отчете (май 1996 года) говорит о 200 длительных перехватах, когда интересами следствия только прикрывалась

опережающая деятельность по обеспечению государственной безопасности. Ни один из этих перехватов не послужил поимке предполагаемого террориста или предотвращению какого бы то ни было правонарушения.[23]

Согласно отчету Комиссии по административному контролю, причины такого лицемерия государственной безопасности кроются в самом тексте соответствующих законов. Их статьи формулируются чрезвычайно широко и предусматривают не только реальное совершение преступлений, но и подготовительные действия.[24] При этом многие преступления связаны с воззрениями людей, их политическими взглядами, а не с активными действиями. Подобным же образом, статья о преступных организациях предусматривает не только конкретную преступную деятельность (будь это убийство, поджог, рэкет, торговля наркотиками или что-то иное), но и предполагаемое участие в такой организации или ее поддержку. Расследование, включающее надзор за телефонными переговорами, может начаться задолго до реальной преступной деятельности и даже до ее подготовки. Таким образом, следственные действия автоматически оказываются опережающими. Что касается расследования дел, связанных с наркотиками, то такой опережающий характер расследования был осознан еще до введения соответствующей статьи в 1994 году.

В своем отчете за 1992 год Комиссия по административному контролю заявила, что телефонный надзор оказался не очень эффективным для сбора улик, зато породил множество новых подозрений и дал сведения относительно преступной сети.[25] Этому опережающему характеру телефонного перехвата отвечают и новые технические средства. Полицию все меньше и меньше интересует передаваемая по телефону и факсу информация и все больше - вступающие в коммуникацию личности. Во все возрастающем числе случаев санкционируется прямой надзор со стороны полиции, без участия специальной службы "Телекома", даже в случаях, когда интересующие полицию люди говорят на иностранном языке.

В отчете Комиссии по административному контролю описывается также практика определения телефонных номеров.[26] Во многом она является результатом расширения телефонной системы. Для того, чтобы представить абоненту подробный счет, телефонные компании по шесть месяцев хранят номера телефонов, куда и откуда звонили, и сведения о продолжительности разговоров. Конфискуя эту информацию, полиция или ведущий дело судья получают почти полное представление о личных связях подозреваемого и не тратят на это ни времени, ни средств.

Если поднадзорное лицо пользуется мобильным телефоном, то телефонная компания также регистрирует, через какую релейную станцию прошел звонок. Поскольку в городской зоне каждая релейная станция нормально обслуживает несколько сотен квадратных метров, то эти данные позволяют также отследить передвижение поднадзорного лица.[27]

Сколько же осуществляется перехватов? Вообще говоря, правительство публикует статистические данные о телефонном надзоре лишь тогда, когда его вынудит это сделать парламент. Систематическая статистика отсутствует. Информация, собранная из разных источников дает основания утверждать, что в 70-е годы происходил постоянный рост количества выданных ордеров (в 1978 году было выдано 104 ордера), а затем эта цифра начала снижаться. Если в 80-е годы федеральный прокурор выдавал в среднем 65 ордеров в год, то в 90-е годы эта цифра снизилась до примерно 50 ордеров в год. В то же время на кантональном уровне число ордеров постепенно увеличивалось с 403 в 1988 г. до 1020 в 1996 г. При этом количество ордеров нельзя путать с количеством прослушивавшихся

телефонов или количеством затронутых надзором лиц. Так, например, Мартин Келлер, высокопоставленный чиновник министерства юстиции, полагает, что один выданный ордер соответствует в среднем двум или трем телефонным номерам или номерам факсов. Количество затронутых надзором лиц обычно значительно больше, ибо ордер может санкционировать надзор за телефоном общественного пользования. В некоторых кантонах определение телефонных номеров, которые были на связи с интересующим телефонным номером, также считается вмешательством в тайну личных коммуникаций, и потому для его осуществления требуется ордер и разрешение. В таких кантонах эта мера включается в статистику. Однако в других кантонах такая практика рассматривается как "нормальная конфискация" и отчета о ней не дают. Не предоставляется и информация и о типе прослушиваемых телефонов, количестве прямых перехватов, перехватов, объектами которых являются носители профессиональных тайн (врачи, священники, адвокаты), продолжительности надзора, его результатах, их использовании в суде и обоснованных с их помощью приговоров.

До 80-х годов применение телефонного надзора контролировалось федеральным прокурором и федеральной полицией. Применялся такой надзор преимущественно в области предполагаемых политических преступлений и в борьбе со шпионажем. Среди выданных между январем 1971 г. и мартом 1974 г. 376 ордеров только 22 касались неполитических правонарушений (все - подделки денег). Поэтому рост числа ордеров во второй половине 70-х годов оправдывали предполагаемым ростом шпионской активности.

Кантональные власти начали проявлять растущий интерес к такому инструменту, как перехват сообщений, начиная с середины семидесятых годов. Однако с конца 80-х число выдаваемых кантональными судьями ордеров на телефонный надзор - из-за возросшего числа расследований по делам о торговле наркотиками - стало расти катастрофически.

Одновременно с этим ростом статистики на кантональном уровне, число ордеров, даваемых федеральным прокурором, в связи с постепенным затуханием холодной войны стало уменьшаться. В результате разрядки напряженности и особенно распада социалистического лагеря в конце 80-х годов пошли на спад как разведывательная активность, так и гонения на коммунистов и подозреваемых в коммунистических настроениях людей. Что же касается 80-х годов, то здесь надо вспомнить, что федеральный прокурор использовал свои полномочия в области политических дел и "сложных" дел, связанных с наркотиками, и предписанные им меры надзора были чрезвычайно продолжительными.

Хотя пока нет еще полных обзоров того, какова статистика ордеров для каждого отдельного типа преступлений, можно полагать, что сегодня 80% ордеров выдаются по поводу преступлений, связанных с наркотиками. В этой области такая исключительная мера, как перехват разговоров, стала обычной. Прослушивают телефоны и для расследования других случаев, зачастую скандальных или попросту абсурдных. К примеру, в 1996 и 1997 годах федеральный прокурор дал указание прослушивать телефоны ряда газет и их редакционных работников. Из кантонов сообщают и об анекдотических случаях: например, в 1995 г. ведущий судья кантона Берн дал разрешение прослушивать телефон людей, чей восемнадцатилетний сын подозревался в рисовании граффити.[28]

Каковы же перспективы швейцарского законодательства в Европейском Суде по правам человека? Процедура имеет основу в национальном законодательстве, она доступна и предсказуема. Однако она не удовлетворяет стандарту "качества закона", ибо главное требование Суда - независимый надзор - ею не предусмотрен. Кроме того, возможность и

широкое использование предварительного прослушивания считается недопустимым с точки зрения Суда. В деле Класса Суд четко сформулировал, что "так называемое пробное или общее наблюдение не разрешается" (Класс, 51). Поэтому, несмотря на относительную открытость процедуры прослушивания телефонных разговоров (последующее уведомление лица о том, что телефон прослушивался, публикация данных о количестве прослушиваний и т.д.), представляется маловероятным, что швейцарское законодательство и практика будут одобрены Судом. Решение Суда по делу Коппа подтверждает этот вывод.

## ШВЕЦИЯ[29]

Согласно п.6 главы 2 Конституции Швеции все шведские граждане защищены от следующих действий публичной власти: насильственного физического воздействия, личного досмотра, досмотра домовладений и квартир и прочих подобных вмешательств, а также от перехвата разговоров и надзора за телефонными разговорами и любыми другими конфиденциальными сообщениями. Соответственно, полиции и другим властям, расследующим преступление, также запрещено проникать в какое-либо закрытое место с целью разместить или изъять оборудование, необходимое для надзора, например, "жучков" или скрытую камеру. Согласно п.12 главы 2 эта конституционная защита может быть ограничена законом, при этом подчеркивается, что такое ограничение может вводиться лишь постольку, поскольку оно необходимо в демократическом обществе. Конкретно это значит, что такое ограничение никогда не может быть более продолжительным, чем это необходимо для достижения цели, ради которой применен принудительный метод, и, что самое важное, не может быть настолько строгим, чтобы это угрожало свободе дискурса как фундаменту существующей демократии. Прямо говорится, что никакие законы, позволяющие применение принудительных мер, не могут навязываться из одних только политических, религиозных, культурных и других подобных мотивов.

Нормами шведского законодательства, которые разрешают перехват разговоров и надзор за телефонами, являются глава 27, п.п. 18-25 Судебного процессуального кодекса (1942, далее СПК) и Закон 1952:98, где содержатся некоторые правила относительно принудительных мер. Последний первоначально замышлялся как временный акт, сроком действия в один год, однако его действие каждый год продлевалось, и он действует до нынешнего времени. Пользуется этим законом преимущественно - если не исключительно - Полиция Безопасности.

В Швеции делается различие между телефонным прослушиванием и телефонным надзором. Тайное прослушивание телефонов регулируется п.18 главы 27 СПК. Оно определяется как тайный перехват или/и запись с помощью каких-либо технических средств разговора между двумя или более лицами, ведущими беседу по телефону. Тайный телефонный надзор определяется как воспрепятствование использованию телефона или тайное получение сведений, сколько сообщений, когда и какого содержания были переданы с одного или более телефонного номера или на этот номер (эти номера) приняты.

Санкционировать тайное прослушивание (тайный телефонный надзор) может только суд, и только прокурор может подать просьбу о выдаче санкции (глава 27 п.21 СПК, первый абзац). Согласно СПК прокурор не имеет права давать предварительный ордер. Соответствующее решение имеет четко обозначенный срок действия и не должно разрешать прослушивание или надзор продолжительностью более одного месяца единовременно (тот же пункт, абзац второй). Мотивировкой этого правила является то,

что редко бывают причины подтверждать принятое решение чаще, чем раз в месяц, и если установить более короткие сроки, то принятие таких решений будет проводиться рутинным образом, без детального рассмотрения (Предложение 1988/89:124, с.54 и далее; Предложение 1995/96:85, с.33). Теоретически такое решение может быть обжаловано, однако, на практике воспользоваться этой возможностью может только прокурор, поскольку у поднадзорного лица нет общественного защитника. Даже после того, как надзор закончится, поднадзорное лицо не имеет права узнать, что оно подвергалось телефонному прослушиванию или телефонному надзору.

В судебном разрешении должен быть точно указан один или более телефонный номер (либо адрес). Решение о прослушивании должно касаться только телефона, с которого подозреваемый может делать звонки, но не телефонов людей, которым он может звонить.

Прослушивание телефона, предпринятое на основании СПК, может использоваться только в превентивной деятельности по предотвращению преступлений (или попытки совершить их, их подготовки или сообщничества), наказание за которые превышает два года тюрьмы. Вместе с тем, тайный телефонный надзор применим, если наказание превышает шесть месяцев тюрьмы. В обоих случаях заявка на санкцию удовлетворяется, если только есть весомые основания для подозрения в совершении или подготовке преступления, и при этом соблюдается принцип пропорциональности. Это значит, что тайное прослушивание телефона или телефонный надзор могут применяться только тогда, когда искомый результат не может быть достигнут иными разумными способами.

Телефонные компании обязаны исполнять решение о прослушивании или телефонном надзоре, а также обязаны создавать свои технические системы таким образом, какой позволял бы использовать эти виды принудительных мер (п.14a, Telelagen 1993:597). Служащие таких компаний обязаны соблюдать секретность. (п.25, Telelagen 1993:597).

Закон 1952:98, специально регулирующий принудительные меры, возник как результат судебного дела о шпионаже. Поэтому он используется - по-видимому, исключительно, - Полицией безопасности. Этот Закон предоставляет широкие полномочия в области тайного надзора и других принудительных мер. Согласно Закону (п.5, абзац второй), прокурор может брать предварительное разрешение на использование любых дозволенных принудительных мер. Это делается, если ожидание судебного решения может замедлить расследование или причинить ему иной ущерб. В таком случае о решении немедленно в письменном виде сообщается суду, который затем рассматривает вопрос (п.6).

Закон 1952 года позволяет использование принудительных мер, включая не только использование технических устройств (кроме подслушивающих), но также перлюстрацию почтовых отправлений, задержание и др., причем не обязательно выполнение вышеизложенного требования, чтобы имелось подозрение в совершении преступления, караемого определенным сроком тюрьмы. В качестве примера можно упомянуть, что задержание для проведения следствия может длиться до четырех недель, в то время как СПК для этой цели позволяет задержание не более, чем на одну неделю. Закон 1952 года оговаривает, к каким преступлениям он применим. В первую очередь это преступления, которые представляют общественную опасность, поджог, диверсия, угон, а также преступления против королевской семьи и, разумеется, преступления против государства и против безопасности Королевства. Недостаточно, чтобы данное преступление упоминалось в этом перечне: требуется также, чтобы подозреваемое преступление in casu имело значение для защиты нации, общественной безопасности, охраны правопорядка, общественного управления или же было направлено против королевской семьи. В

последнем случае Закон 1952 года также упоминает убийство, нападение, шантаж и другие преступления, которые влекут лишение свободы. Использование принудительных мер на основании Закона 1952:98 не оглашается ни перед общественностью, ни даже перед парламентом.

Надзор за законностью при проведении тайного прослушивания и тайного телефонного надзора осуществляют Канцлер Юстиции и парламентский омбудсмен. Они имеют право расследовать решения, санкционирующие такие меры, и внести протест в случае сомнений относительно выдачи санкции. Однако и тот, и другой институт надзора следят лишь за соблюдением установленной процедуры и не рассматривают проблемы доказательств необходимости применения прослушивания либо тайного надзора как такового.

Следует отметить, что прослушивание с помощью "жучков" не разрешено, поскольку нет закона, позволяющего их использовать. Согласно п.9а главы 4 Уголовного кодекса 1962 года использование таких прослушивающих устройств преступно. Это касается не только общественности, но и полиции, включая сюда разведку и Полицию безопасности. Подготовка такого мероприятия, например, путем размещения где-то таких устройств с целью перехвата, также является преступлением (там же, пункт 9в).

Вот некоторые цифры, характеризующие перехват телефонных разговоров на практике. Тайное прослушивание телефона - не считая случаев, когда оно использовалось на основании Закона 1952-го года, - было одобрено в 1996 г. применительно к 397 подозреваемым. Средняя продолжительность прослушивания составила около 47 дней, откуда видно, что срок прослушивания продлевали во множестве случаев. Впрочем, разброс продолжительности очень значителен: от одного дня до 7 месяцев и 23 дней. По сообщениям полиции, прослушивание сыграло роль в 49% предварительных расследований, но нет ни единого случая, когда бы оно привело к осуждению или хотя бы к возбуждению уголовного дела. До 1993 г. ни одна заявка на использование прослушивания не отклонялась, в 1994 г. отклонена одна, а в 1995 г. - отклонены четыре заявки.

В 1996 г. тайный телефонный надзор был разрешен в 99 случаях. В 70 из них было подозрение в преступлении, связанном с наркотиками. Средняя длительность надзора составила 44 дня, но при этом разброс ее очень велик: от 10 дней до 10 месяцев. Только одна заявка была отклонена, но подавший ее обратился в апелляционный суд, который дал соответствующее разрешение.

Очевидно, что использование Закона 1952:98 выглядит сегодня анахронизмом. Кроме того, использование новых специальных средств для снятия информации требует изменения законодательства. В связи с этим была создана специальная комиссия, которая провела расследование дел о прослушивании и других принудительных методах и в марте 1998-го года опубликовала свои предложения относительно будущего законодательства. Комиссия заявила, что есть необходимость разрешить электронное подслушивание, а также расширить полномочия в использовании телефонного прослушивания и других принудительных методов. Вкратце соображения Комиссии таковы:

1. Электронное подслушивание должно быть разрешено при превентивной деятельности по предотвращению преступлений, наказание за которые превышает четыре года заключения. Это будет означать, что, если парламент одобрит соответствующее предложение, то электронное прослушивание сможет применяться обычной полицией при расследовании наиболее тяжких преступлений (убийство, преступления, связанные с

наркотиками, при отягчающих обстоятельствах, шантаж, похищение, разбой, поджог, преступления, влекущие ущерб для общества, и шпионаж). Для Полиции безопасности электронное подслушивание также будет разрешено, если подозреваются иные преступления, перечисленные в Законе 1952-го года. Не остается таких мест, включая, например, спальни, где нельзя было бы применять подслушивающее оборудование;

2. Прослушивание телефонов будет разрешено при превентивной деятельности по предотвращению преступлений, наказание за которые превышает один год заключения (сейчас - два года), и будет разрешено также в применении к абоненту, которому подозреваемый может позвонить. То же самое относится и к будущему применению телефонного надзора; будет необходимо, чтобы подозреваемое преступление каралось всего лишь шестимесячным заключением;

3. Тайный видеонадзор будет разрешен в случае преступлений, наказание за которые составляет более одного (сейчас - два) года тюрьмы, а также будет разрешен применительно к тем местам, куда подозреваемый может прийти (сейчас - только применительно к его дому, квартире и т.п.);

4. Прокурор сможет брать предварительный ордер на использование любых принудительных мер. Это решение должно быть немедленно сообщено суду, который имеет право аннулировать решение прокурора;

5. Будет существовать специальный общественный адвокат, защищающий права подозреваемого. Обсуждалось, не следует ли Швеции, как это сделали большинство западных стран, ввести правило, что лицо, находившееся под надзором, после окончания подслушивания, телефонного прослушивания и т.д. оповещается об этих мерах. Однако сопротивление полицейских властей было настолько упорным, что Комиссия решила выждать некоторое время и лишь затем сделать это предложение.

Подведем итоги. Основой правил телефонного прослушивания в Швеции является установка, что неприкосновенность личности приоритетна по отношению к раскрытию преступления. Процедура имеет основу в национальном законодательстве, она доступна и понятна. Меры, нарушающие неприкосновенность личности, могут, согласно законодательству, использоваться для предотвращения преступлений только в исключительных случаях. Решение о таких мерах должно всегда приниматься судом, и направлены они должны быть против тех, кого есть причины подозревать в намерении совершить преступление (или в попытке его совершить, или в сообщничестве). Список преступлений, при совершении которых может осуществляться прослушивание телефонов, четко описан, число преступлений в этом списке невелико. Данные о количестве перехватов публикуются. Казалось бы, Европейский Суд по правам человека должен одобрить эту процедуру. Однако, положения о надзоре явно недостаточны. Кроме того, наличие в законодательстве Закона 1952:98 совершенно неприемлемо, практика его применения противоречит почти всем стандартам Суда.

## ВЕНГРИЯ[30]

Венгерская конституция не содержит положения о неприкосновенности личной корреспонденции. Однако, Акт N. CXXV от 1995 г. о национальных службах безопасности описывает процедуру ведения прослушивания телефонных разговоров. Согласно этому Акту "для перехвата и записи телефонных и подобных сообщений требуется разрешение". В случае угрозы национальной безопасности генеральный директор соответствующей службы[31] может подать запрос на разрешение

прослушивания телефонных разговоров. Под "угрозой национальной безопасности" понимается угроза независимости или территориальной целостности страны, тайные попытки подорвать экономическую, политическую и оборонную мощь страны, тайные попытки изменить или нарушить, используя незаконные средства, конституционный порядок, измена, терроризм, контрабанда оружия и наркотиков, незаконное распространение изделий и технологий, находящихся под международным контролем.

Запрос должен включать следующие пункты:

1. Размещение и использование спецсредств.

2. Имена лиц, за которыми устанавливается наблюдение.

3. Описание используемых спецсредств.

4. Обоснование необходимости прослушивания.

5. Дата и время начала и окончания прослушивания.

6. Обоснование того, что прослушивание производится в интересах национальной безопасности.

Разрешение на сбор разведывательных сведений может быть выдано только Министром Юстиции. При расследовании уголовных преступлений разрешение выдается судьей, проводящим расследование. Акт ограничивает длительность прослушивания 90 днями, после чего может быть подан и представлен для разрешения повторный запрос. Наконец, в экстренных случаях, генеральный директор может разрешить прослушивание "в течение 72 часов или до решения судьи или Министра Юстиции, которые должны выдать разрешение".

Согласно Акту правительство контролирует и направляет гражданские службы безопасности, назначая для этого специального министра; военные службы безопасности подчиняются министру обороны. Министр, назначенный для контроля и управления гражданскими службами (им не может быть Министр Обороны, Внутренних Дел или Юстиции), определяет конкретные задачи служб, осуществляет надзор за их деятельностью, управляет их функциями и организацией. Он имеет право разрабатывать общие и конкретные инструкции, но не имеет права смещать руководителей служб и мешать их работе в пределах их компетенции. Он уполномочен также направлять рекомендации Премьер-министру относительно назначения и увольнения руководителей этих служб и их заместителей.

Кроме того, закон предполагает независимый надзор над всем процессом. Для этого организуется Парламентский Комитет по национальной безопасности, задачей которого является парламентский надзор над службами национальной безопасности. Комитет состоит из 11 членов и имеет статус постоянного комитета Парламента. Акт определяет, что президентом Комитета должен быть член парламентской оппозиции. Министр, назначенный для руководства службами безопасности, по крайней мере, два раза год должен докладывать Комитету "об общем характере деятельности служб национальной безопасности". Правительство также должно информировать Комитет о своих решениях, связанных со службами безопасности, это делается через ответственного министра. Акт уточняет, что Комитет имеет право запрашивать информацию "о разрешениях использовать секретные спецсредства и методы" у Министров Юстиции и Обороны,

Министра, ответственного за гражданские службы безопасности и генеральных директоров служб безопасности. Кроме того, Комитет имеет право "рассматривать индивидуальные жалобы на незаконные действия служб национальной безопасности" (в случае, когда эти жалобы не охватываются ответственным министром), равно как и получать внутренние доклады, подготовленные службами безопасности для правительства. Комитет информирует заявителя относительно результатов расследования. Если Комитет находит, что служба безопасности осуществила незаконные или недопустимые действия, он может призвать министра провести расследование. Министр должен информировать Комитет о результатах расследования. Комитет имеет право, в рамках закона провести расследование по фактам, если Комитет полагает, что служба безопасности действует в нарушение законов. В ходе такого расследования Комитет имеет право ознакомиться с документами службы безопасности, касающимися расследуемого случая и допросить сотрудников службы безопасности. Комитет может определить ответственных за нарушение и имеет право обратиться к министру и призвать его принять соответствующие меры. Интересно, что если национальная служба безопасности начинает расследование и секретный сбор информации о депутате парламента или членах его семьи, то ответственный министр должен доложить об этом Комитету, но сам депутат не должен быть информирован о происходящем.

В целом можно сказать, что венгерский закон удовлетворяет стандартам, установленным Европейским Судом. Венгерская процедура, несомненно, "имеет основу в национальном законодательстве", в свете обсуждения дела Малоуна. Как акт парламента, эта процедура доступна венгерским гражданам. Она понятна, поскольку имеется определение тех предполагаемых преступлений, при которых вводится прослушивание телефонных разговоров. Процедура удовлетворяет требованию, сформулированному при рассмотрении дела Класса, о том, что прослушивание разрешается только по письменному указанию определенного высшего чиновника или судьи. Временные ограничения также определены.

Надзор по венгерскому закону, по-видимому, удовлетворит Суд, поскольку процедура гарантирует "адекватные и эффективные" меры против злоупотреблений. В деле Класса Суд согласился с немецким законом, который включает парламентскую оппозицию в процесс надзора (Класс, 56). Похожее включение парламентской оппозиции в венгерском законе должно вызвать положительную реакцию Суда. Право Комитета получать информацию от служб безопасности и от правительства относительно разрешений использовать "секретные спецсредства и методы" и рассматривать индивидуальные жалобы о незаконных действиях служб безопасности и проводить расследования по этим жалобам, несомненно, будет одобрено Судом.

Вместе с тем, венгерский закон может быть признан как нарушающий Конвенцию, поскольку в нем явно не хватает некоторых предосторожностей и гарантий. В Акте не указано, что делать с собранными материалами, ничего не сказано о передаче этих данных по инстанциям, о составлении итоговых докладов, об уничтожении материалов, после того, как они перестали быть нужными. Что более важно, Акт ничего не говорит о том, что прослушивание телефонов может быть применено только тогда, когда "есть достаточные основания подозревать лицо в том, что оно планирует, совершает или совершило определенное тяжкое преступление" (Класс, 51).

## ПОЛЬША[32]

Ст.87(2) Польской Конституции гласит: "Неприкосновенность жилья и личной корреспонденции должна быть защищена законом". Однако ст.10 Закона о Службе

Защиты Государства (СЗГ) от 1990 г., с поправками 1995 г., и ст.198 Уголовно-Процессуального Кодекса (оставшаяся от коммунистического режима) описывают нормы прослушивания телефонных разговоров. Существование этих двух законов создало ситуацию, в которой процедура, нацеленная на обеспечение национальной безопасности, в общем, ясна (хотя она содержит много недомолвок), однако правила прослушивания телефонов как часть расследования уголовных дел, не касающихся национальной безопасности, безнадежно размыты и открыты для широких интерпретаций.

По закону о СЗГ, министр внутренних дел может подать генеральному прокурору запрос для дачи письменного согласия на прослушивание телефонных разговоров с целью установления фактов и противодействия "угрозам национальной безопасности, обороне, суверенитету и целостности государства;... , а также шпионажу, терроризму и другим тяжким преступлениям против государства;..., равно как и раскрытию государственных секретов" (ст.1.2.1-3). Прослушивание допустимо также для того, чтобы предотвратить или раскрыть преступления, "караемые по международным договорам и соглашениям" (ст.10.1). Кроме того, прослушивание разрешено для предотвращения преступлений, предусмотренных ст.122-133 уголовного кодекса, то есть "преступлений против основных политических и экономических интересов Польской Республики", производства и/или международной торговли некоторыми запрещенными изделиями[33] и подкупа официальных лиц, что может нанести ущерб национальной безопасности (ст.10a.1.1-3).

