ЗАКОНОДАТЕЛЬСТВО РОССИЙСКОЙ ФЕДЕРАЦИИ О ДОСТУПЕ К ИНФОРМАЦИИ

Краткий обзор и анализ

Елена Константиновна Волчинская,

Советник аппарата Комитета по безопасности Государственной Думы ФС РФ

Член Российского комитета Программы ЮНЕСКО «Информация для всех»

Содержание:

1. Конституционные права граждан на доступ к информации и принципы ограничения этих прав

Конституция РФ (часть 4 статьи 29) устанавливает общее право каждого «свободно искать, получать, передавать, производить и распространять информацию любым законным способом». Право искать и получать информацию рассматривается нами как право доступа. Оно конкретизируется рядом статей Конституции РФ.

Статья 42 устанавливает права каждого на получение достоверной информации о состоянии окружающей среды.

Право каждого на возможность ознакомления с документами и материалами, непосредственно затрагивающими его права и свободы, обеспечивается установленной ч. 2 статьи 24 обязанностью органов государственной власти и органов местного самоуправления, их должностных лиц обеспечить такую возможность.

Требование к опубликованию для всеобщего сведения нормативных правовых актов, затрагивающих права, свободы и обязанности человека и гражданина, (ч. 3 ст. 15), также создает гарантии доступа к такой информации.

Право на информацию о фактах и обстоятельствах, создающих угрозу для жизни и здоровья людей, обеспечивается ответственностью должностных лиц за сокрытие такой информации, установленной ч. 3 статьи 41.

Право свободно производить, передавать и распространять информацию обеспечивается, в первую очередь, гарантией свободы массовой информации (часть 5 статьи 29), свободой литературного, научного, технического и других видов творчества (ч. 1 ст. 44), в процессе которого создается информация, в том числе предназначенная для публичного распространения, а также свободой совести и вероисповедания, включая распространение религиозных и иных убеждений (ст. 28)

Указанные права не являются абсолютными и ограничиваются в интересах других людей, общества в целом и государства.

Конституция РФ устанавливает общие принципы ограничения прав и свобод человека и гражданина (ч. 3 ст. 55) федеральным законом только в той мере, в какой это необходимо в целях защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны и безопасности государства.

Одновременно в ч. 3 ст. 17 установлен общий принцип ограничения гражданских прав «Осуществление прав и свобод человека и гражданина не должно нарушать права и свободы других лиц». Этот принцип конкретизируется правом на личную и семейную тайну (ч. 1 ст. 23), тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений, (ч. 2 ст. 23), запретом собирать, хранить, использовать и распространять информацию о частной жизни лица без его согласия (ч. 1 ст. 24).

Интересы общества защищены конституционным запретом на пропаганду или агитацию, возбуждающие социальную, расовую, национальную или религиозную ненависть и вражду (ч. 2 ст. 29).

Интересы государства обеспечены ограничением свободы распространения информации в целях защиты государственной тайны (ч. 4 ст. 29).

Установленные Конституцией РФ права на получение и распространение информации, обязанности органов государственной власти по обеспечению этих прав и принципы ограничения этих прав характерны для демократических правовых государств, к которым относится и Россия, а также полностью соответствуют международным актам, определяющим общепризнанные права и свободы человека и гражданина, в том числе Всеобщей декларации прав человека, Европейской конвенции о защите прав человека и основных свобод, Международному пакту о гражданских и политических правах и другим.

2. Реализация права на доступ к информации

Законодательство РФ не определяет перечень информации, доступ к которой юридических и физических лиц должен быть обеспечен, и это правильно, поскольку многие законы в рамках сферы правового регулирования устанавливают либо обязанность предоставлять некоторую информацию, либо запрет на ограничение доступа к информации.

Так Федеральный закон №24-ФЗ «Об информации, информатизации и защите информации» в ст. 10 устанавливает указанный запрет:
«3. Запрещено относить к информации с ограниченным доступом:

- законодательные и другие нормативные акты, устанавливающие правовой статус органов государственной власти, органов местного самоуправления, организаций, общественных объединений, а также права, свободы и обязанности граждан, порядок их реализации;
- документы, содержащие информацию о чрезвычайных ситуациях, экологическую, метеорологическую, демографическую, санитарно - эпидемиологическую и другую информацию, необходимую для обеспечения безопасного функционирования населенных пунктов, производственных объектов, безопасности граждан и населения в целом;
- документы, содержащие информацию о деятельности органов государственной власти и органов местного самоуправления, об использовании бюджетных средств и других государственных и местных ресурсов, о состоянии экономики и потребностях населения, за исключением сведений, отнесенных к государственной тайне;
- документы, накапливаемые в открытых фондах библиотек и архивов, информационных системах органов государственной власти, органов местного самоуправления, общественных объединений, организаций, представляющие общественный интерес или необходимые для реализации прав, свобод и обязанностей граждан».

Закон РФ «О государственной тайне» также устанавливает в ст. 7 перечень сведений, которые не подлежат отнесению к государственной тайне:

- о чрезвычайных происшествиях и катастрофах, угрожающих безопасности и здоровью граждан, и их последствиях, а также о стихийных бедствиях, их официальных прогнозах и последствиях;
- о состоянии экологии, здравоохранения, санитарии, демографии, образования, культуры, сельского хозяйства, а также о состоянии преступности;
- о привилегиях, компенсациях и льготах, предоставляемых государством гражданам, должностным лицам, предприятиям, учреждениям и организациям;
- о фактах нарушения прав и свобод человека и гражданина;

- о размерах золотого запаса и государственных валютных резервах Российской Федерации;
- о состоянии здоровья высших должностных лиц Российской Федерации;
- о фактах нарушения законности органами государственной власти и их должностными лицами.

Очевидно, что эти перечни пересекаются, но они имеют различное назначение. Если Федеральный закон «Об информации, информатизации и защите информации» запрещает ограничивать доступ к определенной информации (то есть устанавливать для нее какой-либо режим ограниченного доступа), то Закон РФ «О государственной тайне» вводит ограничения на установление одного из таких режимов - режима государственной тайны.

Федеральный закон «Об информации, информатизации и защите информации» определяет в ст. 3 в качестве направлений государственной политики формирование и защиту государственных информационных ресурсов, а также создание условий для качественного и эффективного информационного обеспечения граждан, органов государственной власти, органов местного самоуправления, организаций и общественных объединений на основе государственных информационных ресурсов.

К сожалению, Закон не обеспечил ясности в содержании и правовом режиме понятия «государственные информационные ресурсы». Между тем, все положения закона, касающиеся права доступа, построены на основе этого понятия.

«Информационные ресурсы» определены как «отдельные документы и отдельные массивы документов, документы и массивы документов в информационных системах (библиотеках, архивах, фондах, банках данных, других информационных системах)» (ст. 2). Из этого следует, что два документа уже могут считаться «информационным ресурсом», но 102 документа не правомерно будет отнести к «информационным ресурсам», если они не включены в информационную систему. При этом не установлен порядок включения документов в информационную систему.

Но поскольку информационные ресурсы объявлены объектом права собственности и элементом состава имущества (ст. 6), можно предположить, что информационные ресурсы не могут считаться таковыми до тех пор, пока они не будут включены в состав имущества, не получат отражения в бухгалтерских документах первичного учета и т.д. Однако даже это предположение не позволяет однозначно выделить из информационных ресурсов государственную часть и установить, кто же конкретно является «собственником» этих ресурсов. Особенно сложно этот вопрос решается в отношении «совместной собственности» Российской Федерации и субъектов Российской Федерации.

Указанным законом установлены и некоторые принципы реализации права доступа к информации из информационных ресурсов и использования этой информации (статьи 12 и 13). В частности, «граждане, органы государственной власти, органы местного самоуправления, организации и общественные объединения обладают равными правами на доступ к государственным информационным ресурсам и не обязаны обосновывать перед владельцем этих ресурсов необходимость получения запрашиваемой ими информации. Исключение составляет информация с ограниченным доступом».

Указанная норма, по существу, заставляет граждан, запрашивающих в органах государственной власти информацию о себе, обосновывать свой запрос, поскольку запрашиваемая информация относится к так называемым персональным данным и является конфиденциальной.

Закон позволяет использовать информацию, полученную на законных основаниях из государственных информационных ресурсов гражданами и организациями, для создания ими производной информации в целях ее коммерческого распространения, при этом в качестве обязательного требования установлена ссылка на источник информации (п. 2 ст. 12).

Закон устанавливает обязанность органов государственной власти, ответственных за формирование и использование информационных ресурсов, обеспечивать условия для оперативного и полного предоставления пользователю документированной информации в соответствии с обязанностями, установленными положениями этих органов (п. 4 ст. 12). Они определяют порядок накопления и обработки документированной информации с ограниченным доступом, правила ее защиты и порядок доступа к ней.

Отказ в доступе к информационным ресурсам, формируемым органами государственной власти и органами местного самоуправления, может быть обжалован в суд (п. 2 ст. 13).

Все информационные ресурсы, необходимые «для обеспечения права граждан на доступ к информации» должны быть зарегистрированы (п. 3 ст. 13). Правительство РФ устанавливает «перечень информационных услуг, предоставляемых пользователям из государственных информационных ресурсов бесплатно или за плату, не возмещающую в полном размере расходы на услуги» (п. 4 ст. 13). Полное возмещение должно осуществляться из средств соответствующих бюджетов.

В течение 9 лет после принятия данного федерального закона не были конкретизированы ни система формирования и развития государственных ресурсов, ни механизмы получения информации из этих ресурсов.

Таким образом, законодательная база для реализации конституционных прав на получение информации, касающейся прав, свобод и обязанностей человека, не была создана.

Две попытки внесения в Государственную Думу проектов федеральных законов «О доступе к информации» не увенчались успехом. Оба проекта по разным основаниям были отклонены, хотя их концепции существенно отличались.

Необходимо признать, что объективно существуют проблемы формирования концепции законопроекта «О доступе к информации». Они связаны, прежде всего, с трактовкой конституционных прав на доступ к информации.

Проблема фокусируется на слове «доступ» и проявляется в формулировании целей закона, правомочий органов, прав граждан и т.д. Для целей закона из комплекса конституционных прав, как правило, выделяются права «искать и получать». Это означает, что лицо вправе искать и получать информацию, а органы обязаны ее предоставить. Когда этот комплекс прав и обязанностей заменяется словом «доступом», устанавливаются своеобразные акценты: на первый план выходит право искать и получать, а не обязанность предоставлять. Однако закон разрабатывается именно для создания механизма обеспечения права. Таким образом, если в названии проекта можно сохранить слово «доступ», то в тексте необходимо более точно употреблять глаголы.

Обязанность органов государственной власти предоставлять информацию, которая следует из права получать, в ряде законопроектов трактуется как «информационная

услуга». Государство, по нашему мнению, не оказывает *услуги* по доступу к информации, это его административная функция. Услуги оказываются на основании договора услуги, который в данном случае не заключается.

Один из законопроектов «О праве на информацию в Российской Федерации», базировался на постулате, что «право на информацию является неотчуждаемым правом человека и гражданина» и оперировал всем комплексом прав, гарантированных в части 4 статьи 29 Конституции РФ. В законопроекте право на информацию рассматривалось как «право каждого свободно искать, получать, передавать, производить и распространять информацию на территории Российской Федерации».

На первый взгляд, выбор указанного комплекса прав в качестве предмета правового регулирования опирается на Конституцию РФ и обусловлен желанием создать основу для максимально полной реализация конституционных положений. Вместе с тем, последующие попытки определить содержание каждого из перечисленных в части 4 ст. 24 Конституции РФ прав, свидетельствуют о неизбежности отсылки к федеральным законам, регулирующим большинство из возможных правоотношений по поводу поиска, получения, передачи, производства и распространения информации[1].

Практически в каждом федеральном законе закреплены право на получение тех или иных сведений или обязанность по предоставлению каких-либо сведений, либо обязанность распространять информацию (доводить до всеобщего сведения). Таким образом попытка реализовать весь комплекс «прав на информацию» лишает законопроект самостоятельного предмета регулирования.

Исходя из этого опыта, представляется целесообразным при разработке нормативной базы для обеспечения доступа к информации ограничиться вопросами, которые в наименьшей степени урегулированы законодательством - это вопросы доступа граждан к информации органов государственной власти РФ и, соответственно, обязанности последних по предоставлению информации.

Вторая проблема концепции связана с составом субъектов, вступающих в правоотношения по поводу доступа к информации. Один из законопроектов исходил из идеи максимального расширения круга субъектов права на информацию, то есть был реализован принцип: «любое лицо вправе получить информацию у любого лица». При этом, законопроект оперировал термином «каждый», относя его к физическим и юридическим лицам, органам государственной власти и органам местного самоуправления.

Такой подход нельзя признать юридически корректным, т.к. термин «каждый» по смыслу Конституции РФ объединяет субъектов правоотношений - физических лиц, имеющих различный правовой статус (граждане РФ, иностранные граждане, лица без гражданства).

