

Ю.А.Нисневич,
доктор политических наук,
директор Института проблем
либерального развития

ЗАЩИТА ИНФОРМАЦИИ В ИНФОКОММУНИКАЦИОННЫХ СИСТЕМАХ И СЕТЯХ*

Системообразующим фактором трансформации человеческой цивилизации на постиндустриальном этапе ее развития является формирование на основе использования новейших информационно-коммуникационных технологий открытой информационной среды с инфраструктурой сетевого типа. Основной задачей инфраструктуры информационной среды является обеспечение свободы и доступности массового обмена информацией и массовых коммуникаций. Транспортная основа сетевой инфраструктуры - национальные телекоммуникационные сети, которые, соединяя между собой разнообразные множества депозитариев, источников и потребителей информации, образуют инфокоммуникационные системы и сети различного функционального назначения, которые в совокупности и составляют национальные сегменты глобальной сети.

Внедрение во все сферы человеческой деятельности современных технологий создания, накопления и распространения информации, средств вычислительной техники и телекоммуникаций, создание принципиально новых и цифровизация традиционных инфокоммуникационных систем и сетей обуславливает качественные изменения и постоянное расширение объемов циркулирующей в таких системах и сетях информации, которая становится ключевым ресурсом для экономического, социального и политического развития общества и государства. При этом следует

учитывать, что информационные ресурсы обладают рядом специфических особенностей.

Во-первых, информационные ресурсы – это продукт интеллектуальной деятельности самих людей, их производителем является все человеческое сообщество. По мере развития цивилизации происходит постоянное возрастание накапливаемых объемов и интенсивности использования этих ресурсов, совершенствование и конвергенция разнообразных форм и способов их представления.

Во-вторых, информационные ресурсы являются существенно неоднородными. Содержание и смысл информации определяют ее ценностные и потребительские характеристики, необходимость свободного распространения или наоборот ограничения доступа, сохранения в тайне для обеспечения защиты прав и интересов человека, общества и государства.

В-третьих, качество информационных ресурсов определяется такими ключевыми показателями как полнота и достоверность информации. Предумышленное или неумышленное искажение полноты и достоверности информации несет существенные угрозы в смысле принятия некорректных управленческих решений с негативными последствиями, манипулятивного воздействия на общественное мнение в узкогрупповых целях, развязывания разрушительных информационных войн. Следует особо отметить, что существенное расширение возможностей и технологий информационного манипулирования, которое предоставляет современная информационная среда, является одним из основных вызовов информационной эпохи.

В-четвертых, информационные ресурсы в смысле права собственности обладают двумя ипостасями: материальной – на них распространяется право вещной собственности и интеллектуальной – на них распространяется право интеллектуальной собственности и авторское право.

В условиях постиндустриального развития национальные и глобальные инфокоммуникационные системы и сети открытого типа охватывают все сферы жизнедеятельности общества и государства, изменяя не только

технологические, но и сущностные основы такой деятельности. Они становятся основным средством использования, обмена и распространения всех видов информационных ресурсов и оперативной информации: текстовых, аудио и видео материалов и сообщений, предназначенных как для массового информирования, включая рекламу, так и для индивидуальных коммуникаций; документированной информации и данных, включая доступ к различным их депозитариям; продукции средств массовой информации и информационных агентств; юридических и финансовых документов, включая транзакции, и т.д.

Интенсивная сетевая информатизация, как и любое глобальное явление, трансформирующее цивилизацию, открывает как новые перспективы и возможности развития, так и порождает определенные угрозы и вызовы. Поэтому проблемы законодательного регулирования информационных отношений и процессов, в том числе и традиционных, в условиях постиндустриальной информационной среды приобретают существенно большую остроту и актуальность, прежде всего в связи с необходимостью поиска адекватных ответов на вызовы и угрозы информационной эпохи в правовом поле.