Запрос министра внутренних дел должен включать точные временные ограничения для прослушивания. Разрешение по такому запросу может быть выдано только генеральным прокурором. Однако в экстренных случаях министр внутренних дел может приказать прослушивать телефонную линию в течение 24 часов, пока он обратится за разрешением к генеральному прокурору (ст.10.2). Далее закон указывает, что прослушивание "устанавливается только тогда, когда другие средства оказались неэффективными или, с большой вероятностью, могут оказаться неэффективными или бесполезными" (ст.10.4). Если благодаря прослушиванию удастся добыть доказательства подготовки или совершения преступления из числа перечисленных выше, то министр внутренних дел должен направить собранные свидетельства генеральному прокурору вместе с представлением о возбуждении уголовного дела (ст.10.5). Прочий собранный материал, не относящийся к этому преступлению, должен быть немедленно уничтожен (ст.10.6).

Наконец, закон о СЗГ гласит, что министр внутренних дел, после консультации с министрами юстиции, национальной обороны и телекоммуникаций, "должен уточнить процедуру и документирование действий, и род технических средств" для телефонного прослушивания.

Поскольку закон о СЗГ утверждает, что его положения имеют силу "в области, которая не покрывается законоположениями Уголовно-Процессуального Кодекса (ст.10.1), следует также исследовать единственную ссылку на телефонный перехват в указанном Кодексе; тем самым обсуждение польской процедуры будет закончено. Ст.198, §1 уголовно-процессуального кодекса содержит следующее простое высказывание:

Почты, отделения телекоммуникационной связи, таможни и транспортные агентства должны по требованию суда или прокурора выдавать любую корреспонденцию или передачу, имеющую отношение к следствию. С выданной информацией может ознакомиться только суд и прокурор.

Таким образом, согласно польскому закону, отделения телекоммуникационной связи обязаны выдавать перехваченную информацию по требованию прокурора. Положения о

надзоре минимальны. Ст.198, §2 гласит, что "ордер на прослушивание телефонных разговоров может быть предварительно обжалован", однако, согласно §3, объект прослушивания можно и не уведомлять о такой апелляции. Наконец, в соответствии с §4 любая собранная информация, не относящаяся к расследуемому преступлению, должна быть возвращена туда, откуда она была взята.

Ясно, что польский закон не удовлетворяет требованиям Европейского Суда по правам человека. Во-первых, процедура, описанная в законе о СЗГ и уголовно-процессуальном кодексе, видимо, не пройдет проверку на доступность, как она сформулирована в деле Малоуна. Ст.10.7 закона о СЗГ ясно формулирует, что конкретные правила должны быть приняты совместно группой министров в ходе консультации. Точно так же ст.198 уголовно-процессуального кодекса не упоминает никакой процедуры, кроме "требования" прокурора. Рассматривая дело Малоуна, Суд ясно указал, что такая процедура не удовлетворяет принципу доступности. Суд признал неприемлемой британскую практику в деле Малоуна, так как "невозможно сказать уверенно, какие полномочия на прослушивание упоминаются в законах, а какие остаются дискреционными полномочиями исполнительной власти" (Малоун, 79) .

Во-вторых, что касается предсказуемости, польский закон не удовлетворяет стандартам Европейского Суда. Хотя закон о СЗГ вроде бы понятен, т.к. содержит перечень преступлений, однако он никак не определяет "угрозу национальной безопасности, обороне, суверенитету и целостности государства". Также не определены термины "тяжкие преступления против государства" и "разглашение государственных секретов". Подобным образом, уголовно-процессуальный кодекс не определяет точно, что значит "имеющая отношение к следствию". Польский закон, несомненно, не удовлетворяет критерию предсказуемости.

Наконец, что касается "качества закона", польская процедура также не удовлетворяет требованиям Суда. Закон не содержит никаких положений о независимом надзоре. Так, по закону о СЗГ министр, назначенный правительством, должен обращаться к генеральному прокурору, назначенному правительством, за разрешением на прослушивание. Уголовно-процессуальный кодекс не предусматривает даже такой в край ограниченный контроль. Наоборот, согласно этому Кодексу, прокурор попросту "требует" доступа к телефонным разговорам, и согласно закону, агентства связи должны подчиняться этому требованию.

## РОССИЙСКАЯ ФЕДЕРАЦИЯ[34]

Прослушивание телефонных переговоров в СССР впервые получило законодательное обоснование в 1990 г., когда был принят закон "О внесении изменений и дополнений в Основы уголовного судопроизводства Союза ССР и союзных республик"[35], до этого прослушивание регламентировалось секретными инструкциями. Согласно ст.35-1 этого Закона телефонные переговоры можно было прослушивать на основании постановления органа дознания или следователя, санкционированного либо прокурором, либо определением суда. Санкция давалась при наличии достаточных оснований полагать, что будет получена информация, имеющая существенное значение для расследования уголовного дела. Прослушивание не могло продолжаться более шести месяцев. Оно могло также проводиться в случае угроз насильственных действий, вымогательства или других противоправных действий в отношении свидетелей или потерпевших в случае их согласия и дачи санкции прокурора или определения суда. При проведении прослушивания и звукозаписи предусматривалось составление протокола с коротким изложением содержания фонограмм, имеющих отношение к делу. Фонограммы должны были

приобщаться к протоколу, а та их часть, которая не имела отношения к делу, должна была быть уничтожена.

Этот закон после распада СССР формально не был отменен, однако отсутствие в уголовно-процессуальном законодательстве Российской Федерации соответствующей процедуры делало невозможным его применение. В дальнейшем право на прослушивание было закреплено за органами внутренних дел и Федеральной Службы Безопасности (ФСБ) в соответствующих федеральных законах 1992 г. и 1995 г., затем право на оперативно-розыскную деятельность (ОРД), в том числе и на прослушивание, получили и другие органы.

Часть 2 ст.23 Российской Конституции 1993 г. содержит следующие гарантии[36]:

Каждый имеет право на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений. Ограничение этого права разрешается только на основании судебного решения.

В законодательстве Российской Федерации два закона описывают, как государство может ограничить указанное право: федеральный закон об органах ФСБ и федеральный закон об ОРД[37]. Оба закона четко согласованы с указанием Конституции, поскольку определяют, что прослушивание телефонных разговоров производится только по решению суда. Группа органов по обеспечению безопасности, называемая "органами ФСБ"[38], имеет право подавать запросы на такие действия.

Согласно ст.8 закона о ФСБ, основными направлениями деятельности ФСБ являются проведение контрразведывательных действий и борьба с преступностью. Действия органов ФСБ, направленные на борьбу с преступностью, подчиняются закону об ОРД (ст.10). Прослушивание телефонных разговоров как одна из разновидностей контрразведывательных действий рассматривается в ст.9 закона о ФСБ. Согласно ст.9, органам ФСБ разрешено проводить контрразведывательные действия, если они считают, что (а) деятельность спецслужб и организаций иностранного государства, а также отдельных лиц угрожает безопасности России; (б) возникла необходимость защиты сведений, составляющих государственную тайну; (в) необходимо установить наблюдение за лицами, оказывающими или оказавшими органам ФСБ конфиденциальную помощь; (г) необходимо обеспечить собственную безопасность.

Если при одном из вышеперечисленных обстоятельств необходимо получить судебную санкцию на телефонное прослушивание, то органы ФСБ "по требованию суда представляют служебные документы, касающиеся оснований для осуществления контрразведывательной деятельности". Закон устанавливает, что перехват телефонных разговоров и другой корреспонденции "допускается только на основании судебного решения", которое хранится в органах ФСБ (ст.9). Представляется, что, по крайней мере, согласно этому закону, при отсутствии решения суда, устанавливать телефонное прослушивание запрещено, несмотря на тот факт, что "требовать" документы о возможном перехвате должен именно суд. Таким образом, похоже, что бремя ответственности за открытие процесса прослушивания возложено на суд.

Такой вывод нельзя сделать относительно прослушивания телефонных разговоров при проведении органами ФСБ разведывательной деятельности. Она осуществляется органами ФСБ во взаимодействии с органами внешней разведки Российской Федерации (ст.11), а порядок и условия этого взаимодействия устанавливаются на основании соответствующих соглашений между ними или совместных нормативных актов. Согласно ст.11 порядок

проведения разведывательных мероприятий, а также порядок использования негласных методов и средств при осуществлении разведывательной деятельности, определяются нормативными актами ФСБ, а сведения об организации, тактике, методах и средствах осуществления такой деятельности составляют государственную тайну. Более ничего в законе о ФСБ об этом не сказано. Таким образом, конституционные гарантии неприкосновенности телефонных переговоров в виде судебного решения при проведении разведывательной деятельности законом явным образом не предусмотрены.

Как сказано выше, обязанности органов ФСБ по борьбе с преступностью определены законом об ОРД. Закон рассматривает прослушивание телефонных разговоров лишь как одну из разновидностей оперативно-розыскных мероприятий. Ст.7 этого закона устанавливает следующие основания для того, чтобы начать розыскные действия:

1. Наличие возбужденного уголовного дела.

2. Ставшие известными органам, осуществляющим ОРД, сведения о:

а) признаках преступления, которое планируется, совершается или было совершено, а также о лицах, его подготавливающих, совершающих или совершивших, если нет достаточных данных для решения вопроса о возбуждении уголовного дела;

б) событиях или действиях, создающих угрозу государственной, военной, экономической или экологической безопасности Российской Федерации;

в) лицах, скрывающихся от органов дознания, следствия и суда или уклоняющихся от уголовного наказания;

г) лицах, без вести пропавших, и об обнаружении неопознанных трупов.

3. Поручения следователя, органа дознания, указания прокурора или определения суда по уголовным делам, находящимся в их производстве.

4. Запросы других органов, осуществляющих ОРД, по основаниям, указанным в настоящей статье.

5. Обеспечение должной безопасности для лиц, находящимся под защитой компетентных федеральных органов.

6. Запросы международных правоохранительных организаций и правоохранительных органов иностранных государств в соответствии с международными договорами Российской Федерации.

Обсуждение прослушивания телефонных разговоров начинается, в частности, в ст.6 закона, которая утверждает, что прослушивание телефонных разговоров "проводится с использованием оперативно-технических сил и средств органов ФСБ и органов внутренних дел".[39] Запрещены какие-либо действия, которые ведутся в нарушение этого закона. Равно как и закон о ФСБ, закон об ОРД описывает условия, которые должны соблюдаться для проведения прослушивания телефонных разговоров. Закон гласит, что такие меры могут быть приняты только на основании судебного решения и при наличии информации:

1. О признаках подготавливаемого, совершаемого или совершенного противоправного деяния, по которому производство предварительного следствия обязательно.

2. О лицах, подготавливающих, совершающих или совершивших противоправное деяние, по которому производство предварительного следствия обязательно.

3. О событиях и действиях, создающих угрозу государственной, военной, экономической или экологической безопасности Российской Федерации. (ст.8)

Заметим, что здесь не уточняется, о каких именно преступлениях идет речь. Ст.8 предусматривает, что в экстренных ситуациях, когда может быть совершено тяжкое преступление, а также при наличии информации по п.3, органы следствия могут установить телефонное прослушивание без ордера суда, при условии, что запрос будет представлен суду в течение суток. Далее статья утверждает, что в течение 48 часов после начала прослушивания осуществляющая его служба обязана получить судебное решение, которое разрешает прослушивание или приказывает его прекратить.

Ст.9 поясняет права и ответственность судьи при выдаче ордеров согласно описанной процедуре. Прежде всего, запрос на прослушивание телефонных разговоров "рассматривается, как правило, по месту проведения таких мероприятий или по месту нахождения органа, ходатайствующего о его проведении". Судья не вправе отказать в рассмотрении поданного запроса. Он может запросить дополнительную информацию, если считает это необходимым. Приняв решение, судья передает его вместе с рассмотренными им материалами следствия руководителю органа, проводящего расследование. Решение судьи должно устанавливать длительность прослушивания в днях, не превышающую шести месяцев. Для продления срока действия прослушивания, судья должен вынести новое решение, основанное "на вновь представленных материалах". Если судья не выдаст разрешения на прослушивание, глава службы имеет право обжаловать его решение в суде высшей инстанции.

Статьи 10 и 11 закона содержат общие указания о том, что делать с собранными материалами. Статья 10 утверждает, что дела оперативного учета могут собираться только при проведении ОРД в соответствии с этим законом. Факт наличия этих дел не является основанием для "ограничения конституционных прав и свобод, а также законных интересов" (ст.10). Ст.11 указывает, что собранные материалы могут служить поводом и основанием для возбуждения уголовного дела, могут быть направлены в орган дознания, следователю или в суд, в производстве которого находится уголовное дело, но только по распоряжению главы службы, уполномоченной осуществлять оперативно-розыскные действия. Эти материалы могут использоваться как доказательство в соответствии с положениями уголовно-процессуального законодательства, регламентирующими собирание, проверку и оценку доказательств.

В статье 5 закона содержатся положения о том, что делать с собранной информацией о лице, в отношении которого в возбуждении уголовного дела отказано либо уголовное дело прекращено в связи с отсутствием в его действиях состава преступления. Если такое лицо "располагает фактами проведения в отношении него оперативно-розыскных мероприятий и полагает, что при этом были нарушены его права", то оно "вправе истребовать от органа, осуществляющего ОРД, сведения о полученной о нем информации в пределах, допускаемых требованиями конспирации и исключающих возможность разглашения государственной тайны".

В случае отказа в предоставлении запрошенных сведений или предоставления их в неполном объеме "лицо вправе обжаловать это в судебном порядке", и в случае признания необоснованным решения органа, осуществлявшего ОРД, об отказе в даче информации судья вправе обязать указанный орган предоставить заявителю эти сведения. Бремя доказывания обоснованности отказа в предоставлении информации возлагается на соответствующий орган, осуществлявший ОРД.

Согласно статье 5, полученные материалы в этом случае хранятся один год, а затем уничтожаются, если служебные интересы или правосудие не требуют иного. За три месяца до дня уничтожения материалов об этом уведомляется соответствующий судья.

Наконец, закон возлагает на Президента России, Федеральное Собрание и Правительство ответственность по осуществлению контроля за оперативно-розыскной деятельностью, в том числе и за прослушиванием телефонных разговоров (ст.20). Общий надзор над применением таких мер является обязанностью Генерального Прокурора и уполномоченных им прокуроров (ст.21). Ст.21 также гласит, что уполномоченный прокурор, по собственной инициативе или в связи с обращениями граждан, может затребовать от руководителя органа следствия документы, послужившие основанием для проведения ОРД с тем, чтобы определить, производилось ли прослушивание телефонных разговоров в соответствии с законом. Неисполнение законных требований прокурора, вытекающих из его полномочий по надзору за ОРД, влечет за собой установленную законом ответственность.

И закон о ФСБ, и закон об ОРД содержат положения о гарантии соблюдения прав и свобод человека и гражданина при осуществлении органами ФСБ своей деятельности и при проведении ОРД. В статье 6 закона о ФСБ и статье 5 закона об ОРД четко сказано, что граждане, полагающие, что органами ФСБ (либо органами, осуществляющими ОРД), нарушены их права и свободы, имеют право обратиться с жалобой в вышестоящий орган ФСБ (либо, соответственно, вышестоящий орган, осуществляющий ОРД), в прокуратуру или в суд по поводу действий органов ФСБ или их должностных лиц (либо, соответственно, органов, осуществлявших ОРД), а также получить необходимые разъяснения и информацию.

Однако в закон об органах ФСБ включены несколько более жесткие требования относительно защиты собранной информации. Закон гласит:

Полученные в процессе деятельности органов ФСБ сведения о частной жизни, затрагивающие честь и достоинство гражданина, или способные повредить его законным интересам, не могут сообщаться органами ФСБ кому бы то ни было без добровольного согласия гражданина за исключением случаев, предусмотренных федеральными законами (ст.6).

В случае, когда сотрудники органов ФСБ нарушили права и свободы человека, глава соответствующего органа ФСБ, прокурор или судья "обязаны принять меры по восстановлению этих прав и свобод, возмещению причиненного ущерба и привлечению виновных к ответственности".

Следует отметить, что в законах о ФСБ и ОРД отсутствуют ограничения на прослушивание лиц, имеющих процессуальный статус - судей, адвокатов , депутатов парламента и т.д. Эти ограничения вводятся другими нормативными актами. Так, согласно решению Конституционного Суда от 20 февраля 1996 г. по делу о проверке конституционности положений частей 1 и 2 ст.18, ст.19 и части 2 ст.20 Федерального

закона "О статусе депутата Совета Федерации и статусе депутата Государственной Думы Федерального Собрания Российской Федерации"[40] ни при каких условиях не разрешается прослушивать телефонные переговоры депутата Федерального Собрания. Согласно ст.16 закона "О статусе судей в Российской Федерации" запрещено прослушивать телефоны судей, пока квалификационная коллегия судей не даст согласие на возбуждение уголовного дела в отношении определенного судьи.

Проверка конституционности отдельных положений закона об ОРД была проведена летом 1998 г. Конституционным Судом Российской Федерации в связи с жалобой журналистки Ирины Черновой, волгоградского корреспондента "Комсомольской правды" на нарушение ее конституционных прав сотрудниками областного УВД, опиравшихся в своих действиях на этот закон. И.Чернова записала на пленку разговор с сотрудником УВД, в котором он угрожал ей обнародованием сведений о ее личной жизни, полученных в результате слежки с применением технических средств, если она не прекратит публиковать материалы, компрометирующие УВД. Чернова обратилась в Волгоградский областной суд с жалобой на действия органов дознания, а именно: заведение на нее в мае 1995 г. дела оперативного учета, проведение в отношении ее оперативно-розыскных мероприятий (ОРМ), уклонение от вынесения по результатам оперативной проверки конкретного решения в соответствии с требованиями УПК (постановление о возбуждении уголовного дела либо отказ в этом), отказ в предоставлении сведений о полученной о ней информации в ходе ОРМ. Областной суд установил, что факты заведения дела оперативного учета и конкретные ОРМ имели место, однако в удовлетворении жалобы отказал, мотивируя отказ возможностью разглашения государственной тайны. Действия УВД он признал обоснованными. В январе 1997 г. Верховный Суд отменил в кассационном порядке решение Волгоградского областного суда как необоснованное и незаконное и направил дело на новое рассмотрение судом первой инстанции. Из определения Верховного Суда следует, что в деле Черновой были нарушены или неправильно применены статьи 5,9,10, и 12 закона об ОРД.

Хотя Конституционный Суд вынес решение о соответствии Конституции положений Закона об ОРД, возложив вину за нарушение прав заявительницы на правоприменительный орган, и прекратил производство по делу, его решение имело и положительное значение.

Суд отметил, что содержание любого закона, основанное на Конституции, должно гарантировать от ошибок и злоупотреблений. Решение Конституционного Суда повлекло за собой изменения к закону об ОРД в декабре 1998 г,, когда Государственная Дума внесла либеральные поправки к ст.5 и 21 Закона, усилив гарантии прокурорского контроля за ОРД.

Хотя российское законодательство, очевидно, имеет много изъянов, оно наиболее соответствует стандартам, установленным Европейским Судом по правам человека среди других посткоммунистических стран, рассмотренных в данной работе. Процедура четко урегулирована законами, принятыми Государственной Думой, и, следовательно, "имеет основу в национальном законодательстве". Как таковая, процедура является доступной. Далее, что касается "качества закона", то требования, сформулированные Судом, присутствуют в российских законах. Прослушивание телефонных разговоров ограничивается случаями, когда уже имеется информация относительно предполагаемого преступления, следовательно, закон запрещает предварительное прослушивание по неподтвержденному фактами подозрению. Прослушивание может быть установлено только по письменному запросу определенных высших чиновников, что соответствует решению Суда в деле Класса. Опять же, в соответствии с делом Класса, прослушивание

телефонных разговоров может быть предпринято только по разрешению судьи. Наконец, определена максимальная длительность прослушивания.

Несмотря на вышеприведенные аргументы, при суммарном рассмотрении российская процедура вряд ли получит одобрение Суда. Во-первых, не определены правила по составлению итоговых докладов и по прохождению перехваченной информации по разным инстанциям, как потребовал Суд при рассмотрении дел Ювига и Крюслена. Во-вторых, ст.6 закона о ФСБ гласит, что информация о личной жизни гражданина, ущемляющая его честь и достоинство, или информация, которая может нанести ущерб его законным интересам, не может передаваться органами ФСБ никому иному. По мнению Суда, такого сорта информация должна уничтожаться (Ювиг, 34). Однако самый большой недостаток российских законов касается требования Суда о "предсказуемости", как она интерпретировалась в деле Малоуна, то есть как возможность гражданина понять, какие его действия приведут к реакции государства и какой именно реакции. В российском законе просто никак не определен перечень преступлений, при которых разрешено прослушивание. Согласно ст.8 закона об ОРД, подозрение в совершении любого преступления может привести к прослушиванию телефонных разговоров, при условии, что существует информация о преступлении, добытая из других источников. Поскольку в законах не указано, какого вида предполагаемые преступления допускают прослушивание телефонных разговоров, вся процедура вряд ли будет признана "предсказуемой" в соответствии с требованиями, описанными Судом в решении по делу Малоуна. Наконец, ведомственный контроль и прокурорский надзор за законностью прослушивания вряд ли будет признан Судом достаточно эффективной гарантией от злоупотреблений.

## РУМЫНИЯ[41]

В Румынии конфиденциальность корреспонденции защищена конституцией, ст.28 которой гласит: "Тайна писем, телеграмм и других почтовых отправлений, равно как телефонных разговоров и других законных средств связи является неприкосновенной". Нормы, определяющие законное прослушивание телефонных разговоров, содержатся в румынском Уголовно-Процессуальном Кодексе (УПК) и в законе о национальной безопасности от 1991 г.

В ст.3 закона о национальной безопасности перечислен обширный список преступлений, которые являются законным основанием для установления прослушивания телефонных разговоров. Это стандартный набор угроз национальной безопасности, таких как государственная измена, вооруженное восстание, политическое убийство, терроризм, кража оружия, боеприпасов, взрывчатых и радиоактивных веществ, токсических или бактериологических материалов и торговля ими. Кроме того, перечисляются такие не очень точно определенные преступления, как "уничтожение, повреждение или приведение в негодность структур, необходимых для нормального развития общественной экономической жизни или национальной безопасности", "разглашение государственных секретов или их небрежное хранение", "нападки на коллектив", и участие в "тоталитарных или экстремистских действиях коммунистического, фашистского или подобного характера, равно как и в расистских, антисемитских, ревизионистских и сепаратистских выступлениях".

Согласно ст.13, любое из вышеперечисленных преступлений может служить основанием для установления прослушивания телефонных разговоров по запросу "компетентных органов национальной безопасности".[42] Запрос направляется прокурору, назначенному Генеральным Прокурором. Запрос должен удовлетворять следующим требованиям:

подаваться в письменной форме;

содержать данные или доказательства о существовании определенной угрозы национальной безопасности;

содержать, если это известно, имя лица, чьи разговоры будут прослушиваться;

содержать общее описание места, где будут производиться разрешенные действия;

содержать сроки прослушивания (ст.13)

Если прокурор удовлетворяет запрос, то его разрешение должно содержать вид сообщения и тип информации, которые разрешается перехватить. Закон устанавливает предельную длительность прослушивания - шесть месяцев. Ст.14 гласит, что "в экстренных случаях, когда имеется явная угроза национальной безопасности", для ведения прослушивания телефонных разговоров можно обойтись без разрешения прокурора, но последнее должно быть получено в течение 48 часов.

Единственным положением, которое касается надзора, состоит в том, что гражданин, полагающий, что его корреспонденция неоправданно перехватывается, может "направить жалобу специально назначенному прокурору, который занимает более высокий пост по отношению к тому прокурору, который разрешил перехват".

Ясно, что румынский закон не соответствует стандартам, установленным Европейским Судом по правам человека. Хотя его нормы основаны на законе, принятом румынским парламентом и, как таковые, "имеют основу в национальном законодательстве" и являются "доступными", трудно надеяться, что они отвечают критерию "предсказуемости". Как говорилось выше, Суд, рассматривая дело Малоуна, определил "предсказуемость" как возможность гражданина "предвидеть (если нужно, с помощью адвоката) с разумной точностью, определяемой конкретными обстоятельствами, следствия, которые данное действие может повлечь за собой" (Малоун, 66). Согласно ст.3 румынского закона предусматривается установление прослушивания телефонных разговоров при подозрении на "уничтожение, повреждение или приведение в негодность структур, необходимых для нормального развития общественной экономической жизни", или "небрежное хранение государственных секретов", или участие в "тоталитарных или экстремистских действиях коммунистического, фашистского или подобного характера, равно как и в расистских, антисемитских, ревизионистских и сепаратистских выступлениях". Ясно, что многие из этих преступлений полностью зависят от политической конъюнктуры и никоим образом не обеспечивают предсказуемость закона.

Что касается "качества" закона, то также маловероятно, что Европейский Суд одобрит румынские нормы. Действительно, письменное разрешение должно включать описание предполагаемого преступления, содержать имя лица, к которому применяется прослушивание (если оно известно), и указывать длительность прослушивания. Закон устанавливает также предельную длительность прослушивания в шесть месяцев при любом виде перехвата. Хотя эти нормы удовлетворяют требованиям Суда, в румынском законодательстве не указано, как составлять итоговые отчеты, каковы правила передачи информации между службами, при каких обстоятельствах материалы должны уничтожаться. Отсутствие этих правил привело к тому, что Суд не признал французскую процедуру при рассмотрении дел Ювига и Крюслена.

Наконец, самым большим недостатком румынского закона является отсутствие какого бы то ни было независимого надзора. Начиная с дела Класса, Суд постоянно повторял, что "при любой системе надзора должны существовать адекватные и эффективные гарантии против злоупотреблений" (Класс, 50). Рассматривая дело Класса, Суд ясно выразил свое мнение, что разрешать перехват должна судебная власть. В случае несоблюдения этого условия, Суд признал, что при некоторых обстоятельствах возможно, чтобы разрешение выдавалось другим органом, если он достаточно независим. Согласно румынскому закону, разрешение выдается прокурором, назначаемым Генеральным прокурором. Судьи не имеют к этому вообще никакого отношения. В румынском законе не предусмотрено создание независимого органа надзора. Ни при каких обстоятельствах Европейский Суд не согласится с системой, в которой единственной гарантией против злоупотреблений есть право гражданина апеллировать к чиновнику, чтобы тот отменил решение нижестоящего чиновника. Несомненно, румынский закон о национальной безопасности от 1991 г. был бы признан нарушающим ст.8 Конвенции , если бы он рассматривался Европейским Судом .