Таким образом распространение комплекса прав человека и гражданина на юридических лиц и органы власти представляется противоречащим норме и духу Конституции РФ. В свою очередь, различный правовой статус субъектов, определенных законопроектом, не позволяет создать единый механизм реализации права на информацию, поэтому предлагаемый подход представляется концептуально неверным.

В одном из инициативных проектов о доступе к информации из сферы действия закона были выведены отношения между органами власти по поводу предоставления

информации, что вряд ли можно признать удачным, поскольку эти правоотношения содержат конфликт интересов и требуют правового решения.

Третья проблема касается определения состава информации, к которой необходимо обеспечить доступ. Во-первых, следует определиться, к чему обеспечивается доступ: *«к информация о чем-то»* или *«к информации из каких-то ресурсов».* Опора на «государственные и муниципальные ресурсы» приводит к переносу в законопроект всех проблем Федерального закона «Об информации, информатизации и защите информации». Юридический смысл, содержание, порядок формирования таких ресурсов до сих пор не определены, по поводу «собственности» на информацию не прекращаются споры. В конечном итоге, лицу, запрашивающему информацию, совершенно не важно, кому именно она принадлежит (принцип формирования ресурсов - право собственности), важно где она лежит и о чем она.

Во-вторых, достаточно сложно установить конечный перечень информации (или хотя бы категорий информации), которая должна находиться в свободном доступе, хотя такой перечень сведений, обязательных для размещения в информационных системах общего пользования, был определен для Правительства РФ и федеральных органов исполнительной власти Постановлением Правительства от 12 февраля 2003 г. № 98. Постановлением предписано федеральным органам исполнительной власти:

- «обеспечить доступ граждан и организаций к информации о деятельности федеральных органов исполнительной власти, за исключением сведений, отнесенных к информации ограниченного доступа, путем создания информационных ресурсов в соответствии с перечнем, утвержденным настоящим Постановлением;
- своевременно и регулярно размещать указанные информационные ресурсы в информационных системах общего пользования, в том числе в сети Интернет;
- систематически информировать граждан и организации о деятельности федеральных органов исполнительной власти иными способами, предусмотренными законодательством Российской Федерации».

Органам исполнительной власти субъектов Российской Федерации и органам местного самоуправления Правительство рекомендует принять меры по обеспечению доступа граждан и организаций к информации о своей деятельности.

Во исполнение указанного Постановления Правительства РФ самим высшим органом исполнительной власти и федеральными органами исполнительной власти были созданы сайты в сети Интернет, которые существенно отличаются как содержанием информации, навигационными возможностями, так и дизайном. По-видимому, здесь необходимы некоторые общие требования, минимальные стандарты, для того, чтобы потребность в информации была удовлетворена оперативно и с наименьшими трудозатратами.

Уместно напомнить, что данное Постановление не распространяется на другие ветви государственной власти: законодательную власть и судебную. Между тем, информация о деятельности этих органов также чрезвычайно важна для реализации конституционных прав и свобод.

Указанное Постановление, хотя и является важным шагом на пути реализации названных прав и свобод, но не создает полноценный механизм доступа к информации.

Масштабы нашей страны и объемы официальной информации (включая законодательство) предопределяют необходимость или даже неизбежность обеспечения

доступа к информации с использованием информационных и телекоммуникационных технологий.

Источником официальной информации всегда были библиотеки, они сохраняют свою роль, но она может быть многократно усилена за счет создания электронных библиотек, правовой статус которых также пока не определен. Если опубликование официальных документов в обычных СМИ всегда лимитировано объемом печатных страниц, то электронные СМИ могут предоставить такую возможность практически безболезненно, прежде всего, электронные СМИ органов государственной власти, для чего они должны быть в этом статусе зарегистрированы.

Второй немаловажный вопрос - как найти информацию (получить доступ). Здесь возможны разные варианты, в том числе:

- самостоятельно (в официальных СМИ, в библиотеках, путем запроса в орган государственной власти или орган местного самоуправления, через подключение к Интернету, как с личного компьютера, так и в пунктах публичного доступа);
- через посредника, который особенно необходим для лиц, не имеющих возможности подключения к Интернету, не имеющих навыков поиска информации и т.п. Такие посредники должны находиться в пунктах публичного доступа (библиотеки, почтовые отделения, помещения органов местного самоуправления).

Создание правовых условий для функционирования инфраструктуры публичного доступа к информации органов государственной власти и органов местного самоуправления - это тоже одна из задач законопроекта «О доступе к информации».

В отсутствие федерального закона органы власти устанавливают самостоятельно правила работы с обращениями граждан, в том числе касающимися запросов на получение той или иной информации[2]. Огромные массивы общественно-значимой информации находятся на хранении в Архивном фонде Российской Федерации, в фондах государственных и муниципальных библиотек, музеев. Доступ к этой информации регламентируют соответственно Основы законодательства Российской Федерации об Архивном фонде Российской Федерации и архивах, Федеральные законы «О библиотечном деле» и «О музейном фонде Российской Федерации и музеях в Российской Федерации». Эта законодательная база сложилась в около 10 лет назад и, естественно, не учитывает новые технологические возможности получения, хранения и предоставления информации.

Наиболее показательным является пример с созданием и функционированием в сети Интернет частных электронных библиотек, деятельность которых не регулируется законом, вследствие чего в процессе этой деятельности нередко нарушаются права авторов, представленных в таких библиотеках изданий. Правительство РФ подготовило новую редакцию федерального закона «Об Архивном фонде и архивах в российской Федерации». Этот законопроект под названием «Об архивном деле в Российской Федерации» внесен в Государственную Думу 02.12.2003 г. и принят в первом чтении 19.03.2004 г. Законопроект учитывает, что в состав архивов могут входить электронные документы, но не предусматривает при этом никаких особенностей их хранения и предоставления. Исходя из вышесказанного, можно утверждать, что нормативную правовую базу, обеспечивающую реализацию конституционных прав и свобод граждан по доступу к информации, отличает противоречивость и фрагментарность, она базируется на нормативных правовых актах органов исполнительной власти, а полноценное законодательное обеспечение отсутствует.

Противоречивость и неразвитость правового регулирования общественных отношений в информационной сфере приводят к серьезным негативным последствиям:

- не обеспечивается эффективная реализация и защита конституционных прав личности на неприкосновенность частной жизни, личную и семейную тайну, защиту чести и достоинства (на это указывают масштабы неконтролируемого распространения баз, содержащих персональные данные, распространение таких данных в Интернете и т.п.);
- слабо реализуется возможность конституционных ограничений свободы массовой информации в интересах защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов граждан, обеспечения обороноспособности страны и безопасности государства (об этом свидетельствует содержание материалов бумажных и электронных СМИ, повсеместное нарушение ими Закона «О рекламе», не регулируемое распространение порнографической информации и информации о сексуальных услугах и т.п.);
- не созданы благоприятные условия для свободного и оперативного доступа к информации органов государственной власти и органов местного самоуправления, непосредственно затрагивающей права и свободы личности, хотя начало положено формированием сайтов органов исполнительной власти;
- правоприменительная практика выявила несовершенство системы защиты государственной тайны, которая недостаточно ориентирована на современные угрозы, исходящие от использования новых информационных технологий и компьютерных сетей;
- не обеспечена защита прав участников электронной коммерции, они работают на свой страх и риск, особенно велик этот риск у покупателей;
- отсутствуют правовые механизмы противодействия манипулированию информацией, что проявляется, с одной стороны, в невозможности легко проверить достоверность предоставляемой информации, а с другой стороны, в распространении средств и методов манипулирования информацией, особенно в рамках избирательных кампаний;
- увеличились масштабы нарушения прав интеллектуальной собственности, что связано с развитием Интернета, сложностью контроля за использованием в Сети объектов интеллектуальной собственности, распространением электронных библиотек, деятельность которых не регулируется;
- отсутствует защита интересов государства и общества в сфере использования государственных информационных ресурсов, не определены принципы отнесения информационных ресурсов к государственным и к национальному достоянию, не обеспечен беспрепятственный доступ к государственным ресурсам и порядок их создания, развития, поддержания.

3. Реализация права на распространение информации

Право на распространение информации[3] реализуется, прежде всего, средствами массовой информации, деятельность которых регламентируется специальным законодательством.

Базовыми для этого законодательства являются следующие законы: Закон Российской Федерации «О средствах массовой информации», Закон Российской Федерации «Об авторском праве и смежных правах, Федеральные законы «О порядке освещения деятельности органов государственной власти в государственных средствах массовой информации», «О рекламе», «О государственной поддержке средств массовой информации и книгоиздания в Российской Федерации», «Об экономической поддержке районных (городских) газет».

Наряду с этим, многие федеральные законы содержат положения, устанавливающие правила распространения массовой информации или рекламы применительно к определенным ситуациям или объектам. К этой группе законов можно отнести Федеральные законы, связанные с выборами в органы государственной власти и проведением референдумов[4]; связанные с ограничением распространения той или иной информации[5]; с пропагандой той или иной информации[6].

Распространение массовой информации регулируется также Федеральным законом «Об обязательном экземпляре документов», который обеспечивает поступление изданий в государственные и муниципальные библиотеки, и, косвенно, Федеральным законом «О связи», устанавливающим порядок распределения радиочастотного спектра, выделение полос радиочастот и присвоение (назначение) радиочастот или радиочастотных каналов, в том числе в интересах распространения продукции средств массовой информации.

Даже простое перечисление законов, так или иначе регулирующих деятельность СМИ, свидетельствует о том, что некоторые виды СМИ, такие как радио и телевидение, не имеют специального законодательства. Некоторые нормы содержатся в Законе РФ «О средствах массовой информации», но их явно недостаточно. Однако подготовка проекта федерального закона «О радиовещании и телевизионном вещании» безуспешно осуществляется в Государственной Думе на протяжении двух созывов.

Базовое законодательство о массовой информации сложилось в середине 90-х годов прошлого века и, по общему мнению, не отвечает требованиям сегодняшнего дня, поэтому ведется подготовка новых редакций или проектов масштабных изменений законов «О средствах массовой информации» и «Об авторском праве и смежных правах».

Проект федерального закона «О внесении изменений в Закон Российской Федерации «Об авторском праве и смежных правах» принят Государственной Думой во втором чтении 21.04.2004 г. Он предусматривает, в том числе дополнение в статью 19, позволяющее получать в библиотеках «во временное безвозмездное пользование» экземпляры произведений, выраженных в цифровой форме, при этом они предоставляются только в помещениях библиотек при условии исключения возможности создания копий этих произведений в цифровой форме. Это положение уже учитывает, что библиотеки будут, с одной стороны, накапливать произведения, выраженные в цифровой форме, а с другой стороны, переводить в цифровую форму свои фонды. Законопроект запрещает также осуществление действий, направленных на снятие ограничений использования произведений или объектов смежных прав, установленных путем применения технических средств защиты авторского права и смежных прав, а также изготовление, распространение, сдачу в прокат, предоставление во временное пользование, импорт, рекламу любого устройства или его компонентов, их использование в целях получения дохода либо оказание услуг в случаях, если в результате таких действий становится невозможным использование технических средств защиты авторского права и смежных прав либо эти технические средства не обеспечивают надлежащую защиту указанных прав.

Нетрудно заметить, что приведенные положения законопроекта корреспондируются с Законом США, известным как DMCA (Digital Millennium Copyright Act) и направлены на защиту прав авторов произведений, выраженных в цифровой форме, использующих для защиты авторских прав технические устройства (программные комплексы), затрудняющие или предотвращающие несанкционированное копирование или изменение произведения, либо позволяющие контролировать доступ к ним.

Развитие Интернета активизировало процесс конвергенции традиционных СМИ с новыми техническими возможностями, возникли интернет-СМИ, цифровое телевидение и цифровое радиовещание (передача теле- и радиопрограмм через Интернет). Законодательство пока не откликнулось на это новые реалии.

Формы и способы правового регулирования таких СМИ зависят от того, как быстро и в какой степени конвергенция будет трансформировать рынки услуг связи. Учитывая большой разброс мнений в этой области и международный аспект проблемы, Европейская Комиссия приняла в 1997 году Предварительный доклад по конвергенции телекоммуникаций, средств массовой информации и информационных технологий[7].

Одна из проблем связана с тем, что интернет-СМИ не подпадают под признаки СМИ, установленные Законом для традиционных СМИ, в частности к ним не применимо требование указать при регистрации предполагаемую территорию распространения и предполагаемую периодичность выпуска. Тем не менее Минпечати, не меняя Закон, активно регистрировало интернет-СМИ, указывая в традиционном свидетельстве о регистрации территорию распространения как «ближнее и дальнее зарубежье». Для чего же нужна официальная регистрация «виртуальным» изданиям? Как минимум, для использования возможности аккредитации. Иначе, журналисту такого издания может быть отказано в получении информации и допуске в органы государственной власти.

Вторая проблема проистекает из особенности глобальной сети, в которой легко создать сайт (регистрируя его не обязательно в своей стране), размещать на нем информацию для всеобщего сведения, но при этом не приобретать статус СМИ.

