"ПРАВО ЗНАТЬ: история, теория, практика"
N 1–2 (61–62) январь–февраль 2002 г.

НАМЕРЕНИЯ – БЛАГИЕ
Борясь с терроризмом, силовые ведомства заодно берут под контроль всю информационную сферу

Так получилось, что в папке материалов для этого выпуска рядом легли два сообщения. Одно было посвящено тому, что 20 декабря 2001 года большинством голосов депутатов Государственной Думы (374 – за, 4 – против, воздержавшихся нет) был принят в первом чтении проект Федерального закона "О внесении изменений в статью 4 Закона Российской Федерации "О средствах массовой информации" и в статью 15 Федерального закона "О борьбе с терроризмом". Прежде всего изменения предполагается внести в статью 4 Закона РФ "О средствах массовой информации". В данной статье, как известно, содержится запрет на злоупотребление свободой массовой информации. В соответствии со ст. 16 того же Закона, нарушение редакцией требований статьи 4 является основанием для вынесения предупреждений со стороны Минпечати, а также прекращения судом деятельности СМИ. В изложенную в законопроекте новую редакцию статьи в понятие "злоупотребление свободой массовой информации" включено использование СМИ "для пропаганды или оправдания экстремизма". Помимо самих СМИ, запрет распространен, по терминологии законопроекта, и на "компьютерные сети информации".

Изменения, вносимые законопроектом в Федеральный закон "О борьбе с терроризмом" от 25 июля 1998 года, конкретизируют ограничение распространения информации, имеющей значение для проведения контртеррористических операций. К такой информации относятся сведения, раскрывающие специальные технические приемы и тактику проведения контртеррористической операции, а также сведения, распространение которых способно затруднить проведение контртеррористической операции и создать угрозу жизни и здоровью людей, оказавшихся в зоне проведения контртеррористической операции или находящихся за пределами указанной зоны. Законопроектом установлен абсолютный запрет на распространение указанной информации любыми способами, в том числе, как особо оговорено законопроектом, и через СМИ.

Кроме этого уточнений, пункт 3 части 2 статьи 15 Закона расширен за счет запрета распространять не только "информацию, служащую пропаганде или оправданию терроризма и экстремизма", но и "высказывания террористов и экстремистов". Однако указанием на них как авторов высказываний, запрещенных к распространению, законопроект не ограничивается. Им вводится сложно сконструированное понятие "иных лиц. препятствующих осуществлению контртеррористических операций, которые пропагандируют и (или) оправдывают сопротивление проведению контртеррористических операций в любой форме", в отношении высказываний которых установлен аналогичный запрет на распространение.

Во втором материале сообщалось о том, что в МВД разрабатываются законопроекты, где предлагается обязательная регистрация пользователя Интернета в органах внутренних дел. Это означает, что при покупке модема или при подключении к прямой линии доступа в сеть нужно будет сначала получить разрешение в отделении милиции. Будет предусмотрен и комиссионный сбор в пользу государства. В пресс–службе министерства опровергли эти сообщения и подчеркнули, что МВД не собирается в какой–либо степени ограничивать россиянам пользование Интернетом.

Что касается поправок к законам, то, как отмечается в комментарии Института проблем информационного права(См.: ЗиП, 11–12, 2001 г.), вопросы вызывает использование в

законопроекте терминов, не имеющих определения в действующем законодательстве. В первую очередь это касается терминов "экстремизм" и "экстремисты". Дело в том. что до сих пор не принят внесенный правительством Закон "О противодействии политическому экстремизму", на который можно было бы опираться при толковании и применении норм законов. которые содержат или будут содержать указанные термины. Не имея формальных оснований обвинить редакции СМИ в пропаганде терроризма, МПТР потенциально сможет выносить предупреждения за "пропаганду или оправдание экстремизма". Возможность эта будет тем шире, чем более расплывчато будет интерпретироваться властными органами содержание понятий "экстремизм" и "оправдание", также не имеющее четкого юридического содержания. Исходя из сказанного. Институт проблем информационного права предлагает отказаться от включения в статью 4 Закона "О СМИ" понятия "экстремизм" до момента его определения на законодательном уровне.