## УКРАИНА[43]

В ст.31 Конституции Украины, принятой 26 июня 1996 г., говорится, что "каждому гарантируется тайна переписки, телефонных разговоров, телеграфной и иной корреспонденции. Исключения могут быть установлены только судом в случаях, предусмотренных законом, с целью предотвратить преступление или установить истину при расследовании уголовного дела, если иными способами получить информацию невозможно".

Порядок осуществления таких исключительных мер регулируется Законом Украины "Об оперативно-розыскной деятельности", который был принят 18 февраля 1992 г. (с изменениями и дополнениями в 1992-1998 гг.)[44].

Право проводить оперативно-розыскные мероприятия, в том числе, прослушивание телефонных разговоров и перлюстрацию телеграфно-почтовых сообщений, предоставлено в соответствии со ст.5 Закона Украины "Об оперативно-розыскной деятельности":

подразделениям органов внутренних дел (криминальной и специальной милиции, специальным подразделениям по борьбе с организованной преступностью, оперативно-розыскным подразделениям Государственной автомобильной инспекции);

органам Службы безопасности (разведке, контрразведке, военной контрразведке, подразделениям защиты национальной государственности, борьбы с коррупцией и организованной преступной деятельностью, оперативно-техническим органам, органам оперативного документирования);

пограничным войскам (подразделениям по оперативно-розыскной работе);

управлению государственной охраны (подразделению оперативного обеспечения охраны);

органам государственной налоговой службы (оперативным подразделениям налоговой милиции);

органам и учреждениям Государственного департамента по вопросам исполнения наказаний (оперативным подразделениям).

Это право зафиксировано и в соответствующих законах, регулирующих деятельность этих ведомств (ст.10 Закона Украины "О милиции", ст.25 п.8 Закона "О Службе Безопасности Украины" и т.д.).

Основания для проведения оперативно-розыскной деятельности определены в ст.6 Закона "Об оперативно-розыскной деятельности": это наличие достаточной информации о преступлениях совершенных или готовящихся, о лицах, к ним причастных, о лицах, скрывающихся от органов следствия или уклоняющихся от отбывания наказания, о лицах, пропавших без вести, о разведывательно-подрывной деятельности спецслужб иностранных государств, организаций и отдельных лиц против Украины, а также по запросам полномочных органов о проверке лиц в связи с их допуском к государственной, военной и служебной тайне и при необходимости в получении разведывательной информации в интересах безопасности общества и государства. При этом понятия "достаточность информации" и "интересы общества и государства" не определяются, что, на наш взгляд, дает возможность живой власти толковать их в своих интересах. Следует также отметить, что при отсутствии перечисленных в этой статье оснований оперативно-розыскная деятельность запрещается.

Ст.8 этого Закона перечисляет права подразделений, осуществляющих оперативно-розыскную деятельность. Согласно п.9, они имеют право "снимать информацию с каналов связи и использовать иные технические средства для получения информации". В соответствии с той же ст.8 снятие информации с каналов связи, применение других технических средств получения информации, а также контроль почтово-телеграфных отправлений, производятся как исключительные меры с санкции Генерального прокурора Украины или его заместителей, прокурора республики Крым, прокуроров областей, города Киева и других приравненных к ним прокуроров в случае, если другим способом невозможно добыть фактические данные для обеспечения защиты общества и государства от преступных посягательств" (заметим, что негласное проникновение в жилые помещения, визуальное наблюдение в них может иметь место лишь с санкции Генерального прокурора или его заместителей). Кроме того, исключительно с целью получения разведывательной информации ст.8 предусматривает возможность проведения оперативно-розыскных действий в порядке, согласованном с Генеральным прокурором Украины. Что означает такое согласование - не определено. В ст.9 Закона сделано следующее уточнение: "Оперативно-розыскные мероприятия, связанные с временным ограничением прав человека, проводятся с санкции прокурора с целью предотвращения тяжких преступлений, их пресечения и раскрытия, розыска лиц, уклоняющихся от отбывания уголовного наказания или пропавших без вести, пресечения разведывательно-подрывной деятельности против Украины. В случае оперативной необходимости неотложного осуществления этих мер оперативно-розыскные подразделения обязаны в течение 24 часов сообщить прокурору об их применении и основаниях для их проведения". Таким образом, прослушивание может быть применено только в случае тяжких преступлений (понятие тяжкого преступления определено в ст.7-1 Уголовного кодекса Украины).

Следует отметить, что п.9 Раздела 15 Конституции Украины "Переходные положения" оставляет за прокуратурой полномочия в соответствии с действующим законодательством до введения законов, регулирующих деятельность государственных органов по контролю за соблюдением законов, и до сформирования системы досудебного следствия и введения в действие законов, регулирующих ее функционирование. Однако постановление Пленума Верховного Суда Украины "Об использовании Конституции Украины при осуществлении правосудия" №9 от 1 ноября 1996 г. обусловило изменение процедуры получения санкции на телефонное прослушивание. В п.22 этого Постановления ясно

указано, что статьи 9 и 13 "Переходных положений" не распространяются на действие статей 30 и 31 Конституции и что "разрешение на проникновение в жилище или иное владение лица, на наложение ареста на корреспонденцию, ее выемку в почтово-телеграфных учреждениях и на снятие информации с каналов связи дается только судом"[45]. Поэтому санкцию на прослушивание телефонных разговоров стал давать не прокурор, а судья. При этом, никакие изменения на эту тему в закон об ОРД внесены не были. Уголовно-процессуальный кодекс тоже не содержит каких-либо указаний на сей счет. По-видимому, процедура получения санкции в суде регулируется ведомственными инструкциями. Из общения с сотрудниками правоохранительных органов можно заключить, что санкцию дает уполномоченный судья областного суда.

Кроме Закона об ОРД о прослушивании телефонов упоминается также в Законе "Об организационно-правовых основах борьбы с организованной преступностью". В соответствии со ст.15 этого закона специальным подразделениям МВД и СБУ по борьбе с организованной преступностью дано право "по предварительной санкции прокурора дополнительно использовать специальные технические средства в следующих случаях:

а) контроля, фиксации и документирования разговоров и других действий лиц при наличии оснований считать их причастными к организованной преступной деятельности;

б) фиксации и документирования факта телефонного разговора между гражданами, посылки письма или телеграфного сообщения без нарушения тайны смысла телефонного разговора, письма или телеграфного сообщения;

в) обеспечения личной безопасности и безопасности жилья и имущества сотрудников указанных подразделений, участников уголовного судопроизводства, их близких родственников (по их согласию), в случае угрозы нанесения им ущерба в связи с их участием в борьбе с организованной преступностью."[46]

Фактические данные, полученные и зафиксированные сотрудниками специальных подразделений с использованием технических средств, согласно той же ст.15 могут быть использованы как доказательство в судопроизводстве. Однако, поскольку уголовно-процессуальное законодательство не регламентирует использование сведений, полученных таким образом в качестве доказательств, эта норма работать не может.

Законом установлены определенные ограничения на проведение оперативно-розыскных мероприятий в отношении некоторых категорий граждан. Так, в соответствии с ч.2 ст.10 Закона "Об адвокатуре" запрещается прослушивание телефонных разговоров адвокатов в связи с оперативно-розыскной деятельностью без санкции Генерального прокурора, его заместителей, прокуроров Республики Крым, г.г. Киева и Севастополя. Не допускается обыск, осмотр личных вещей и багажа, транспорта, жилого или служебного помещения, а также прослушивание телефонных разговоров депутата Верховной Рады Украины (ч.2 ст.27 Закона "О статусе народного депутата Украины"). Проникновение в жилье или служебное помещение судьи, его личный или служебный транспорт, проведение там осмотра, обыска или выемки, прослушивание его телефонных разговоров, личный обыск судьи, а также осмотр, выемка его корреспонденции, вещей и документов могут проводиться только с санкции Генерального прокурора Украины при наличии возбужденного уголовного дела (ч.4 ст.13 Закона Украины "О статусе судей"). Кроме того, статья 11 Закона об ОРД запрещает привлекать к выполнению оперативно-розыскных задач медицинских работников, священнослужителей, адвокатов, если объект ОРД является их клиентом или пациентом.

В ст.9 Закона "Об оперативно-розыскной деятельности" сформулированы гарантии законности при осуществлении ОРД. При наличии оснований для проведения ОРД заводится оперативно-розыскное дело (за исключением проверки лиц в связи с их допуском к государственной, военной и служебной тайне). Постановление о заведении такого дела подлежит утверждению начальником органа, осуществляющего ОРД. Если в течение шести месяцев не будут установлены данные, указывающие на признаки преступления в действиях лица, в отношении которого осуществлялись оперативно-розыскные меры, оперативно-розыскное дело уничтожается. Все сведения, полученные в результате оперативно-розыскной деятельности, которые касаются личной жизни, чести и достоинства человека, сохранению не подлежат и должны быть уничтожены, если только они не содержат информацию о запрещенных законом действиях.

В случае нарушения прав и свобод человека, а также в случае, если причастность к правонарушению лица, в отношении которого осуществлялись оперативно-розыскные меры, не подтвердилась, соответствующие органы, их проводившие, обязаны восстановить нарушенные права и возместить материальный и моральный ущерб. Однако ст.9 не содержит обязательства информировать в таких случаях лицо о проведении в отношении него оперативно-розыскных мероприятий, поэтому остается неясным, как лицо узнает о том, что, например, была нарушена тайна переписки и телефонных переговоров.

В ст.9 Закона предусмотрено также право граждан Украины и других лиц получить от органов, на которые возложено осуществление оперативно-розыскной деятельности, письменное объяснение по поводу ограничения их прав и свобод и обжаловать эти действия. В случае нарушения тайны переписки или прослушивания телефонных разговоров обжалование будет возможно только в случае разглашения информации, содержащейся в деле или оперативном обращении.

Таким образом, если прослушивание телефона не сопровождается другими оперативно-розыскными мероприятиями, которые невозможно сохранить в тайне, то возможность эффективного обжалования представляется сомнительной.

Контроль за проведением оперативно-розыскной деятельности в соответствии со ст.9 возложен на те же органы, которые и осуществляют эту деятельность (МВД, СБУ, Госкомитет по охране государственной границы и т.д.). Надзор за соблюдением законности при проведении ОРД осуществляется Генеральным прокурором Украины и подотчетными ему прокурорами Республики Крым, областей, Киева и Севастополя. Законодательством предусмотрен также парламентский контроль за деятельностью СБУ (он осуществляется Комитетом по вопросам национальной безопасности и обороны) и за исполнением законов в сфере борьбы с коррупцией и организованной преступностью (его осуществляет Комитет по вопросам законодательного обеспечения правоохранительной деятельности и борьбы с организованной преступностью и коррупцией), однако, на наш взгляд, парламентский контроль неощутим или, по крайней мере, об этом контроле общественности ничего не известно.

Наказание за нарушение тайны переписки, телефонных переговоров и телеграфных сообщений предусматривается ст.131 Уголовного кодекса Украины в редакции Закона Украины "О внесении изменений и дополнений в некоторые законодательные акты Украины в части ответственности за правонарушения в области связи" от 1 октября 1996 г., № 386/96-ВР в виде исправительных работ до одного года или штрафа от 25 до 35 необлагаемых налогом минимальных доходов граждан (т.е. примерно от $95 до $135).

В то же время использование связи с целью, противоречащей интересам государства, карается в соответствии с новой редакцией ст.148-3 Кодекса Украины об административных правонарушениях штрафом в размере от 50 до 150 необлагаемых налогом минимальных доходов граждан (т.е. примерно от $190 до $570, следует учесть, что средняя зарплата в Украине составляет сегодня примерно $35 и что работники бюджетной сферы получают ее с опозданием от 4 месяцев до одного года). Это сопоставление наглядно показывает приоритет ценностей и интересов государства над ценностями и интересами граждан.

Удовлетворяет ли украинское законодательство о прослушивании стандартам, установленным Европейским Судом по правам человека? Несмотря на многие положительные моменты, которые будут, безусловно, одобрены Судом - процедура имеет основу в национальном законодательстве, предсказуема, санкция на прослушивание дается судом и только в том случае, когда "другим способом невозможно добыть фактические данные для обеспечения защиты общества и государства от преступных посягательств", существует четкое указание об уничтожении полученных в результате ОРД сведений, касающихся личной жизни, чести и достоинства человека - Суд вряд ли сочтет ее удовлетворительной. Суд, по-видимому, признает законодательство недостаточно доступным из-за отсутствия описания процедуры получения санкции на прослушивание. Эта процедура должна быть четко описана в законе об ОРД при проведении прослушивания с целью предотвращения и пресечения тяжких преступлений, и в уголовно-процессуальном кодексе при проведении следствия после возбуждения уголовного дела. Далее, украинское законодательство явно недостаточно для того, чтобы удовлетворить критерию "качества закона", оно не содержит достаточно эффективных гарантий против злоупотреблений. Во-первых, отсутствуют какие-либо указания о длительности прослушивания, во-вторых, почти ничего не сказано о передаче собранных материалов по инстанциям, о составлении итоговых докладов, в-третьих, закон не содержит запрета вести пробное прослушивание, более того, оно разрешается при проведении ОРД по делам об организованной преступности, в-четвертых, независимый надзор за законностью явно недостаточен, особенно если сравнивать его с немецкой или венгерской процедурой парламентского контроля. На наш взгляд, перечень преступлений, при которых разрешено прослушивание телефонов - все преступления, относящиеся к тяжким - необходимо было бы сузить и четко перечислить в законе.

Необходимо дополнить закон описанием процедуры получения и продления санкции на прослушивание судом, нормой об ограничении длительности прослушивания, нормой о запрете пробного прослушивания ("хронометража"), а также правилами обмена собранными материалами между инстанциями и правилами составления итогового отчета. По нашему мнению, необходимо сделать процедуру прослушивания более прозрачной, введя норму об обязательном информировании лица, чей телефон прослушивался, после окончания прослушивания и ознакомлении лица с той частью дела оперативного учета, которая не содержит сведений, составляющих государственную тайну. При таком условии положения Закона об обжаловании незаконных действий служб, осуществляющих ОРД, смогут быть реализованы.

* * *

Деннис Телльборг[47]

ПОМОГАЕТ ЛИ ТАЙНЫЙ НАДЗОР В БОРЬБЕ С ПРЕСТУПНОСТЬЮ?

Один из первых вопросов, который должен быть поставлен, - насколько необходимы развернутые принудительные меры для успешной борьбы с преступлениями? На мой взгляд, это давно следует обсудить. Среди всех шведских властей только Комиссия по наркотикам по-настоящему пыталась взвесить все "за" и "против". Комиссия заключает: "Стоит отметить, что уже сегодня мы имеем весьма высокую раскрываемость преступлений - именно тех тяжких преступлений, в случае которых предполагается применять эти принудительные меры. Страны, где эти принудительные меры разрешены, едва ли похвастаются лучшими успехами. Это показывает, что хорошие результаты могут быть достигнуты компетентно осуществленными традиционными розыскными мерами, без обращения к этим изощренным техническим устройствам". Далее, как указывает эта же Комиссия, разрешение применять все более и более изощренные методы может вызвать обоюдную гонку технических средств, так что выигрыш в целом может оказаться весьма невелик (см. SOU 1988:46, с. 145). Вместе с тем, если измерять выигрыш даже не только соблюдением прав человека, но и доверием общества к полиции (а, в конечном счете, вероятно, и к остальным публичным властям), то он катастрофически сократится, ибо граждане понимают, что полиция будет использовать свои широкие полномочия для слежки за их частной жизнью.

Поэтому в далекой перспективе возможный урон способен обесценить выигрыш от раскрытия нескольких дополнительных преступлений.

Во-вторых, как показывает практика (см. раздел "Швеция" - прим. составителя), просьба о разрешении на тайный надзор, как правило, никогда не бывает отклонена или же это случается чрезвычайно редко. Это касается как, собственно, заявки на проведение надзора, так и последующего продления санкции. Одно из возможных объяснений состоит в том, что эти заявки всегда настолько хорошо обоснованы, что неизменно встречают поддержку. Такое объяснение выглядит странно, если учесть, что полиция не готова отчитаться ни об одном случае, когда бы надзор привел бы к вынесению приговора или хотя бы к возбуждению уголовного дела. Наоборот, красноречивым свидетельством является отсутствие такого отчета. При этом полиция заявляет - не предоставив никакой возможности реального контроля, - что надзор принес значительную пользу приблизительно в 50% предварительных розыскных мероприятий. Понимать это надо таким образом, что в 50% случаев, когда на более или менее обычных основаниях было дано и продлено разрешение проводить тайный надзор, например, прослушивание телефона, этот надзор не имел никакого значения даже для предварительных розыскных мероприятий. Следовательно, и иначе говоря, надзор не помог даже снять с поднадзорного лица имевшиеся относительно него подозрения. Таким образом, очевиден вывод, что создавшаяся ситуация рождает у судей и оперативных полицейских органов чувство общего интереса. Профессиональные суждения полицейских принимаются без серьезной критики; происходит так потому, что суд желает избежать возможного в будущем публичного скандала и нападок со стороны полиции и скорее склонен удовлетворить, чем отклонить, соответствующую заявку.

Разумеется, существует возможность, что Канцлер Юстиции или парламентский омбудсмен (они оба имеют право проявить инициативу и расследовать решения, санкционирующие тайный надзор) вынесут протест на любой сомнительный случай выдачи разрешений. При этом, однако, по сообщению парламентского омбудсмена, обе эти надзорные инстанции следят лишь за тем, чтобы суд, вынося решения, не нарушал установленной процедуры. В результате парламентский омбудсмен воздерживается от каких-либо критических заявлений по поводу использования судами действующего законодательства и трактовки ими бремени доказательства, когда речь идет о проведении полицией негласных мер (SOU 1998:46, с. 423).

Одна из главных причин такого положения, по-моему, в том, что никто не признает (да и могут ли?), что главной функцией негласного надзора является не изобличение преступника. Напротив, - это касается не только Полиции безопасности, но и всех криминальных ведомств - все тайные методы, такие как прослушивание телефонов, электронное прослушивание и т.п., удобны, чтобы установить само наличие преступления. Иными словами, то, что пытаются выяснить, невозможно конкретизировать на том этапе, когда подается формальная заявка на разрешение тайных мер - прослушивания, электронного прослушивания и т.п. Следовательно, это самые общие методы расследования, а не методы сбора улик против конкретного лица. Именно таким образом эти методы и применяются, так что юридическое одобрение со стороны суда превращается в пустую игру. Позволю себе подробнее остановиться на этом вопросе.

Основой правил шведского Правительственного Акта и Судебного процессуального кодекса является установка, что неприкосновенность личности приоритетна по отношению к раскрытию преступления. Меры, нарушающие неприкосновенность личности, могут, согласно законодательству, использоваться для раскрытия преступлений только в исключительных случаях. Решение о таких мерах должно всегда приниматься судом, и направлены они должны быть против тех, кого есть причины подозревать в уже совершенном преступлении (или, по крайней мере, в попытке его совершить или в сообщничестве). Этого, я уверен, отнюдь недостаточно, когда полиция ведет сыскную деятельность против организованной преступности, торговцев наркотиками и т.д., и недостаточно для Полиции безопасности: во всех этих случаях полицейские органы работают преимущественно до совершения преступления, а не задним числом. Цель телефонного прослушивания (или всякой иной принудительной меры) здесь в том, чтобы непредвзятым образом собрать информацию о лице, организации или событии с целью определить, каким образом будет вестись дальнейшее расследование. Естественно, прослушивание телефонов является одним из многих методов оперативно-розыскной деятельности. Но даже здесь прослушивание служит не столько сбору улик, сколько планированию действий.

Противоречие между целью телефонного прослушивания, как она определена в Судебном процессуальном кодексе (т.е. - поимкой преступников), и его удобством как средства предотвращать преступления породило такую тактику полиции, когда она представляет не все уже имеющиеся у нее материалы. "Из тактических соображений" может показаться разумным придержать какую-то информацию на месяц - ради того, чтобы суд продлил свою санкцию на прослушивание телефона.

В итоге суду каждый раз из всей собранной информации представляется лишь малая доля, на основании которой суд продлит санкцию.[48]

Здесь, возможно, таится одно из объяснений, почему суды, интуитивно чувствуя истинную цель этих мер, почти всегда удовлетворяют заявки на использование принудительных методов, даже если результат дает так мало для возбуждения уголовного дела и вынесения приговора лицам, подвергнутым прослушиванию по решению суда. Положение, хочу добавить, усугубляется тем, что отказавшийся выдать санкцию судья рискует впоследствии подвергнуться суровым нападкам, например, если террорист совершит нападение, которого можно было избежать благодаря прослушиванию телефона. С другой стороны, выдавая санкции на сотни тайных перехватов, судья совершенно ничем не рискует. В Швеции подвергнутое надзору лицо никогда не будет извещено об этом, независимо от того, осуществлялось ли подслушивание, прослушивание телефона и иные принудительные меры законным или незаконным образом.

Эту точку зрения разделяют ныне трое судей из так называемой Комиссии по подслушиванию. Они пишут: "В системе, где нет надзора, неизбежно в конечном счете, что лица, принимающие решения, приноравливаются к интересам друг друга и начинают придерживаться одних и тех же взглядов на уместность принудительных мер. Поэтому возрастает риск, что решение о таких мерах будет приниматься чисто автоматически" (SOU 1988:46, c. 518). Осмелюсь сказать - а в Норвегии это уже стало эмпирическим фактом (см. так называемый "Lund-report", Rapport till Stortinget 1995-96, n 15), - что главным образом именно по этой причине заявки на использование телефонного прослушивания почти никогда или никогда не отклоняются. То же самое, конечно, относится и к электронному прослушиванию и т.д. Естественно, опасность, что суд разрешит противозаконное электронное прослушивание, ничуть не меньше, чем в случае с прослушиванием телефонов.

Если же принять точку зрения полиции, что эти меры необходимы для успешной борьбы с преступностью - а уже, по-видимому, слишком поздно, чтобы повернуть дело вспять, - то необходимо, как представляется, признать, что эти меры являются опережающими и таковыми останутся в дальнейшем. Необходимо также признать, что суд не является и не может являться гарантией от злоупотреблений, как это предполагается ныне, и как всем хотелось бы предполагать. Единственным способом избежать злоупотреблений является прозрачность процедур: нужно ввести правила - как ввели Германия и Австрия, а также многие другие страны, - согласно которым поднадзорное лицо информируется о принятых мерах, когда перехват закончится. Это дает ему единственную возможность требовать возмещения ущерба, если против него применялись противозаконные принудительные меры. Если по таким делам будут проводиться судебные разбирательства, то власти, принимающие решение о принудительных мерах, будут нести свою ответственность. Полагаю, что при таком положении заявки будут рассматриваться более придирчиво, с большим чувством ответственности, с большим учетом прав человека и возможных нежелательных последствий в каждом отдельном случае. Вероятно, это единственный способ получить уверенность, что система соответствует требованиям Европейской Конвенции по правам человека.

Перевод Геннадия Зельдовича

## Контроль за информацией в электронных средствах коммуникаций

## РОССИЙСКАЯ ФЕДЕРАЦИЯ [49]

После введения в действие закона об ОРД в ФСБ и Министерстве связи приступили к реализации на предприятиях связи доступа к коммуникациям в порядке проведения оперативно-розыскных мероприятий. С этой целью был подписан приказ №226 от 24 июня 1992 г. (впоследствии он был дополнен и изменен приказом №112 от 13 сентября 1995 г.), согласно п.1 которого организациям и предприятиям связи предписывалось "обеспечить предоставление оперативно-техническим подразделениям Министерства безопасности возможности осуществления оперативно-розыскных мероприятий по контролю почтовых отправлений, прослушиванию телефонных и иных переговоров, снятию информации с технических каналов связи и оказывать им необходимое содействие". Приказ предписывает предоставление служебных помещений с необходимыми коммуникациями, линий, каналов, линейно-кабельных сооружений, выполнение необходимых проектных, научно-исследовательских и опытно-конструкторских работ и т.д. Во исполнение этого приказа были разработаны и утверждены Технические требования к системе технических средств по обеспечению функций оперативно-розыскных мероприятий на электронных АТС (СОРМ). Письмом

Минсвязи №252-у от 11 ноября 1994 г. был регламентирован порядок внедрения СОРМ на "электронных телефонных станциях, выпускаемых отечественной промышленностью и закупаемых за рубежом, устанавливаемых на сети связи общего пользования, а также на ведомственных и коммерческих сетях отечественного производства, входящих во Взаимоувязанную сеть России". Письмо обязывало согласовать мероприятия по внедрению СОРМ с региональными подразделениями Федеральной службы контрразведки (правопреемника Министерства безопасности). Согласно письму, требования СОРМ становятся "неотъемлемой частью лицензий на осуществление деятельности по связи при применении АТС".

Технические требования дают представление о характере и объемах контроля телефонных разговоров. Максимальное число номеров контролируемых абонентов на электронных АТС должно определяться из расчета 128 для станции емкостью 10000 номеров (при этом может контролироваться одновременно не более 28 абонентов), но не должно превышать 1024 при увеличении емкости станции до максимальной (при этом одновременно может контролироваться 168 абонентов). Для междугородной и международной связи СОРМ должна обеспечить одновременный контроль до 240 каналов (линий). Предусматривается две категории контроля - полный и статистический. При полном контроле на пульт управления правоохранительного органа передается в реальном масштабе времени информация о фазах установления соединений, номер телефонов вызывающего и вызываемого абонентов, время начала и конца разговора, а также съем и трансляция разговора. При статистическом контроле разговорный канал не подключается к пульту управления, а передаются только телефоны абонентов и время начала и конца разговора.

В 1998 г. в печати появились сообщения о проекте СОРМ-2, который распространяет контроль на электронные сети. Нормативными документами по СОРМ-2 мы почти не располагаем. Из доступных сообщений можно заключить, что СОРМ-2 предусматривает поставку каждым провайдером (фирмам, предоставляющим услуги по доступу к компьютерным сетям) в региональное отделение ФСБ оборудования, программного обеспечения, выделение и резервирование канала связи для обеспечения возможности ФСБ перехватывать сообщения любого клиента этого провайдера.