И третья проблема, связанная также с особенностями Сети, это сложность (хотя не невозможность) контроля соответствия содержания сайта или интернет-СМИ (даже зарегистрированного на территории России) требованиям отечественного законодательства о СМИ.

Российский сегмент Интернет насыщен средствами массовой информации. На региональных серверах можно получить бесплатный доступ к некоторым электронным газетам и веб-версиям печатных изданий. На федеральном уровне этот перечень существенно шире и информативней, но доступ к номерам все же платный. Большинство из представленных СМИ - традиционные СМИ (журналы, газеты, радиостанции), имеющие в Интернет электронную (точнее будет сказать - цифровую) версию. Но есть и чисто цифровые СМИ.

Цифровые СМИ можно разделить и по другому критерию. Некоторые из них являются, практически, зеркалом бумажных изданий. Другие издательства в электронной версии используют новые возможности информационных технологий и создают новый продукт, по своей функциональности приближающийся к полнотекстовым базам данных с использованием гипертекста**,** в котором информация объединена не по выпускам (номерам), а по тематике.

Еще одно специфическое явление в интернет-СМИ это информационные агентства (некие квазиСМИ), представляющие пользователям материалы, позаимствованные из различных СМИ. При этом происходит «обезличивание информации». У изданий в электронном виде не остается персонального имиджа.

Как журналисты, так и «читатели» нередко рассматривают СМИ в Интернете как оплот свободы печати, поскольку независимость сегодня гораздо проще поддерживать в Интернете, чем в печатной прессе. При этом подразумевается, что основное достоинство Интернета - отсутствие предварительной цензуры, понимая под цензурой установленное законодательством требование предварительно согласовывать с определенными должностными лицами содержание материалов, подготовленных редакциями СМИ. Именно в этом смысле существует конституционный запрет на цензуру. Цензура может быть не предварительной, а последующей (анализ содержания вышедших в свет СМИ), но с позиции закона это не цензура, а контроль. В результате такого контроля могут быть обнаружены нарушения законодательства и приняты соответствующие меры. Такой выборочный контроль, по существу, осуществляли Минпечати РФ и ФСТР РФ. Можно говорить о контроле содержания со стороны редактора и самоконтроле журналиста не только в связи с требованиями Закона РФ «О средствах массовой информации», но и с позиций соответствия принятой редакцией концепции данного СМИ. Такой контроль нельзя назвать цензурой, он естественен и необходим, в первую очередь, для защиты конституционных прав граждан, основ конституционного строя, морали и нравственности.

Существуют международные стандарты, направленные против злоупотребления свободой слова. В части 3 статьи 19 Международного пакта о гражданских и политических правах предусмотрено, что пользование этими свободами налагает особые обязанности и особую ответственность и, следовательно, может быть сопряжено с некоторыми ограничениями, которые должны быть установлены законом и являются необходимыми:
а) для уважения прав и репутации других лиц;
б) для охраны государственной безопасности, общественного порядка, здоровья или нравственности населения[8].

Закон РФ «О средствах массовой информации» в ст. 4 «Недопустимость злоупотребления свободой массовой информации» устанавливает запрет на использование СМИ в целях совершения уголовно наказуемых деяний, для разглашения сведений, составляющих государственную или иную специально охраняемую законом тайну, для осуществления экстремистской деятельности, а также для распространения передач, пропагандирующих порнографию, культ насилия и жестокости. Запрещается также использование в продукции СМИ скрытых вставок, воздействующих на подсознание людей и (или) оказывающих вредное влияние на их здоровье. Запрещаются распространение в средствах массовой информации, а также в компьютерных сетях сведений о способах, методах разработки, изготовления и использования, местах приобретения наркотических средств, психотропных веществ и их прекурсоров, пропаганда каких-либо преимуществ использования отдельных наркотических средств, психотропных веществ, их аналогов и прекурсоров, за некоторым исключением, а также распространение иной информации, распространение которой запрещено федеральными законами.

Такие законы были перечислены выше. За нарушение данного запрета установлена ответственность. Однако административная ответственность предусмотрена только за злоупотребление свободой массовой информации в виде использования в информационных материалах скрытых вставок.

Уголовная ответственность непосредственно за злоупотребление свободой массовой информации не установлена, хотя пропаганда терроризма и экстремизма может рассматриваться как пособничество совершению уголовно наказуемого деяния, а лица, распространяющие соответствующую информацию, - как соучастники преступления (.пособник, подстрекатель). Эти лица могут нести уголовную ответственность, согласно

ст. 33 УК РФ, по статье Особенной части УК РФ за совершенное преступление. Однако в интересах правоприменения можно было бы дополнить соответствующие статьи УК РФ самостоятельными составами, включающими этих субъектов преступления.

В целом, необходимо исходить из того, что нарушение права гражданина останется нарушением, совершено ли оно в реальном или виртуальном мире, поскольку нарушение или преступление всегда реально. Клевета, посягательства на честь и достоинство человека, совершенные в виртуальном мире, затрагивают реального человека в реальном мире, осложняют его реальную жизнь. И вполне естественно, что ответственность должна наступать по законам реального мира.

Распространение интернет-СМИ, наряду с возникающими проблемами правового регулирования, технологически упрощает выявление нарушения авторских прав, хотя одновременно усложняет их защиту.

С позиций развития законодательства о СМИ, рассмотренные выше особенности интернет-СМИ позволяют утверждать, что:
а) контроль содержания информации на сайтах СМИ необходим, возможен и должен быть узаконен;
б) средства массовой информации представлены в Интернете по разному и далеко не все из них должны подпадать под регулирование законодательством о СМИ. В частности, информационно-рекламные сайты, созданные для повышения конкурентоспособности традиционных СМИ, по нашему мнению, не могут относиться к СМИ.

Практика использования материалов, полученных из Сети, в публикациях СМИ и практика размещения на сайтах сетевых изданий авторских материалов, опубликованных в традиционных изданиях, заставляет задуматься о некоторых проблемах исполнения законодательства об авторском праве и этикете журналистов. При этом нарушение закона и этикета объясняется часто желанием сделать более доступными полезные для общества публикации. На самом деле, причины другие - незнание закона или пренебрежением законом.

С одной стороны, часто уязвима позиция авторов. Далеко не всегда авторы должным образом защищают свои произведения, «публикуемые» в Сети. Во-вторых, авторские договора, как правило, не содержат специальных положений, касающихся возможности и условий опубликования произведения в сетевом издании, наряду с печатным. Наряду с этим, журналисты довольно часто используют материалы, полученные из Сети, без ссылок не только на авторов, но и на сетевой адрес. При использовании материалов, защищенных авторским правом, такие действия должны рассматриваться как нарушение закона. Тем не менее, достаточно просто поместить как на страницах печатного издания, так и на web-страницах ссылки на другие web-сайты, содержащие материалы, защищенные авторским правом, что позволит пользователю легко к ним добраться.

Проблема установления ссылок пересекается с проблемой разграничения рекламы и других материалов, публикуемых в СМИ. Если в традиционных изданиях реклама четко отделяется, хотя всем известно о наличии «скрытой рекламы» в заказных статьях, то в Сети с помощью использования гипертекстовых ссылок стираются различия между рекламой, новостями и материалами по связям с общественностью. Во всяком случае, журналист, распространяющий информацию в нарушение действующего Закона «О средствах массовой информации» должен помнить, что может найтись лицо, которое потребует через суд восстановить нарушенные права. А за ссылки, по-видимому, должен отвечать тот, кто их устанавливает.

Информационно-коммуникационные технологии обеспечили новые возможности для так называемого «прямого маркетинга» - адресного предложения товаров или услуг потенциальному потребителю. Этот способ, продемонстрировавший свою высокую эффективность, привел к массовому распространению незапрашиваемых рекламы и иных предложений коммерческого характера с использованием электронной почты. Это явление получило в мире название «спам» и стало всеобщим бедствием, с которым страны пытаются бороться сначала техническими средствами, а затем и правовыми.

На самом деле возможности этой борьбы ограничены рамками национального законодательства, при том, что большая часть спама рассылается из-за рубежа, а также невозможностью решения проблемы только правовыми или только техническими средствами. Понимание этого побудило начать разработку проектов законодательных норм, дополняющих действующие федеральные законы «О связи», «О рекламе», Кодекс РФ об административных правонарушениях и Уголовный кодекс РФ, направленных на запрет массовой рассылки по электронным адресам пользователей, не запрашиваемых ими электронных рекламных предложений. По-видимому, эти нормы должны будут корреспондироваться с положениями проекта федерального закона «Об информации персонального характера», который находится на рассмотрении в Государственной Думе.

4. Ограничения права на доступ и распространение информации

Проблема реализации конституционных прав и свобод в информационной сфере, прежде всего по доступу к общественно-значимой открытой информации не решается достаточно эффективно не только в силу отсутствия единого нормативного акта, регламентирующего механизмы реализации основных прав, включая обязанности государственных органов по формированию государственных информационных ресурсов и получению информации из таких ресурсов.

Особую проблему представляет отсутствие систематизации и должной детализации регулирования института конфиденциальной информации, что не позволяет четко установить (на уровне федерального закона, как того требует Конституция РФ) ограничения права на доступ к информации. Это не только законодательная, но и общетеоретическая проблема, поскольку российскими законами установлено более 30 видов информации ограниченного доступа, режимы различных тайн вводятся бессистемно, виды тайн строго не структурированы, по поводу правового содержания различных тайн нет единого мнения.

Не очевидны различия между информацией, доступ к которой ограничен, и конфиденциальной информацией[9]. Нет определенности в правовом содержании понятия «конфиденциальная информация», что позволяет расширять сферу информации с ограниченным доступом[10]. Кроме того, в российском законодательстве часто используется словосочетание «разглашение тайны», имея в виду разглашение информации, эту тайну составляющей. Вместе с тем, введение де-юре таких основных видов конфиденциальной информации как коммерческая тайна, служебная тайна, личная и семейная тайны, профессиональные тайны и персональные данные, обуславливает создание правовых механизмов их защиты.

Защита государственной тайны регламентируется Законом РФ «О государственной тайне» и принятыми в соответствии с ним нормативными правовыми актами. Закон работает 10 лет, уже очевидны пробелы и устаревшие положения, по ряду положений есть решения

Конституционного Суда РФ[11], касающиеся допуска адвокатов и участия ответчиков, не имеющих допуска к государственной тайне, в закрытых уголовных и арбитражных процессах. Это обусловливает актуальность совершенствования Закона, соответствующие изменения и дополнения готовятся.

Обязанность по защите профессиональной тайны и состав защищаемой информации проистекают из специальных законов, в том числе: Федеральные законы «О связи», «О частной охранной и детективной деятельности», «Основы законодательства о нотариате», «Основы законодательства РФ об охране здоровья граждан», «О банках и банковской деятельности», «О профилактике заболевания СПИД», «О психиатрической помощи и гарантиях прав граждан при ее оказании», «Об адвокатской деятельности и адвокатуре в Российской Федерации», «О трансплантации органов и (или) тканей человека», Семейный кодекс РФ и др.

Анализ содержания сведений, составляющих профессиональную тайну, свидетельствует о том, что в этом режиме охраняется, как правило, коммерческая тайна юридических лиц либо сведения персонального характера, доверенные специалисту в рамках его профессиональной деятельности. Общая правовая регламентация защиты профессиональных тайн отсутствует, обладатели этой тайны вправе самостоятельно определить организационные, технические и правовые средства, достаточные для защиты соответствующих сведений, поскольку их разглашение влечет установленную законом ответственность.

Существующие нормы федерального законодательства не определяют мер защиты коммерческой тайны, законные (и не законные) способы ее получения, не устанавливают ответственности лиц, которым она стала известна в силу различных обстоятельств, то есть не создают конкретные механизмы реализации прав обладателей коммерческой тайны. Правовые основания для защиты коммерческой тайны содержатся в ряде актов российского законодательства:

- статья 34 Конституции Российской Федерации, запрещающая недобросовестную конкуренцию и гарантирующая защиту интеллектуальной собственности;
- статья 139 части первой и статьи 771, 772 части второй Гражданского кодекса Российской Федерации, закрепляющие институт коммерческой тайны в стране и определяющие основные принципы соблюдения конфиденциальности при выполнении научно-исследовательских, опытно-конструкторских и технологических работ;
- статья 10 Закона РФ «О конкуренции и ограничении монополистической деятельности на товарных рынках», устанавливающая, что разглашение коммерческой тайны является актом недобросовестной конкуренции;
- статья 151 Основ гражданского законодательства Союза ССР и республик, обеспечивающая правовую охрану секретов производства (ноу-хау);
- Постановление Правительства РСФСР от 05.12.95 № 35 «О перечне сведений, которые не могут составлять коммерческую тайну»;
- Указ Президента РФ № 188 от 6 марта 1997 года «Об утверждении перечня сведений конфиденциального характера», согласно которому, коммерческая тайна это сведения, связанные с коммерческой деятельностью, доступ к которым ограничен в соответствии с ГК РФ и федеральными законами.

