УДК 347.121.1 (575.2) (04)

НЕКОТОРЫЕ ПРОБЛЕМЫ ОСУЩЕСТВЛЕНИЯ ПРАВА НА НЕПРИКОСНОВЕННОСТЬ ЧАСТНОЙ ЖИЗНИ

Н.О. Пак

Рассматриваются некоторые вопросы осуществления права на неприкосновенность частной жизни в сети Интернет, а также некоторые аспекты компьютерных преступлений, нарушающих право граждан на неприкосновенность частной жизни.

Ключевые слова: неприкосновенность; частная жизнь; компьютерные преступления.

Право на неприкосновенность частной жизни в зависимости от отраслевой принадлежности – это и конституционное право (согласно пункту 3 статьи 14 Конституции Кыргызской Республики от 5 мая 1993 года № 157 "каждый имеет право на неприкосновенность своей частной жизни, уважение и защиту чести и достоинства"), и нематериальное благо, регулируемое гражданским законодательством (пункт 1 статья 50 Гражданского кодекса Кыргызской Республики от 8 мая 1996 года № 15 (часть I)).

В цивилистике под осуществлением права понимается реализация возможностей, предоставляемых законом или договором обладателю субъективного права [1, 316]. Иными словами, под осуществлением права понимается поведение лица, соответствующее содержанию принадлежащего ему права, то есть реализацию права в конкретных действиях управомоченного лица. Субъективное гражданское право предоставляет лицу, которому это право принадлежит, возможность определенного поведения. А осуществление права является реализацией этих возможностей. Проявлением свободы поведения служит широкое усмотрение лица при выборе варианта своего поведения в пределах, предусмотренных гражданским правом [2, 30].

Право на неприкосновенность частной жизни – это сложное по структуре субъективное гражданское право, включающее в себя другие права (правомочия). Под правом на неприкосновенность частной жизни понимается возможность обособления частной жизни, самостоятельного решения всех вопросов личной жизни и запрет вмешательства третьих лиц, кроме случаев, предусмотренных законом или согласованных с гражданином [3, 184].

Конец XX – начало XXI века характеризуется повсеместной информатизацией современного общества, заменой сетью Интернет* иных средств передачи информации и внедрением новейших средств телекоммуникации и связи практически во все сферы человеческой деятельности. Развитие информационных технологий, новых электронных средств связи повлекли за собой не только позитивные, но и негативные изменения, могущие привести к нарушению права на неприкосновенность частной жизни человека.

Электронная почта (E-mail) является наиболее распространенной формой общения пользователей в сети Интернет. Однако во всемирной компьютерной сети нетрудно найти всевозможные советы по так называемому "взлому" почтовых ящиков, вплоть до указания необходимых программ, алгоритма действий и т.п.

* Интернет (англ. Internet, сокр. от Interconnected Networks – объединенные сети) – глобальная телекоммуникационная сеть информационных и вычислительных ресурсов.

В то же время, кроме почтовых ящиков, подвергаются большой угрозе и базы данных компаний. К примеру, в 1997 году в Российской Федерации (г. Санкт-Петербург) была пресечена деятельность преступной группы, которая занималась продажей компакт-дисков, содержащих похищенную у одной из компаний по оказанию услуг сотовой связи базу данных ее абонентов с полной информацией о каждом из них. Таким образом, одновременно с неправомерным доступом к информации компании были нарушены права каждого абонента данной компании на неприкосновенность их частной жизни (персональных данных).

Информация персонального характера (персональные данные) – это зафиксированная на материальном носителе информация о конкретном человеке, отождествленная с конкретным человеком или которая может быть отождествлена с конкретным человеком, позволяющая идентифицировать этого человека прямо или косвенно, посредством ссылки на один или несколько факторов, специфичных для его биологической, экономической, культурной, гражданской или социальной идентичности. К персональным данным относятся биографические и опознавательные данные, личные характеристики, сведения о семейном, финансовом положении, состоянии здоровья и прочее (статья 3 Закона Кыргызской Республики "Об информации персонального характера" от 14 апреля 2008 года №58).

Совершая гражданско-правовые сделки в сети Интернет, проходя процесс регистрации на различных сайтах, необходимо заполнить определенные поля, в том числе фамилию, имя, отчество, дату рождения и т.д. В этой связи возникает вопрос, каким образом хранится данная информация и кто, в случае разглашения указанных сведений, должен нести ответственность.