Постиндустриальная информационная среда существенно расширяет потенциальные возможности обеспечения права на информацию, относящегося в соответствии с Всеобщей Декларацией прав человека (1948) к категории основных прав и свобод человека и гражданина. Однако право на информацию как и другие права и свободы не является безграничным. Любые права и свободы действительно являются таковыми лишь до тех пор пока их осуществление не нарушает те или иные права других людей, а также конституционные права и обязанности иных субъектов общественных отношений, таких как добровольные объединения граждан, субъекты предпринимательской и иной экономической деятельности, органы государственной власти и местного самоуправления.

В этом аспекте действительно необходимыми являются определенные законодательные ограничения права на информацию, которое устанавливается статьей 29 Конституцией РФ (1993) как право каждого свободно искать, получать, передавать, производить и распространять информацию любым законным образом, т.е. как право свободно осуществлять весь набор действий с информацией. Суть таких законодательных ограничений должна состоять не в том, чтобы ограничить право на информацию как таковое, а лишь в том, чтобы ограничить в той или иной степени полную свободу действий с информацией, которую принято называть конфиденциальной, законодательно регламентировать круг субъектов и порядок работы с такой информацией.

Необходимость ограничения в указанном выше смысле права на информацию федеральным законом с целью защиты государственной тайны зафиксирована в той же статье 29 Конституции РФ. В развитие этой нормы в 1993 года был принят Закон РФ «О государственной тайне». Этот закон установил ограничения на действия с информацией, содержащей сведения, составляющие государственную тайну, которые объективно необходимы для того, чтобы в условиях свободы информации органы государственной власти имели возможность выполнять свои функции и обязанности по защите интересов страны, ее обороноспособности, безопасности, включая экономическую, территориальной целостности, по предотвращению преступлений и т.д.

Однако российский законодатель, успешно позаботившись о защите интересов государственной власти в информационной сфере, до настоящего времени не сделал того же в полном объеме в отношении граждан, их добровольных объединений и субъектов экономической деятельности.

Конституция РФ в статье 23 устанавливает, что каждый имеет право на неприкосновенность частной жизни, личную и семейную тайну, защиту своей чести и доброго имени. Каждый имеет право на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений.

Ограничение этого права допускается только на основании судебного решения.

Защита тайны связи на законодательном уровне обеспечивается статьей 63 Федерального закона «О связи» (2003), которая устанавливает, что на территории Российской Федерации гарантируется тайна переписки, телефонных переговоров, почтовых отправлений, телеграфных и иных сообщений, передаваемых по сетям электросвязи и сетям почтовой связи. Обязанность по обеспечению соблюдения тайны связи возлагается на операторов связи. Ограничение права на тайну связи допускается только в случаях, предусмотренных федеральными законами, что в определенной степени расширяет соответствующее конституционное положение.

Однако обеспечение права на неприкосновенность частной жизни, личную и семейную тайну, а тем более на защиту чести и доброго имени не сводится только к защите тайны связи. Наибольшую угрозу этим правам особенно в условиях всепроницающей сетевой информационной среды представляют различные действия с информацией персонального характера как со стороны государства, естественно стремящегося взять своих граждан под максимальный контроль, так и со стороны различных негосударственных организаций и отдельных лиц, стремящихся извлечь ту или иную выгоду от использования и распространения такой информации.

Информация персонального характера или персональные данные представляет собой информацию о конкретном человеке, отождествляемую с конкретным человеком или которая может быть с ним отождествлена, и позволяющую прямо или косвенно идентифицировать этого человека. К персональным данным относятся: биографические и номинативные данные, личные характеристики, сведения о семейном, социальном, служебном и имущественном положении, образовании, профессии, информация о семейной жизни, состоянии здоровья, привычках, увлечениях, нравственных, политических, религиозных и сексуальных предпочтениях и многое другое. Распространение такой информации без согласия самого человека может как

способствовать формированию его положительного образа в общественном сознании, так и нанести непоправимый урон, моральный вред, особенно если такая информация недостоверна или преднамеренно искажена. Именно поэтому непосредственно Конституция РФ в статье 24 устанавливает, что сбор, хранение, использование и распространение информации о частной жизни лица без его согласия не допускаются, т.е. устанавливается конституционный запрет на несанкционированные самим человеком действия с информацией персонального характера.