Кроме этого коммерческая тайна упоминается, но не конкретизируется в законах и иных нормативных актах, которых более двухсот. Однако указанные нормы не только не создают механизма защиты коммерческой тайны, но и содержат внутренние противоречия. Эти обстоятельства предопределяют необходимость разработки

специального закона. Во многих странах до сих пор правовые нормы о защите коммерческой тайне включены в различные кодексы и законы. Однако наблюдается тенденция разработки единого или унифицированного нормативного акта (например, в США, Корее, Таиланде, Китае и других странах).

Первая попытка разработки и принятия закона «О коммерческой тайне» была сделана в период 1996-1999 гг. Закон был принят Государственной Думой, поддержан Советом Федерации, но отклонен Президентом РФ. Новую версию закона Правительство РФ внесло в 2003 году, он был принят Государственной Думой, но отклонен Советом Федерации. В настоящее время в федеральный закон вносятся изменения и дополнения в соответствии с решениями Согласительной комиссии, состоящей из депутатов Государственной Думы и членов Совета Федерации.

Учитывая наличие разрозненных норм в российском законодательстве, закон призван сыграть роль кодифицирующего акта. Он безусловно не сможет и не должен определять все меры защиты коммерческой тайны. Обладатель соответствующей информации самостоятельно выбирает меры ее защиты, адекватные ценности защищаемой информации. Задача же государства – создать механизмы защиты:
а) своих интересов (через сохранение в режиме государственной тайны производственной или коммерческой информации, полученной предпринимателем, но влияющей на состояние обороны и безопасности государства);
б) интересов общества (путем установления перечня информации, которая должна быть доступна обществу, то есть на нее не может распространяться режим коммерческой тайны);
в) интересов хозяйствующего субъекта (защищая его права от нарушений и наказывая нарушителя).

Закон позволит решить ряд принципиальных вопросов, имеющих большое значения для товаропроизводителя. Прежде всего, это содержание понятия «коммерческая тайна». Здесь не только вопрос разведения служебной и коммерческой тайн, но и формирование перечня сведений, для которых не может быть установлен режим коммерческой тайны.

Принципиален вопрос о том, какие права возникают у обладателя информации, составляющей коммерческую тайну, когда они возникают и когда прекращаются. Право на отнесение информации к информации, составляющей коммерческую тайну, принадлежит обладателю этой информации, при условии, что он получил ее законным способом и не нарушает ограничения, установленные законом. Законным считается получение информации самостоятельно при осуществлении исследований, систематических наблюдений или иной деятельности. Важно, что одна и та же информация может быть получена параллельно разными лицами, при этом она считается полученной законным способом.

Лицо, которое отнесло информацию к коммерческой тайне и установило для нее соответствующий режим, является обладателем информации, составляющей коммерческую тайну, и вправе распоряжаться такой информацией (использовать в собственном производстве или вводить в хозяйственный оборот), изменять и отменять режим, требовать его исполнения от лиц, которому такая информация передается по договору или в соответствии с законом.

Нельзя обязать обладателя какой-либо информации устанавливать режим коммерческой тайны - это его право, но без установления соответствующего режима (с принятием мер защиты) информация не будет иметь статус коммерческой тайны, а защита прав на нее не

будет поддержана государством. Помимо снятия режима коммерческой тайны путем волеизъявления обладателя, он может быть снят по решению суда в случае незаконного отнесения сведений к коммерческой тайне.

Закон предусматривает право обладателя коммерческой тайны требовать от лиц, получивших коммерческую тайну в результате случайности или ошибки, обеспечить охрану ее конфиденциальности (то есть далее не разглашать), а в случае, если такое лицо отказывается принять необходимые меры, обладатель вправе требовать в судебном порядке защиты своих прав. Это право позволяет минимизировать ущерб обладателю вследствие разглашения коммерческой тайны, при этом учитывается мировая практика защиты коммерческой тайны, когда чаще всего «добросовестный получатель» оказывается «недобросовестным» охотником за коммерческими секретами. Эта норма не является особо обременительной и заставляет лицо, получившее доступ к коммерческой тайне по ошибке (при условии, что на документе имеются все реквизиты и гриф - т.е. меры охраны приняты), не использовать информацию, составляющую коммерческую тайну, в ущерб интересам ее обладателя.

Некоторые проблемы вызвало регулирование защиты информации, составляющей коммерческую тайну, в рамках трудовых отношений. Эти проблемы проистекали из положений Трудового кодекса РФ, который не предусматривает пролонгацию обязательств работника по сохранению коммерческой тайны за пределы трудовых отношений. В практике развитых стран в трудовых контрактах присутствуют обязательства работника, снижающие риск его участия в недобросовестной конкуренции против работодателя, в том числе: по неразглашению информации, составляющей коммерческую тайну работодателя, в течение определенного срока после окончания трудовых отношений, или запрещающие бывшему работнику наниматься на работу к конкурентам бывшего работодателя. Иногда предусматривается право бывшего работодателя сообщать новому работодателю о том, что работник был допущен к коммерческой тайне, в связи с чем новый работодатель не должен использовать известную работнику информацию, чтобы не быть обвиненным в недобросовестной конкуренции.

Со временем какие-то обычаи делового оборота укоренятся и в России. Пока же Закон прямо предусматривает обязанность работника не разглашать информацию, составляющую коммерческую тайну, обладателями которой являются работодатель и его контрагенты, после прекращения трудового договора в течение срока, установленного отдельным соглашением между работодателем и работником, причем это соглашение должно быть заключено в период срока действия трудового договора.

Трудовой кодекс РФ создал коллизию норм с Гражданским кодексом РФ, статья 139 которого предусматривает, что работник должен возместить убытки, причиненные работодателю, в случае его вины за разглашение коммерческой тайны. В соответствии же с трудовым законодательством работник обязан возместить только прямой действительный ущерб, нанесенный работодателю. При разглашении коммерческой тайны материального ущерба может просто не быть, а вот убытки, включая недополученную выгоду, могут разорить работодателя. В условиях указанного противоречия работодатель будет вынужден сначала уволить работника, допустившего разглашение коммерческой тайны, а потом предъявить ему гражданско-правовой иск о возмещении убытков.

Некоторые проблемы наступления ответственности в связи с нарушением прав обладателя коммерческой тайны, будут рассмотрены в следующем разделе.

Объектом защиты должна быть также информация**,** получаемая от различных субъектов органами государственной власти в режиме конфиденциальности или генерируемая в этих органах и не предназначенная для общего сведения. Такая информация охраняется в режиме служебной тайны. Правовой институт служебной тайны должен быть установлен федеральным законом, как того требует Конституция РФ. Кроме того, необходимо создать правовые рамки, препятствующие развитию коррупции в органах власти на почве информационной закрытости, и правовые гарантии для защиты конфиденциальной информации, представляемой в органы власти физическими и юридическими лицами.

Проект федерального закона «О служебной тайне» разрабатывается в Комитете Государственной Думы по безопасности. Основные идеи проекта ФЗ сводятся к следующему.

Режим служебной тайны может устанавливаться только в органах государственной власти (федеральных и субъектов федерации), а также в подчиненных им организациях, то есть в сфере государственного управления.

Охраняться в режиме служебной тайны должна информация, которая в соответствии с законодательством поступает в органы власти, уже находясь в режиме конфиденциальности, установленном ее обладателем (коммерческая тайна, профессиональная, банковская и др.)

Наряду с этой информацией в режиме служебной тайны может охраняться внутрисистемная информация, генерируемая в самом органе, которую до определенного времени не целесообразно обнародовать в интересах государственного управления или которая в обобщенном виде может создать угрозу государственной безопасности, но в силу законодательных ограничений не может быть отнесена к государственной тайн.

Поскольку сформулировать полный перечень такой информации не представляется возможным, а ограничить потенциальный волюнтаризм чиновников необходимо, была предпринята попытка сформулировать принципы отнесения сведений к служебной тайне и дать перечень сведений, отнесение которых к служебной тайне не допускается.

В законопроекте определен порядок отнесения сведений к служебной тайне, снятие ограничений на распространение сведений, составляющих служебную тайну, и полномочия органов по распоряжению сведениями, составляющими служебную тайну.

Устанавливаются права и ответственность руководителей органов государственной власти и органов местного самоуправления при отнесении сведений к служебной тайне.

Установлены основные положения по организации системы защиты служебной тайны, которая базируется на открытых перечнях информации, охраняемой в этом режиме, обязательствах работников и исполнителей по договорам с органами государственной власти, требованиях по физической защите информации и др. Определяется порядок доступа иных органов власти, граждан и организаций к информации (сведениям), составляющей служебную тайну и максимальный срок действия режима.

Заинтересованные лица вправе поставить вопрос о досрочном снятии ограничений на распространение сведений, составляющих служебную тайну.

Еще более уязвимым объектом защиты является информация персонального характера (персональные данные). Информация, непосредственно связанная с конкретным человеком (факты его биографии, номинативные (назывные) данные, национальность, место жительства, сведения о заболеваниях, о профессиональных знаниях и навыках, о семейной жизни, привычках, увлечениях, нравственные, политические, сексуальные и религиозные пристрастия и многое другое), составляет большую или даже большую часть циркулирующей в обществе информации.

Распространение такой информации без согласия человека может способствовать формированию его положительного имиджа (например, информация о наградах или иных заслугах), а может нанести непоправимый урон, моральный вред, особенно если такая информация недостоверна. Вся эта информация вполне может быть использована, в том числе недобросовестно, в интересах предпринимательской деятельности.

Поэтому обращение с информацией персонального характера требует особой регламентации. Эта необходимость давно учитывается законодателем. Например, информация о наличии вклада в банк определенного лица и о размере этого вклада является банковской тайной (Федеральный закон «О банках и банковской деятельности»). В рамках защиты государственной тайны охраняется информация о некоторых категориях лиц, допущенных к государственной тайне (в том числе, осуществляющих разведывательную, контрразведывательную и оперативно-розыскную деятельность - Закон РФ «О государственной тайне»).

Информация о незапатентованном коммерчески выгодном изобретении и изобретателе может составлять коммерческую тайну организации, использующей изобретение. Информацию персонального характера мы также доверяем, адвокатам, связистам, нотариусам и представителям других профессий, которые обязаны сохранять ее в тайне (профессиональная тайна). Эту информацию собирают органы государственной власти и органы местного самоуправления для реализации возложенных на них функций.

Служащие данных органов также обязаны охранять персональные данные других лиц, ставшие им известными в связи с выполнением служебных обязанностей (служебная тайна). Таким образом, большая часть информации персонального характера охраняется тем или иным режимом ограниченного доступа. Однако этого оказывается недостаточно для защиты интересов личности, с которой связана такая информация.

Развитие современных информационных технологий, сопровождающееся созданием многочисленных и мощных компьютерных баз данных, аккумулирующих информацию о людях, легкость распространения информации из таких баз (в том числе по Интернету), простота их копирования, объединения («слияния»), возможность модификации информации и т.п. породили дополнительные угрозы интересам личности, в том числе, угрозу стать «прозрачной» как для государства, так и для общества (в том числе - работодателя), то есть возможность лишиться некоторой естественной информационной приватности, лишиться части прав на защиту privacy в терминологии англосаксонских стран.

Совет Европы и иные международные организации предъявляют определенные требования к защите персональных данных. Эта защита осуществляется в интересах:

- *личности* (сведения, составляющие личную и семейную тайны, некоторые профессиональные тайны)

- *общества* (сведения о руководителях коммерческих организаций, изобретателях, ответственных служащих, составляющие коммерческую, служебную и некоторые профессиональные тайны)
- *государства* (информация о секретоносителях - государственная тайна).

При этом Конвенция и Директивы СЕ связывают правовую защиту персональных данных именно с их автоматизированной обработкой.

В России термин «персональные данные» возник впервые в Федеральном законе «Об информации, информатизации и защите информации», который заложил некоторую основу для реализации соответствующих положений Конституции РФ и норм международного права, но механизма защиты этих данных он не создал. Будучи «рамочным» законом, он не учитывал особенностей автоматической обработки персональных данных. Разработка специального законопроекта началась в России более 8 лет назад. Законопроект «Об информации персонального характера» был внесен депутатами Государственной Думы в апреле 1998 года. В течение последующих лет проект не представлялся на обсуждение Государственной Думы. В октябре 2000 г. группа депутатов внесла в Государственную Думу новый вариант проекта федерального закона «Об информации персонального характера». Принципиальное концептуальное отличие данного варианта законопроекта заключалось в том, что он не предусматривал создание независимого института Уполномоченного по правам персональных данных (как это сделано в большинстве европейских стран и в первом законопроекте), а шел по пути наделения Правительством РФ одного из органов исполнительной власти соответствующими функциями.