По поводу определения понятия компьютерного преступления выдвигаются различные точки зрения. Например, Ю.М. Батурин придерживается мнения, что компьютерных преступлений как особой группы преступлений не существует. Однако автор отмечает, что многие традиционные виды преступлений модифицировались по причине вовлечения в них компьютерной техники, и поэтому правильнее было бы говорить о компьютерных аспектах преступлений, не выделяя их в обособленную группу преступлений [4, 129]. Ученый В.Б. Вехов считает, что под компьютерными преступлениями следует понимать предусмотренные уголовным законодательством общественно опасные действия, совершенные с использованием средств электронно-вычислительной (компьютерной) техники [5, 24].

Мотивы компьютерных преступлений могут быть различными: деньги, любопытство, месть, вызов обществу, авантюризм и т.п.

К видам совершения правонарушений, посягающих на неприкосновенность частной жизни, могут быть отнесены непосредственный (активный) и электромагнитный (пассивный) перехват, аудио- и видеоперехват и т.д.

Непосредственный перехват осуществляется с помощью непосредственного подключения к телекоммуникационному оборудованию компьютера, компьютерной системы или сети. К видам непосредственного перехвата может быть отнесен перехват сообщений.

Однако не все перехватывающие устройства требуют непосредственного подключения к системе. Данные и информация могут быть перехвачены не только в канале связи, но и в помещениях, в которых находятся средства коммуникации, а также на значительном удалении от них. Впервые дистанционный перехват информации с дисплея компьютера открыто был продемонстрирован в марте 1985 года в Каннах на Международном конгрессе по вопросам безопасности ЭВМ. Сотрудник голландской телекоммуникационной компании Вим-Ван-Эк поразил специалистов тем, что с помощью разработанного им устройства из своего автомобиля, находящегося на улице, он смог "снять" данные с экрана дисплея компьютера, установленного на восьмом этаже здания, расположенного в ста метрах от автомобиля [6, 37].

Что касается видео- и аудиоперехвата, то данные способы представляются достаточно опасными и распространенными, так как в этом случае не обязательно проникать внутрь помещения – достаточно приблизиться к нему снаружи или же перехватывать информацию с определенного расстояния с использованием различных технических средств.

Кроме того, к способам нарушения права на неприкосновенность частной жизни (в частности, права на тайну переписки) могут быть отнесены специальные программы HACK-TOOLS (инструменты взлома). Эти программы работают по принципу перебора символов, которые возможно ввести через клавиатуру персонального компьютера [5, 66]. Как показали результаты экспериментов, проведенных специалистами, чаще всего в качестве паролей пользователи компьютеров используют имена,

фамилии и их производные (22,2%); даты рождения, знаки зодиака свои и близких (11,8 %); интересы (хобби, спорт, музыка) (9,5%) и проч. Однако в большинстве случаев с использованием специальных программ пароль возможно подобрать [7, 287–288].

К мерам предупреждения компьютерных преступлений в первую очередь могут быть отнесены нормы законодательства, устанавливающие ответственность за указанные выше противоправные деяния. Впервые преступлением было объявлено несанкционированное получение компьютерных данных в Швеции в 1973 году, в американских штатах Аризона и Флорида – в 1978 году, когда законом "Computer crime act of 1978" устанавливалась уголовная ответственность за компьютерные преступления [8, 36].

Компьютерные преступления очень сложно предотвратить и доказать, поскольку методы защиты значительно отстают от средств нападения. Более того, информация о последних, а также различные программы для их осуществления свободно распространяются в сети Интернет, что в значительной мере увеличивает число потенциальных преступников и позволяет им совершать преступления, не обладая специальными знаниями.

Одной из целей защиты информации и прав субъектов в области информационных процессов и информатизации в Кыргызской Республике является защита конституционных прав граждан на сохранение личной тайны и конфиденциальности персональных данных в информационных системах (статья 19 Закона Кыргызской Республики "Об информатизации" от 8 октября 1999 года №107).