Интенсивное развитие и повсеместное внедрение современных информационно-коммуникационных технологий, систем и сетей обеспечивает широкие возможности для создания многочисленных и мощных баз данных, легкость распространения информации из различных баз, простоту ее копирования, агрегирования и модификации и т.п. При этом существенно возрастают информационные угрозы неприкосновенности частной жизни в смысле «прозрачности» каждого человека как для государства, так и для других людей, преднамеренного манипулирования информацией персонального характера. Поэтому в условиях интенсивной сетевой информатизации особое внимание как на национальном, так и на международном уровне уделяется законодательным проблемам защиты информации персонального характера. Сегодня более чем в 20 странах действуют специальные законы, а также принят ряд международных нормативных правовых актов, посвященных проблемам использования персональных данных.

В российском законодательстве основы регулирования отношений в связи с использованием информации персонального характера определены Федеральным законом «Об информации, информатизации и защите информации» (1995). Статья 11 этого закона закрепляет следующие базовые принципы работы с такой информацией:

персональные данные относятся к категории конфиденциальной информации, для них должен быть установлен режим ограниченного доступа, а лица, нарушающие этот режим, несут ответственность;

запрещается сбор, хранение, использование и распространение персональных данных без согласия субъекта этих данных;

состав собираемых персональных данных должен соответствовать целям их сбора;

персональные данные не могут быть использованы в целях причинения имущественного и морального вреда гражданам;

деятельность негосударственных организаций и частных лиц, связанная с обработкой и предоставлением пользователям персональных данных подлежит обязательному лицензированию;

в судебном порядке по требованию субъекта может быть установлена неправомерность деятельности органов государственной власти и организаций по сбору персональных данных.

Федеральный закон «Об информации, информатизации и защите информации» определяет только основы, но не сам законодательный механизм регулирования отношений в связи с использованием информации персонального характера. Для этой цели данным законом предусматривается специальный федеральный закон об информации персонального характера. К сожалению, до настоящего времени такой специальный закон в России так и не принят, хотя соответствующие проекты вносились в Государственную Думу первого, второго и третьего созывов.

Федеральный закон об информации персонального характера должен регламентировать условия законности работы с информацией персонального характера; порядок формирования массивов персональных данных органами государственной власти и местного самоуправления, юридическими и физическими лицами; права субъекта персональных данных; права, обязанности и ответственность держателя (обладателя) массивов таких

данных, а также формы государственного регулирования работы с персональными данными.

Настоятельная необходимость в скорейшем принятии данного закона обусловлена тем, что это позволит обеспечить законодательную защиту информационной неприкосновенности частной жизни, личной и семейной тайны, что особенно актуально в условиях нарастающей сетевой информатизации всех сфер жизнедеятельности человека.

Помимо таких категорий конфиденциальной информации как государственная, личная и семейная тайны, установленных Конституцией РФ, первая часть Гражданского кодекса РФ (1994) в статье 139 вводит категорию служебной или коммерческой тайны. В соответствии с этой статьей информация составляет служебную или коммерческую тайну в случае, когда информация имеет действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам, к ней нет свободного доступа на законном основании и обладатель информации принимает меры к охране ее конфиденциальности.

Очевидно, что коммерческая или служебная тайна являются существенным элементом деятельности всех юридических лиц, включая и некоммерческие организации. Именно поэтому информация, составляющая коммерческую тайну, представляет собой реальный товар, имеющий достаточно высокую стоимость и значительный оборот на рынке незаконной информационной продукции. Законодательное регулирование всего комплекса отношений в связи с использованием информации, составляющей коммерческую тайну, принципиально необходимо для пресечения незаконного оборота такой информации и в качестве эффективной меры противодействия в условиях рыночной экономики таким негативным явлениям как недобросовестная конкуренция и коррупция. Однако судьба российского закона о коммерческой тайне во многом схожа с судьбой закона об информации персонального характера.