В последнее время появились новые виды предпринимательской деятельности, непосредственно связанные с использованием персональных данных, например, уже упоминаемый выше прямой маркетинг или издание многочисленных энциклопедий (справочников) персоналий. Эта вроде бы легальная деятельность, тем не менее, не регулируется с позиций защиты персональных данных.

Очевидно, что персональные данные, накапливаемые для прямого маркетинга, в подавляющем числе случаев получены незаконно и используются в целях, с субъектом не согласованных. Реалии компьютерно-телекоммуникационной действительности обостряют ситуацию с защитой персональных данных. Именно в рамках оказания информационных и телекоммуникационных услуг собираются и используются большие массивы персональных данных пользователей (абонентов). Именно в Сети отнюдь не в режиме конфиденциальности находится огромное количество персональных данных.

Именно в Сети наблюдается неконтролируемое распространение сетевых почтовых адресов пользователей, которые справедливо было бы отнести к персональным данным. Именно в Сети упрощается донельзя прямой маркетинг, подчас переходящий в «спам». Угрозы, которые создает интересам различных субъектов неконтролируемые сбор, распространение и использование персональных данных с использованием информационно-телекоммуникационных технологий, трудно переоценить. Однако сам факт того, что работа над проектом федерального закона «Об информации персонального характера» в Государственной Думе не ведется, несмотря на многочисленные рекомендации различных общественных слушаний по данному вопросу, свидетельствует об отсутствии политической воли.

Распространение незаконно полученных баз персональных данных это выгодный бизнес, а получение таких баз это условие прибыльности деятельности охранных и детективных

агентств, служб безопасности предприятий и других организаций. Эти сведения не бывают лишними и при проведении избирательных кампаний. Таким образом, у государства (в лице чиновников и политиков) нет стимула к созданию системы правовой защиты персональных данных, а у общества нет потенциала, чтобы заставить государство такую систему создать.

5. Защита информации от искажения, модификации и незаконного копирования

Информация, содержащаяся в государственных, корпоративных и частных информационных ресурсах или системах, должна защищаться от искажения, модификации и незаконного копирования не только с помощью особых режимов доступа, использования и распространения, но и посредством специальных программно-технических и аппаратных средств защиты, в том числе, антивирусных программ, сетевых экранов, программных средств, реализующих криптографические алгоритмы, электронной цифровой подписи и других.

Правовую базу технической защиты информации составляют Федеральные законы «Об информации, информатизации и защите информации» (статьи 19–22, устанавливающие общие принципы защиты), «Об электронной цифровой подписи», «О лицензировании отдельных видов деятельности» (ст. 17), «О сертификации продукции и услуг», а также принятые в соответствии с ними Постановления Правительства РФ.

В соответствии с законодательством РФ лицензированию подлежат следующие виды деятельности:

- деятельность по распространению шифровальных (криптографических) средств;
- деятельность по техническому обслуживанию шифровальных (криптографических) средств;
- предоставление услуг в области шифрования информации;
- разработка, производство шифровальных (криптографических) средств, защищенных с использованием шифровальных (криптографических) средств информационных систем, телекоммуникационных систем;
- деятельность по выдаче сертификатов ключей электронных цифровых подписей, регистрации владельцев электронных цифровых подписей, оказанию услуг, связанных с использованием электронных цифровых подписей, и подтверждению подлинности электронных цифровых подписей;
- деятельность по выявлению электронных устройств, предназначенных для негласного получения информации, в помещениях и технических средствах (за исключением случая, если указанная деятельность осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя);
- деятельность по разработке и (или) производству средств защиты конфиденциальной информации;
- деятельность по технической защите конфиденциальной информации;
- разработка, производство, реализация и приобретение в целях продажи специальных технических средств, предназначенных для негласного получения информации, индивидуальными предпринимателями и юридическими лицами, осуществляющими предпринимательскую деятельность.

Информационные системы органов государственной власти РФ, субъектов РФ других государственных органов и организаций, которые обрабатывают документированную информацию ограниченного доступа, подлежат обязательной сертификации.

Защита локальных компьютерных систем и сетей осуществляется собственниками этих объектов самостоятельно или с привлечением специализированных организаций. Правовую основу такой защиты, наряду с указанными выше нормативными правовыми актами, составляет Федеральный закон «О связи». В отношении средств защиты информации, содержащей сведения, составляющие государственную тайну, действуют особые правила. Допуск предприятий, учреждений и организаций к проведению работ, связанных с использованием сведений, составляющих государственную тайну, созданием средств защиты информации, а также с осуществлением мероприятий и (или) оказанием услуг по защите государственной тайны, осуществляется путем получения ими в порядке, устанавливаемом Правительством Российской Федерации, лицензий на проведение работ со сведениями соответствующей степени секретности.

Лицензия на проведение указанных работ выдается на основании результатов специальной экспертизы предприятия, учреждения и организации и государственной аттестации их руководителей, ответственных за защиту сведений, составляющих государственную тайну, расходы по проведению которых относятся на счет предприятия, учреждения, организации, получающих лицензию. Средства защиты информации, составляющей государственную тайну, должны иметь сертификат, удостоверяющий их соответствие требованиям по защите сведений соответствующей степени секретности.

Таким образом в настоящее время способы и средства защиты информации подчинены достаточно жесткому государственному регулированию, представляется, что не все из этих ограничений оправданны. Средства защиты информации, предназначенные исключительно для внутренних целей организации, не должны подлежать обязательной сертификации, а деятельность по их созданию и использованию − лицензированию, поскольку в этом случае требуемый уровень надежности защиты информации определяется самой организацией, исходя из ее частных интересов.

Средства защиты информации, используемые (или предназначенные для использования) в государственных органах, а также услуги по защите информации в государственных органах или органах местного самоуправления должны подлежать обязательной сертификации, так как это является условием соблюдения безопасности государственных информационных ресурсов и информационного обмена между органами, что в конечном итоге может сказаться на защищенности системы государственного управления.

В настоящее время принято два положения, устанавливающих основания и порядок получения лицензий на деятельность по защите конфиденциальной информации. Документы содержат схожие положения, касающиеся порядка получения лицензии, отличия заключаются в том, что Положение о лицензировании деятельности по разработке и (или) производству средств защиты конфиденциальной информации содержит дополнительные требования, предъявляемые к соискателям лицензии, осуществляющим деятельность в области разработки и (или) производства средств защиты конфиденциальной информации, устанавливаемых на объектах Администрации Президента Российской Федерации, Совета Безопасности Российской Федерации, Федерального Собрания Российской Федерации, Правительства Российской Федерации, Конституционного Суда Российской Федерации, Верховного Суда Российской Федерации и Высшего Арбитражного Суда Российской Федерации.

Основную проблему применения данных положений представляет проблема определения субъектов, на которых распространяются требования Положений, и содержание понятия конфиденциальной информации. Последнее является следствием противоречий в

действующем законодательстве. Первое же обусловлено неточностью формулировок в Постановлении Правительства РФ № 29 «О лицензировании деятельности по технической защите конфиденциальной информации», которое не делает различия между предприятиями, обеспечивающими техническую защиту принадлежащей им конфиденциальной информации, и предприятиями, оказывающими на возмездной основе услуги по технической защите такой информации.

В случае осуществления деятельности по разработке и (или) производству средств защиты конфиденциальной информации в системе госуправления, к соискателям лицензии предъявляются дополнительные требования, в частности:

1. соблюдение лицензиатом режима конфиденциальности при обращении со сведениями, которые ему доверены или стали известны по работе: обеспечение ограничения круга лиц, допущенных к конфиденциальной информации, установление порядка допуска лиц к работам, связанным с использованием конфиденциальной информации, организация обеспечения безопасности ее хранения, обработки и передачи по каналам связи и установление обладателем конфиденциальной информации требований к обеспечению безопасности этой информации;
2. наличие условий, предотвращающих несанкционированный доступ к средствам защиты конфиденциальной информации, обеспечивающих хранение нормативной и эксплуатационной документации, инсталляционных дискет и дистрибутивов программных и программно-аппаратных средств защиты конфиденциальной информации в металлических шкафах (хранилищах, сейфах), оборудованных внутренними замками, а также хранение дубликатов ключей от металлических шкафов (хранилищ, сейфов) и входных дверей в сейфе ответственного лица, назначенного руководством лицензиата;
3. аттестование средств обработки информации, используемых для разработки средств защиты конфиденциальной информации, а также для автоматизированного учета в соответствии с требованиями по защите информации с использованием лицензионных программного обеспечения для электронно-вычислительных машин и баз данных;
4. выполнение требований государственных стандартов Российской Федерации, конструкторской, программной и технологической документации, единой системы измерений, системы разработки и запуска в производство средств защиты конфиденциальной информации, в соответствии с которыми конструкторская документация лицензиата имеет номер, зарегистрированный в государственном реестре разрабатывающих предприятий, а нормативные правовые акты по разработке, конструкторская документация и технические условия обеспечивают соответствие показателей продукции нормам и требованиям, установленным Федеральным агентством правительственной связи и информации при Президенте Российской Федерации в пределах его компетенции;
5. наличие системы учета изменений, внесенных в техническую и конструкторскую документацию, и системы учета готовой продукции;
6. наличие у руководителя лицензиата и (или) уполномоченного им лица высшего образования и (или) профессиональной подготовки в области защиты информации с квалификацией «специалист по защите информации» и производственным стажем в области лицензируемой деятельности не менее 5 лет.

Эти требования уравнивают конфиденциальную информацию с информацией, составляющей государственную тайну, что не правомерно. Требования о сертификации средств защиты информации содержится в п. 2 Указа Президента РФ от 3 апреля 1995 г. № 334 «О мерах по соблюдению законности в области разработки производства,

реализации и эксплуатации шифровальных средств, а также предоставления услуг в области шифрования информации» (с изм. и доп. от 25 июля 2000 г.). Он предусматривает необходимость сертификации только шифровальных средств и средств технической защиты информации, используемых государственными организациями и предприятиями и предприятиями, выполняющими госзаказ.

По отношению к защите конфиденциальной информации действует Приказ ФАПСИ от 23 сентября 1999 г. № 158 «Об утверждении Положения о порядке разработки, производства, реализации и использования средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну (ПКЗ-99)», который предусматривает, что при принятии решения о необходимости криптографической защиты подлежащей в соответствии с действующим законодательством обязательной защите конфиденциальной информации требования данного Положения являются обязательными для:

- государственных органов и государственных организаций;
- юридических лиц и индивидуальных предпринимателей, осуществляющих виды деятельности, подлежащие в соответствии с законодательством Российской Федерации лицензированию;
- негосударственных организаций и физических лиц при необходимости обмена конфиденциальной информацией с государственными органами, государственными организациями или другими организациями, выполняющими государственные оборонные заказы;
- других организаций независимо от их организационно-правовой формы и формы собственности при выполнении ими государственных оборонных заказов.

В отношении иных лиц требования Положения носят рекомендательный характер. В целом ситуация с сертификацией средств защиты информации достаточно запутанная. Это обусловлено тем, что Закон РФ от 10.06.1993 № 5151-1 «О сертификации продукции и услуг» утратил силу в связи с принятием Федерального закона от 27.12.2002 № 184-ФЗ «О техническом регулировании», а в развитие последнего пока не приняты технические регламенты и иные предусмотренные им нормативные правовые акты. Общий принцип таков: обязательной сертификации подлежат товары (работы, услуги), в отношении которых такое требование установлено НПА, сертификация остальных товаров (работ, услуг) − добровольная. Сейчас требования об обязательной сертификации предусмотрены следующими законами: ФЗ «Об участии в международном информационном обмене» (ст. 17) устанавливает, что при ввозе информационных продуктов, информационных услуг в Российскую Федерацию импортер представляет сертификат, гарантирующий соответствие данных продуктов и услуг требованиям договора. Средства международного информационного обмена, которые обрабатывают документированную информацию с ограниченным доступом, а также средства защиты этих средств подлежат обязательной сертификации.

Сертификация сетей связи производится в порядке, определяемом Федеральным законом «О связи». ФЗ «Об информации, информатизации и защите информации» (ст. 19) предусматривает сертификацию: информационных систем, баз и банков данных, предназначенных для информационного обслуживания граждан и организаций, информационных систем органов государственной власти Российской Федерации и органов государственной власти субъектов Российской Федерации, других государственных органов, организаций, которые обрабатывают документированную информацию с ограниченным доступом, а также средств защиты этих систем.

В целом ситуация с правовым регулированием защиты информации позволяет сделать следующие выводы:

1. лицензирование деятельности по защите информации является избыточным, оно фактически по своему назначению дублирует собой сертификацию;
2. сертификация средств защиты информации призвана обеспечить качество этих средств и услуг по защите, но не всегда гарантирует надежность этих средств и не всегда обеспечивает их эффективное использование, так сертифицированные средства электронной цифровой подписи «не понимают» друг друга;
3. задача контроля за осуществлением такого рода деятельности практически не решаема из-за большого числа лиц, способных заниматься такого рода деятельностью, относительной легкости создания и распространения средств защиты информации.