Каковы правовые основания для внедрения СОРМ-2? В соответствии со ст.14 Закона "О связи" все предприятия связи, независимо от ведомственной принадлежности и форм собственности, должны оказывать содействие органам, осуществляющим ОРД, в проведении оперативно-розыскных мероприятий на сетях связи. В соответствии со ст.6 Закона об ОРД перечень видов специальных технических средств, предназначенных для негласного получения информации в процессе осуществления ОРД, устанавливается правительством Российской Федерации. В лицензиях провайдеров всегда присутствовала фраза: "Сеть должна отвечать эксплуатационно-техническим требованиям по обеспечению и проведению оперативно-розыскных мероприятий в соответствии с Законом об ОРД". Таким образом, провайдеры как будто не могут противиться внедрению СОРМ-2. Сейчас Госсвязьнадзор переоформляет лицензии провайдеров, а сами они выполняют новые требования: дорабатывают программное обеспечение, обеспечивают региональное отделение ФСБ выделенной линией и компьютером. Причем осуществляют все эти мероприятия за собственные средства. Ведь согласно п.4 ст.5 Приложения к приказу Минсвязи №25 от 18.02.97 затраты на аппаратно-программные средства СОРМ и каналообразующую аппаратуру, а также оборудование пункта управления СОРМ финансируются за счет средств провайдеров, а линии (каналы) связи между станционным оборудованием СОРМ и пунктом управления СОРМ - при наличии технической возможности ФСБ - за ее счет, при отсутствии таковой - на договорной основе с провайдером в соответствии с действующим законодательством. При этом затраты на

оборудование пункта управления СОРМ ФСБ гарантирует возместить в срок, не превышающий одного года.

В то же время статья 19 Закона об ОРД ясно указывает, что финансирование ОРД осуществляется за счет средств государственного бюджета. Кроме того, на наш взгляд, решение о финансировании провайдерами таких мероприятий нарушает свободу предпринимательства и право частной собственности, защищаемые статьями 34 и 35 Конституции Российской Федерации. К тому же первая часть ст.34 о свободе предпринимательской деятельности не подлежит ограничению согласно ст. 56 Конституции. Поэтому практика выдавливания денег у провайдеров для финансирования работы ФСБ представляется незаконной и могла бы быть оспорена в Конституционном Суде. Однако провайдеры предпочитают не ссориться с органами власти, поскольку они в условиях российского бизнеса очень уязвимы и могут быть быстро разорены. Дополнительные расходы они неизбежно будут компенсировать за счет удорожания услуг, а это только будет замедлять и без того недостаточно быстрое развитие информационной среды в России.

Итак, права и интересы провайдеров грубо нарушены. Возникает и другой, не менее важный вопрос: не угрожает ли внедрение СОРМ-2 правам их клиентов? Заметим прежде всего, что, все, что было сказано выше о несовершенстве российского законодательства, регулирующего прослушивание телефонных разговоров, относится и к СОРМ-2. Далее, российское правозащитное сообщество убеждено в том, что СОРМ сводит на нет необходимость получения санкции в суде перед каждым снятием информации - мол, зачем: все готово, подключайся и снимай. Нам эти опасения представляются беспочвенными. На самом деле с прослушиванием телефонных разговоров та же ситуация, и это вопрос скорее общего доверия к правоохранительным органам, сам по себе СОРМ-2 здесь ни при чем. Проблема видится в ином. Интернет не знает государственных границ, и, перехватывая сообщения какого-либо гражданина России, органы ФСБ с неизбежностью будут вмешиваться в процесс его информационного обмена с гражданами иных государств, на перехват сообщений которых ФСБ, вообще говоря, права не имеет. Очевидно, законодательство нуждается в доработке. Следует также отметить, что провайдеры должны будут изъять из договоров с клиентами обязательство сохранять конфиденциальность сообщений клиента, поскольку клиент может обратиться в суд с иском о привлечении провайдера к ответственности, хотя съем информации мог быть проведен ФСБ, о чем ни клиент, ни провайдер просто могут не знать. Хорошим примером законодательного решения этих проблем может послужить немецкий закон о телекоммуникациях (см. Приложение).

## УКРАИНА[50]

Если в России речь идет о контроле содержания сообщений в электронных сетях, то в Украине можно наблюдать административное ограничение прежде всего самого доступа к сетям. Поэтому вопрос о контроле за информацией в электронных сетях должен быть рассмотрен сначала в более широком контексте контроля доступа к информации вообще.

Основными законодательными актами в области свободы информации являются Закон Украины "Об информации", принятый 2 октября 1992 г., Закон "О государственной тайне", принятый 21 января 1994 г. и "Перечень сведений, составляющих государственную тайну", утвержденный 3 августа 1995 г. Принятие Закона "Об информации" - безусловное достижение молодого государства. Этот закон еще до принятия Конституции гарантировал право на доступ к информации , определяя систему отношений и обязательств в этой области, принятую для демократического государства.

Удачным надо признать и Закон "О государственной тайне".Однако впоследствии эти достижения были во многом сведены на нет нормативными актами исполнительной власти.

Ст.34 Конституции Украины, принятой 28 июня 1996 г., гарантирует "право на свободу мысли и слова, на свободу выражения своих взглядов и убеждений". Каждому предоставляется "право свободно собирать, хранить, использовать и распространять информацию устно, письменно или другим способом по своему выбору. Осуществление этих прав может быть ограничено законом в интересах национальной безопасности, территориальной целостности либо общественного порядка с целью предупреждения беспорядков или преступлений, для охраны здоровья населения, для защиты репутации или прав других людей, для предупреждения разглашения информации, полученной конфиденциально, либо для поддержания авторитета и непредвзятости правосудия." Как видно, круг ограничений достаточно широк, однако каждое из них должно быть определено законом.

В первой части ст.17 Конституции Украины обеспечение информационной безопасности Украины объявлено "делом всего Украинского народа". Прокомментировать это положение весьма трудно, если только не считать делом всего Украинского народа препятствовать поползновениям государства нарушать право на информацию под видом защиты информационной безопасности.

В январе 1997 г. Верховная Рада одобрила "Концепцию (основы государственной политики) национальной безопасности Украины". В числе основных принципов ее обеспечения названы приоритет прав человека, верховенство права и демократический гражданский контроль за военной сферой и другими структурами в системе обеспечения национальной безопасности. Среди прочих возможных угроз национальной безопасности названы и угрозы в информационной сфере - "информационная экспансия со стороны других государств, утечка информации, составляющей государственную и другую, предусмотренную законом, тайну, а также конфиденциальной информации, являющейся собственностью государства". Среди основных направлений государственной политики национальной безопасности в информационной сфере обозначены принятие комплексных мер по защите своего информационного пространства и вхождению Украины в мировое информационное пространство; устранение негативных факторов нарушения информационного пространства, информационной экспансии со стороны других государств; разработка и внедрение необходимых средств и режимов получения, хранения, распространения и использования общественно значимой информации, создание развитой инфраструктуры в информационной сфере.

В апреле 1997 г. были проведены парламентские слушания "Свобода слова в Украине: состояние, проблемы, перспективы". В рекомендациях участников слушаний отмечено, в частности, что "Интернет может усилить угрозу для государственных тайн, личной конфиденциальной информации граждан и увеличить зависимость национального информационного пространства от зарубежной продукции, чужой информационной политики".

Осенью 1997 г. в нескольких газетных публикациях можно было прочесть, что Интернет составляет угрозу моральности населения и безопасности государства, что по электронным каналам распространяется порнография. Об Интернете как информационной среде, без которой сегодня невозможно существование страны, считающей себя цивилизованной, в статьях ничего не говорилось.

8 октября 1997 г. Кабинет Министров принял концепцию технической защиты информации (ТЗИ). ТЗИ определена в концепции как деятельность, направленная на обеспечение инженерно-техническими средствами порядка доступа, целостности и доступности (невозможности блокирования) информации, которая составляет государственную и иную предусмотренную законом тайну, конфиденциальной информации, а также целостности и доступности открытой информации, важной для личности, общества и государства. Это определение уточняет один из принципов формирования и проведения государственной политики в сфере ТЗИ: "обязательность защиты инженерно-техническими средствами информации, которая составляет государственную и иную предусмотренную законом тайну, конфиденциальной информации, являющейся собственностью государства, открытой информации, важной для государства, независимо от того, где указанная информация циркулирует, а также открытой информации, важной для общества и государства, если эта информация циркулирует в органах государственной власти и органах местного самоуправления, Национальной академии наук, Вооруженных Силах, иных военных формированиях, органах внутренних дел, на государственных предприятиях, в государственных учреждениях и организациях." Из понятий, упоминаемых в этом перечне, ясно определено законом только понятие государственной тайны. "Иная, предусмотренная законом тайна" на самом деле никаким законом Украины не определена. Неясным является понятие "конфиденциальной информации, являющейся собственностью государства": согласно ст.30 Закона "Об информации" конфиденциальная информация может быть собственностью только юридических и физических лиц, но не государства. Безнадежно размытым является понятие "открытой информации, важной для государства, независимо от того, где указанная информация циркулирует". Можно сделать вывод, что решения, какую информацию нужно защищать, будут принимать государственные служащие по своему разумению, и возможность произвола здесь ничем не ограничена. Концепция предполагает создание подразделений ТЗИ всюду, где необходимо защищать информацию. На наш взгляд, есть серьезные основания опасаться, что реализация этой Концепции существенно ограничит доступ к официальной информации.

4 февраля 1998 г. Верховной Радой был принят Закон "О Национальной программе информатизации", одной из двух главных целей которой заявлено обеспечение информационной безопасности государства, а генеральным государственным заказчиком которой является центральный орган исполнительной власти, определенный Кабинетом Министров. В тот же день была принята "Концепция Национальной программы информатизации", в которой важным фактором преодоления отставания Украины в области информатизации была названа государственная политика информатизации. Днем раньше был подписан Указ Президента о создании Комиссии по информационной безопасности. Ее руководитель, генерал-лейтенант СБУ Александр Белов, в своих публикациях неоднократно совершенно справедливо подчеркивал, что основной угрозой для информационной безопасности Украины является медленный качественный и количественный рост украинского сегмента Сети.

22 апреля 1998 г. Президент Украины Леонид Кучма подписал Указ №346/98 "О некоторых мерах по защите интересов государства в информационной сфере", предписывающий Госкомсвязи Украины обеспечить выход в заграничные сети передачи данных только через сети предприятий (операторов) "Укртелеком", "Укркосмос", "Инфоком", а всем министерствам, другим центральным и местным органам исполнительной власти, а также предприятиям, учреждениям и организациям, которые имеют в своем составе режимно-секретные подразделения (РСП), передавать данные через сети указанных предприятий (операторов).

На наш взгляд, Указ противоречит Конституции Украины и может быть оспорен в Конституционном суде: нарушается право свободно распространять информацию (ст.34). Нарушена также ст.10 Европейской Конвенции о правах человека, которую Украина обязана соблюдать. Грубо нарушается и ст.42 Конституции (свобода предпринимательской деятельности, недопущение злоупотреблений монопольным положением на рынке) и ряд статей Закона "Об ограничении монополизма и недопущении недобросовестной конкуренции в предпринимательской деятельности". Ибо требование пользования исключительно сетями "Укртелекома", "Укркосмоса" и "Инфокома" и есть ни что иное, как "навязывание таких условий договора, которые ставят контрагентов в неравные условия" (ст.4),"вытеснение с рынка или ограничение доступа на него продавцов, покупателей, других предпринимателей" (ст.5), "дискриминация предпринимателей органами власти и управления" (ст.6). И не спасает положение оговорка, что "законодательными актами Украины могут быть установлены исключения из положений ст.6 с целью обеспечения национальной безопасности, обороны, общественных интересов", потому что Указ - не законодательный акт.

Фактически Указ обеспечивает монополию на внешние каналы "Укртелекому", "Укркосмосу" и "Инфокому", и это при том, что цены на услуги у них и так непомерно высоки. К сожалению, Указ полностью соответствует государственной политике информатизации. Прочитав "Концепцию Национальной программы информатизации", легко убедиться, что государство намерено руководить процессом развития информационного рынка. Опасная для страны и пагубно самонадеянная тенденция! Информационный рынок должен быть защищен от монополии государства в первую очередь. Ведь и сейчас развитие Интернета сдерживается прежде всего монополией Укртелекома на каналы связи, цена аренды которых в 6-8 раз выше, чем в Чехии и США!

Вторая причина принятия Указа, на наш взгляд, - намерение контролировать информацию в электронных сетях. Эти соображения не покажутся беспочвенными, если прочесть статью председателя Госкомитета по охране государственных тайн и технической защите информации Павла Мысника в "Урядовом курьере" от 12 февраля 1998 г., в котором он, в частности, пишет:

"Информация в нынешнем мире ценится чрезвычайно высоко, ибо она является тем стартовым капиталом, который может обеспечить непредсказуемо большую отдачу в будущем. Тяжело наблюдать, как ныне растекаются, а иногда и совсем утрачиваются для нас возможности, заложенные в информации. В этом плане меня особенно беспокоит сбор научной информации. За достаточно скромные (в долларовом эквиваленте) гранты скупаются научные разработки и идеи наших исследователей. Тотальное собирание информации - не на пользу нашему государству, его будущему. Поэтому руководители Национальной академии наук, министерств и ведомств, в системе которых действуют научно-исследовательские институты, должны больше интересоваться, куда отплывает информация - крайне необходимая нашему государству, перспективная для его развития!".

Указ был подвергнут резкой критике как специалистами, так и общественностью и, возможно, поэтому пока не претворяется в жизнь.

27 ноября 1998 г. Кабинет Министров Украины утвердил Постановлением № 1893 "Инструкцию о порядке учета, хранения, сбережения и использования документов, дел, изданий и других материальных носителей информации, содержащих конфиденциальную информацию, которая является собственностью государства". По иронии судьбы эта Инстукция была опубликована в "Урядовом курьере" 10 декабря, в день 50-летия

принятия Всеобщей декларации прав человека. Эта Инструкция нарушает ст.34 Конституции, поскольку ограничения свободы информации устанавливаются законом. Понятие конфиденциальной информации, являющейся собственностью государства, нигде в законодательстве не определено, в ст.30 Закона "Об информации" органы государственной власти и местного самоуправления не упоминаются в качестве владельцев, распорядителей или пользователей конфиденциальной информации.

В соответствии с п.2 Постановления центральные и местные органы исполнительной власти и органы местного самоуправления должны разработать в шестимесячный срок и ввести в действие перечни конфиденциальной информации, являющейся собственностью государства, этой информации присваивается гриф "Для служебного пользования" (ДСП). Кто конкретно, исходя из каких критериев, решает, какие сведения являются конфиденциальными, а какие - нет, Инструкция не определяет. Будут ли доступны сами перечни, из Инструкции также не ясно, тем более, что каждое ведомство может иметь свой перечень. Однако ясно, что, согласно п.3 Постановления, выполнять Инструкции должны не только органы власти, но и предприятия, учреждения и организации независимо от форм собственности. Теперь опять в полную силу заработают РСП - печально известные первые отделы.

В перечни может войти не только информация, которая создается самим органом власти, но и информация, которая находится в его распоряжении и пользовании (п.1 Инструкции). Таким образом, любая информация, попавшая в государственный орган, может быть по желанию его руководителя объявлена конфиденциальной, о чем создатель этой информации может даже и не догадываться.

Согласно п.5 Инструкции, документы органов законодательной власти, высших органов исполнительной власти и судебной власти, вышедшие в свет в 1991 году и позже без грифа ограничения доступа, но не опубликованные в официальной печати, рассматриваются как материалы, содержащие сведения ограниченного распространения с грифом "ДСП".

Условия хранения, размножения и рассылки документов с грифом ДСП не менее жесткие, чем для документов, содержащих сведения, составляющие государственную тайну: регистрация и уничтожение всех черновиков и вариантов документов, запрет на обозначение фамилий и даже должностей руководителей организации и т.д. (п.п. 17-28 Инструкции).

Ознакомление представителей СМИ с документами с грифом ДСП разрешается только по письменному разрешению руководителя организации в каждом конкретном случае и только после рассмотрения этого вопроса экспертной комиссией, которая принимает письменное решение о целесообразности передачи документа журналисту. Только по письменному разрешению руководителя, подготовленному после письменного решения комиссии, сотрудники канцелярии, РСП и других структурных подразделений выдадут нужный документ. Представляется, что вероятность получения журналистом информации с грифом ДСП очень мала, тем более, что ответственность за разглашение конфиденциальной информации несет руководитель органа, ее выдавшего, а не журналист. Что такое экспертная комиссия, кто в нее входит, каков регламент ее работы - из текста Инструкции не ясно. Из текста Инструкции видно только, что в ее состав входят "сотрудники канцелярии, РСП и других структурных подразделений".

П.32 Инструкции предписывает дела с несекретными документами относить к категории с грифом ДСП, если среди документов, входящих в дело, хотя бы один документ имеет

гриф ДСП. Таким образом, может быть ограничен доступ фактически к любой информации.

О страхе органов власти перед свободным распространением информации ярко свидетельствуют п.п. 51 и 52 Инструкции, которыми предписывается документы, дела и издания с грифом ДСП, которые не имеют научную и историко-культурную ценность и утратили практическое значение, уничтожать, но перед этим в обязательном порядке измельчить так, чтобы их было невозможно прочесть.

Следует упомянуть также о законопроекте "Об информационном суверенитете и информационной безопасности Украины". К нему можно было бы отнестись как к курьезу, если бы он не прошел уже согласование во всех инстанциях и должен быть вынесен на рассмотрение Верховной Рады Украины. К сожалению, основная идея законопроекта, хотели того или нет его авторы,- государственная монополия на информацию и полное огосударствление информационной сферы. Так, осуществление информационного суверенитета включает в себя "законодательное определение и обеспечение государством стратегических направлений развития и защиты национального информационного пространства, целостной информационной политики" (ст.2), хотя кажется очевидным, что главная задача государства - поощрение многообразия информационных и политических позиций, поскольку решения должны приниматься на основе широкой общественной дискуссии. Казалось бы, государство должно было бы стремиться к разгосударствлению предприятий связи, чтобы ускорить развитие информационной сферы. В тексте же проекта, наоборот, "государство выступает гарантом целостности национального информационного пространства Украины на основе единой государственной политики, определенной законами, обязательными для всех участников информационной деятельности в национальном информационном пространстве Украины независимо от форм собственности и сохранения права собственности государства на ведущие объекты национального информационного пространства, использования ним (государством - прим. составителя) надлежащей базы и экономических рычагов для осуществления регулятивного влияния на общественные отношения в сфере информации" (ст.4). Через весь текст законопроекта красной нитью проходит идея защиты информационной безопасности, понимаемой как "защищенность жизненно важных интересов общества, государства и личности, которой (защищенностью - прим. составителя) исключается причинение им ущерба из-за неполноты, несвоевременности и недостоверности информации, из-за негативных последствий функционирования информационных технологий или вследствие распространения информации, запрещенной или ограниченной для распространения законами Украины" (ст.3). Обращает на себя внимание то, что впереди опять-таки государство, а не личность, и то, что государство берет на себя смелость определять, какая информация является "недостоверной" либо "искаженной" и потому ее надо запретить для распространения. Законопроект вводит понятие "национальных информационных ресурсов исключительно государственного значения" (ст.10), к которым относятся такие информационные ресурсы, которые "могут существенно влиять на состояние национальной безопасности Украины... и на ее информационный суверенитет". Законопроект предполагает выкуп таких ресурсов, если они созданы "вне государственной собственности", у юридических и физических лиц, а собственник таких невыкупленных государством ресурсов "обязан обеспечить их охрану и сохранение и может распоряжаться ими только с учетом положений, установленных законами Украины". Остается только удивляться, как могли ведомства согласовать этот законопроект.

14 декабря 1998 г. был подписан Указ Президента Украины "О мерах по усилению контроля за разработкой, изготовлением и реализацией технических средств негласного

получения информации", в котором устанавливается, что разработка, изготовление и реализация специальных технических средств (в том числе иностранного производства) для снятия информации с каналов связи, других средств негласного получения информации возможны только при наличии лицензии, выданной в порядке, предусмотренном ст.4 Закона Украины "О предпринимательстве". А в середине января 1999 г. Верховная Рада приняла дополнение к этому Закону, устанавливающее, что лицензии выдает СБУ. В интервью, данном газете "День" зам. начальника СБУ генерал-лейтенантом Владимиром Пристайко по этому вопросу, он сказал, что такие предложения СБУ давало еще в 1991 году, однако они не были учтены. В 1994 году дополнения, аналогичные нынешним, были приняты и до декабря 1997 г. СБУ выдавало такие лицензии, однако потом лицензирование было отменено и СБУ вновь добилось права выдавать лицензии, поскольку масштабы использования тайной слежки негосударственными структурами становятся все больше, и притом эти деяния практически остаются безнаказанными. Еще в 1996 г. СБУ был подан законопроект об административной и уголовной ответственности за незаконное использование технических средств негласного получения информации, однако до сих пор он Верховной Радой не рассмотрен. Лицензирование также необходимо для проведения СБУ экспертизы разрабатываемых средств, потому что могут быть придуманы такие волны, которые будут угнетать волю человека и вредить его здоровью.

27 июня 1999 г. был подписан Указ №737/99 "О лицензировании отдельных видов предпринимательской деятельности", в котором с целью защиты интересов государства в сфере связи устанавливалось, что деятельность, связанная с оказанием услуг по передаче данных в сетях общего пользования может осуществляться только при наличии лицензии, а одним из лицензионных условий оказания услуг телефонной связи и услуг по передаче данных в сетях является "укомплектование субъектом предпринимательской деятельности - оператором связи системы связи, функционирование которой он обеспечивает, специальными техническими средствами для снятия информации с каналов связи". Представляется очевидным, что это означает начало внедрения проекта, аналогичного российской СОРМ-2. И так же, как и в России, затраты на его реализацию органы власти начинают перекладывать на провайдеров. Можно ли надеяться на то, что СБУ будет так же, как все клиенты, оплачивать предоставление услуг по реализации необходимых оперативно-розыскных мероприятий? Будут ли произведены подсчеты, насколько дорогим окажется этот проект, как он скажется на развитии информационной среды в Украине? Жизнь постепенно ответит на эти вопросы. Хотелось бы надеяться, что перед принятием решений по этим принципиально важным для будущего страны проблемам они будут публично обсуждаться.

## МЕЖКОНТИНЕНТАЛЬНЫЙ ПРОЕКТ: СИСТЕМА "ECHELON"

СИСТЕМА "ECHELON" И КУЛЬТ(УРА) ЭЛЕКТРОННОГО ПОДСЛУШИВАНИЯ[51]

Мэтью В.Бил (Matthew W. Beale)

"Господу мы себя вверяем, а остальных проверяем". Типичная навязчивая, почти юмористическая фраза из суперкрутого научно-фантастического романа, не правда ли? На самом деле эта звонкая завлекалочка приветствует посетителей одного популярного сервера, представляющего в Интернете организацию, торгующую средствами электронного наблюдения. Причем клиентами этой организации являются отнюдь не полиция и не разведывательные органы.

Как свидетельствует присутствие шпионской литературы в торговых центрах, на лотках и в Интернете, интерес потребительского рынка к электронному шпионажу в самом разгаре. Откуда же взялось столь явное неуважение к частной жизни? Кто же повлиял - прямо или косвенно - на наше отношение? Отвечая на подобные вопросы, пожалуй, нужно начать с Агентства национальной безопасности США, которое активно фигурирует в бесчисленных конспирологических теориях.

Как утверждается в одном из номеров 1977 года ежеквартального информационного бюллетеня "Каверт экшн" (Covert Action), а также в целом ряде других отчаянных изданий, США, прежде всего через Агентство национальной безопасности, в сотрудничестве с Великобританией, Канадой, Австралией и Новой Зеландией занимается созданием всемирной сети перехвата и анализа всех электронных средств связи - телефона, факса, электронной почты, телекса, сотовой телефонной связи. Некоторые называют "Echelon" - таково кодовое название этого колоссального проекта - величайшим достижением США современной эпохи технической "революции".

Система "Echelon" состоит из следующих элементов. Прежде всего это спутники слежения, расположенные на геостационарной орбите, которые держат под колпаком немыслимое количество электронных средств связи. Затем - суперкомпьютеры, способные, говорят, анализировать в день по три миллиарда сообщений. Кроме того, в системе имеются передающие станции, принадлежащие соответствующим организациям стран-участниц, таким как австралийский Defense Signals Directorate, новозеландское Government Communications Security Bureau и канадское Communications Security Establishment. Эти точки подслушивания перехватывают, записывают и декодируют сообщения, пропуская всю информацию через так называемые "Словари Echelona" - компьютеры, содержащие постоянно обновляемые списки ключевых слов.

Так, например, электронные письма, содержащие слова "порно", "героин" или "бомба", могут пометить и сохранить по крайней мере в пяти международных центрах. К сожалению, взамен вы не получите официального сообщения: "поздравляем, на вас заведен файл". Шутка.

Все это может показаться надуманным, неким параноидальным кошмаром, навеянным недавно появившимся фильмом "Враг государства" (Enemy of the State). В СМИ была большая шумиха о возможности реального существования суперсовременной технологии слежения, изображенной в этом блокбастере (авторы которого подарили нам такие прекрасные фильмы, как Top Gun, сериал Beverly Hills Cop, The Rock, Crimson Tide), в котором рассказывается, как невинный человек вынужден скрываться, потому что его объявили угрозой "национальной безопасности" США. Несмотря на наличие типичных для Голливуда случаев "искажения реальности", многие из крутых шпионских игрушек, показанных в фильме, основываются на технологиях, которые либо уже существуют, либо вот-вот возникнут. Система "Echelon" - наглядный пример последних.

Рассмотрим подробнее, как работает эта система. Например, она захватывает трафик в Интернете на уровне TCP/IP. Для сканирования данных аналоговой передачи, таких как телефонный звонок, используется технология автоматического распознавания голоса. Но кто же является объектом этих операций?