Общепризнанно, что право на неприкосновенность частной жизни (наряду с правом на жизнь, правом на честь и достоинство и др.) является необходимым условием жизни человека в любом обществе и должно обязательно признаваться и защищаться государством. Однако право на неприкосновенность частной жизни в сети Интернет практически не защищено. В соответствии со Стратегией развития страны на 2009–2011 годы, утвержденной Указом Президента Кыргызской Республики от 31 марта 2009 года №183, меры будут направлены в первую очередь на защиту прав человека, в том числе права на неприкосновенность частной жизни и обеспечение верховенства закона в Кыргызской Республике.

Не случайно во многих странах общество и государственные структуры придают огромное значение проблеме свободы в области информации, форм ее получения и распространения. Представляется необходимым в данной сфере добиться определенного баланса открытости и ограничения получения и использования информации. Понятно, что данная сфера общественных отношений не может оставаться без законодательного регулирования. Однако для урегулирования ранее неизвестного объекта отношений необходим междисциплинарный подход, сочетание технических, экономических, финансовых и юридических знаний. Более того, необходимо учитывать один из ключевых моментов, которым является крайне стремительное развитие технологий [9, 633].

Европейским союзом 24 октября 1995 года была принята Директива 95/46/ЕС о защите прав частных лиц применительно к обработке персональных данных и о свободном движении таких данных, призывающая государства-члены привести свои национальные законы о неприкосновенности частной жизни в соответствие со стандартами этого документа. Позднее, 15 декабря 1997 года, была также принята Директива 97/66/ЕС Европейского союза, касающаяся использования персональных данных и защиты неприкосновенности частной жизни в сфере телекоммуникаций. В данной Директиве предусмотрена обязанность провайдеров общедоступных телекоммуникационных услуг принимать соответствующие технические и организационные меры к обеспечению безопасности своих услуг. Кроме того, данным документом также предусматривается обязанность стран-членов обеспечивать конфиденциальность коммуникаций, осуществляемых посредством общедоступной телекоммуникационной сети и общедоступных телекоммуникационных услуг. В частности, они должны налагать запрет на запись, прослушивание и иные виды перехвата или контроля над коммуникациями иными лицами, кроме пользователей, без согласия последних, за исключением случаев, когда это юридически разрешено.

Вопрос об ответственности интернет-провайдеров за нарушения в области неприкосновенности частной жизни является весьма дискуссионным. Законодательство в сфере информационной деятельности в Кыргызской Республике только начинает формироваться, является разрозненным, и поэтому постановка вопроса о его систематизации представляется преждевременной.

На данном этапе крайне важным представляется, в первую очередь, выработать единый понятийный аппарат, что существенным образом повлияет на процесс нормотворчества и правоприменительную практику. Кроме того, в качестве первого шага по усовершенствованию законодательства Кыргызской Республики в сфере информационных технологий можно предложить принятие закона "Об Интернете", предусматривающего круг субъектов правоотношений, принципы регулирования, вопросы международного сотрудничества и т.п.

Многие зарубежные страны имеют богатый опыт в этом направлении, поэтому представляется обоснованным адаптировать его к законодательству Кыргызской Республики, что позволит создать собственную эффективную систему обеспечения безопасности компьютерных систем и защитить право граждан на неприкосновенность их частной жизни.

Литература

1. Гражданскоеправо:Учеб.Т.1/Подред.А.П.Сергеева, Ю.К. Толстого. М.: Проспект, 2003.
2. Комментарий к Гражданскому кодексу Российской Федерации части первой (постатейный) / Под ред. О.Н. Садикова. М: ИНФРА-М, 2003.
3. *Малеина М.Н.* Личные неимущественные права граждан: понятие, осуществление, защита. М.: МЗ Пресс, 2000.
4. *Батурин Ю.М.* Проблемы компьютерного права. М.: Юрид. лит., 1991.
5. *Вехов В.Б.* Компьютерные преступления: Способы совершения и раскрытия. М.: Право и Закон, 1996.
6. Совещание по вопросам компьютерной преступности // Проблемы преступности в капиталистических странах. М.: ВИНИТИ, 1986.
7. *Лучин И.Н., Желдаков А.А., Кузнецов Н.А.* Взламывание парольной защиты методом интеллектуального перебора // Информатизация правоохранительных систем / Академия МВД России. 1996. № 2.
8. Законодательные меры по борьбе с компьютерной преступностью // Проблемы преступности в капиталистических странах. 1988. № 4.
9. Право Европейского союза: Учеб. для вузов / Под ред. С.Ю. Кашкина. М.: Юристъ, 2002.