Кроме того, в области защиты информации имеет критическое значение только надежность тех или иных средств, а не возможность их использования (создания, распространения) как таковая: сам факт создания, распространения или использования средств защиты информации, оказания услуг по защите информации не создает угрозы причинения вреда здоровью, имуществу либо безопасности. Это означает, что все необходимое регулирование оборота средств защиты информации и услуг по ее защите можно осуществлять исключительно за счет сертификации указанных средств и услуг.

Вместе с тем, законодательством РФ установлено требование обязательной сертификации по отношению ко всем шифровальным средствам, иным средствам защиты информации, услугам по защите информации. Требует пересмотра и система регулирующих органов в области защиты информации. Необходимо разграничить полномочия органов, осуществляющих сертификацию и лицензирование в области защиты информации, и органов, осуществляющих разработку и поддержание информационных систем государственных органов.

1. Ответственность за нарушения прав на доступ к информации, распространение информации и ограничения права

Проблемы обеспечения доступа к информации не решаются еще и потому, что недостаточно эффективны правовые нормы юридической ответственности за нарушение указанных прав[12]. Кодекс об административных правонарушениях РФ содержит более 20 статей[13], но практики его применения практически нет, поскольку он недавно введен в действие. Около 10 статей в Уголовном кодексе РФ. Гражданский кодекс РФ также предусматривает гражданско-правовую ответственность за непредоставление информации или предоставление ложной информации.

Так, ответственность за неправомерный отказ в предоставлении гражданину информации предусмотрена статьей 5.39 Кодекса Российской Федерации об административных правонарушениях и статьей 140 Уголовного кодекса Российской Федерации. Под действие этих статей подпадают и такие деяния, как неправомерное установление режима служебной тайны для определенной категории сведений, затрагивающих права и свободы гражданина. Законодательством РФ предусмотрена гражданско-правовая, административная и уголовная ответственность за разглашение различных видов тайн. Уголовная ответственность за разглашение государственной тайны предусмотрено несколькими статьями Уголовного кодекса РФ (Статья 275 «Государственная измена», Статья 283 «Разглашение государственной тайны», Статья 284 «Утрата документов, содержащих государственную тайну»). За разглашение государственной тайны

ответственность наступает в случае, если защищаемые сведения разгласило лицо, которому они стали известны по службе или по работе.

Исходя из этого, к ответственности может быть привлечено лицо, не имеющее допуска к государственной тайне, например, журналист, которому соответствующие сведения были сообщены без указания, что они составляют государственную тайну. Данное положение не корреспондируется с законодательство о государственной тайне, поскольку последнее распространяется только на должностных лиц и граждан, взявших на себя обязательства или обязанных по своему статусу исполнять требования данного законодательства (ст. 1 Закона РФ «О государственной тайне»). Однако статус журналиста не предполагает «автоматическое» исполнение им требований указанного законодательства.

Обозначенная правовая коллизия должна быть устранена в результате совершенствования норм уголовной ответственности за разглашение государственной тайны. Кроме уголовной ответственности предусмотрена административная ответственность за нарушение условий, предусмотренных лицензией на проведение работ, связанных с использованием и защитой информации, составляющей государственную тайну, созданием средств, предназначенных для защиты информации, составляющей государственную тайну, осуществлением мероприятий и (или) оказанием услуг по защите информации, составляющей государственную тайну, а также за использование несертифицированных средств, предназначенных для защиты информации, составляющей государственную тайну (пп. 3 и 4 ст. 13.12 КоАП РФ).

Кроме того, наказываются в административном порядке лица, осуществляющие без лицензии деятельность, связанную с использованием и защитой информации, составляющей государственную тайну, созданием средств, предназначенных для защиты информации, составляющей государственную тайну, осуществлением мероприятий и (или) оказанием услуг по защите информации, составляющей государственную тайну (п. 2 статьи 13.13). Уголовная ответственность за разглашение коммерческой тайны установлена в ст. 183 УК РФ. Основанием для санкций является собирание сведений, составляющих коммерческую тайну, путем похищения документов, подкупа или угроз, а равно иным незаконным способом, а также незаконное разглашение или использование сведений, составляющих коммерческую тайну, без согласия владельца лицо, которому она была доверена или стала известна по службе или работе. Следовательно, для наступления уголовной ответственности необходимо доказать незаконный способ получения сведений, незаконное использование, а также корыстную заинтересованность или крупный ущерб (в зависимости от размеров санкций).

КоАП РФ предусматривает административную ответственность юридических и физических лиц за «разглашение информации с ограниченным доступом» (ст. 13.14), под которой понимается «информация с ограниченным доступом (за исключением информации, разглашение которой влечет уголовную ответственность)». Следовательно, действие ст. 13.14 распространяется на случаи разглашения коммерческой тайны, не причинившие крупный ущерб или совершенные по оплошности (без личной заинтересованности).

Что касается гражданско-правовой ответственности, то статья 139 ГК РФ в качестве основного способа защиты предусматривает возмещение причиненных убытков (с учетом реального ущерба и упущенной выгоды согласно статье 15 ГК РФ). Наряду с этим возможно применение и других способов защиты, указанных в статье 12 ГК РФ. Важно, что статья 139 ГК РФ предусматривает введение имущественной ответственности работника перед своим работодателем за разглашение коммерческой тайны.

Помимо работника Гражданско-правовую ответственность несут: работники, связанные с обладателем трудовым договором и специальным соглашением о неразглашении коммерческой тайны; контрагенты, связанные с обладателем коммерческой тайны гражданско-правовым договором, а также органы государственной власти (их должностные лица), получившие информацию, составляющую коммерческую тайну, по закону.

Федеральным законом «О коммерческой тайне», принятым Государственной Думой и не поддержанным Советом Федерации, предусматривалось право обладателя в случае невозможности определения размера ущерба или вреда, причиненного нарушением прав на коммерческую тайну, требовать вместо возмещения убытков выплаты по усмотрению суда компенсации в сумме от 50 до 50000 минимальных размеров оплаты труда, устанавливаемых законодательством Российской Федерации.

Кроме этого, в целях обеспечения иска обладателя информации, составляющей коммерческую тайну, и пресечения действий, нарушающих его права, суд по заявлению обладателя такой информации мог бы запретить ответчику использовать информацию, составляющую коммерческую тайну, в соответствии с законодательством о гражданском судопроизводстве. Однако эти положения не были поддержаны Советом Федерации и Согласительной комиссией и исключены из закона. Ответственность за разглашение сведений, составляющих служебную тайну, предусмотрена статьей 13.14 Кодекса Российской Федерации об административных правонарушениях («Разглашение информации с ограниченным доступом») и статьями 155, 183, 293 Уголовного кодекса Российской Федерации. Трудовой кодекс Российской Федерации предусматривает ряд положений, определяющих дисциплинарную, административную, гражданско-правовую, уголовную ответственность лица, разгласившего сведения, составляющие в том числе служебную тайну (статьи 37, 243), причем в случае разглашения указанных сведений, на работника возлагается материальная ответственность в полном размере причиненного ущерба.

Определенную проблему представляет установление норм ответственности за нарушения прав субъекта персональных данных, нарушения порядка работы с персональными данными, невыполнения предписаний органов, обеспечивающих государственное регулирование работы с персональными данными (дисциплинарная, административная, уголовная, гражданско-правовая ответственность). В Кодексе РФ об административных правонарушениях предусмотрена ст. 13.11 «Нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональные данные)» с санкциями для юридических лиц от 50 до 100 МРОТ.

Необходим тщательный анализ норм уголовно-правовой (ст.ст. 129 «Клевета», 137 «Нарушение неприкосновенности частной жизни», 138 «Нарушение тайны переписка, телефонных переговоров, почтовых, телеграфных и иных сообщений», 155 «Разглашение тайны усыновления», 272 «Неправомерный доступ к компьютерной информации» УК РФ) и гражданско-правовой защиты (ст.ст. 151 «Компенсация морального вреда», 152 «Защита чести, достоинства и деловой репутации», 1100 «Основания компенсации морального вреда» ГК РФ) ответственности и анализ правоприменения с возможным уточнением этих норм. Самостоятельное значения для защиты информации, представленной в машиночитаемой форме (компьютерной информации), имеют статьи Главы 28 УК РФ «Преступления в сфере компьютерной информации».

Уголовно наказуем неправомерный доступ к охраняемой законом компьютерной информации, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование информации, нарушение работы ЭВМ, системы ЭВМ или их сети (ст. 272); создание программ для ЭВМ или внесение изменений в существующие программы, заведомо приводящих к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети, а равно использование либо распространение таких программ или машинных носителей с такими программами (ст. 273) и нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети лицом, имеющим доступ к ЭВМ, системе ЭВМ или их сети, повлекшее уничтожение, блокирование или модификацию охраняемой законом информации ЭВМ, если это деяние причинило существенный вред (ст. 274).

Эта ответственность введена в 1996 году, но применяется достаточно активно, поскольку количество преступлений в сфере компьютерной информации увеличивает ежегодно более, чем в 10 раз. Однако практика правоприменения выявила ряд недостатков в формулировании оснований для ответственности, которые не позволяют обеспечить необходимую эффективность защиты прав обладателей информации, владельцев систем ЭВМ и сетей ЭВМ. Так, положения статьи 272 распространяются только на «охраняемую законом информацию», то есть на ту, для которой установлен специальный правовой режим ограничения доступа. С этим нельзя согласиться, тем более, что защите подлежит и открытая информация, размещаемая на публичных сайтах сети Интернет, поскольку она также не должна подвергаться модификации или искажению уже потому, что предназначена для копирования.

Ответственность, предусмотренная ст. 273, наступает за создание, распространение или использование вредоносных программ, под которыми понимаюсь, прежде всего вирусные программы. Однако в последнее время особую угрозу стал представлять спам, который характеризуется рассылкой с использованием специальных программ-роботов коммерческих и иных сообщений посредством стандартной электронной почты. Вызывает сомнения возможность использования статьи 273 для привлечения к ответственности распространителей спама, хотя ответственность за указанное деяние обязательно должна быть установлена.

Диспозиция статьи 274 также не позволяет привлечь ее для борьбы со спамерами, поскольку даже если массовая рассылка заблокирует почтовый ящик и информация, ожидаемая пользователем не будет им получена во время, эту информацию далеко не всегда можно отнести к «охраняемой законом» как это предусматривает ст. 274.

Практиками оспариваются и санкции рассматриваемых статей, поскольку вред, причиненный компьютерной информации, системам управления различными объектами, в том числе особо опасными, может быть не сопоставим с установленными мерами наказания.

7. Проблемы и особенности доступа к информации и защиты права на информацию в Интернете

Проблемы, связанные с деятельностью посредством Интернета, лежат в двух плоскостях: Интернет как телекоммуникационная среда (регулируется законодательством о связи) и информация, размещаемая в Интернете (регулируется общим законодательством об информации).

Федеральный закон «О связи» устанавливает в статье 1 следующие цели правового регулирования:

- создание условий для оказания услуг связи на всей территории Российской Федерации;
- содействие внедрению перспективных технологий и стандартов;
- защита интересов пользователей услугами связи и осуществляющих деятельность в области связи хозяйствующих субъектов;
- обеспечение эффективной и добросовестной конкуренции на рынке услуг связи;
- создание условий для развития российской инфраструктуры связи, обеспечения ее интеграции с международными сетями связи;
- обеспечение централизованного управления российскими радиочастотным ресурсом, в том числе орбитально-частотным, и ресурсом нумерации;
- создание условий для обеспечения потребностей в связи для нужд государственного управления, обороны страны, безопасности государства и обеспечения правопорядка.

Однако оценить, насколько эффективно эти цели обеспечиваются законом пока не представляется возможным, поскольку он вступил в силу только с 1 января 2004 года. Вместе с тем в процессе обсуждения проекта закона отдельные положения его концепции подвергались критике. В частности, следующие. Особенность инфраструктуры связи, состоящая в том, что она не совпадает с географическими границами государства, требует тщательного определения сферы правового регулирования. В Законе для этих целей используется понятие «юрисдикция» (преамбула, ст. 3), причем, в отличие от прежней редакции Федерального закона, деятельность в области связи в Российской Федерации и деятельность под юрисдикцией Российской Федерации различаются.

Наряду с этим, в п. 1 ст. 12 сети связи общего пользования дифференцируются на определяемые «географически в рамках обслуживаемой территории» и «не географически в пределах Российской Федерации», что не очевидно по смыслу и создаст очевидные проблемы в процессе правоприменения. Не определено используемое в законе понятие «российский сегмент международных сетей» (ст. 25) и не ясно, по каким признакам он выделяется.

Не четко определены субъекты правоотношений, деятельность которых регулируется Законом. Таких субъектов несколько, в том числе, операторы связи и организации связи. При этом оператор связи определяется как юридическое лицо или индивидуальный предприниматель, оказывающий услуги связи на основании лицензии, а организация связи - юридическое лицо или индивидуальный предприниматель, осуществляющие деятельность в области связи в качестве основного вида деятельности.