Насколько известно, система "Echelon" работает не так, как другие системы электронного слежения, разработанные в эпоху холодной войны. Эта система направлена не на военные цели, а в основном на правительственные, производственно-коммерческие и, что звучит уже более двусмысленно, на иные организации. Несмотря на то, что с окончанием

холодной войны шпионаж имел тенденцию сосредотачиваться почти исключительно на промышленной и торговой сфере, потребности борьбы с терроризмом, если взять всего лишь один пример, существенно расширяют круг потенциальных объектов слежки, включая в него рядовых граждан.

И вот здесь в нашей истории, естественно, появляются - и слава Богу! - наши борцы за гражданские права и начинают отстаивать упоминавшееся выше право на неприкосновенность частной жизни. Существуют законы, в том числе в США, защищающие граждан от необоснованного или несанкционированного прослушивания их телефонных разговоров и других посягательств на индивидуальные свободы. Однако тот факт, что в настоящее время электронное слежение приобрело международные масштабы, несколько затемняет вопрос и создает возможности для злоупотреблений. Ведь не существует законов, запрещающих Агентству национальной безопасности прослушивать разговоры, скажем, британских граждан. Точно так же отсутствие соответствующего законодательства позволяет иностранным службам шпионить за американцами.

Осенью 1998 года, когда конгресс США под сурдинку принял закон, разрешающий Федеральному бюро расследований (ФБР) заниматься роуминговым прослушиванием, зона возможного произвола в отношении американских граждан еще более расширилась. В соответствии с Intelligence Authorization Act Conference Report (H.R. 3694), который приняли без открытых слушаний, за закрытыми дверями, включив в него весьма спорные положения, ранее отвергавшиеся конгрессом, - ФБР разрешается прослушивать любые телефоны в окружении подозреваемого, будь то домашние, платные, общественные и проч.

Это решение - только один пример "социального заказа" ФБР, который был практически неукоснительно исполнен законодателями. Кроме того, теперь закон обязывает телефонные компании и Интернет-провайдеров предоставлять ФБР информацию о своих клиентах. Очевидно, что отсюда - лишь один шаг до того полномасштабного электронного шпионажа, о котором мы говорили выше. Но конгрессменам следовало бы помнить народную мудрость: "Не рой другому яму, сам в нее попадешь".

Вернемся к фильму "Враг государства". Случайно или нет, цитата, с которой начинается данная статья, взята с информационного сервера Стива Урига, который, кстати, являлся техническим консультантом фильма. Напомним, что именно он рекламирует продукцию своей компании широкой публике. Это к вопросу о дистанции между Голливудом и реальностью.

Утрата определенных прав во имя троянского коня национальной безопасности - далеко не единственная угроза, которой подвергаются граждане. Одна из самых оживленных незатухающих дискуссий по проблемам Интернета связана с вопросом права на конфиденциальность и неприкосновенность частной жизни. Достаточно посмотреть наугад заголовки в американской прессе, чтобы убедиться в этом.

Когда корпорация "Интел" представила свой новый микропроцессор "Pentium III", его встретили без того единодушного энтузиазма и бравурной музыки, которым обычно пресса встречала новые технические достижения. Целый ряд журналистов резко выступили против появления Pentium III на рынке. Более того, такие организации, как Американский союз защиты гражданских свобод (American Civil Liberties Union), Информационный центр электронной конфиденциальности (Electronic Privacy Information Center), Прайвэси интернейшнл (Privacy International) и Junkbusters, призвали бойкотировать корпорацию "Интел". Что же вызвало такую реакцию?

Дело в том, что "Интел" планировала оснастить каждый микропроцессор идентификационным серийным номером, который легко считывается, когда пользователь входит в режим online. "Интел" утверждает, что такое решение может, в частности, способствовать безопасности электронной коммерции. Благодетели наши! Скорее всего, это обезопасит сетевое сообщество лишь от самых неискушенных хакеров. Профессионалы сетевого преступного мира легко найдут средства преодолеть это незначительное препятствие.

Проблема здесь, конечно, заключается в том, что, получая возможность считывать идентификационный номер, милые ребята, подвизающиеся на несколько одиозном поприще маркетинга, не говоря уже о правительственных агентствах, смогут отслеживать онлайновую деятельность пользователей и с легкостью составлять профили и досье на основе этой информации. И это, как очевидно, только начало.

Согласно Марку Ротенбергу, директору Информационного центра электронной конфиденциальности (EPIC), для отмены бойкота "Интел" должна была выполнить два условия. Во-первых, на будущих процессорах "Pentium III" не должно быть серийных номеров. Во-вторых, заключение соглашения об отзыве всех уже поставленных процессоров с серийными номерами. В результате "Интел" дала согласие на компромиссный вариант - поставку микропроцессоров с отключенными серийными номерами. Более подробную информацию о деятельности групп в защиту неприкосновенности частной жизни можно получить на сервере http://www.privacy.org/bigbrotherinside/.

Но и без таких технологий идентификации, как чип Pentium III, онлайновая конфиденциальность уже сейчас - вещь практически не встречающаяся. Говоря по-простому, в наши дни это редкость. Вспомните об этом, когда в следующий раз вам захочется посочувствовать любимой поп-звезде, жалующейся на отсутствие частной жизни. Их заботы, в определенном смысле, имеют прямое отношение и к вам.

Существуют и другие достойные упоминания дискуссии по вопросам электронного шпионажа и охраны сферы частной жизни - например, о шифровальной технологии и инициативах Clipper Chip. Шифровальная технология, ранее являвшаяся привилегией немногих избранных, в основном тех, кто связан с разведывательной деятельностью, в семидесятые годы стала доступна широкой общественности. А с пришествием Интернета в его нынешней инкарнации потребность в этой технологии и стремление ею обладать стали расти в геометрической прогрессии. Правительство США настаивает на принятии технологии Clipper Chip - шифровального средства, которое, как оно надеется, станет общепринятой технологией. Что ему это даст? Беспрепятственный доступ к шифровальным ключам, что позволит получать любую информацию, которую оно пожелает. Более подробно о Clipper Chip и шифровальной технологии можно узнать на сервере http://courses.ncsu.edu/CSC379/readings/encryption/endex.html.

Таким образом, идет ли речь об электронной слежке одних за другими, или о шпионаже за ними со стороны третьих сил, существует темная и малоизвестная сторона этой фантастической эры информации.

Как замечают некоторые специалисты, перехват информации, которую можно перехватить, - то есть практически любой информации - это "честная игра". Я не буду сейчас перечислять всех этих вещей, чтобы не способствовать развитию паранойи (хотя великий Уильям С.Берроуз, ныне покойный, однажды заметил, что параноик - это всего лишь человек, которому известны факты). Я просто хочу призвать вас научиться

критически относиться к восторженной трескотне, умело производимой PR-отделами компаний высоких технологий, видеть за ней реальность и не бояться формулировать неприятные вопросы, к которым подводит данная статья.

Перевод с английского Татьяны Чернышевой

## НАЦИОНАЛЬНАЯ БЕЗОПАСНОСТЬ И СИСТЕМА ECHELON[52]

Вскоре после окончания Второй мировой войны в 1947 году правительства Соединенных Штатов, Соединенного Королевства, Канады, Австралии и Новой Зеландии подписали пакт, известный как "Quadripartite", или соглашение "Соединенное Королевство - Соединенные Штаты" (UKUSA). Они намеревались установить договоренности о том, каким образом можно достичь общих интересов в области национальной безопасности. Этим соглашением пять государств поделили планету на пять сфер влияния, и для каждой страны были определены специальные цели. Соглашением UKUSA предусмотрена стандартизация терминологии, кодированных слов, процедур перехвата информации, мероприятия по сотрудничеству, обмен информацией и доступ к средствам обслуживания. Важной частью соглашения был обмен информацией и персоналом. Благодаря этому оперативные работники специальных служб связи Новой Зеландии GCSD имеют возможность использовать в Канберре инструменты Австралийского Директората защиты связи для контроля за местными средствами коммуникаций и передавать результаты работы спецслужбам Австралии. И ни одно из этих государств не обязано формально давать согласие или сообщать о перехвате информации.

Наиболее тесные связи в границах пакта UKUSA установлены между Агентством национальной безопасности США (NSA) и Британским штабом правительственной связи (GCHQ). Штаб этого альянса расположен в Менвис Хилл (Menwith Hill) на севере Англии. База с двумя дюжинами антенн и широкими возможностями компьютерных средств предусматривает возможности для подслушивания широкого спектра способов коммуникаций. С появлением системы INTELSAT и цифровой телесвязи в Менвисе и на других станциях развиты возможности для снятия информации с широкого спектра средств коммуникаций: факсимильная телексная связь, звуковые сообщения. Широко распространено предположение, что Менвис Хилл имеет 40 000 каналов, которые обеспечивают доступ к большинству европейских и советских сетей коммуникаций.

В отчете Европейского парламента, опубликованном в конце 1997 года, подтверждается, что "Проект "Echelon" дает возможность NSA осуществлять поиск практически во всех информационных сетях с помощью "ключевых слов". Содержание сообщений не анализируется постоянно и не просматривается в режиме реального времени, однако ежедневные доклады предоставляют информацию, которая помогает спецслужбам определять цели для своей дальнейшей деятельности. Автоматический контроль звуковых способов коммуникации может быть не за горами. Система распознавания голоса "Oratory" уже несколько лет используется для перехвата и анализа дипломатических телефонных разговоров. В отчете "Оценка технологий политического контроля" сказано: "По всей Европе все средства телефонной и факсимильной связи, а также сообщения электронной почты регулярно перехватываются Агентством национальной безопасности Соединенных Штатов, при этом определенная информация передается с континента на стратегический узел в Лондоне, потом с помощью спутника в Форт Мед (Fort Meade) в Мериленде через важный узел в Менвис Хилл, что вблизи Северного Йорка в Соединенном Королевстве". Отчет вызвал волну обеспокоенности, которая привела к обсуждению этой проблемы в Европейском парламенте 14 сентября 1998 года. В "компромиссном решении", выработанном в этот день четырьмя главными сторонами,

содержится призыв к более сильному контролю за деятельностью специальных служб и использованию "средств защиты" от их произвола.

Перевод с английского Романа Романова

## СОЕДИНЕННЫЕ ШТАТЫ АМЕРИКИ[53]

### CALEA - ЗАКОН О СОДЕЙСТВИИ ПРАВООХРАНИТЕЛЬНЫМ ОРГАНАМ В ОБЛАСТИ КОММУНИКАЦИЙ

CALEA (Communications Assistance for Law Enforcement Act) иногда называют законом о "цифровой телефонии". CALEA вырос в 1994 году из идеи, в соответствии с которой правоохранительные структуры сохраняли возможности слежки в условиях развития коммуникационных технологий.

С того времени, как Конгресс принял CALEA, Федеральное бюро расследований пробовало использовать этот закон, чтобы закрепить возможности слежки в национальных системах связи. Телефонные компании уступили некоторым требованиям, но воспротивились остальным. В апреле 1998 года Центр демократии и технологии составил обращение в Федеральную комиссию по связи (Federal Communications Commission, FCC); Комиссия, в свою очередь, подала запрос в ФБР, чтобы выяснить, собирается ли эта спецслужба пойти дальше, чем определено законом, по пути вторжения в частную жизнь граждан.

В октябре 1998 года Комиссия в порядке эксперимента согласилась с большинством предложений ФБР, включая интеграцию следящих устройств в сотовые и другие беспроводные телефоны. В то же время Комиссия составила запрос по поводу слежки в сетях с пакетной передачей данных (в т.ч. Интернет - прим. перев.).В сентябре 1998 года Комиссия по связи отложила введение CALEA в действие на 20 месяцев - до июня 2000 года.

### ФБР ИСПОЛЬЗУЕТ CALEA, ЧТОБЫ РАСШИРИТЬ ВОЗМОЖНОСТИ "ПРОСЛУШИВАНИЯ" КОММУНИКАЦИЙ

Хотя вначале речь шла о том, чтобы новые технологии цифровой телефонии не становились препятствием для оперативно-розыскных мероприятий, впоследствии все свелось к попыткам ФБР использовать эти технологии для расширения собственных возможностей слежки.

История этого закона показывает, что Конгресс намеревался предоставить телефонным компаниям преимущественное право решать, каким образом встраивать механизмы слежки в свои сети. Несмотря на это четкое намерение, ФБР в 1996-1997 годах пыталось полностью контролировать процесс внедрения CALEA. При этом ФБР требовало от компаний использовать устройства с такими характеристиками, чтобы спецслужбы получали еще более широкие возможности для слежки, чем раньше. Под давлением ФБР компании беспроводной телефонии согласились внедрить системы прослушивания сотовых телефонов. Бизнесмены также уступили требованию, чтобы операторы связи, использующие популярные протоколы "коммутации пакетов данных", передавали правительству полностью содержание коммуникаций своих клиентов - даже в том случае, если органы имеют решение суда только на перехват наименее "чувствительных" данных ("кто кому звонит").

Несмотря на уступки, ФБР по-прежнему чувствует себя неудовлетворенным этим компромиссным планом. В марте 1998 г. ФБР направило свое собственное обращение в Федеральную Комиссию по связи, перечисляя дополнительные нужды. В частности, речь шла о возможности продолжать прослушивание разговора с участием нескольких человек после того, как объект наблюдения повесил трубку; собирать данные об участниках разговора, даже если они не являются объектами наблюдения; идентифицировать телефонные номера, набираемые после звонка.

В июле 1998 года организации, защищающие право на неприкосновенность частной жизни, обратились в Федеральную Комиссию по связи с просьбой обуздать требования ФБР в рамках CALEA. В ответ ФБР распространило на Капитолийском холме письмо с предложением переделать CALEA таким образом, чтобы учесть все свои предложения, включая возможность точного определения местонахождения владельца сотового телефона, а также не подвергать CALEA общественному обсуждению. Центр демократии и технологии призвал Комиссию отвергнуть предложение ФБР, что и было сделано.

Однако в октябре 1998 года Федеральная комиссия по связи в порядке эксперимента согласилась с предложениями ФБР, в том числе с возможностью определения местонахождения хозяина беспроводного телефона. Комиссия согласна, что упомянутые положения должны быть включены в CALEA.

Источник: Центр развития демократии и технологии (http://www.cdt.org)

НОВАЯ КРИТИКА В АДРЕС MICROSOFT

Американская фирма Microsoft вновь подверглась критике в связи с защищенностью производимого ею программного обеспечения. По утверждению экспертов, операционная система Windows, установленная на более чем 90% компьютеров планеты, содержит секретный код, который позволяет Агенству Соединенных Штатов по национальной безопасности проникнуть в любой созданный в системе Windows файл. Microsoft утверждает, что код этот вполне безобидный и является лишь стирающим устройством, разрешение на экспорт которого должно было быть получено от Агенства по национальной безопасности. В начале сентября компания временно сняла с пользования свою систему электронной почты Hotmail, после того, как она была взломана хакерами.

Русская служба Би-Би-Си

## ЕВРОПЕЙСКИЙ СОЮЗ[54]

ЕВРОПЕЙСКИЙ СОЮЗ СПЕЦСЛУЖБ ИЛИ ЧТО НАМ ИЗВЕСТНО ОБ ENFOPOL[55]

После серии статей наших корреспондентов Эриха Мохеля и Кристианы Шульцки-Хаддути о далеко идущих планах Европейского союза по установлению контроля за телекоммуникациями, Telepolis разместил на своем сервере первый вариант проекта ENFOPOL. Далее изложены основные моменты статей и отчетов, написанных Эрихом и Кристианой.

Проект ENFOPOL нацелен на все виды телекоммуникаций, включая компьютерные данные (обычные или шифрованные) и мобильную телефонию (в том числе новую систему "Иридиум" и другие спутниковые системы). Реализация этого плана означает установку слежки за любым видом связи без исключения. Поскольку сегодня данные между странами передаются очень быстро, ENFOPOL стремится избежать проблем с

"нестыковками" в национальных законодательствах и подразумевает контроль за центральной базой проекта Iridium в Италии. Однако, среди возможных источников информации для европейских полицейских структур называются и компании, предоставляющие международные каналы связи.

Представители Iridium пока не сказали ничего существенного о новом проекте, если не считать заверений, что Iridium будет подчиняться законам всех стран, где действуют его операторы. Сотрудник крупной международной компании довольно жестко заявил, что его фирма будет игнорировать такие предложения. Нашему журналу, впрочем, пока неизвестны случаи обращения такого рода со стороны спецслужб.

Надо отметить, что ENFOPOL (в отличие от проекта ECHELON) - не установившийся порядок, а проект системы сотрудничества между полицейскими силами разных стран. Однако, ENFOPOL вовсе не является чем-то, оторванным от реальности. Многие из его параграфов и даже стиль изложения напоминают последние законопроекты, обнародованные (или уже действующие) в Германии и Австрии. Там законопроекты требовали от провайдеров Интернет предоставить правоохранительным органам возможность получать доступ к персональной информации пользователей. Правительства были вынуждены смягчить формулировки после того, как проекты подверглись жесткой критике со стороны общественности и лоббистских групп (в основном представлявших интересы провайдеров Интернет и телефонных компаний). Сходство проекта ENFOPOL с законодательными инициативами Германии и Австрии означает, что руководители полиции европейских стран пытаются создать гармоничную систему законов по контролю за Интернет в европейском масштабе.

Подтверждением этой точки зрения служит и статья в лондонской "Санди Таймс". Автор утверждает, что идея создания общеевропейской полицейской службы поддерживается рядом европейских политиков. В частности, один немецкий чиновник заявил, что Германия стремится к более тесному политическому сотрудничеству, и что совместная работа полиции, безусловно, является достижением на этом пути. Министр иностранных дел Германии Йошка Фишер сказал, что, по его мнению, будущей Европе нужна общая внешняя политика.

Но Евросоюз не одинок в своих стараниях. На слушаниях в Европарламенте в сентябре 1998 г. всплыли факты сотрудничества между ЕС и ФБР, цель которых - построение глобальной системы контроля за телекоммуникациями. Проект ENFOPOL нужно рассматривать именно в этом контексте. Если он получит зеленый свет, это означает не только всемогущество спецслужб, но и законодательное признание существующих систем слежки, таких как ECHELON.

Полиция часто ссылается на то, что она "не успевает" за организованной преступностью и терроризмом в условиях развития высоких технологий и при открытых границах. Однако, сами полицейские ничуть не лучше: если следовать их логике, граждане лишаются права на неприкосновенность частной жизни. Более того, методы слежки приводят к мысли о медленном возвращении к образу мышления "Большого Брата". Политики и общественные деятели принимают решения на высоком уровне, в отрыве от общества. Тем временем в самом обществе вполне открыто продолжается обсуждение проблемы. Со стороны кажется, что эти процессы не имеют отношения к реальной жизни. Официальные лица стараются уделять ENFOPOL как можно меньше внимания. Технические описания мало что говорят большинству простых людей. Написанные на языке крупных телефонных и спутниковых компаний, провайдеров Интернет, - тех, кто в основном

оказывает услуги другим фирмам, - они почти всегда непонятны обычному пользователю Сети.

Требования ENFOPOL, регламентирующие контроль за коммуникациями, не могут быть реализованы без серьезного вмешательства в работу действующих коммерческих систем. Не стоит преждевременно обвинять коммерсантов в нарушении права своих клиентов на неприкосновенность частной жизни. Но если это нарушение станет частью общеевропейской законодательной системы, думается, компании вряд ли 6удут выступать в качестве защитников гражданских прав. Нет ничего, что свидетельствовало бы об их решительном духе в этой области, - по крайней мере, пока речь не идет о бизнесе. (Так, немецкие провайдеры воспротивились введению нового закона потому, что на них ложились все расходы по его реализации).

Вероятно, лучшая возможность приподнять завесу секретности - начать общественное обсуждение проблемы. Поэтому мы решили обнародовать на нашем сервере первоначальный вариант проекта ENFOPOL от 3 сентября 1998 г. Мы будем обновлять информацию по мере поступления новых документов по ENFOPOL.

ENFOPOL В 1998 ГОДУ АМЕРИКАНЦЫ НАЖИМАЮТ НА КНОПКИ РУКАМИ ЕВРОПЕЙСКИХ ПОЛИЦЕЙСКИХ[56]

Наконец, и в Лондоне узнали о последнем варианте проекта ENFOPOL 98. Судя по имеющейся информации, хотя название ключевого документа и было изменено, чиновники из ЕС по прежнему намерены проголосовать за проект до конца мая. Они стараются ускорить этот процесс, несмотря на сильное противодействие общественности в Германии и Австрии и недавнюю отрицательную реакцию Европарламента.

Новый документ называется ENFOPOL 19. Он был получен на этой неделе Каспером Боуденом из Лондонского Фонда исследований информационной политики.

Говорится, что ENFOPOL 19 появился на свет во время встречи руководителей полиции в Брюсселе 11 марта и был опубликован 15 марта. Британское правительство заявило в связи с этим: "Германия, которая председательствует в ЕС, надеется, что проект получит одобрение Совета по юридическим и внутренним вопросам в мае". Совет будет заседать 27-28 мая.

ENFOPOL 19 по-прежнему вызывает озабоченность своей целью "перехвата телекоммуникаций с учетом развития новых технологий". Однако, теперь вместо подробного и полного описания требований слежки за Интернет и другими коммуникациями, полиция делает вид, что ничего нового вообще не происходит.

Со ссылкой на первый документ ЕС о контроле за коммуникациями 1995 года, авторы ENFOPOL 19 говорят, что "нужды правоохранительных органов... должны быть учтены как в существующих, так и в новых коммуникационных технологиях, в частности, спутниковых коммуникациях и Интернет". Таким образом, согласно ENFOPOL 19 "технические требования" 1995 года "должны интерпретироваться... для применения к Интернет, статической и динамической IP-адресации, номерам кредитных карточек, адресам e-mail". В самом деле, документ 1995 года ничего не говорил о кредитных карточках и их применении для контроля за телекоммуникациями.

В новом документе подчеркивается, что для "прослушивания" Интернет необязательно собирать данные об отправителе и получателе, так как они включены в каждый "пакет

данных" или IP-пакет. Таким образом, специального регулирования для Интернет не потребуется.

Но это обманный маневр. Последующие варианты проекта ENFOPOL 98 показали, что первоначальный, полный противоречий план, обнародованный журналом Telepolis, был расчленен минимум на пять частей, которые теперь рассматриваются отдельно друг от друга.

Планы контроля за проектом Iridium и другими спутниковыми системами связи выделены в отдельный блок и обсуждаются на самом высоком уровне в ЕС.

Часть проекта ENFOPOL 98, где речь идет о сборе персональных данных граждан, будет включена в "другие резолюции Совета".

Предполагается, что еще одна резолюция потребует от провайдеров Интернет установить у себя в офисах высокоскоростные системы связи. Эти "системы перехвата" будут установлены в зоне особой секретности, куда будут иметь доступ только специально отобранные и проверенные сотрудники. Это предложение не входит в ENFOPOL 19.

Если следовать ENFOPOL 19, некоторые контролирующие системы будут управляться через "виртуальный интерфейс". По сути это означает установку специального программного обеспечения в точках доступа к Интернет, контролируемого правительственными спецслужбами.

Нововведения, касающиеся криптографии, тоже будут рассматриваться отдельно.

Правоохранительные органы рассчитывают, что предыдущие и новые резолюции сформируют вместе единый пакет, снабженный подробными инструкциями по перехвату сообщений Интернет. Пакет будет включать "технические описания", взятые из первоначального проекта ENFOPOL 98. Если этот трюк удастся, ENFOPOL 98 может миновать проверку и "пройти" частями, пока Европарламент будет находиться в невесомости в связи с июньскими выборами.

Но самый главный секрет ENFOPOL 98 до сих пор не был раскрыт. Сей противоречивый текст вовсе не был написан европейскими чиновниками. И ENFOPOL 98, и документ 1995 года были составлены группой под названием ILETS, состоящей из представителей спецслужб и правоохранительных органов разных стран при доминирующей роли США. В ILETS не входит никто из деловых, правозащитных или юридических кругов, компетентных в вопросах права на неприкосновенность частной жизни.

Последние шесть лет группа ILETS лоббирует свои "рекомендации" в европейских правительствах, превращая их таким образом в законы, новые сети и системы связи. Их деятельность никогда не освещается в национальных законодательных собраниях, Европарламенте и даже в Конгрессе США.

До того момента, как Telepolis обнародовал ENFOPOL 98, деятельность ILETS оставалась в тени.

ЕВРОПА ГОЛОСУЕТ ЗА СИСТЕМУ ШПИОНАЖА[57]

Европейские провайдеры Интернет на этой неделе выразили свое возмущение: Европарламент проголосовал за проект, обязывающий провайдеров и телефонные

компании предоставлять правоохранительным органам полномасштабный доступ к Интернет в реальном времени.

В прошлую пятницу Европейский парламент принял резолюцию о законном перехвате связи в области новых технологий (известный также как ENFOPOL), которая наложила дополнительные обязательства на провайдеров Интернет и других операторов связи. Эти обязательства включают установку систем мониторинга (в реальном времени) содержимого Интернет, данных о клиентах и об их адресатах.

В соответствии с официальными документами, полиции нужна также возможность определять географическое местоположение владельцев сотовых телефонов, расшифровывать закодированные сообщения (для тех провайдеров, которые предлагают клиентам средства шифрования), осуществлять перехват сообщений, причем все это - в течение нескольких минут или часов.

В резолюции содержится даже требование к провайдерам Интернет предоставлять возможность отслеживать действия пользователя в разных сетях, а также те услуги, которыми он/она пользуется. Провайдер должен обеспечивать возможность параллельного "прослушивания", а результирующие данные должны передаваться правоохранительным органам в читаемом формате.

Ассоциация европейских провайдеров Интернет выразила негативное отношение к резолюции, заявив, что это ошибочное, непроработанное решение.

"Один парламентский комитет проголосовал против предложения, другому не дали возможности высказаться, к тому же голосование проходило в пятницу, когда три четверти членов парламента отсутствовали. Это совершенно неадекватная резолюция", - прокомментировал ситуацию спикер Ассоциации провайдеров.

Он сказал, что документ вызовет серьезные проблемы в связи с конституционными гарантиями, и не соответствует законодательству о защите данных.

Английский провайдер Linx заявил, что, помимо посягательства на право на неприкосновенность частной жизни, ENFOPOL вообще вряд ли реально осуществим.