Первый проект Федерального закона «О коммерческой тайне» был внесен Правительством РФ в Государственную Думу в 1995 году, но не был принят даже в первом чтении. В 1996 году Государственная Дума второго созыва приняла решение о доработке этого проекта и после почти трехлетней работы в 1999 году Федеральный закон «О коммерческой тайне» был принят парламентом. Однако Президент РФ отклонил данный закон, а Государственная Дума не смогла преодолеть вето Президента. Основной причиной отклонения послужило включение в текст закона специальной главы, посвященной правовой охране секретов производства (ноу-хау), что Президент посчитал концептуально неприемлемым. В марте 2003 года Правительство РФ внесло в Государственную Думу третий вариант проекта Федерального закона «О коммерческой тайне».

Концепция данного проекта закона основана на том, что обладатель информации, составляющей коммерческую тайну, самостоятельно определяет необходимые меры по ее защите и при этом законодательно обеспечиваются механизмы защиты прав и интересов всех субъектов отношений в связи с использованием такой информации. Проект закона включает следующие основные положения, которые концептуально представляются достаточно обоснованными:

право на отнесение информации к коммерческой тайне и определение перечня и состава такой информации принадлежит ее обладателю, которым может быть любое физическое или юридическое лицо, включая иностранные физические и юридические лица, занимающееся предпринимательской деятельностью на территории Российской Федерации;

законодательно устанавливается перечень информации, которая не может составлять коммерческую тайну, и предусматривается возможность отнесения коммерческой тайны к государственной тайне;

режим коммерческой тайны и необходимые меры по охране конфиденциальности информации, составляющей коммерческую тайну, определяются самостоятельно ее обладателем, но эти меры не должны

представлять опасность для жизни и здоровья людей и нарушать законные права и интересы физических и юридических лиц;

все имущественные права на информацию, составляющую коммерческую тайну, принадлежат ее обладателю, который имеет право на возмещение убытков, причиненных в связи с ее разглашением, незаконным получением и использованием третьими лицами;

определены права и обязанности работодателя и работника при осуществлении трудовых отношений и после их прекращения по обеспечению охраны информации, составляющей коммерческую тайну организации и (или) ее контрагентов;

должностные лица и другие работники органов государственной власти и местного самоуправления несут ответственность в случае нарушения ими конфиденциальности информации, составляющей коммерческую тайну, а причиненные при этом ее обладателю убытки возмещаются из средств соответствующего бюджета;

предусматривается ответственность как за неправомерное отнесение сведений к коммерческой тайне, так и за разглашение, незаконное собирание, получение или использование информации, составляющей коммерческую тайну.

Наибольшее возражение вызывает кочующее из одного проекта данного закона в другой положение о том, что обладатель коммерческой тайны обязан по требованию любых органов государственной власти и органов местного самоуправления предоставлять им безвозмездно информацию, составляющую коммерческую тайну, в случаях, когда это необходимо для выполнения данными органами функций в рамках их компетенции, установленной федеральными законами. Учитывая тот факт, что в действующем законодательстве однозначно не определены функции и компетенция органов государственной власти, а тем более органов местного самоуправления, для реализации которых этим органам необходим доступ к коммерческой тайне конкретных организаций, данное положение

необоснованно расширяет круг лиц, имеющих законное право на неограниченный доступ к любой информации, составляющей коммерческую тайну любой организации. Фактически коммерческая тайна перестает быть действительно тайной в силу ее доступности широкому кругу третьих лиц и создаются условия, благоприятствующие возникновению коррупционных отношений в связи с информацией, составляющей коммерческую тайну, в системе органов государственной власти и местного самоуправления. При этом в том же законопроекте для судебных и следственных органов, которым в определенных случаях действительно необходим доступ к информации, составляющей коммерческую тайну конкретной организации, установлен более жестко ограниченный порядок доступа к такой информации. А именно только по запросу суда (судьи), прокурора, а при наличии согласия прокурора – органов предварительного следствия и дознания и только по делам, находящимся в их производстве. Возможно доступ органов государственной власти и, что более сомнительно, органов местного самоуправления к коммерческой тайне должен быть законодательно предусмотрен, но только на основании судебного решения по аналогии с предусмотренным Конституцией РФ ограничением права на тайну связи.