Получается, что действие федерального закона не распространяется на лиц, оказывающих услуги связи без лицензии (например, услуги бесплатной электронной почты), и на лиц, осуществляющих эту деятельность не в качестве основной. При этом, во-первых не ясно, какие виды деятельности, кроме услуг связи, составляют деятельность в области связи. Во- вторых, не ясен юридический смысл понятия «основная деятельность». Понятие «основной вид деятельности» и принципы выделения таких видов деятельности гражданским законодательством не установлены.

На практике обозначение в уставе основного (основных) видов деятельности есть результат «самоидентификации» субъекта и означает, что он объявляет о своей относительной специализации. Однако требование определять основной вид деятельности гражданское законодательство не устанавливает, равно это никак не влияет на получение

лицензий на «основной» или «дополнительный» вид деятельности. Таким образом, применение подобного критерия юридического смысла не имеет.

Вопросы собственности на средства и системы связи, пользования землями связи и взаимоотношений с надзирающим органом регулируются только применительно к организациям связи. Все остальные положения законопроекта распространяются только на операторов связи, включая их права и обязанности. Таким образом Закон не устанавливает права и обязанности предприятия связи, не являющегося оператором.

Закон выделяет среди операторов связи оператора, занимающего существенное положение на сети связи общего пользования, и оператора универсального обслуживания. Содержание понятия «оператор, занимающий существенное положение на сети связи общего пользования» (ст. 2), оперирует недостаточно точным критерием («оператор, который вместе с аффилированными лицами обладает в географической зоне нумерации или на всей территории Российской Федерации не менее 25 процентов монтированной емкости»). Такой оператор вместе с аффилированными лицами может осуществлять различные виды услуг, в связи с чем не ясно, как будет определяться указанный критерий. Не ясно также, каким образом будет доводится до других операторов информация о том, что тот или иной оператор является оператором, занимающим существенное положение на сети связи общего пользования.

В мире используются несколько методик, которые могут помочь в определении оператора, занимающего существенное положение на рынке. Так, например, в Директиве Европейского Союза 3672/01 об общем регулировании электронных телекоммуникационных услуг используется качественный критерий для определения позиции, которую занимает такое предприятие, - экономически сильная позиция, позволяющая ему вести себя в существенной степени независимо от конкурентов и, соответственно, от потребителей. Применение этой методики потребует проведения глубокого экономического анализа, к которому наши органы управления связью еще не готовы. Используется также методика, основанная на оценке общего дохода предприятия в определенном сегменте рынка.

В американском законе о телекоммуникациях (1996 г.) выделены кроме того и другие типы операторов и для каждого из них установлены обязанности. Так, более жесткие требования установлены для операторов локального обмена, предоставляющих услуги местной телефонной связи, причем. операторы, занимающиеся предоставлением услуг мобильной связи не включаются в данную группу операторов. На операторов локального обмена, объединенных в ассоциацию, налагаются дополнительные требования. С развитием Интернета возникла необходимость дифференцировать провайдеров связи, выделив сервис-провайдеров и установив для них права и обязанности. Это также не было реализовано в Федеральном законе.

Закон реализует идею лицензирования деятельности по оказанию только возмездных услуг связи, при этом перечень наименований услуг связи, которые образуют лицензируемые виды деятельности, и перечни лицензионных условий не установлены в Законе, а должны утверждаться постановлением Правительства РФ (ст. 29). В свое время деятельность в области связи была выведена из сферы действия Федерального закона «О лицензировании отдельных видов деятельности». Но, очевидно, что и на эту сферу деятельности должны распространяться основные принципы реформы системы лицензирования, закрепленные в Федеральном законе. Это, прежде всего, сокращение лицензируемых видов деятельности в результате оптимизации механизмов государственного регулирования.

Все способы госрегулирования - лицензирование, регистрацию, сертификацию, разрешения и т.п. - целесообразно было бы проанализировать в совокупности и устранить целевое дублирование. Произойдет ли сокращение сферы лицензирования в области связи - пока оценить невозможно. Второй принцип реформы системы лицензирования - установление непосредственно в законе ограниченного перечня лицензируемых видов деятельности. Если этого не сделать, использование всех разрешительных механизмов переносится на подзаконный уровень, что противоречит как ФЗ «О лицензировании отдельных видов деятельности» и требованиям Гражданского кодекса РФ (ст. 49)., так и принципам российского права, в соответствии с которыми ограничения прав физических и юридических лиц должны устанавливаться законом.

Таким образом в соответствии с ФЗ «О связи» целесообразность установления лицензирования на виды деятельности в области связи не подлежит контролю, хотя, очевидно, что множественность лицензий, которые должен сейчас получать один оператор связи, в конечном итоге отражается на себестоимости услуг, то есть на потребителях. Похожая ситуация наблюдается в вопросах сертификации средств связи. В указанном Законе (ст. 41) не установлены ни принципы обязательной сертификации, ни виды средств связи, подлежащих обязательной сертификации. Перечень подлежащих обязательной сертификации средств связи, утверждаемый Правительством Российской Федерации, включает в себя укрупненные виды оборудования:

- средства связи, выполняющие функции систем коммутации, цифровых транспортных систем, систем управления и мониторинга, а также оборудование, используемое для учета объема оказанных услуг связи в сетях связи общего пользования;
- оконечное оборудование, которое может привести к нарушению функционирования сети связи общего пользования;
- средства связи технологических сетей связи и сетей связи специального назначения в части их присоединения к сетям связи общего пользования;
- радиоэлектронные средства связи;
- оборудование средств связи, в том числе программное обеспечение, обеспечивающее выполнение установленных действий при проведении оперативно-розыскных мероприятий.

Правительство Российской Федерации определяет порядок организации и проведения работ по обязательному подтверждению соответствия средств связи, порядок аккредитации органов по сертификации, испытательных лабораторий (центров), проводящих сертификационные испытания, и утверждает правила проведения сертификации.

До принятия Закона деятельность органов по надзору за связью фактически финансировалась за счет средств организаций, за которыми устанавливались контроль и надзор. При внесении Правительством РФ проекта федерального закона «О связи» в Государственную Думу впервые в российском законодательстве была сделана попытка “узаконить” (установить в законе) принцип финансирования деятельности по надзору за связью - «за счет отчислений операторов связи, относимых в соответствии с Налоговым кодексом Российской Федерации к прочим расходам, связанным с производством и (или) реализацией продукции и услуг, и иных источников, не запрещенных законодательством Российской Федерации».

До сих пор этот порядок определялся актами Правительства РФ. В соответствии с Постановлением Правительства РФ от 28 апреля 2000 г. № 380 «О реорганизации системы

государственного надзора за связью и информатизацией в Российской Федерации» финансирование деятельности управлений по надзору за связью и информатизацией в субъектах Российской Федерации осуществляется за счет отчислений организаций, предоставляющих услуги в области связи и информатизации, и средств, получаемых из других источников в соответствии с законодательством Российской Федерации.

Приказом Минсвязи РФ от 18 апреля 2001 г. № 126 «О введении норматива отчислений» был установлен размер таких отчислений − 0,3% от доходов организации-оператора. Такая логика и практика представляется, по меньшей мере, спорной. Функция надзора - это функция государственного управления, то есть деятельность, осуществляемая за счет бюджета. Именно так финансируются надзирающие органы в других сферах деятельности (в том числе: Госатомнадзор, геодезический надзор, Росхлебинспекция, Госгортехнадзор и другие).

Положения законопроекта противоречили ряду принципов защиты прав юридических лиц и индивидуальных предпринимателей при проведении государственного контроля (надзора) (ст. 3), установленных Федеральным законом «О защите прав юридических лиц и индивидуальных предпринимателей при проведении государственного контроля (надзора)», в том числе о недопустимости взимания органами государственного контроля (надзора) платы с юридических лиц и индивидуальных предпринимателей за проведение мероприятий по контролю, за исключением случаев возмещения расходов органов государственного контроля (надзора) на осуществление исследований (испытаний) и экспертиз, в результате которых выявлены нарушения обязательных требований.

Кроме того, Бюджетный кодекс Российской Федерации (ст. 84) определяет, что обеспечение деятельности, федеральных органов исполнительной власти и их территориальных органов осуществляется «исключительно из федерального бюджета». В окончательной редакции Федерального закона был принят следующий механизм финансирования надзорного органа (ст. 27). «2. Финансирование государственного надзора за связью осуществляется из средств федерального бюджета, выделенных федеральному органу исполнительной власти в области связи отдельной строкой федерального закона о федеральном бюджете на соответствующий год, за счет отчислений операторов связи в доходы федерального бюджета. Средства, получаемые за счет отчислений операторов связи, зачисляются в доходы федерального бюджета и учитываются в доходах и расходах федерального бюджета отдельно. Положение о взимании и расходовании этих средств утверждается Правительством Российской Федерации».

Действие пункта 2 статьи 27 было приостановлено с 1 января по 31 декабря 2004 года Федеральным законом от 23.12.2003 № 186-ФЗ «О федеральном бюджете на 2004 год». Таким образом, в текущем году деятельность контролирующих органов в области связи финансируется, видимо, по прежней схеме. Закон не решил ряд проблем, в том числе связанных с обеспечением тайны связи, предоставлением сведений об абонентах и оказанных им услугах, взаимоотношениями операторов связи и субъектов оперативно-розыскной деятельности. Понятие « тайны связи» не было введено Законом, в связи с чем сохранилась неопределенность. Как результат, в процессе правоприменения суды по разному решают вопрос о распространении на ту или иную информацию тайны связи. По нашему мнению понятие тайны связи можно определить как тайна содержания переписки, телефонных переговоров, почтовых отправлений, телеграфных и иных сообщений, передаваемых по сетям электрической и почтовой связи. Информация об абонентах, оказанных им услугах и иная технологическая информация, накапливаемая оператором в

связи с предоставлением услуг связи, должна быть предоставлены представителям органов, осуществляющих оперативно-розыскную деятельности и следственные действия. Порядок предоставления такой информации может быть определен в подзаконном акте, но сама обязанность и условия получения информации должны быть установлены в законе. Особенности розыскной и следственной работы (скрытность и оперативность) обуславливают необходимость оперативного доступа к данным об абонентах без обозначения объекта заинтересованности, поэтому соответствующим органам, по видимому, должна быть предоставлена возможность доступа к базам данных об абонентах (предполагается, что в этих базах содержится только номинативная информация (ФИО, адрес, номер телефона или IP-адрес).

Второй пласт проблем, связанных с развитием Интернета, это проблемы ограничения прав на распространения через Интернет информации, которая по законам страны не подлежит распространению. В связи с этим возникают следующие вопросы:

- каков правовой статус провайдеров Интернета?
- должны ли провайдеры нести ответственность за содержание распространяемой ими информации?
- как обеспечить ответственность провайдеров, учитывая экстерриториальность Интернета?

Все страны в одинаковой степени осознают данные проблемы, но по разному подходят к их решению. Большинство стран не форсирует разработку новых законов, а пытаются применять действующие, при необходимости их совершенствуя. Решение этой проблемы путем применения законов о печати показало недостаточную их эффективность.

Сервис-провайдер никак не может выступать в качестве СМИ и нести ответственность за содержание информации, передаваемой с его помощью. Тем не менее, провайдеры в ряде стран (Германия, США, Великобритания, Япония и другие) по собственной инициативе стали запрещать доступ к «сомнительным» узлам в Сети, особенно, если пользователи обратили их внимание на содержание информации. При этом активно используются программно-технические средства. Эта идея в той или иной степени реализована в Билле о клевете (Defamation Bill), принятом в Великобритании. Сервис-провайдер не должен вмешиваться в содержимое электронных досок объявлений, но если он обнаружит, что предоставил доступ к непристойной или клеветнической информации, он обязан принять немедленно меры и будет нести ответственность за предоставленный материал.

Провайдеры в Японии переработали свои контракты, включив в них право предотвращать распространение порнографических изображений. Китай пошел по пути организационных ограничений, сократив до двух количество международных шлюзов в Интернет в стране и заставив своих граждан - пользователей Интернета регистрироваться в течение 30 дней в отделах общественной безопасности в своих префектурах. В Германии принят закон, согласно которому провайдеры несут ответственность за содержание информации, обязаны блокировать распространение любых запрещенных материалов, о которых им становится известно. Для этих целей они обязаны иметь в штате специальных сотрудников, которые просматривали бы информацию, предназначенную для детей.

В США был принят так называемый Акт о благопристойности (CDA’96 - Communication Decency Act), действие которого было приостановлено по решению Федерального (Верховного) суда США, посчитавшего формулировку Акта слишком неопределенной. Многие эксперты справедливо считают, что проблему содержания информации невозможно только решить правовыми методами, необходимо использование технических средств: технология создала угрозу, технология должна ее уничтожить».

Большинство крупных российских провайдеров также старается самостоятельно принимать решения по нераспространению запрещенной информации, если на нее обратили внимание, соответствующие положения включаются в договора с потребителями, однако обязанность следить за содержанием передаваемой информации, законом не установлена и не может быть установлена.