"Всякий, кто имеет хоть какое-то понятие об Интернет, понимает, что ENFOPOL нереалистичен", - сказал исполнительный председатель Linx Кейт Митчелл. - "Причина этого в том, что кучка сотрудников правоохранительных органов разработала свое изобретение в вакууме без публичного обсуждения".

Он сказал, что Европейский союз только приблизился к пониманию сущности Интернет и по-прежнему считает, что мы живем в мире, где каждое государство имеет одну государственную телефонную компанию.

"В реальности существует множество провайдеров, операторов связи и т.д., и совсем необязательно крупных", - заметил Митчелл. - "Уверенность, что все можно проконтролировать из какой-то центральной точки, - ошибка. Они бы еще вспомнили доску и мел!"

Он сказал, что расходы провайдеров нельзя посчитать ("слишком много неизвестных").

Митчелл поделился и другими опасениями. Он предположил, что пользователи из других стран будут стараться обмениваться данными "в обход" Европы, что нанесет ущерб европейской экономике.

Парламент заявил, что резолюция не носит обязательный характер, но в самой резолюции содержится призыв к странам-членам ЕС принять соответствующие законы.

Дополнение к резолюции гласит, что ЕС намерен в июле 2000 года проверить, насколько страны-члены ЕС продвинулись в принятии законов, соответствующих резолюции.

## БРИТАНСКИЙ ПАРЛАМЕНТ ПРОТИВ ЕВРОПЕЙСКОЙ СИСТЕМЫ СЛЕЖКИ В ИНТЕРНЕТ[58]

Планы Европейского союза заставить провайдеров Интернет и других поставщиков телекоммуникаций открыть правоохранительным органам доступ к информации клиентов являются неоправданными и нереальными. К такому выводу пришли британские парламентарии на своей недавней сессии.

Комитет по торговле и промышленности Палаты общин, выступивший в среду с отчетом против правительственного законопроекта об электронной торговле, рассмотрел также и резолюцию ЕС, известную как ENFOPOL.

В интервью, данном во вторник, председатель Комитета лейборист Мартин О'Нейл (Martin O'Neill) заявил, что в связи с ENFOPOL Комитет опасается появления нереалистичных требований к провайдерам и ухудшения ситуации в области прав человека.

"Мы думаем, что аргументы правозащитников перевешивают аргументы спецслужб, - сказал парламентарий. - Если бы они [спецслужбы] четко сказали, каких результатов они хотят достичь, люди, возможно, согласились бы с ними. Иначе все это похоже на прыжки в темноте".

По мнению защитников гражданских прав и провайдеров Интернет, одной ссылки на необходимость борьбы с преступностью недостаточно для того, чтобы спецслужбы получили в свое распоряжение круглосуточный доступ ко всем текстовым электронным сообщениям в реальном времени.

Основная головная боль провайдеров Интернет и других операторов связи - цена, которую им придется платить за реализацию ENFOPOL.

"Планы по созданию такого "щита" имеют такую же малую связь с реальностью, как и программа "звездных войн", - сказал О'Нейл. - Мы не верим, что они станут реалистичнее в будущем".

Комитет также заявил, что правительство Великобритании должно больше внимания уделять международной сущности Интернет.

"Правительство должно следить за международными исследованиями с тем, чтобы страна не отставала от остальной Европы," - заметил О'Нейл. Он добавил, что очень важно не сбиваться с пути создания в Британии наилучших условий для электронной торговли. В отчете Комитета содержится призыв определить статус европейских резолюций для страны.

"ЕС принял резолюцию в 1995 году, а в 1998 появился ENFOPOL. Но принципы резолюции 1995 года не были использованы в нашем законодательстве. Тут еще много противоречий".

Ранее в этом же месяце члены Европарламента проголосовали за резолюцию по ENFOPOL.

"Мы думаем, что правительство должно расставить все точки над "i" и сказать, какие обязательства несут провайдеры Интернет", - сказал О'Нейл.

В среду Комитет подверг критике пассивную позицию правительства в деле пересмотра Закона о перехвате коммуникаций (некоторые называют этот закон более действенным средством установления контроля за Интернет и криптографией, чем непопулярные предложения законопроекта об электронной торговле или резолюции ENFOPOL).

"Мы хотим, чтобы правительство обнародовало причины изменений в практике перехвата сообщений в связи с законопроектом об электронной торговле", - сказал О'Нейл.

Правительство никак не прокомментировало эти слова, сказав лишь, что относится с интересом к отчету парламентского комитета и ответит на все предложения в установленном порядке.

## АЗИЯ[59]

ЦЕНЗУРА И ОГРАНИЧЕНИЯ ТОРМОЗЯТ РАЗВИТИЕ ИНТЕРНЕТ НА БЛИЖНЕМ ВОСТОКЕ

(пресс-релиз правозащитного исследования)

(Вашингтон, 8 июля 1999 г.) Цензура, ограничение доступа и высокие цены по-прежнему препятствуют развитию Интернет на Ближнем Востоке и в Северной Африке. К такому выводу пришла организация Human Rights Watch в своем только что опубликованном отчете. HRW пишет, что во многих странах региона свободный обмен информацией через Интернет невозможен. В то же время, говорится в отчете, попытки препятствовать информационным потокам обречены на провал, и уже примерно миллион жителей арабского мира подключены к Интернет.

Прикрываясь лозунгом борьбы с порнографией, правительства Саудовской Аравии, Туниса, Бахрейна, Ирана и Объединенных Арабских Эмиратов закрыли доступ к некоторым онлайновым источникам по правам человека и политическим Web-серверам. Ирак и Ливия вообще не имеют подключения к Интернет. Сирия остается единственной страной в регионе, которая имеет такое подключение, но отказывает в доступе собственным гражданам. Тунис первым принял Интернет-ориентированные законы, согласно которым критика в Интернет подлежит тем же ограничениям, что и в других средствах массовой информации.

"Власти региона привыкли контролировать СМИ, но они не могут сделать то же самое со свободным Интернет,-говорит Хэнни Мегалли (Hanny Megally), исполнительный директор Human Rights Watch по Ближнему Востоку и Северной Африке. - Вместо того, чтобы строить барьеры, которые долго не продержатся, правительства могли бы помочь широкому развитию телекоммуникаций".

Многие пользователи обеспокоены технической слежкой за своими действиями в Интернет и за своей электронной почтой. Подобные страхи понятны в регионе, где полиция часто прибегает к прослушиванию телефонов и факсов диссидентов, а телекоммуникации по-прежнему находятся в основном в руках государства. Так, житель Бахрейна провел почти два года в тюрьме по подозрению в том, что он отправлял информацию политического характера оппозиции, находящейся за границей.

Однако, развитие методов защиты от цензуры и слежки - таких как шифрование, анонимная пересылка писем, "анти-цензурные" серверы, беспроводная связь - опережает развитие технологий контроля, отмечает Human Rights Watch.

Жители Ближнего Востока уже используют Интернет для того, чтобы преодолеть информационные барьеры. Местные правозащитные организации распространяют новости куда более эффективно, чем раньше, а газеты публикуют электронные статьи, которые цензура вырезала из печатных вариантов. Убеждения, которые ограничиваются или запрещаются - такие как про-исламистские взгляды в Алжире - распространяются в этих странах по Интернет.

Не все правительства пытаются активно контролировать Интернет. В Египте и Иордании допускается размещение в Интернет новостей и комментариев, даже если они не прошли цензуру для печати. Косвенным инструментом контроля за этой ситуацией являются цены: доступ к Интернет стоит в некоторых странах около 70 долларов в месяц, что делает Сеть доступной лишь для небольшой "элитной" части общества.

"Распространение информации по Интернет может показаться не столь актуальным в странах, где пытки являются привычным делом, а компьютер не считается предметом быта, доступным средней семье, - считает Мегалли. - Но на самом деле Интернет играет огромную роль именно в странах с репрессивными режимами, жители которых получают мощный инструмент для передачи информации".

За медленным стартом Интернет на Ближнем Востоке и в Северной Африке следует его развитие. Арабские СМИ все чаще обсуждают Интернет, который стал темой для нескольких конференций. По крайней мере, в 14 странах работают Интернет-кафе. Но регион по-прежнему отстает в развитии от Северной Америки, Южной Америки, Европы и Азии в смысле количества подключенных к Интернет на тысячу человек. На это влияет также недостаток ресурсов на арабском языке и устаревшее телекоммуникационное оборудование.

В своем 92-страничном исследовании Human Rights Watch обнародовала принципы защиты права на неприкосновенность частной жизни, права на ассоциации и свободу слова в сети. В числе этих рекомендаций:

- механизмы цензуры (если они используются) должны находиться в руках пользователей, а не правительства;

- люди должны иметь возможность использовать средства сильной криптозащиты;

- правительственная слежка за электронными коммуникациями не должна безосновательно нарушать право на неприкосновенность частной жизни и другие гражданские права и должна предоставлять возможность юридического контроля со стороны;

- частные лица должны иметь возможность передавать и получать информацию анонимно.

Электронная версия этого отчета (на английском и арабском языках) доступна по адресу: http://www.hrw.org/advocacy/internet/mena/index.htm

НЕ ДАДИМ ПРОТОЛКНУТЬ ЗАКОН О ПРОСЛУШИВАНИИ![60]

Срочное обращение

Законопроект принят в Палате представителей без обсуждения

В 7 часов вечера 28 мая 1999 года на заседании юридического комитета Палаты представителей японского парламента коалиция трех политических партий страны JI-JI-KO проголосовала за законопроект, посвященный слежке и контролю за организованной преступностью. JI-JI-KO состоит из Либерально-демократической партии Jimin, Либеральной партии Jiyu и партии Kohmei. Эти три партии вместе составляют большинство в парламенте. Сторонники неспешного обсуждения законопроекта - Демократическая партия Minshu, Коммунистическая партия Kyosan, Социал-демократическая партия Shamin - бойкотировали это заседание Комитета, заявив, что его целью было лишь скорейшее голосование без всякой дискуссии. Тем не менее, комитет выделил время для выступлений представителей трех отсутствующих партий. Парламентарии потратили время на то, чтобы продемонстрировать свою готовность к дискуссии "для протокола", после чего законопроект был выставлен на голосование и одобрен.

Закон о полицейском мониторинге несет массу противоречий

Закон о слежке противоречит японской Конституции, так как открывает полиции возможности для доступа к электронной почте пользователей Интернет. Это нарушает наше право на тайну коммуникаций, отраженное в 21 статье Конституции. Более того, закон изменит саму сущность полиции, которая превратится в организацию, осуществляющую мониторинг частной жизни граждан на весьма приличные деньги из государственного бюджета. Решение JI-JI-KO принять подобный законопроект без обсуждения само может сравниться с действиями организованной преступности.

Незаконное полицейское прослушивание остается без комментариев

Желающие могут проследить за практикой незаконной полицейской слежки в нашей стране. Эта практика подтверждается многочисленными свидетельствами, в частности, сотрудников фирм, поставлявших полиции инструменты для прослушивания, и частных специалистов по прослушиванию. Придание этой практике законного статуса является грубым и неприемлемым шагом.

Голосование недействительно! Мы требуем отмены закона

Группы граждан, высказывающиеся против закона, разделяют позицию трех партий (Minshu, Kyosan, Shamin), которые считают, что заседание Юридического Комитета 28 мая прошло с процедурными нарушениями. Следовательно, полагают эти силы, результат голосования недействителен. Если подобная попытка будет повторена на сессии Палаты представителей, мы будем вынуждены заявить, что коалиция JI-JI-KO принесла в жертву право японских граждан на частную жизнь полицейскому мониторингу и контролю. Мы снова и снова повторяем, что этот закон должен быть отменен.

Заявление подписали: Демократический женский клуб, Японская католическая миссия за справедливость и мир, Ассоциация за закрытие военной базы в Ацуги, Ассоциация потребителей Японии, Буддистская церковь Nihon-zan Myoho-ji, "Женщины против милитаризма", организация "Компьютерный доступ в Японии" (JCA), Ассоциация против расовой дискриминации MUKUGE и другие организации.

(Перевод с английского.

Японские названия могут содержать ошибки)

## ВЕЛИКАЯ КИТАЙСКАЯ СТЕНА В ИНТЕРНЕТЕ[61]

Андрей Травин

andrew@travin.dnttm.rssi.ru

В середине нынешнего года было принято решение, что в десяти крупных китайских городах вскоре будут находиться правительственные серверы, призванные отфильтровать весь информационный поток, поступающий в китайскую часть Интернета. Определять информацию, которая будет доступна через Сеть самому почтительному из народов, - первостепенная задача этой "дигитальной китайской стены", хотя некоторые усилия предполагаются и на предмет того, чтобы самому Китаю правильно выглядеть для остального интернетовского сообщества.

Для управления и контроля Интернет в той ее части, что издавна зовется Поднебесной - ChinaNet, правительство Китая (в лице телеграфного агентства Синьхуа и других национальных агентств новостей) учредило организацию, которая для внешнего мира была обозначена английским наименованием China Internet Corporation (CIC). Для нее были выделены штаб-квартира в Гонконге и зарегистрирован национальный домен. Надо сказать, что официально CIC была создана в 1995 году для практической реализации (при стратегическом партнерстве с Министерством связи КНР) проекта "Китайская Всемирная Паутина", предусматривавшего предоставление онлайновых информационных услуг на китайском языке пользователям Internet в 200 основных городах Китая.

До сих пор всем близко знакомым с сетевыми реалиями экспертам было очевидно, что регулирование национального Интернета возможно лишь с помощью лицензирования средств массовой информации в Сети и изменением национальной законодательной базы в соответствии с этими самыми сетевыми реалиями. Фильтрация информационного потока в Интернете, где каждый IP-пакет до последней возможности ищет (и, как правило, находит) свой путь прохождения к адресату, до настоящего времени представлялась неосуществимой. Однако в стране, где еще до нашей эры были введены единые письменные знаки, упорядочены меры весов и длины, введена одинаковая ширина колеи для повозок и было приказано делать обрядовую утварь и оружие по единому образцу, возможно, впервые в истории удастся строго отфильтровать каждый байт информации, передающийся по проводам китайской Сети. Что ж, пожалуй, главное, начать, а там посмотрим, что получится, ведь если перефразировать известный китайский афоризм, стена в десять тысяч ли начинается с первого камня - процессора правительственного сервера.

Как известно, первый император Китая Цинь Шихуанди приказал построить Великую китайскую стену после того, как придворный предсказатель изрек фразу о том, что "погубят Цинь хусцы, что на севере". И чтобы оградить свою страну (империю Цинь) от

"северных дикарей", император повелел возвести невиданные по своей масштабности оборонительные укрепления. Именно так на севере империи началось строительство "Вань ли чан чэн"

("Стены длиной в десять тысяч ли"), известной европейцам как Великая китайская стена.

Есть такая примета: там, где имеется тоталитарный режим, там есть и ограничение свободного потока информации. (Поэтому, скажем, во Вьетнаме Интернет-кафе закрываются по политическим причинам, а в Нью-Йорке по соображениям рентабельности).

Нынешние правители Поднебесной не могут прямо заявить, что строительство оборонительных укреплений в китайской части Сети призвано сохранить их власть над страной. И защита от "дикарей" формулируется теперь как "защита национальной культуры и социальных ценностей". Не знаю, какими приказами наследники "желтого императора" повелели отсекать на входе в Китай происки "желтой прессы" и вообще нежелательную грязную ложь и чистую правду. Но, кстати, достаточно оригинальной получилась формулировка ограничения на поступление в китайскую Сеть порнографии - как "способной ухудшить тяжелую демографическую ситуацию в стране".

Как бы то ни было, недавней памяти попытки ограничения поступающей информации для пользователей America online показали что такая фильтрация производится по-хамски и, главное, очень неумело. Надо полагать, что китайская попытка "установить баланс свободного потока информации" будет еще более чудовищна с точки зрения свободного информационного обмена.

Запад пока не делал каких-либо публичных шагов, призванных воспрепятствовать реализации китайского "железного занавеса" в преимущественно медно-волоконной Сети. Во время последней (30 июня 1998) встречи секретаря американского Департамента торговли William Daley с главной публичной фигурой CIC - Peter Yip стороны обсудили большое количество разнообразных вопросов электронной торговли и других коммерческих применений Интернета. Заходил ли там разговор по теме настоящей заметки - не сообщается.

Как известно, драма повторяется как фарс. Великая китайская стена пережила тысячелетия. И в этом ее значение, потому что камни, положенные в ее основание, заставляли умы философствовать (Борхес, к примеру). Дигитальная китайская стена возникает тогда, когда время само летит как камень, сорвавшийся в пропасть, и в новой эпохе бастион китайской цензуры скорее всего умрет, не родившись. И поэтому не сильно тянет философствовать на тему, объявленную в заголовке, - обычно философствуют о вечном. Лучше закончим рассказ на лирической ноте.

Поэт танской эпохи Бо Цзюй-и более тысячи лет назад написал о препятствиях, которые создают расстояния:

У ручья зачерпнул

быстро бьющей журчащей воды.

Как вскипает, гляжу,

бирюзово-зеленая пыль.

Только жаль, не могу

чашку вкусного чая налить.

И послать далеко -

человеку, влюбленному в чай.

Даже в век Интернета невозможно выполнить такое желание. Но имеется возможность сделать так, чтобы в тот же вечер далекий адресат прочитал само посвященное ему стихотворение. Право, жаль, что и подобные интимные моменты могут стать предметом вмешательства сил, которые разбивают "полноводную реку" Интернет, словно Хуанхэ, изначально свободно катящую свои воды, на ручейки "дистиллированной воды".

По этому поводу стоит вспомнить, что "желтый" император Цинь Шихуанди посылал строить Великую Стену и всех несправедливых судий.

Сайт правительственного проекта "Китайская Всемирная Паутина" http://www.cww.com

Агентство новостей Синьхуа http://www.xinhua.org

Два сайта China Internet Corporation (CIC) http://www.china.com и http://www.hongkong.com

Вице-президент CIC Peter Yip
http://www.china.com/cic5html/corp/pressroom/corp_news/photo/980630-3a.jpg

Источник:Russian Journal mailto:russ@russ.ruhttp://www.russ.ru/

ИНДИЯ ОБЪЯВЛЯЕТ О ПЛАНАХ КОНТРОЛИРОВАТЬ ИНТЕРНЕТ[62]

Правительство Индии объявило о плане по установлению контроля за Интернет, который может снизить скорость передачи данных в сетях и взвинтить цены. В соответствии с планом провайдеры Интернет должны подключить свои компьютеры к оборудованию государственных структур, в частности Разведывательного Бюро и Департамента исследований и анализа (обе организации расположены в Нью-Дели).

Источники в промышленных кругах заявили, что эти меры означают замедление передачи информации в Интернет. Правительство намеревается также возложить обязанность по установке оборудования на самих провайдеров. Эти мероприятия отразятся на стоимости доступа для корпоративных пользователей и ударят по развивающейся промышленности страны.

План уже одобрен внутриведомственным комитетом по безопасности Интернет (в числе структур, подчиненных премьер-министру). Перед тем, как вступить в силу, он должен быть ратифицирован парламентом страны.

ВЬЕТНАМ ГОТОВИТСЯ ВВЕСТИ КОНТРОЛЬ НАД ИНТЕРНЕТ[63]

Ханой, Вьетнам (сообщение "Ассошиэйтед пресс"). Полиция города Хо Ши Мин обратилась к правительству страны с предложением передать полный контроль над Интернет местному Народному комитету. Об этом сообщила в минувшую среду вьетнамская печать.

Во вторник на брифинге бывшего премьер-министра Vo Van Kiet, посвященном общественному порядку, глава полиции заявил, что враждебные Вьетнаму силы из-за границы используют Интернет для передачи в страну документов негативного и реакционного содержания, говорится в заметке в газете "Молодежь".

Народный комитет состоит из полиции, Департамента культуры и Департамента науки и технологии. Как пишет газета, полиция сообщила о большом количестве документов государственной важности, попавших в Интернет и потерявших таким образом гриф "секретно". Полиция заявила также, что в Интернет были опубликованы многие статьи вьетнамских диссидентов.

Полицейские отметили, что кражи пользовательских паролей и незаконное использование Сети наносят ущерб государству и его гражданам, и предложили штрафовать за подобные правонарушения.

Правительство боится утратить контроль за информационными потоками и свою монополию на телекоммуникации. Интернет официально разрешен во Вьетнаме в декабре 1997 года и сегодня насчитывает около 30 тысяч пользователей.

## КОНТРОЛЬ КОММУНИКАЦИЙ И БОРЬБА ЗА СОБЛЮДЕНИЕ ПРАВ ЧЕЛОВЕКА[64]

ГЛОБАЛЬНАЯ КАМПАНИЯ ЗА СВОБОДУ В ИНТЕРНЕТ[65]

ПРИНЦИПЫ

Коалиция организаций под названием Глобальная кампания за свободу в Интернет (The Global Internet Liberty Campaign) была создана на ежегодном собрании Internet Society в Монреале. В число членов коалиции входят American Civil Liberties Union, Electronic Privacy Information Center, Human Rights Watch, Internet Society, Privacy International, Association des Utilisateurs d'Internet и другие организации, занимающиеся защитой прав человека и гражданских свобод.

Задачами Глобальной кампании за свободу в Интернет являются:

- запрет цензуры онлайновых коммуникаций;

- введение законодательных разграничений ответственности владельцев онлайновых материалов и провайдеров телекоммуникаций;

- противодействие косвенным ограничениям свободы слова в Интернет - таким, как чрезмерный государственный или частный контроль за компьютерами или программами, телекоммуникациями или иными принципиальными компонентами Интернет;

- вовлечение в развитие Глобальной информационной инфраструктуры (Global Information Infrastructure, GII) жителей стран с нестабильной экономикой, недостаточно развитой инфраструктурой или отставанием в области высоких технологий;

- запрещение дискриминации по признаку расы, цвета кожи, пола, языка, религии, политических и иных убеждений, национального или социального происхождения, имущественного положения, рождения и др.;

- недопущение использования информации, собранной в рамках GII, в целях, отличных от первоначальных, и раскрытия этой информации без разрешения субъекта; обеспечение людям возможности доступа к персональным данным о себе в Интернет и возможности вносить исправления в эти данные, если они содержат ошибки;

- обеспечение всем пользователям возможности использовать криптографические методы защиты своих данных без каких-либо ограничений.

УЧАСТНИКИ GILC

В Интернет нет границ. Действия частных лиц, правительственных структур, международных организаций - все они могут иметь положительный эффект для развития Интернет. Участники GILC объединились, чтобы защищать основные права человека - такие, как свобода слова и право на неприкосновенность частной жизни - для всех пользователей Интернет.

ALCEI - Associazione per la Liberta nella Comunicazione Elettronica Interattiva *

American Civil Liberties Union *

Applied Research and Communications Fund

Arge Daten

Association des Utilisateurs d'Internet *

Association pour la Promotion d'Internet en Polynesie Francaise

Bulgarian Institute for Legal Development

Bevcom Internet Technologies

Canadian Journalists for Free Expression

Campaign Against Censorship of the Internet in Britain

Centre for Applied Legal Studies, University of the Witwatersrand School of Law.

Center for Democracy and Technology

CITADEL-EF France*

Committee to Protect Journalists

CommUnity - The Computer Communicators Association

Computer Professionals for Social Responsibility

Cyber-Rights & Cyber-Liberties (UK)

CypherNet *

Derechos Human Rights

Digital Citizens Foundation Netherlands

Digital Freedom Network

Equipo Nizkor

engagierte Computer ExpertInnen (eCE)

Electronic Frontiers Australia *

Electronic Frontier Canada *

Electronic Frontier Foundation *

Electronic Frontiers Texas *

Electronic Privacy Information Center *

Federation Nationale des Associations de Consommateurs du Quebec

Feminists Against Censorship

Forum InformatikerInnen fuer Frieden und gesellschaftliche Verantwortung (FIfF) e.V.

Forderverein Informationstechnik und Gesellschaft (FITUG)

Fronteras Electronicas Espana (FrEE) *

Human Rights Network

Human Rights Watch *

Hungarian Civil Liberties Union

Imaginons un Reseau Internet Solidaire (IRIS)

Index on Censorship

Internet Freedom

Internet Society *

National Council for Civil Liberties (Liberty)

NetAction *

OpenNet

Open Society Institute

Peacefire *

PEN American Center

Privacy International *

Public Interest Advocacy Center, Ottawa

quintessenz e-zine *

Singapore Internet Community (SInterCom)

XS4ALL Foundation

(звездочкой помечены организации-учредители GILC)

## Заключение

Первую часть книги мы начали с описания международных правовых норм, касающихся практики тайного прослушивания представителями государственной власти. Далее были описаны пять дел, рассмотренных Европейским Судом по правам человека, и обсуждены весьма сложные критерии, выработанные Судом при рассмотрении этих дел. Затем было дано описание законов одиннадцати европейских стран, определяющих процедуру прослушивания телефонных разговоров, равно как и основания этих законов в каждом государстве. Мы рассмотрели конституционные и/или иные законодательные нормы, регулирующие право государства перехватывать телефонные сообщения, а также обстоятельства, при которых государство имеет право это делать. В частности, особое внимание было уделено процедурам получения разрешения на прослушивание, принятым в каждой стране, и эффективности надзора за законностью прослушивания. Обсуждение законов каждой из рассмотренных стран было завершено анализом соответствия процедуры прослушивания нормам, установленным Европейским Судом.

Оказалось, что наличие конституционных гарантий неприкосновенности частной жизни (Германия, Швеция, Польша, Россия, Румыния, Украина) или их отсутствие (Объединенное Королевство, Франция, Финляндия, Швейцария, Венгрия) слабо связано с качеством законов. Можно сказать с уверенностью, что Европейский Суд признает приемлемым немецкое и финское законодательство. По-видимому, Суд одобрит французскую, шведскую и венгерскую процедуры. Вызывает большие сомнения принятие Судом швейцарской процедуры. Что же касается британской, российской, польской, румынской и украинской процедур, то, по-видимому, они не удовлетворяют указанным критериям Суда.