Другим вопросом, который задают эксперты Института проблем информационного права, является использование термина "компьютерные сети информации". Во–первых, подобное нововведение не является оправданным, поскольку то, что понимается под этим термином, уже сформулировано, причем более удачно, в Законе РФ "О СМИ". Речь идет о статье 24 Закона "О СМИ" "Иные средства массовой информации", в которой используется термин "телекоммуникационные сети". Но более серьезное возражение против использования этой формулировки в Законе "О СМИ" вызывает то. что регулирование содержания информационно–телекоммуникационных сетей вовсе не является предметом Закона "О СМИ".

Что касается использования термина "терроризм", то в законопроекте заложена еще одна проблема, не являющаяся столь очевидной на первый взгляд. Дело в том, что этим понятием на сегодняшний день оперируют два закона – Уголовный кодекс и собственно Федеральный закон "О борьбе с терроризмом". Учитывать это различие необходимо в силу того, что редакции СМИ, соблюдая запрет на распространение высказываний террористов, должны учитывать, что Федеральный закон "О борьбе с терроризмом" определяет термины "терроризм" и "террорист" в более широком смысле, чем Уголовный кодекс РФ. (В Уголовном кодексе терроризм определен в части 1 статьи 205 как "совершение взрыва, поджога или иных действий, создающих опасность гибели людей, причинения значительного имущественного ущерба либо наступления иных общественно опасных последствий, если эти действия совершены в целях нарушения общественной безопасности, устрашения населения либо оказания воздействия на принятие решений органами власти, а также угроза совершения указанных действий в тех же целях". Федеральный же закон "О борьбе с терроризмом" в значительной степени расширил понятие терроризма, включив в него более широкий круг террористических действий. К преступлениям террористического характера им также отнесены захват заложника, распространение заведомо ложного сообщения об акте терроризма, организация незаконного вооруженного формирования или участие в нем, посягательство на жизнь государственного или общественного деятеля, нападение на лиц или учреждения, которые пользуются международной защитой.).

По Уголовному кодексу террорист понимается в более узком смысле: как лицо, осужденное судом за совершение террористических действий, перечень которых, опять же, меньше перечня террористических действий, данного в Федеральном законе "О борьбе с терроризмом". Кроме того, необходимо учитывать, что Закон был принят позже Уголовного кодекса, и поэтому возможна ситуация, при которой правоприменитель будет исходить из определения терминов "терроризм" и "террорист", установленного именно Законом. Тем самым число лиц, высказывания которых СМИ запрещено обнародовать, будет больше, если исходить из определения, данного в Федеральном законе "О борьбе с терроризмом", нежели чем это следует из смысла данного термина в Уголовном кодексе.

Кроме того, необходимо будет разрешить вопрос о том, будет ли полностью запрещено обнародовать в СМИ высказывания террористов. Иными словами, возможен ли будет пересказ журналистами идей террористов, можно ли их сопровождать негативными комментариями, либо любая форма информирования аудитории об идеях терроризма запрещена?

Возвращаясь к вопросу о желании МВД создать систему обязательной регистрации пользователей Интернета, напомним, что, по данным специального корреспондента газеты "Новые известия" Марата Хайруллина, поправка к Закону "О безопасности", предполагающая регистрацию пользователей Интернета в органах внутренних дел, "проходит в центральном аппарате МВД на уровне референта министра внутренних дел".

Об этом журналист сказал в эфире радиостанции "Эхо Москвы". Подготовка такой поправки, предположил журналист. вызвана недавним заявлением ООН о том, что в ближайшее время проблема информационной, компьютерной преступности будет стоять так же остро, как и проблема терроризма и наркобизнеса. В связи с этим, полагает М. Хайруллин, "наши решили принять упредительные меры" и, возможно, объявить Интернет зоной национальной безопасности России.