Передача информации по компьютерным сетям может рассматриваться как экспорт или импорт. Таможенное регулирование в этом случае практически не может действовать, хотя ФЗ «Об участии в международном информационном обмене» и еще ряд законов такую возможность предусматривают. В том числе, контроль содержания информации на предмет наличия в ней сведений, составляющих государственную тайну, сведений о недрах, о технологиях двойного применения, продукции военного назначения, шифровальных средств, отнесения ее к общероссийскому национальному достоянию и архивному фонду, вывоз которой ограничен законодательством РФ. Таможенный контроль по этим основаниям не имеет смысла. Неконтролируемое распространение, использование (в том числе, перемещение через границу РФ) необходимо пресекать иными средствами. Более того, ФЗ «Об участии в международном информационном обмене» содержит положение о необходимости лицензирования деятельности по международному информационному обмену в случаях, когда в результате этой деятельности вывозятся за пределы территории Российской Федерации государственные информационные ресурсы либо ввозится на территорию Российской Федерации документированная информация для пополнения государственных информационных ресурсов за счет средств федерального бюджета или средств бюджетов субъектов Российской Федерации. Данное положение не может применяться из-за исключения данного вида деятельности из перечня лицензируемых, однако из Федерального закона оно не исключено Регулирование прав и обязанностей провайдеров в связи с контролем содержания информации, передаваемой по сетям связи, и нарушением иных прав пользователей услуг связи, таких как «спам», потребует внесения изменений в Федеральные законы «О связи», «О государственном регулировании внешнеторговой деятельности», «Об участии в международном информационном обмене», «Об информации, информатизации и защите информации», в Таможенный кодекс РФ, а также ведомственные правовые акты.

Необходимо повысить эффективность государственного регулирования в области связи. Государственная политика должна быть направлена на:

1. создание, развитие, сохранение и эффективное использование информационных ресурсов, в том числе путем доступа к ним через Интернет, а также путем сохранения «цифрового наследия» (термин введен в проекте Рекомендаций ЮНЕСКО), то есть ресурсов, создаваемых и существующих исключительно в электронном виде;
2. создание, развитие, защиту и эффективное использование инфраструктуры связи, обеспечивающей передачу и доступ к информационным ресурсам;
3. поддержку отечественного производителя средств и систем связи, развитие конкуренции на рынке средств, систем и услуг связи.

Первая задача системно не решается, нет единой системы учета ресурсов, не получило достаточного наполнения понятие «государственные информационные ресурсы», нет концепции управления этими ресурсами, нет системы доступа к ним. Хотя эти цели обозначены в Декларации Комитета министров Совета Европы «О европейской политике в области новых информационных технологий» (1999).

Вторая задача в той иной степени начинает решаться Министерством связи, которое разрабатывает проекты Концепций развития отрасли, обеспечения ИБ, развития рынка телекоммуникационного оборудования.

Государство весьма скупо стимулирует отечественного производителя средств и систем связи, за исключением некоторых проектов ФЦП «Электронная Россия». Участие государства как собственника на рынке телекоммуникаций целесообразно только при решении задач государственной экономической и социальной политики, безопасности государства и др., но никак не с целью извлечения максимальной прибыли.

В связи с государственной политикой в информационно-телекоммуникационной сфере необходимо обеспечить открытость деятельности всех органов, осуществляющих эту политику, включая открытость процесса принятия решений и публикацию принятых решений с разъяснениями; создание эффективных механизмов апелляций на решения регулирующего органа; тщательная проверка бюджета законодательной властью и т.д.

Кроме того, целесообразно повысить межведомственную координацию органов, отвечающих за проведение государственной политики на рынке телекоммуникационных услуг, в том числе, все решения Минсвязи РФ, регулирующие деятельность операторов связи и воздействующие на себестоимость услуг связи, должны проходить обязательное согласование с органом, регулирующим тарифы .

Всемирная встреча на высшем уровне по вопросам информационного общества, состоявшаяся 10-12 декабря 2003 г. в Женеве, определила приоритеты и вектор развития законодательства в данной сфере в контексте глобальных процессов становления информационного общества как общества, «в котором каждый мог бы создавать информацию и знания, иметь к ним доступ, пользоваться и обмениваться ими, с тем чтобы дать отдельным лицам, общинам и народам возможность в полной мере реализовать свой потенциал, содействуя своему устойчивому развитию и повышая качество своей жизни на основе целей и принципов Устава Организации Объединенных Наций и соблюдая в полном объеме и поддерживая Всеобщую декларацию прав человека».

План действий, принятый на Всемирной встрече, предусматривает, что к 2005 году все страны должны разработать всеобъемлющие, перспективные и устойчивые национальные электронные стратегии. Ведущая роль в этом процессе должна принадлежать органам государственного управления. Частный сектор и гражданское общество, в диалоге с органами государственного управления, должны сыграть важную консультативную роль в формировании национальных электронных стратегий.

Укрепление доверия и безопасности при использовании информационных и коммуникационных технологий (ИКТ) названо в документах Всемирной встречи одним из ключевых принципов построения открытого информационного общества. При этом информационная безопасность и безопасность сетей (которые рассматриваются как два самостоятельных направления), вместе с защитой неприкосновенности частной жизни и прав потребителей составляют основу для доверия со стороны пользователей ИКТ.

Реализация указанного принципа предусматривает, в том числе:
а) укрепление доверия пользователей, повышение надежности и защиты целостности данных и сетей связи; анализа существующих и потенциальных угроз в области ИКТ и др.;

b) сотрудничество органов государственного управления в с частным сектором в целях предупреждения и обнаружения актов киберпреступности и ненадлежащего использования ИКТ и реагирования на эти проявления;
c) просвещение пользователей относительно неприкосновенности частной жизни при работе в онлайновом режиме и способов ее защиты;
d) принятие необходимых мер на национальном и международном уровнях для защиты от спама;
e) проведение на национальном уровне оценки внутреннего законодательства с целью ликвидации препятствий для эффективного использования документов и осуществления сделок в электронной форме, в том числе использования электронных методов аутентификации;
f) обмен позитивным опытом в области информационной безопасности и безопасности сетей и поощрение его использования всеми заинтересованными сторонами;
g) назначение координаторов для реагирования в режиме реального времени на происшествия в сфере безопасности и объединение этих координаторов в открытую сеть для обмена информацией и технологиями реагирования на происшествия.

В документах Всемирной встречи указывается на необходимость формирования, развития и внедрения глобальной культуры кибербезопасности в сотрудничестве со всеми заинтересованными сторонами и компетентными международными организациями. Это означает деятельность, направленную на предотвращение возможности использования ИКТ в целях, которые несовместимы с задачами обеспечения международной стабильности и безопасности и способны оказать отрицательное воздействие на целостность государственных инфраструктур, нанося ущерб их безопасности, включая предотвращение использования информационных ресурсов и технологий в преступных и террористических целях.

Одним из элементов благоприятной среды для формирования и существования информационного общества названо верховенство права. Таким образом документы, принятые на Всемирной встрече, вместе с Доктриной информационной безопасности Российской Федерации определяют стратегию деятельности общества и государства в создании условий для формирования информационного общества в России, включая перспективные задачи правового обеспечения этих процессов. Положения этих документов должны лечь в основу государственной информационной политики, предусматривающей, в том числе, комплексное, взаимоувязанное развитие законодательства.

Примечания

---

[1] *В том числе, «О средствах массовой информации», «О порядке освещения деятельности органов государственной власти в государственных средствах массовой информации», «Об общественных объединениях», «Об акционерных обществах», «Об основах государственного обязательного страхования», «О выборах Президента Российской Федерации», «Об основных гарантиях избирательных прав граждан на участие в референдуме в Российской Федерации», «О государственном банке данных о детях, оставшихся без попечения родителей», «О защите прав потребителей», «О рекламе», «О государственном земельном кадастре», «О защите конкуренции на рынке ценных бумаг», «О борьбе с терроризмом», «О гидрометеорологической службе», «О негосударственных пенсионных фондах», «О науке и государственной научно-технической политике», «О геодезии и картографии», «О животном мире», «О библиотечном деле», «О пожарной безопасности», «Об авторском праве и смежных*

правах», «О чрезвычайном положении», «О защите населения и территорий от чрезвычайных ситуаций природного и техногенного характера», Основы законодательства об архивах, Гражданский кодекс РФ, Семейный кодекс РФ, Гражданский процессуальный кодекс РФ и многие другие.

[2] *Так, Федеральная служба безопасности Российской Федерации руководствуется в своей деятельности Инструкцией о порядке рассмотрения предложений, заявлений и жалоб граждан в органах Федеральной службы безопасности, утвержденной Приказом от 4 декабря 2000 г. № 613. Министерство внутренних дел Российской Федерации регламентировало свою работу с обращениями граждан Инструкцией по делопроизводству и порядку работы с обращениями граждан в центральном аппарате и подчиненных подразделениях МВД России, утвержденной Приказом от 1 марта 1999 г. № 150. Аналогичную Инструкцию о порядке рассмотрения обращений граждан в Государственном комитете Российской Федерации по рыболовству принял названный комитет (Приказ от 28 июня 2002 г. № 261). Судебный департамент при Верховном Суде Российской Федерации выпустил свою Инструкцию о порядке рассмотрения обращений граждан и ведения делопроизводства по ним в Судебном департаменте при Верховном Суде Российской Федерации (утв. Приказом ВС РФ от 23 декабря 1998 г. № 112). Генеральная прокуратура Российской Федерации приказом от 15 января 2003 г. № 3 утвердила Инструкцию о порядке рассмотрения и разрешения обращений и приема граждан в органах и учреждениях прокуратуры Российской Федерации, в Министерстве обороны действует Инструкция о работе с обращениями граждан в Вооруженных Силах Российской Федерации (утв. приказом от 29 декабря 2000 г. № 615. Аналогичная инструкция имеется в Совете Федерации Федерального Собрания РФ.*

[3] *Предлагается различать право распространения информации и право передачи, последнее может пониматься как юридически - передача информации на определенных условиях от одного лица другому, так и физически - передача информации по каналам связи.*

[4] *«О выборах Президента Российской Федерации», «О выборах депутатов Государственной Думы Федерального Собрания Российской Федерации», «Об основных гарантиях избирательных прав и права на участие в референдуме граждан Российской Федерации», «Об обеспечении конституционных прав граждан Российской Федерации избирать и быть избранными в органы местного самоуправления».*

[5] *«О противодействии экстремистской деятельности», «О борьбе с терроризмом», «О лекарственных средствах», «О наркотических средствах и психотропных веществах», «О безопасном обращении с пестицидами и агрохимикатами», «О государственном регулировании производства и оборота этилового спирта, алкогольной и спиртосодержащей продукции».*

[6] *«О физической культуре и спорте в Российской Федерации», «О национально-культурной автономии», «О рынке ценных бумаг».*

[7] *Актуальные проблемы правового регулирования телекоммуникаций. М.: Центр «Право и СМИ», 1998, с. 69.*

[8] *Олег Винокуров, Владимир Ефимов «Скальпель цензора (юридические аспекты)», Мир Интернет, №11 1998.*

[9] *Так в соответствии со ст. 2 ФЗ «Об информации, информатизации и защите информации» по конфиденциальной информацией понимается «документированная информация, доступ к которой ограничивается в соответствии с законодательством Российской Федерации», а п. 2 статьи 10 этого же закона предусматривает две категории информации с ограниченным доступом: информацию, отнесенную к государственной тайне, и конфиденциальную информацию.*

[10] *Так, например, в соответствии со статьей 16 Таможенного кодекса РФ не должна разглашаться «информация, составляющая государственную, коммерческую, банковскую и иную охраняемую законом тайну, а также конфиденциальная информация», что не соответствует положениям п. 2 статьи 10 Федерального закона «Об информации, информатизации и защите информации».*

[11] *Постановление Конституционного Суда Российской Федерации от 27 марта 1996 г. № 8-П «По делу о проверке конституционности статей 1 и 21 Закона Российской Федерации от 21 июля 1993 года «О государственной тайне» в связи с жалобами граждан В.М. Гурджиянца, В.Н. Синцова, В.Н. Бугрова и А.К. Никитина»; Определение Конституционного Суда Российской Федерации от 10 ноября 2002 г. № 293-О «По жалобе открытого акционерного общества «Омский каучук» на нарушение конституционных прав и свобод статьей 21 Закона Российской Федерации «О государственной тайне».*

[12] *УК РФ: ст. 137 - нарушение неприкосновенности частной жизни, 140 - отказ в предоставлении гражданину информации, 285-287 - злоупотребление должностными полномочиями, превышение должностных полномочий и др.; ГК РФ: ст. 151 - компенсация морального вреда, 152 - защита чести, достоинства и деловой репутации и др.*

[13] *Ст. 5.6, 5.17, 5.25, 5.39, 8.5, 13.11, 13.12, 13.14, 13.19, 14.25, 15.19, 15.21 и др.*