Рассмотрение практики прослушивания телефонов в разных странах дает основание для двух выводов. Первый: в тех странах, где данные о перехватах публикуются, суды, как правило, не отказывают спецслужбам в выдаче санкции на прослушивание и продлении санкции. С большой степенью вероятности можно ожидать, что суды редко отказывают в санкции и в тех странах, где информация о количестве перехватов остается закрытой. Поэтому, хотя на важности получения санкции судебного органа неоднократно настаивал Суд, представляется не менее важной прозрачность процедуры прослушивания для реализации контроля. Этого можно достичь введением нормы об обязательном информировании лица о том, что его телефон прослушивался, после окончания прослушивания. Второй вывод: во всех без исключения странах спецслужбы хотели бы

получить такое законодательство о прослушивании, которое облегчало бы их работу, и это им удается ровно в той степени, в какой позволяет это сделать гражданское общество. Чем более оно инертно, тем хуже работают процедуры контроля и тем выше вероятность злоупотреблений.

Во второй части книги рассмотрены национальные и международные проекты "прослушивания" электронных сетей коммуникаций, особое внимание при этом уделено российской и украинской ситуации. На наш взгляд, приведенная информация убедительно свидетельствует о кардинальном изменении картины общения людей в мире из-за появления новых информационных технологий и о грядущих еще больших изменениях. Однако, поскольку природа человека не меняется, новые технологии несут не только невиданные возможности для интеллектуального и технического прогресса, но и неожиданные средства и способы совершения преступлений. Преступность стала гораздо изощренней, взявши на вооружение информационные технологии, и, естественно, спецслужбы должны владеть адекватными возможностями для предупреждения и расследования преступлений. Вследствие этого и появляются такие проекты, как Echelon, ENFOPOL, COPM и другие. В то же время законодатель не поспевает за бурным развитием новых технологий, которые сразу и осмыслить непросто. В целом ситуация таит в себе новые угрозы свободе человека, и прежде всего праву на доступ к информации и на неприкосновенность частной жизни. Поэтому представляется чрезвычайно важным осмысление сущности информационных отношений в новых условиях, разработка и формулирование новых гарантий защиты прав человека.

В Приложении мы публикуем текст немецкого закона об информационных и коммуникационных услугах, вступившего в силу два года назад. Это один из немногих законов в современном мире, который регулирует развитие информационной среды и признан экспертами одним из лучших.

Е.Е.Захаров

## Приложение

# НЕМЕЦКИЙ ЗАКОН ОБ ИНФОРМАЦИОННЫХ И КОММУНИКАЦИОННЫХ УСЛУГАХ

1 августа 1997 вступил в силу Закон, регламентирующий условия предоставления информационных и коммуникационных услуг (ЗИКУ). Этот закон, называемый также законом о мультимедиа, включает в общей сложности 11 статей.

Закон предусматривает следующие регламентации:

Статья 1 (Закон о телеуслугах).

Условия для предоставления и использования телеуслуг посредством свободы доступа, а также ликвидации пробелов в области защиты прав потребителя и установления ответственности предоставителя услуг.

Статья 2 (Закон о защите данных, предоставляемых телеуслугами).

Специфическая регламентация защиты данных, предоставляемых с помощью телеуслуг, принимая во внимание повышенный риск при сборе, обработке и использовании сведений, имеющих личностный характер.

Статья 3 (Закон о цифровой подписи).

Создание единой бундесинфраструктуры для обеспечения введения цифровой подписи.

Статья 4 (Изменения в уголовном кодексе) и Статья 5 (Изменения Закона о правонарушениях).

Определение основных понятий в уголовном кодексе и законе о правонарушениях, принимая во внимание наличие возможностей использования и распространения сведений, могущих привести к правонарушениям.

Статья 6 (Изменение Закона о распространении сочинений, наносящих вред моральному здоровью молодежи).

Основная часть раздела об особом регулировании защиты молодежи в рамках ЗИКУ, имеющем целью обеспечение эффективной защиты молодежи и единое толкование основных терминологических понятий; а также введение технических средств защиты в сочетании с введением рекомендованных услуг, а также использование рекомендаций уполномоченных по делам защиты молодежи в качестве отправного пункта для пользователей и консультанта для предоставления услуг.

Статья 7 (Изменения в Законе об авторском праве).

Введение в практику Директивы Европейского парламента Совета Европы от 11 марта 1996 о правовой защите баз данных (RL96/9/EG) посредством соответствующего изменения авторского права.

Статья 8 (Изменение Закона о тарифах) и Статья 9 (Изменение порядка предоставления тарифов).

Распространение защиты прав потребителя, указанных в законе о тарифах и в положении о предоставлении тарифов, на новые возможности для пользователей, возникшие в результате появления новых услуг.

Статья 10 (Возврат к единому уровню администрирования) и Статья 11 (Вступление в силу).

Правовая регламентация (возврат к единому уровню администрирования и порядок вступления в силу).

БЮЛЛЕТЕНЬ ЗАКОНОВ ФРГ

ЧАСТЬ I

Опубликован в Бонне 28 июля 1997 №52

ЗАКОН ОБ ИНФОРМАЦИОННЫХ И КОММУНИКАЦИОННЫХ УСЛУГАХ

Статья 1

Закон об использовании телеуслуг

§1

Цель закона

Целью настоящего Закона является создание единых и экономичных условий пользования услугами, предоставляемыми с помощью электронных средств информации и коммуникации.

§2

Область распространения

(1) Настоящее предписание распространяется на все услуги, предоставляемые с помощью электронных средств информации и коммуникации, предназначенных для индивидуального использования комбинированных данных, таких как рисунки, изображения, звук и в основе которых лежит принцип передачи с помощью телекоммуникации (телеуслуг).

(2) Телеуслугами в соответствии с §1 являются:

1. Предложения в области индивидуальной коммуникации (например, создание телебанка данных, обмен данными).

2. Предложения информации или коммуникации, если не требуется редакционного оформления при формировании общественного мнения (услуги в предоставлении различного рода данных, например, информация по транспорту, о погоде, об окружающей среде или биржевые сводки, распространение информации о товарах и услугах).

3. Предложения по использованию линий Интернет либо иных сетей.

4. Предложения по использованию телеигр.

5.

Предложения товаров и услуг, хранящихся в электронной базе данных, с интерактивным доступом к базе данных и возможностью прямого заказа.

(3) Действие абзаца 1 настоящего Закона распространяется на все виды телеуслуг, независимо от того, предоставляются ли они полностью либо частично бесплатно, либо за плату.

(4) Этот Закон не распространяется на:

1. Оказание телекоммуникационных услуг и на услуги телекоммуникации, регулируемые Законом от 25 июля 1996 / BGBI.1 с. 1120[66]

2. Трансляцию радиопрограмм в соответствии с §2 Договора о государственном радиовещании,

3. Услуги, в содержании которых требуется редакционная правка для формирования общественного мнения, согласно §2 государственного Договора о средствах массовой информации в редакции от 20 января - 7 февраля 1997.

(5) Документы, регламентирующие деятельность прессы, остаются без изменений.

§3

Определение терминологических понятий

Согласно настоящему Закону

1. "предоставителем услуг" является юридическое или физическое лицо либо группа лиц, предоставляющие в пользование собственные либо чужие телеуслуги, либо обеспечивающие доступ к таковым.

2. "пользователем" является юридическое или физическое лицо, либо группа лиц, имеющих спрос на телеуслуги.

§4

Свобода доступа

В рамках настоящего Закона телеуслуги являются свободными для пользования и регистрации.

§5

Мера ответственности

(1) Предоставитель услуг отвечает за содержание предоставляемых собственных услуг согласно общему законодательству.

(2) Предоставитель телеуслуг отвечает за содержание чужих предоставляемых услуг лишь в том случае, когда ему известно содержание предоставляемых услуг, и у него имеется техническая возможность и готовность приостановить пользование этими услугами.

(3) Предоставитель услуг не несет ответственности за содержание чужих услуг, в случае если он обеспечивает лишь доступ к пользованию ими. Предоставлением доступа к пользованию услугами является автоматическое и кратковременное обладание чужим содержанием на основании спроса потребителя.

(4) Согласно общему законодательству, предоставитель услуг несет ответственность за приостановку пользования услугами, имеющими противозаконный характер, если ему, согласно §85 Закона о телекоммуникациях и с целью сохранения тайны, стало известно об их содержании и у него имеется техническая возможность для такой приостановки.

§6

Реквизиты предоставителя услуг

Предоставитель услуг обязан подать следующие сведения:

1. имя и адрес, а также

2. в случае объединения лиц или групп лиц имена, фамилии и адреса заместителей.

Статья 2

Закон о защите данных, предоставляемых с помощью телеуслуг

§1

Область распространения

(1) Настоящее предписание распространяется на защиту сведений, имеющих персональный характер, согласно Закону о телеуслугах.

(2) Ввиду отсутствия в настоящем Законе дополнительных оговорок, действие настоящего предписания распространяется на защиту персональных данных, даже в случае, если последние не переработаны и не используются в виде базы (архива) данных.

§2

Определение терминологических понятий

В настоящем Законе

1. "предоставителем услуг" является юридическое или физическое лицо либо объединение лиц, имеющих телеуслуги для использования, либо обеспечивающие доступ к ним.

2. "пользователем" является физическое либо юридическое лицо либо объединение лиц, использующих телеуслуги.

§3

Основные положения для обработки персональных данных

(1) Предоставитель услуг может обрабатывать и использовать персональные данные либо с согласия пользователя, либо в рамках иных предписаний.

(2) Предоставитель услуг может использовать имеющиеся данные для других целей лишь в рамках настоящего Закона либо иных предписаний, или с согласия пользователя.

(3) Предоставитель услуг не имеет права ставить предоставление телеуслуг в прямую зависимость от согласия пользователя на обработку и использование его личных данных в иных целях, если у пользователя нет альтернативных путей доступа к телеуслугам, либо доступ осуществляется неприемлемым для пользователя способом.

(4) Выбор оборудования для осуществления телеуслуг должен преследовать цель не собирать, не обрабатывать и не использовать никакой информации, имеющей персональный характер, либо использовать минимально возможное ее количество.

(5) До начала сбора данных пользователь должен быть проинформирован о способе, объеме, месте и цели сбора, обработки и использовании его персональных данных. При наличии автоматизированных способов сбора, переработки и использования информации, позволяющих дальнейшую идентификацию пользователя, последний должен быть проинформирован до начала действия этих способов. Пользователь должен иметь возможность в любой момент отозвать содержание уведомления. Пользователь имеет

право отказаться от уведомления. Уведомление и отказ должны фиксироваться протокольно. Отказ от уведомления не должен рассматриваться как согласие в соответствии с абзацем 1 и 2.

(6) Перед подачей заявления о своем согласии пользователь должен быть проинформирован о своем праве в любое время отозвать свое заявление. Действие этого права распространяется на будущее. Об этом также говорится в предложении 3 абзаца 5.

(7)

Согласие может быть также передано с помощью электронных средств, если предоставитель услуг будет уверен в том, что:

1. оно получено в результате однозначных и осознанных действий пользователя,

2. оно не может быть изменено,

3. его автор может быть установлен,

4. оно зафиксировано протокольно и

5. оно может быть в любой момент времени отозвано пользователем.

§4

Обязанности предоставления услуг по правовой защите сведений

(1) При наличии технической возможности предоставитель услуг должен предоставить пользователю возможность пользоваться и оплачивать телеуслуги анонимно либо под псевдонимом и проинформировать об этом пользователя.

(2) Предоставитель телеуслуг с помощью своих технических и организационных мер должен обеспечить:

1. возможность для пользователя в любой момент прекратить свои отношения с предоставителем услуг,

2. возможность стирания данных непосредственно после окончания процесса использования, если нет необходимости их дальнейшего накопления с целью получения платы за услуги,

3. пользователю защиту от внимания третьих лиц при пользовании телеуслугами,

4. возможность раздельной обработки сведений, имеющих персональный характер, одним пользователем при использовании им различных телеуслуг; сведение воедино этих сведений является недопустимым, если это не требуется по соображениям оплаты.

(3) Пользователю должны быть сообщены способы перехода к иному предоставителю услуг.

(4) Специфика использования телеуслуг раскрывается лишь при наличии псевдонима. Она не должна сводиться воедино с данными о носителе псевдонима.

§5

Исходные данные

(1) Предоставитель услуг имеет право сбора, обработки и использования сведений о пользователе, если они необходимы ему для заключения, оформления либо изменения договорных отношений по использованию телекоммуникационных услуг с пользователем (исходные данные).

(2) Обработка и использование исходных данных о пользователе с целью консультации, заключения сделок, маркетинга либо правового оформления договора по использованию телекоммуникационных услуг допустим лишь при наличии ясного согласия пользователя.

§6

Сведения для пользования и расчета за пользование телекоммуникационными услугами

(1) Предоставитель услуг имеет право собирать, обрабатывать и использовать персональные данные о пользователе, если это необходимо для:

1. обеспечения возможности использовать телеуслуги (сведения для пользования) или

2. расчета за пользование телекоммуникационными услугами (сведения для расчета).

(2) Предоставитель услуг обязан стереть (уничтожить):

1. сведения для пользования сразу же непосредственно по окончании процесса пользования упомянутыми услугами, кроме данных, необходимых для расчета за пользование,

2. сведения для расчета, в случае если они не требуются для произведения расчетных платежей за пользование телекоммуникационными услугами; данные о пользователе, необходимые для расчета за услуги, сохраняемые по требованию пользователя и согласно абзацу 4 для оформления отдельных одиночных заказов на пользование услугами, должны быть уничтожены не позднее, чем 80 дней спустя после подачи заказа на пользование услугами, однако в течение этого срока требования об оплате могут быть оспорены и могут не оплачиваться.

(3) Передача сведений для пользования и для оплаты другому предоставителю услуг или третьему лицу не допускаются. Полномочия исполнительных служб остаются неизменными. Предоставитель услуг, обеспечивающий лишь доступ к пользованию телеуслугами, имеет право передавать иному предоставителю услуг, чьими услугами в данный момент пользуется пользователь, лишь:

1. анонимные данные для пользования с целью маркетинга,

2. сведения для расчета за услуги с целью оплаты.

(4) В случае, если предоставитель услуг заключил с третьим лицом договор об отчислении средств, он имеет право сообщить этому третьему лицу сведения для расчета, необходимые для произведения такового. В этом случае третье лицо несет ответственность за сохранение тайны связи.

(5) В счет об оплате за пользование телекоммуникационными услугами могут не включаться сведения о предоставителе услуг, времени начала пользования, длительности пользования, способе, содержании и частоте пользования телеуслугами, если пользователь оформит отдельный одиночный заказ.

§7

Право пользователя на получение сведений справочного характера.

Пользователь имеет право на бесплатное получение от предоставителя услуг в любое время информации о собираемых на него сведениях. Эти сведения могут быть предоставлены также с помощью электронных средств связи. Право на получение справок в случае краткосрочного сбора сведений согласно §33 абз. 2 предл. 5 Закона ФРГ о защите данных не отменяется §34 абз. 4 упомянутого Закона.

§8

Контроль за соблюдением защиты данных.

(1) Согласно §38 Закона ФРГ о защите данных, меры контроля за соблюдением настоящего Закона осуществляются и в том случае, если отсутствуют предпосылки для его нарушения.

(2) Уполномоченный по делам защиты данных осуществляет контроль за соблюдением мер защиты при предоставлении телекоммуникационных услуг и дает свое заключение в рамках отчета §26 абз. 1 Закона о защите данных.

Статья 3.

Закон о цифровой подписи[67]

§1

Цель и область применения Закона.

(1) Целью настоящего Закона является создание правовых условий для адекватного осуществления цифровой подписи, в рамках которых можно было бы надежно выявить любые подделки подписи либо подписанных сведений.

(2) Настоящим Законом допускается применение и других способов цифровой подписи.

§2

Определение терминологических понятий.

(1) Согласно настоящему Закону цифровой подписью называется личная печать, которая с помощью соответствующего ключа, снабженного сертификатом соответствующих служб, позволяет установить владельца ключа, а также подделки данных.

(2) Сертификационной службой, согласно настоящему Закону, является физическое или юридическое лицо, удостоверяющее присвоение цифрового ключа частному лицу и имеющее в соответствии с §4 необходимое разрешение.

(3) Сертификатом, согласно настоящему Закону, является специальное снабженное цифровой подписью цифровое удостоверение о присвоении цифрового ключа частному лицу (сертификат о цифровом ключе), или специальное цифровое удостоверение, содержащее, со ссылкой на сертификат о цифровом ключе, дополнительные сведения (атрибутивный сертификат).

(4) Штемпелем срока, согласно настоящему Закону, является снабженное цифровой подписью цифровое удостоверение центра сертификации о необходимости предоставления определенных данных к определенному моменту времени.

§3

Компетентные инстанции

Выдача разрешений и сертификатов, а также надзор за соблюдением настоящего Закона и правопорядка находится в компетенции соответствующих инстанций согласно §66 Закона о телекоммуникациях.

§4

Лицензия центра сертификации

(1) Открытие центра сертификации требует наличие лицензии соответствующего компетентного органа власти.

(2) В выдаче лицензии может быть отказано, когда наличествуют факты, свидетельствующие о том, что заявитель не выявил необходимый уровень компетентности, если заявитель не сможет доказать наличие у него специальных знаний для работы данного органа, либо если окажется, что после открытия этого центра не будут соблюдены другие необходимые предпосылки, согласно настоящему Закону и §16 правительственного распоряжения.

(3) Необходимым уровнем компетентности (надежности) будет обладать лицо, предоставившее гарантии соблюдения всех необходимых для функционирования центра сертификации правовых регламентирующих предписаний. Уровень специальных знаний будет считаться достаточным, если все лица, занятые в работе центра сертификации, обнаружат наличие у них необходимых для работы сведений, опыта и навыков. Остальные необходимые для функционирования центра сертификации предпосылки будут считаться соблюденными, если меры по выполнению требований безопасности, согласно настоящему Закону и §16 правительственного распоряжения, будут концептуально представлены на рассмотрение компетентным органам, а их выполнение сможет быть проверено и подтверждено уполномоченными для этих целей службами.

(4) Разрешение на открытие центра сертификации в случае необходимости, может иметь дополнительные определения уточняющего характера с целью более точной проверки выполнения центром предписаний настоящего Закона и §16 правительственного распоряжения.

(5) Компетентные органы выдают соответствующий сертификат на ключи для дешифрации подписи, которые применяются для подписания сертификатов. Порядок выдачи сертификатов сертификцентрами действует также и в отношении выдачи сертификатов компетентными органами. Последние должны в любой момент

предоставить возможность с помощью обычных средств телекоммуникации проверить или отозвать выдаваемые ими сертификаты. Этот порядок распространяется также на информацию о реквизитах центра сертификации (адрес и номер телефона), прекращении действия выдаваемых им сертификатов, о приостановке деятельности центра, а также об отзыве или изъятии разрешения.

(6) Согласно настоящему Закону и §16 правительственного распоряжения в государственную казну взимается плата (налоги и издержки).

§5

Выдача сертификатов

(1) Лица, ходатайствующие о выдаче сертификатов, должны быть надежно идентифицированы в сертификационном центре. Центр выдачи сертификатов должен подтвердить степень соответствия подписи и лица путем выдачи сертификата подписи и обеспечить в любое время любому лицу возможность с помощью обычных средств телекоммуникационной связи проверить, а при необходимости и с согласия владельца аннулировать сертификат подписи, а равно и атрибутивный сертификат.

(2) Центр сертификации должен по требованию заявителя включить в содержание сертификата подписи и атрибутивного сертификата сведения о его полномочиях выступать от имени третьего лица, если будет получено ясное согласие этого третьего лица.

(3) Центр сертификации должен по требованию заявителя ввести в сертификат вместо имени заявителя его псевдоним.

(4) Центр сертификации должен принять меры предосторожности для того, чтобы исключить возможность уничтожения, изменения либо подделки данных для сертификата. Он также должен принять меры предосторожности для сохранения в тайне ключа личной подписи. Сбор и накопление ключей личных подписей центром сертификации не допускается.

(5) Центр сертификации для осуществления своей деятельности должен иметь проверенный и надежный персонал. Для изготовления ключа подписи, а также сертификатов, должны применяться технические средства согласно §14. Это относится также и к техническим средствам для проверки сертификатов согласно пункту 2 абзаца 1.

§6

Порядок осведомления

Центр сертификации, согласно §5 абз. 1, должен уведомить заявителя о мерах по обеспечению надежности подписи и ее проверки. Он также должен уведомить заявителя о технических средствах, соответствующих требованиям §14 абз. 1, а также о порядке личной цифровой подписи. Центр сертификации должен также сообщить с течением времени о возможности повторного подписания данных, если с течением времени степень защищенности подписи окажется недостаточной.

§7

Содержание сертификатов

(1) Сертификат с ключом цифровой подписи должен иметь следующие данные:

1. имя владельца подписи, снабженное во избежание ошибок необходимым дополнением либо исключающим ошибки псевдонимом,

2. соответствующим ключом подписи владельца,

3. обозначение алгоритмов, с помощью которых можно использовать ключ подписи владельца, а также ключ центра сертификации,

4. номер сертификата,

5. начало и конец срока действия сертификата,

6. название центра сертификации и

7. данные об ограничении действия ключа подписи.

(2) Данные о полномочиях выступать от имени третьих лиц, а также о иных допусках можно приводить как в ключевом, так и в атрибутивном сертификате.

(3) Другие данные ключевой сертификат может приводить только с согласия заинтересованных лиц.

§8

Запрет действия сертификата.

(1) Центр сертификации должен наложить запрет на действие сертификата, если окажется, что владелец подписи или его заместитель передали для данного сертификата неправильные данные (§7), либо если центр сертификации прекратил свою деятельность и не передал права на ее возобновление другому центру сертификации либо соответствующие компетентные органы, согласно §13 абз. 5 пункт 2, не потребуют наложения запрета. Запрет на действие должен иметь срок, после которого деятельность может быть возобновлена. Запрет деятельности не имеет обратной силы.

(2) Если сертификат содержит данные о третьем лице, то последнее имеет право требовать наложение запрета деятельности данного сертификата.

(3) Соответствующие компетентные органы, согласно §4, могут наложить запрет на действие выданного ими сертификата, если центр сертификации прекратил свою деятельность, либо в случае изъятия разрешения.

§9

Таймер времени

Центр сертификации должен, в случае необходимости, снабдить цифровые данные таймером времени. §5 абз. 5 пункты 1 и 2 действуют соответственно.

§10

Документация

Центр сертификации должен документально оформить меры по соблюдению выполнения настоящего Закона и §16 правительственного предписания таким образом, чтобы обеспечить в любой момент возможность проверки данных и их идентичности.

§11

Прекращение деятельности

(1) В случае прекращения своей деятельности центр сертификации должен в кратчайший срок заявить об этом соответствующим компетентным органам и обеспечить передачу действующих сертификатов иному центру сертификатов либо наложить запрет на их действие.

(2) Центр сертификации, прекращающий свою деятельность, должен передать, согласно §10, всю соответствующую документацию другому центру либо соответствующим компетентным органам.

(3) Центр сертификации, прекращающий свою деятельность, должен незамедлительно объявить о ходатайстве соответствующих компетентных органов об объявлении конкурса.

§12

Защита данных

(1) Центр сертификации имеет право получить сведения, имеющие персональный характер лишь от заинтересованного лица и только для оформления сертификата. Сбор данных о третьих лицах допускается только с согласия этих третьих лиц. Для иных, не указанных в пункте 1 целей эти данные могут использоваться лишь в рамках настоящего Закона и других правовых документов либо с согласия заинтересованных лиц.

(2) Если лицо, владеющее ключом к подписи, имеет псевдоним, то данные о его идентификации могут быть переданы соответствующим органам по их запросу лишь в случае, если это необходимо для исполнения штрафных санкций, для предотвращения опасности нарушения общественного порядка и безопасности либо для исполнения обязанностей конституционных федеральных либо земельных органов, федеральной службы связи, военной безопасности и служб по борьбе с криминальными правонарушениями. Раскрываемые сведения фиксируются документально. Заинтересованное лицо информируется о раскрытии тайны псевдонима как только интересы следствия позволят это сделать, либо интересы заинтересованного лица не возобладают.

(3) Федеральный закон защиты данных имеет оговорку, согласно которой проверка может проводиться и в том случае, если нет предпосылок для нарушения предписаний и инструкций по защите данных.

§13

Контроль и исполнение обязательств

(1) По отношению к центру сертификации компетентный орган может осуществить мероприятия по обеспечению выполнения требований настоящего Закона и соответствующих предписаний. Так, соответствующий компетентный орган может запретить использование несоответствующего технического оборудования, а также полностью или частично приостановить деятельность всего центра сертификации. Лицам, не имеющим соответствующего разрешения, может быть запрещено занятие сертификационной деятельностью.

(2) С целью осуществления надлежащего надзора и проверок, центры сертификации должны обеспечить доступ компетентным органам, согласно абз. 1 п. 1, в служебные помещения в рабочее время, предоставлять по требованию необходимые книги, рисунки, чертежи, справки и другие документы, предоставлять необходимые сведения и оказывать необходимую помощь. Лицо, ответственное за выдачу сведений справочного характера, может отказаться от дачи сведений в случае, если дача этих сведений может привести к опасности возникновения в его лично адрес либо адрес перечисленных в §383 абз. 1 п.13 гражданско-процессуального кодекса служащих судебного преследования за совершенное должностное преступление, либо возбуждения судебного процесса, согласно Закону о правонарушениях. Лицо, ответственное за выдачу сведений справочного характера, должно быть проинформировано об этом своем праве.

(3) При невыполнении обязанностей в соответствии с настоящим Законом и соответствующими предписаниями и в случае возникновения предпосылок для изъятия разрешения, соответствующие компетентные органы должны изъять разрешение, если все перечисленные в абз. 1 п. 2 меры не привели к ожидаемым результатам.

(4) В случае изъятия разрешения либо приостановления деятельности центра сертификации соответствующие компетентные органы должны обеспечить передачу деятельности другому центру сертификации либо обеспечить продолжение действия договора с владельцем ключа подписи. Этот порядок действует также и в случае объявления конкурса, если разрешенная деятельность не может быть осуществлена.