О подготовке в МВД подобных поправок свидетельствуют и "доклады ученых межведомственной комиссии по информационной безопасности, которая создана при Совете Безопасности России", заметил М. Хайруллин. Кроме того, по словам журналиста, некоторые провайдерские фирмы сообщили о посещениях фирм людьми из органов, которые интересовались тем, как можно контролировать их дело.

"Со стороны властей естественно наложить лапу на свободу печати, телевидение – уничтожить единственный независимый канал, и забыть про Интернет", – сказал М. Хайруллин.

Эта новость, независимо от степени своей достоверности, вновь обострила интерес общественности к проблеме контроля Интернета со стороны силовых ведомств. Одни полагают, что опасность сильно преувеличена. Так например, директор программы "Глобальные инициативы политики Интернета" юрист Федор Кравченко считает, что от опасности государственного контроля над Интернетом Россию "серьезно страхует подпись Путина под Хартией глобального информационного общества, которая была подписана в 2000 году в Окинаве". Такое мнение он высказал в эфире радиостанции "Эхо Москвы". Ф. Кравченко уверен. что "сделать такой шаг назад Россия не смогла бы без потери своего мирового имиджа по информационным вопросам", учитывая серьезное внимание Европы к тому, насколько страна не является тоталитарной в информационных вопросах".

Коснувшись перспективы внесения поправок в Закон "О безопасности", предполагающих регистрацию пользователей Интернета в органах внутренних дел, Ф. Кравченко заметил, что такой законопроект "абсолютно бессмысленен", так как в нем "нет моментов, которые могут реально угрожать Интернету", а кроме того, такой документ "просто не может пройти через Госдуму".

В то же время Ф. Кравченко признал, что реально эффективный контроль за Интернетом возможен только там, где контролируется физическое подключение человека к Сети. Ф. Кравченко не исключает, что подобный законопроект может быть внесен от имени депутата Госдумы, однако юрист считает маловероятным, что законопроект будет исходить от имени МВД и правительства. "Все подобные проекты вкатываются через депутатов как пробные шары и не доходят, как правило, даже до первого чтения", – заметил он.

Другие, например, депутат Госдумы С. Юшенков, полагают, что ограничение доступа в Интернет вполне вписывается в Доктрину информационной безопасности. Как отметил в своем выступлении в эфире радиостанции "Эхо Москвы" С. Юшенков, "ограничения при пользовании Интернетом –это, конечно же, бред, но он вполне укладывается в логику Доктрины информационной безопасности, в которой очень четко прописана необходимость установления госконтроля заСМИ".

По словам С. Юшенкова, уже неоднократно наблюдались "попытки со стороны различных министерств и ведомств в той или иной степени взять под контроль Интернет, обязать провайдеров, чтобы они фактически бесплатно, за свой счет, предоставляли возможность соответствующим структурам пользоваться интернет–ресурсами и просматривать все сообщения интересующих их лиц".

В связи с этим "публикации СМИ, в общем–то, недалеки от истины", считает он. На взгляд С. Юшенкова, "в головах некоторых законодателей и представителей исполнительной власти время от времени возникают такие мысли, и они заявляют, например, что в борьбе с терроризмом необходимо ужесточить контроль за Интернетом"(Источник: Агенство"Эхо Москвы", 1 февраля 2002 г.).