Законодательная регламентация работы с различными категориями конфиденциальной информации является одним из существенно значимых направлений в рамках общей проблемы законодательного регулирования прав на различные виды документированной информации.

Другое не менее значимое направление в рамках этой общей проблемы, связанное непосредственно с использованием инфокоммуникационных систем и сетей, - это законодательное регулирование электронного документооборота, т.е. процессов создания, хранения и обмена различными видами документов, представленных в электронном виде. Ключевым элементом электронного документооборота является электронная цифровая подпись (ЭЦП). Федеральный закон «Об электронной цифровой подписи» (2002) установил следующие принципы использования ЭЦП:

ЭЦП в электронном документе юридически равнозначна собственноручной подписи в документе на бумажном носителе;

для создания ключа подписи используются только сертифицированные средства электронной подписи;

выдача сертификата ключа подписи, включающего сам ключ, осуществляется удостоверяющими центрами, которыми могут быть как государственные, так и коммерческие организации;

деятельность удостоверяющего центра по выдаче сертификатов ключей подписи в информационных системах общего пользования должна быть лицензирована с учетом способности центра нести гражданскую ответственность;

в корпоративных информационных системах по соглашению участников системы функции удостоверяющего центра могут выполняться одним из участников;

ЭЦП, используемые в информационных сетях общего пользования, регистрируются удостоверяющими центрами и включаются единый государственный реестр, который ведет уполномоченный федеральный орган исполнительной власти, контролирующий правильность использования ЭЦП.

Закон предусматривает также защиту прав обладателей ЭЦП и условия приостановления действия и (или) аннулирования сертификата ключа подписи, определяет порядок использования ЭЦП в сфере государственного управления и в корпоративных информационных системах, а также условия признания иностранных сертификатов ключей подписи.

Однако наличие данного закона является необходимым, но недостаточным условием для полноценного законодательного регулирования электронного документооборота. Необходим не только закон об ЭЦП, но и специальный Федеральный закон «Об электронном документе», регламентирующий весь комплекс общественных отношений, возникающих в связи с использованием электронных документов.

Два проекта такого закона был внесен депутатами в Государственную Думу в конце 2000 и начале 2001 года, однако до настоящего времени они не рассмотрены даже в первом чтении. Эти во многом подобные законопроекты определяют общий юридический порядок использования в электронном документообороте электронного документа, подписанного ЭЦП и обладающего юридической силой, одинаковой с письменным документом, который может представляться в качестве судебных доказательств.

Законопроекты устанавливают общие требования к электронному документу и его структуре; определяют юридическую значимость такого документа, порядок хранения, обмена и подтверждения подлинности электронного документа, ведения электронных архивов; устанавливают ответственность участников электронного документооборота, включая информационного посредника, при использовании электронных документов.

К вопросам законодательного регулирования электронного документооборота тесно примыкают вопросы законодательного регулирования электронной торговли, в основе которой лежит ЭЦП и электронный документ. Проект Федерального закона «Об электронной торговле», внесенный группой депутатов и согласованный с Правительством, был принят Государственной Думой в первом чтении еще в середине 2001 года, но с тех пор его дальнейшее рассмотрение было приостановлено.

Данный законопроект определяет правовые условия совершения сделок и иных юридических действий в сфере электронной торговли, осуществляемой по телекоммуникационным сетям. Законопроект закрепляет права и обязанности лиц, осуществляющих электронную торговлю, включая информационного посредника, определяет правила совершения сделок с использованием электронных документов, подписанных электронной цифровой подписью или иным аналогом собственноручной подписи, устанавливает соответствие сделки с использованием электронных документов формальным требованиям к письменной форме сделки, предусмотренным действующим гражданским законодательством.