(5) Выданный центром сертификации сертификат является действительным до момента изъятия его или приостановки его действия. Соответствующие компетентные органы могут приостановить действие сертификата при наличии фактов, свидетельствующих о том, что данный сертификат является фальшивым либо недостаточно проверенным, либо что технические средства, применяемые для изготовления ключей подписи, являются недостаточно надежными и допускают незаметные искажения подписи либо подписываемых данных.

§14

Технические средства

(1) Для изготовления и хранения ключей подписи, а также для изготовления и проверки цифровой подписи необходимы технические средства, имеющие необходимые меры предосторожности для надежного обнаружения искажения цифровой подписи либо подписываемых данных, а также для защиты от противоправного использования личного ключа подписи.

(2) Для изображения подписываемых документов необходимыми являются технические средства, позволяющие однозначно определить способ изготовления цифровой подписи и установить, к каким данным относится данная цифровая подпись. Для проверки

подписанных данных необходимо применять технические средства, позволяющие определить идентичность и неизменность подписанных данных, к каким данным относится данная подпись и кому она принадлежит.

(3) Технические средства с помощью которых, согласно §5 абз. 1 п.2, осуществляется проверка и аннулирование сертификатов с ключом подписи, должны иметь необходимые меры предосторожности для защиты сертификата от неправомочных изменений и несанкционированного запрета.

(4) Согласно абз. 1-3, технические средства должны быть надлежащим образом проверены в соответствии с уровнем развития техники на данном этапе, а степень соответствия требованиям должна быть документально подтверждена соответствующими компетентными органами.

(5) Технические средства, изготавливаемые и используемые в соответствии с правилами и нормами, действующими в других странах Европейского Союза либо в странах, входящих на договорных основах в Европейское экономическое пространство, должны по своим защитным качествам и свойствам соответствовать абзацам 1-3. В отдельных случаях по требованию соответствующих компетентных органов должны быть предъявлены доказательства соответствия требованиям, изложенным в п. 1. В случае, если для доказательства степени соответствия защитных свойств технических средств требованиям, изложенным в пп. 1-3, необходимо иметь подтверждение соответствующих компетентных органов, аналогичные подтверждения должны быть представлены соответствующими компетентными органами других стран-членов Европейского Союза или стран, входящих в Европейское экономическое пространство.

§15

Зарубежные сертификаты

(1) Цифровые подписи, которые могут быть проверены с помощью ключа подписи, на который имеется зарубежный сертификат страны-участницы Европейского Союза либо государства, входящего в Европейское экономическое пространство и которые обладают адекватной степенью защиты, приравниваются к цифровым подписям, действующим согласно настоящему Закону.

(2) Действие абзаца 1 распространяется также и на другие государства, с которыми имеются соответствующие соглашения.

§16

Правительственное предписание.

Федеральное правительство уполномочено через свои постановления издавать необходимые для выполнения требований, изложенных в §§3-15, правовые предписания, касающиеся:

1. детальной разработки порядка выдачи, приостановки действия и изъятия разрешения, а также порядка приостановки деятельности центра сертификации,

2. вопросов, связанных с налогообложением, согласно §4 абз. 6 и величиной налогов,

3. подробного определения обязанностей центра сертификации,

4. срока действия полномочий сертификата ключа подписи,

5. подробного определения порядка контроля центра сертификации,

6. разработки подробных требований, предъявляемых к техническим средствам, а также проверки технических средств и выдачи удостоверений об их соответствии необходимым нормам,

7. срока и порядка изготовления новой цифровой подписи.

Статья 4

Изменения в уголовном кодексе

Уголовный кодекс в редакции от 10 марта 1987 (БЗ ФРГ с. 945, 1601) с изменениями статьи 1 от 1 июля 1997 (БЗ ФРГ с. 1607) изменяется следующим образом:

1. §11 абз. 3 излагается в следующей редакции:

"(3) К разряду сочинений относятся носители звука и изображения, упоминаемые в тех правовых предписаниях, которые ссылаются на настоящий абзац".

2. §74 изменяется следующим образом:

а) в абзаце 3 после слова "сочинения" добавляется: "(§11 абз. 3)".

б) в абзаце 4 слова "если хотя бы часть" заменяются словами: "если сочинение либо хотя бы часть сочинения".

3. В §86 абз.1 после слова "выполняет" добавляются слова: "или обеспечивает доступность в накопителях данных".

4. §184 изменяется следующим образом:

а) в абз.4 после слова "действительное" добавляется: "или близкое к действительному".

б) в абз.5 п.1 после слова "действительное" добавляется: "или близкое к действительному".

Статья 5

Изменение закона о правонарушениях

Закон о правонарушениях в редакции от 19 февраля 1987 (БЗ ФРГ, ч.1, с.602) с изменениями ст.19 от 18 июня 1997 (БЗ ФРГ, ч.1, с.1430), изменяется следующим образом:

1. в §116 абз.1, абз.1 п.2 и§123 абз.2 п.1 после слов: "носители изображения" ставится запятая и добавляются слова: "накопители данных".

2. §119 изменяется следующим образом:

а) в абз.1 п.2 после слова "изображения" добавляются слова: "или благодаря доступности накопителей данных".

Статья 6

Изменение закона о распространении сочинений, наносящих вред моральному здоровью молодежи

Закон о распространении сочинений, наносящих вред моральному здоровью молодежи в редакции от 12 июля 1985 (БЗ ФРГ ч.1, с.1502) с изменениями статьи 16 абз.1 от 28 октября 1994 (БЗ ФРГ с.3186) изменяется следующим образом:

1. заглавие излагается в следующей редакции:

"З А К О Н"

о распространении сочинений и сообщений в средствах массовой информации, наносящих вред моральному здоровью молодежи".

2. §1 абз.3 излагается в следующей редакции:

"(3) К сочинениям приравниваются носители звука и изображения, рисунки и другие изображения. Сочинениями по настоящему Закону не являются, согласно §2 Государственного договора по радиовещанию, передачи радиовещания, а также сообщения служб выдачи и изъятия разрешений, если для них требуется редакционная правка с целью формирования общественного мнения, согласно Государственному договору о средствах массовой информации в редакции от 20 января-7 февраля 1997."

3. §3 изменяется следующим образом:

а) в абз.1 после пункта 3 ставится запятая и добавляется пункт 4 следующего содержания:

"4. распространяются службами информации и коммуникации или иным способом."

б) в абзац 2 добавляется следующее предложение:

"Действие пункта 4 первого абзаца не распространяется на случай, если в результате принятых технических мер предосторожности возникает ситуация, при которой абоненту, заключившему договор пользования сроком на полный год, может быть ограничено предложение и распространение внутри страны."

4. §5 абзац 3 излагается в следующей редакции:

"(3) Действие абзаца 2 не распространяется:

1. если деловое отношение завершилось заключением соответствующей сделки, либо

2. если в результате предпринятых мер предосторожности для детей и молодежи исключается возможность получения сведений либо ознакомления с ними."

5. После §7 вводится §7a:

"§7a

Уполномоченный по делам защиты молодежи.

Предоставителю информационных и коммуникационных услуг, в основе которых лежит принцип передачи с помощью телекоммуникации, необходимо пригласить уполномоченного по делам защиты молодежи, если в содержании предоставляемых услуг имеется информация, могущая нанести вред моральному здоровью молодежи. Уполномоченный по делам защиты молодежи осуществляет консультации пользователя и предоставителя услуг в вопросах защиты молодежи. Он участвует в планировании предоставляемых услуг и оформлении общих правил пользования. Он имеет право предложить предоставителю услуг ограничить предоставляемые услуги. Обязанностью предоставителя, согласно предложению 1, является организация добровольного самоконтроля для выполнения требований, изложенных в предложениях 2-4."

6. После §21 абз.1 п.3 добавляется пункт 3a следующего содержания:

"3a. Вопреки требованиям, изложенным в §3 абз.1 п.4, распространяет, предоставляет или делает доступным иными способами."

7. §18 излагается в следующей редакции:

"§18

(1) Сочинение подлежит ограничению, согласно §§3-5, даже без подробного ознакомления и внесения в списки литературы, подлежащей ограничению, если оно полностью либо в основных чертах совпадает с таковыми, уже занесенными в списки для ограничения. Это касается и случаев, когда суд в своем решении констатировал, что сочинение обладает порнографическим содержанием либо содержанием, перечисленным в §130 абз.2 либо §131 Уголовного кодекса.

(2) В случае наличия сомнений в выполнении условий, изложенных в абз.1, председательствующий прилагает заключение соответствующего федерального контролирующего органа. При этом наличие ходатайства (§11 абз.2 предл.1) не является обязательным. §12 действует соответственно.

(3) Если рассматриваемое сочинение внесено в список литературы, подлежащей ограничению, то §19 действует соответственно."

8. §18a вычеркивается.

9. §2 изменяется следующим образом:

а) прежним текстом становится абзац 1.

б) вводится абзац 2 следующего содержания:

"(2) Если занесение в списки для ограничений не принимается во внимание, председательствующий может потребовать приостановки деятельности."

10. §21a абз.1 излагается в следующей редакции:

"(1) Противоправно действует лицо, которое:

1. вопреки требованиям §4 абз.2 предл.2 не проинформирует покупателя о наличии ограничения сбыта,

2. вопреки требованиям §7a абз.1 предл.1 не воспользуется услугами уполномоченного по делам защиты молодежи либо не организует добровольный самоконтроль для выполнения настоящих требований."

Статья 7

Изменения в законе об авторском праве

Закон об авторском праве от 9 сентября 1965 (БЗ ФРГ с.1273) с изменениями статьи 5 от 19 июля 1996 (БЗ ФРГ с.1014) изменяется следующим образом:

1. §4 излагается в следующей редакции:

"§4

Сборники и банки данных.

(1) Собрание произведений, данных или других независимых элементов, которые на основе своего выбора или расположения являются личными духовными творениями (сборники), подлежат защите по закону так же, как и самостоятельные произведения, несмотря на наличие правовой защиты отдельных элементов.

(2) Банком данных, в соответствии с настоящим Законом, является сборник, элементы которого расположены в методическом или систематическом порядке, и доступ к которым осуществляется с помощью электронных средств либо иным способом. Компьютерная программа, применяемая для создания банка данных либо для доступа к его элементам (§69a), не является составной частью банка данных."

2. §23 предл.2 изменяется следующим образом:

а) после слова "искусства" слово "или" заменяется запятой.

б) после слова "архитектура" добавляются слова: "или о переработке либо оформлении банка данных."

3. §53 изменяется следующим образом:

а) после абзаца 4 добавляется абзац 5 следующего содержания:

"(5) Действие абзаца 1, а также абзаца 2 пункты 2-4 не распространяется на базы данных, элементы которых могут быть доступны с помощью электронных средств. Действие пункта 1 абзаца 2 распространяется на такие банки данных при условии, что данные, имеющие научный характер, не будут применяться в коммерческих целях."

б) абзацы, имевшие номера 5 и 6, получают соответственно номера 6 и 7.

4. После §55 добавляется §55a следующего содержания:

"§55a

Использование банка данных.

Допустимыми являются обработка, а также размножение банка данных, запущенного в оборот с согласия автора владельцем, путем продажи части банка данных, подлежащей размножению, уполномоченным, необходимым в остальных случаях для пользования этой частью, либо лицом, которому база данных становится доступной на основе заключенного - с автором либо с согласия последнего с третьим лицом - договора, если и поскольку для доступа к элементам банка данных и для его обычного использования обработка и размножение является необходимыми. Если на основе договора, согласно предложению 1, доступна только часть банка данных, то допустимыми являются обработка и размножение только этой части. Иные договорные соглашения являются недействительными."

5. §63 абз.1 изменяется следующим образом:

а) после предложения 1 добавляется предложение 2 следующего содержания:

"Подобное же действие распространяется и на случаи, указанные в §53 абз.2 п.1 и абз.3 п.1, для размножения базы данных."

б) предложения 2 и 3 становятся соответственно предложениями 3 и 4.

6. После §87 добавляется раздел следующего содержания:

"Шестой раздел

Защита основателя банка данных.

§87a

Определение понятий.

(1) Банком данных, согласно настоящему Закону, является собрание произведений, данных или иных независимых элементов, расположенных в систематическом или методическом порядке и доступных с помощью электронных или иных средств, сбор, проверка или изображение которых требует значительных инвестиций. Банк данных со значительно измененным содержанием считается новым банком данных, поскольку это требует значительных инвестиций.

(2) Основателем банка данных, согласно настоящему Закону, является лицо, сделавшее необходимые инвестиции, упоминаемые в абзаце 1.

§87б

Права основателя банка.

(1) Основатель банка данных имеет исключительное право на размножение, распространение и публичное отображение банка данных в полном объеме либо в значительной его части. К размножению, распространению либо публичному

отображению существенной части банка данных приравнивается систематическое и повторяющееся размножение, распространение либо публичное отображение несущественных его частей, если подобные действия мешают нормальному использованию банка данных, либо наносят ущерб законным интересам основателя банка.

(2) §17 абз.2 и §27 абз.2 и 3 применяются соответственно.

§87в

Ограничения прав основателя банка данных.

(1) Размножение существенной части банка данных допускается:

1. для частного использования; это положение не распространяется на банк данных, элементы которого по отдельности доступны с помощью электронных средств,

2. для собственного использования с научной целью, если размножение осуществляется с этой целью и не преследует коммерческих целей,

3. для собственного использования в целях обучения в некоммерческих учебных заведениях для начального и продвинутого обучения, а также для профессионального обучения в количестве, необходимом для оборудования одного учебного класса.

В случаях, упоминаемых в пп.2 и 3, необходимо точно указать источник.

(2) Размножение, распространение и публичное отображение существенной части банка данных допускается при рассмотрении дела в суде, в третейском суде или административном учреждении, а также в целях общественной безопасности.

§87г

Срок действия прав.

Права основателя банка данных утрачивают законную силу спустя пятнадцать лет со дня объявления о создании банка, однако не позднее пятнадцати лет после создания банка данных, если в течение этого срока о его создании не было объявлено. Срок действия прав рассчитывается согласно §69.

§87д

Договоры пользования банком данных

Договорное соглашение, которым владелец запущенной в обращение путем продажи с согласия основателя банка данных части банка данных, доступ к которой в иных случаях мог бы быть осуществлен лишь с согласия уполномоченного лица либо лица, имеющего доступ к банку данных на основе договора, заключенного с основателем банка данных, либо с согласия последнего с третьим лицом, берет на себя обязательства не осуществлять размножение, распространение или публичное отображение незначительной части банка данных, является недействительным, если эти действия препятствуют нормальной эксплуатации банка данных или наносят непреднамеренный ущерб интересам основателя банка данных".

7.

В §108 абз. 1 после п. 7 добавляется следующий пункт:

"8. использует банк данных вопреки §87б абз. 1"

8. В §119 абз.3 после слова "фотографии" слово "и" заменяется запятой и после слова "звуконоситель" добавляются слова: "и банки данных, подпадающие под действие §87б абз.1".

9. После §127 добавляется §127а следующего содержания:

"§127а

Защита основателя банка данных

(1) Под защиту §87б попадают государственные служащие ФРГ, а также юридические лица, находящиеся в правовом поле настоящего Закона. Необходимо также принять действие §120 абз.2.

(2) Юридические лица, организованные на основе права ФРГ либо иного перечисленного в §120 абз. 2 п. 2 государства, не находящиеся в правовом поле настоящего Закона, попадают под действие §87б в случае, если:

1. главное управление или главный филиал этого юридического лица находится на территории одного из указанных в §120 абз. 2 п. 2 государств или

2. уставное местопребывание находится на территории одного из упомянутых в п.1 государств, и деятельность этого юридического лица обнаруживает фактическую связь с экономикой ФРГ либо одного из вышеупомянутых государств.

(3) В остальных случаях граждане других государств, а равно юридические лица пользуются правовой защитой на основе межгосударственных договоров, а также соглашений, которые Европейское сообщество заключает с третьими странами; эти соглашения публикуются федеральным министерством юстиции в бюллетене законов ФРГ".

10. После §137е добавляется §137ж следующего содержания:

"§137ж

Регламентация на переходный период при реализации директивы 96/9/ЕС

(1) Действие §23 предл. 2, §53 абз. 5, §§55а и 63 абз. 1 предл. 2 распространяется также на банки данных, созданные до 1 января 1998.

(2) Предписания шестого раздела второй части распространяются также на банки данных, созданные за период между 1 января 1983 и 31 декабря 1997. Срок действия защиты в этом случае исчисляются с 1 января 1998.

(3) Действие §§55а и 87д не распространяется на договоры, заключенные до 1 января 1998".

Статья 8

Изменения закона о тарифах

В §1 Закона о тарифах от 3 декабря 1984 (БЗ ФРГ, с. 1429) добавляется следующее предложение:

"При расчетах за информационные и коммуникационные услуги могут указываться данные об уровне цен текущих платежей".

Статья 9

Изменение в положении об обозначении цены

Положение об обозначении цены от 14 марта 1985 (БЗ ФРГ, с. 580), впоследствии измененное Положением от 14 октября 1992 (БЗ ФРГ, с. 1765) изменяется следующим образом:

1. В §3 абз. 1 добавляется следующее предложение:

"Местом указания платежа является также экран дисплея. Если размер платежа приводится на дисплее и указывается в единицах измерения, то могут быть бесплатно предоставлены отдельно данные о текущем использовании".

2. §8 абз. 2 п. 2 излагается в следующей редакции:

"2 §3 абз. 1 предл. 1, 2 или 4, либо абз. 2 также в связи с §2 абз. 5 о состоянии, предоставлении или сохранении списка цен или о предоставлении указателя цен".

Статья 10

Возврат к единому уровню регламентации

Части Положения об обозначении цен, имеющие в качестве правовой основы статью 8, могут быть изменены на основе §1 Закона о тарифах.

Статья 11

Вступление в силу

Настоящий Закон, за исключением статьи 7, вступающей в силу 1 января 1998, вступает в силу с 1 августа 1997.

Конституционные права федерального совета соблюдены. Настоящий Закон является законченным и публикуется в бюллетене законов ФРГ.

Берлин, 22 июля 1997. Подписи высших должностных лиц ФРГ

---

[1] Термины "прослушивание телефонных разговоров", "прослушивание телефонов" и

"перехват телефонных разговоров" используются в этой книге как синонимы и означают тайный перехват телефонных разговоров третьей стороной, действующей от имени государства.
[2] Обзор работы David Murgio. Telephone Tapping in International Law and Seven European Countries. - The Helsinki Foundation for Human Rights, Warsaw, Poland, 1996 (в дальнейших ссылках - D.Murgio) и статьи Larence Lustgarten. Telephone Tapping in Great Britain - the Legal Structure.
[3] (Серия A, N 28), (1979-80) 2 EHRR 214. Взято из WestLaw.
[4] Ссылаясь на судебные документы, мы будем записывать их в скобках, указывая имя подателя заявления и номера параграфа в публикации Серии A.
[5] Статья 25(1) устанавливает право "любого лица, неправительственной организации или группы лиц, которые утверждают, что явились жертвами нарушения... прав, установленных Конвенцией..." обратиться в Европейскую Комиссию по правам человека, если соответствующее государство признает "компетенцию Комиссии получать такие жалобы".
[6] (Серия A, N 82) (1985) 7 EHRR 14. Взято из Lexis-Nexis.
[7] (Серия A, N 176-B) (1990) 12 EHRR 528. Взято из Lexis-Nexis.
[8] (Series A, No 176-B) (1990) 12 EHRR 547. Взято из Lexis-Nexis.
[9] (Серия A, N 277-B) (1994) 17 EHRR 462. Взято из Lexis-Nexis.
[10] Перевод соответствующего раздела работы D.Murgio.
[11] Обзор работы D.Murgio и статьи Larence Lustgarten. Telephone Tapping in Great Britain - the Legal Structure.
[12] D.Murgio.
[13] Нормы о прослушивании телефонов, изложенные в Дополнении G-10 к Основному Закону Федеральной Республики Германии и поддержанные Судом в деле Класса, составляют сейчас единый закон на эту тему для объединенной Германии.
[14] Обзор статьи Kirsi Piispanen. Every word you say: legal norms regulating collection of information by police force in Finland.
[15] D.Murgio.
[16] Обзор статьи Heiner Busch. Telephone surveillance in Switzerland Practice, Law and Perspectives of Change Brief General Information.
[17] Verordnung uber den Dienst fur die Uberwachung des Post - und Fernemeldeverkehs vom 1. Dezem - ber 1997.
[18] Bericht der Parlamentarischen Untersuchungleommission yom. 22 November 1989 - Vorkommnisse im EFPD.
[19] Bericht der parlamentarischen Untersuchungskommission, op. cit. (note 3), pp. 144-148
[20] Nationalrat - Geschaftsprufungskommission: Die Felefonuberwachung im Bund. Bericht der Geschaftsprufungs commission des Nationalrates an den Bundesrat uber ihre Inspektion vom9. November 1992, Berne 10 nov. 1992.
[21] Staatsschutz in der Stadt Zii rich. Bericht der Untersuchungskommission an den Gemeinderut von Zurich, Zurich february 1991, особенно см. pp. 161 ss.
[22] op. cit. (прим. 3), p. 147.
[23] Sonderbeauftragter furdie Staatsschutzakten de Bundes: Schlussbericht, Berne 2 may 1996.
[24] op. cit (прим. 7), p. 14.
[25] op. cit (прим. 7), p. 17-18.
[26] op. cit. (прим. 7), p. 12.
[27] Об этой практике писала пресса, Sonntagszeitung 27. 12. 1997.
[28] Der Bund, 7. 2. 1996.
[29] Обзор статьи Dennis Toellborg. Report on Wire Tapping Legislation in Sweden.
[30] Использованы работа D.Murgio и отчеты венгерского участника Проекта "Службы безопасности в условиях конституционной демократии" Марты Пардави.
[31] Термин "службы национальной безопасности" включает гражданские (Служба

Разведки, Служба Национальной Безопасности и Специальная Служба Национальной Безопасности) и военные (Служба Военной Разведки, Служба Военной Безопасности) службы безопасности.
[32] D.Murgio.
[33] А именно: оружие, боеприпасы, взрывчатые вещества, наркотики и психотропные вещества, ядерные и радиоактивные материалы.
[34] Раздел написан составителем, при этом частично использованы замечания D.Murgio.
[35] Известия, 1990, 24 июня.
[36] Конституция Российской Федерации. - М.: Юридическая литература, 1995. - с.11.
[37] Все цитаты из этих законов даются по изданию: Спецслужбы России: законы и комментарий. Авт.-сост. А.Ю.Шумилов. М.: Юристъ, 1997. - 344 с.
[38] "Органы ФСБ" включают Российскую Федеральную Службу Безопасности, ее региональные управления (отделы), а также ее управления (отделы) в различных воинских формированиях (ст. 2 Закона о ФСБ).
[39] Право на проведение ОРД имеют органы внутренних дел, органы федеральной службы безопасности, федеральные органы налоговой полиции, государственной охраны, органы пограничной службы, таможенные органы и службы внешней разведки (ст. 13).
[40] Конституционный Суд Российской Федерации. Постановления. Определения.1992 - 1995. М., 1997, с.135-139..
[41] D.Murgio.
[42] Эти органы включают: Румынскую разведывательную службу, Иностранную разведывательную службу, Охранную службу, а также три министерства - Обороны, Внутренних дел и Юстиции (ст. 6).
[43] Раздел написан составителем.
[44] Здесь и далее Закон цитируется по изданию: Ведомости Верховной Рады Украины, 1992,№39, ст.572.
[45] Постановления Пленума Верховного Суда Украины (1995 - 1998). - Бюллетень законодательства и юридической практики Украины, №8, 1998. - с.55.
[46] Ведомости Верховной Рады Украины, 1994, №24, ст.184.
[47] Перевод заключительной части работы: Dennis Toellborg. Report on Wire Tapping Legislation in Sweden.
[48] Подробности и конкретные примеры даны в: Toellborg. Undercover in Sweden. The Swedish Security Police and Their Modi Operandi, in Fijnaut /Marx, Police Surveillance in Comparative Perspective, Kluwer 1995/.
[49] Раздел написан составителем.
[50] Раздел написан составителем.
[51] Русский Журнал. Net-культура http://www.russ.ru/journal/netcult Статья перепечатывается с любезного разрешения издателей Русского Журнала
[52] Отрывок из доклада Privacy International "An International Survey of Privacy Laws and Practice"
[53] Бюллетень российской правозащитной сети "Права человека в России", №38, с.15-17, перевод с английского Сергея Смирнова.
[54] Бюллетень российской правозащитной сети "Права человека в России", №38, с.17-26, перевод с английского Сергея Смирнова.
[55] Армин Медош Опубликовано 29 ноября 1998 г. в немецком электронном журнале Telepolis http://www.telepolis.de
[56] Дункан Кэмпбелл, "Гардиан", 29 апреля 1999 г.
[57] Мэдлейн Эйси. Опубликовано в электронном журнале TechWeb http://www.techweb.com 13 мая 1999 г.
[58] Мэдлейн Эйси. Опубликовано20 мая 1999 г. в электронном журнале TechWeb http://www.techweb.com/wire/story/TWB19990520S0022
[59] Бюллетень российской правозащитной сети "Права человека в России", №38, с.26-31

(кроме статьи А.Травина), перевод с английского Сергея Смирнова.
[60] Источник: Toshimaru Ogura, ogr@nsknet.or.jp http://www.jca.ax.apc.org/~toshi
[61] Перепечатывается с любезного разрешения редакции "Русского журнала"
[62] S.J. Singh (Нью-Дели, Индия). Оригинал:
http//www.data.com/story/DCM19990426S0001
[63] Источник - HURlNet, The Human Rights Information Network
sdenney@OCF.Berkeley.EDU, 19 мая 1999 г.
[64] Бюллетень российской правозащитной сети "Права человека в России", №38, с.31-33.
Перевод с английского Сергея Смирнова.
[65] Оригинал на сервере GILC: http:/www.gilc.org
[66] BGB -Бюллетень законов ФРГ (БЗ ФРГ)
[67] Указания, содержащиеся в Директиве 83/189/EWG Совета Европы от 28 марта 1983, относящиеся к области нормативов и технических предписаний при различных способах передачи информации (ABT EG N.L.109 с.8) с внесенными изменениями Директивой 94/10/EG Европейского парламента Совета Европы должны приниматься к сведению.