Комментируя эти сообщения и высказывания, следует сказать о том, что борьба с терроризмом и киберпреступ–ностью действительно выходит на передний план во всем мире. Активно ведется она и в России. Нам уже приходилось писать о том, что Интернет сильно раздражает тех, кто раньше направлял и контролировал информационные потоки. С другой стороны, ни для кого не секрет, что современные системы телекоммуникаций практически прозрачны для подслушивающего оборудования. Некоторые системы даже выполняют дополнительную роль и образуют национальную сеть перехвата. Соответствующие работы ведутся и на Западе, и на Востоке, и на Севере, и на Юге. Что касается России, то поначалу инициатива КГБ по созданию с 1994 года системы оперативно–розыскных мероприятий (СОРМ), предполагавшей техническое и юридическое обеспечение доступа этого ведомства к информации, передаваемой по электронным каналам связи (от обычных телефонов до сотовых и пейджинговых систем), прошла практически незамеченной. Однако важнее то, что система эта уже действует, гарантируя спецслужбам доступ к информации, проходящей через телефонные станции: аппаратура СОРМ непременно включается в комплект технических средств новых станций, а обязательство обеспечивать работу СОРМ входит в лицензии всех операторов сотовой телефонии и пейджинговых систем.

СОРМ легко позволяет получать и накапливать информацию о корреспондентах, с которыми поддерживается связь по электронной почте, наборе посещаемых страниц и чатов, читаемых и отвечаемых сообщениях в ньюсгруппах и их тематике, точках входа в Интернет и т.д. За получение и постоянную актуализацию такого рода информации традиционными методами пришлось бы выкладывать колоссальные деньги в расчете на каждого "опекаемого", так что можно было не опасаться массового применения таких приемов. Здесь же составление досье даже на каждого пользователя провайдера и автоматическое его пополнение элементарно автоматизируются и позволяют создавать в итоге базы данных для дальнейшей оперативной разработки... на сотни тысяч человек сегодня и много больше – в будущем.

Совсем недавно начальник Управления "Р" ГУВД Москвы (Столичное подразделение по борьбе с преступлениями в сфере высоких технологий) Дмитрий Чепчугов в интервью "Независимой газете" рассказал о том, что его служба была создана еще в 1983 году, но, поскольку тогда не существовало понятие "компьютерная преступность", перед ней ставились другие задачи. В частности, борьба с радиохулиганством. "Сегодня подобного явления практически нет, и в этом наша заслуга", – заявил шеф столичной

"компьютерной контрразведки".

"Функции настоящего правоохранительного органа на Управление "Р" были возложены в 1997 году – с принятием нового кодекса, в котором появился параграф, посвященный компьютерным преступлениям, а также статей Конституции о правах граждан и юридических лиц на защиту собственной информации, банковскую тайну. Сегодня Управление "Р" как субъект оперативно–розыскной деятельности структурно входит в систему службы криминальной милиции", – отметил Чепчугов.

"Сеть только кажется непрозрачной, – подчеркнул Чепчугов, – на самом деле она весьма упорядочена".

Но не надо быть семи пядей во лбу, чтобы понять, что простым контролем за СМИ и подключением к Интернету, да еще в одной отдельно взятой стране, проблему терроризма и киберпреступности не решишь.

Если бы законодатели и представители исполнительной власти действительно думали о борьбе с обычным и кибер–терроризмом. то они изучили бы уже существующий опыт. Так, например. 23 сентября 1994 г. было принято решение Европейского суда по правам человека по делу "Йерсилд против Дании". Фабула такова: заявитель взял у трех представителей расистской молодежной группы интервью, в ходе которого они произносили оскорбительные и уничижительные высказывания в адрес эмигрантов и этнических групп. Вариант интервью, отредактированный и сокращенный, но сохранивший некоторые из этих высказываний и дополненный замечаниями журналиста, комментировавшего позиции этих молодых людей, был передан в эфир Датской радиовещательной корпорации как один из материалов большой программы. Программа была выпущена в свет в связи с проходившей в стране дискуссией о расизме с намерением установить, кто именно выражает ненависть к меньшинствам и каков менталитет этих людей. Журналисту и руководителю отдела новостей телекомпании были предъявлены обвинения в пособничестве и подстрекательстве этих молодых людей к распространению расистских высказываний.