Незавершенность до настоящего времени формирования законодательства об электронном документообороте и об электронной торговле представляет собой заметное препятствие на пути расширения возможностей внедрения новых информационно-коммуникационных технологий, систем и сетей в сферу гражданских отношений и государственного управления.

С учетом качественно новых возможностей обработки всех видов информации, которые предоставляют современные информационно-коммуникационные технологии, предельно обостряется проблема защиты прав интеллектуальной собственности на информационную продукцию. Призванные обеспечивать такую защиту институты авторского и смежных прав, составляющие самостоятельную область законодательства, уже сегодня объективно нуждаются в определенной адаптации к условиям всепроницающей трансграничной информационной среды сетевого типа на основе обобщения и анализа правоприменительной практики как на национальном, так и на международном уровне. Такая адаптация необходима для обеспечения комфортных условий в смысле защиты авторских прав для массового использования инфокоммуникационных систем и сетей во всех сферах творческой и интеллектуальной деятельности.

Признание права вещной собственности на информацию обуславливает необходимость законодательного регулирования товарных отношений, объектом которых является информация, с использованием общих подходов и принципов законодательного противодействия экономическому монополизму на информационном рынке на основе его дерегуляции и гибкого контроля за концентрацией собственности. Следует отметить, что Гражданский кодекс РФ (1994) в статье 128 указывает на информацию как на самостоятельный объект гражданских прав в ряду таких объектов, как вещи и иное имущество, деньги и ценные бумаги, работы и услуги, результаты интеллектуальной деятельности. Однако Гражданский кодекс не внес окончательную ясность в решение юридической проблемы включения

информации во всем многообразии ее видов и форм в систему гражданско-правовых отношений.

Представляется, что в настоящее время гражданско-правовые и товарные отношения, объектом которых является информация, отрегулированы в недостаточной степени, что существенно сдерживает развитие российского рынка информации, основной «площадкой» которого в современных условиях и являются инфокоммуникационные системы и сети. Законодательная либерализация информационного рынка, обеспечивающая конкурентное развитие множества различных производителей информации и информационных услуг, вывод информации как товара из теневого оборота, неизбежно повлечет за собой интенсификацию внедрения и использования инфокоммуникационных систем и сетей, увеличение числа пользователей и трафика сетей связи.

При этом для всех категорий пользователей инфокоммуникационных систем и сетей существенно повышается значимость проблемы защиты информационных ресурсов и информационных потоков, циркулирующих в таких системах и сетях. Основные угрозы информационной безопасности пользователей в условиях сетевой инфокоммуникационной инфраструктуры представляют, прежде всего, различные компьютерные преступления (неправомерный доступ к компьютерным информационным ресурсам и базам данных, распространение компьютерных вирусов и другие), а также несанкционированный доступ к средствам и сооружениям связи как с целью незаконного получения информации, так и с целью незаконного использования каналов связи.

Защита от компьютерных преступлений включает как меры программно-технического характера, так и меры административного и уголовного преследования за совершение таких преступлений. На законодательном уровне проблема сегодня состоит в совершенствовании законодательных норм ответственности за компьютерные преступления,

приобретающие все более изощренный характер, на основе накопления и анализа опыта судебной практики их применения.

Обязанность по обеспечению защиты средств и сооружений связи от несанкционированного доступа к ним статьей 7 Федерального закона «О связи» (2003) возложена на операторов связи. Однако практическая реализация этого положения, скорее всего, потребует дополнительной разработки специальных законодательных норм или специальных нормативно-правовых актов, регулирующих правовые, имущественные и иные отношения, связанные с исполнением такой обязанности именно операторами связи.

В заключение следует отметить, что наличие эффективной законодательной защиты информации, дифференцированной по ее видам, представляет собой одно из ключевых условий, благоприятствующих расширению масштабов массового использования инфокоммуникационных систем и сетей различными категориями пользователей и увеличению объемов и интенсивности циркулирующих в них информационных потоков. А именно эти два фактора и определяют экономическую эффективность и инвестиционную привлекательность всех отраслей информационной индустрии, включая и телекоммуникационную.