Суд постановил, что при оценке используемых журналистами приемов судам не следует подменять взгляды отдельных лиц мнением прессы, но в связи со ст. 10(2) Европейской конвенции о правах человека следовало принимать во внимание конкретную роль журналиста в распространении рассматриваемых высказываний. Он также подчеркнул, что спорный материал был попыткой исследовать конкретные аспекты вопроса, который уже заботил общественность. При решении дела суд исходил из факта передачи материала в эфир в рамках серьезной информационной программы и предназначения его для хорошо информированной аудитории. Суд также отметил, что аморальность, опасность и противозаконность пропаганды расовой ненависти не были в этом выпуске выражены в явной форме, но вводные сведения к проведенному интервью, отмежевание журналиста от его собеседников, опровержение некоторых расистских утверждений и общая характеристика этих утверждений как антиобщественных составили достаточный противовес.

Что касается киберпреступности, то ни для кого не секрет, что глобальная всемирная сеть Интернет, объединившая миллионы компьютеров, расположенных в разных странах, и открывшая широчайшие возможности для получения и обмена информацией, действительно все чаще используется в преступных целях. Поэтому можно понять озабоченность правоохранительных органов появлением нового вида преступлений – "транснациональных компьютерных преступлений". В международном сообществе тоже разрабатываются методы борьбы с терроризмом в Сети, но несколько другие. В частности, 23 ноября прошлого года в Будапеште состоялась конференция, посвященная проблеме киберпреступности. 30 стран подписали

конвенцию – первую международную программу по борьбе с кибертерроризмом. Конвенция разрабатывалась Советом Европы в течение 4 лет, в ней рассматриваются законы по борьбе с неавторизованным доступом к компьютерным сетям, перехватом данных, интернет–мошенничеством, детской порнографией и компьютерным пиратством. Конвенцию подписали США, Канада, Япония, Украина, среди неприсоединившихся к конвенции государств – Россия, Дания. Чехия.

Конвенцией по борьбе с киберпреступностью предусмотрены скоординированные действия на национальном и межгосударственном уровнях, по пресечению несанкционированного вмешательства в работу компьютерных систем, незаконного перехвата данных и вмешательства в компьютерные системы.

Принятие в Конвенции статьи "Поиск и конфискация сохраненных компьютерных данных" дает возможность одной стороне добиться сохранения важной информации, необходимой для расследования преступления, которая находится в юрисдикции другой стороны. Насколько известно, провайдер услуг Интернет, как правило, располагает данными об информационном обмене сообщениями в прошлом, которые можно получить с помощью оборудования, регистрирующего конкретные аспекты информационного обмена, включая время, продолжительность и дату любого сообщения. Такие данные хранятся обычно в течение ограниченного периода времени, зависящего от коммерческих потребностей оператора или поставщика услуг, а также юридических требований, касающихся неразглашения частной информации. Национальное законодательство многих стран разрешает правоохранительным или судебным органам издавать распоряжение, касающееся сбора данных информационного обмена. 8 то же время в тех случаях, когда данные информационного обмена являются частью сообщения, например "заголовок" сообщений, передаваемых по электронной почте, сбор таких данных может рассматриваться как перехват самого сообщения и по этой причине подпадать под юридические ограничения.

Важным является положение Конвенции, которое дает возможность принимать законодательные и другие меры, уполномочивающие ее компетентные власти конфисковать или подобным образом обезопасить от уничтожения данные, которые имеются у провайдера и необходимы для расследования. Положения статьи "Быстрая консервация данных, сохраненных в компьютерной системе" и статьи "Быстрая консервация и раскрытие данных трафика" дает возможность правоохранительным органам проводить расследования таких преступлений или предпринимать действия для сохранения данных, которые могут быть уничтожены по истечении определенного периода времени.

В общем, бороться с терроризмом и киберпреступностью надо. Вопрос лишь в том, в какой мере тотальный контроль за СМИ и Интернетом поможет этой борьбе и как не переступить ту тонкую грань, которая отделяет борьбу с преступниками от тотального контроля за гражданами.

Аналитическая группа ПФ "КСДИ"