УЧЕНЫЕ ЗАПИСКИ КАЗАНСКОГО УНИВЕРСИТЕТА
Том 156, кн. 4 Гуманитарные науки *2014*

УДК 343.34

УГОЛОВНО-ПРАВОВАЯ ХАРАКТЕРИСТИКА ПОСЯГАТЕЛЬСТВ НА ПЕРСОНАЛЬНЫЕ ДАННЫЕ, ОБРАБАТЫВАЕМЫЕ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ

Р.Р. Гайфутдинов

Аннотация

В статье рассматриваются актуальные вопросы уголовно-правовой характеристики деяний, посягающих на персональные данные физических лиц, на основе анализа действующего уголовного и административного законодательства и достижений современной теории права. Выявлены проблемные моменты квалификации преступлений против охраняемого порядка обработки и целостности персональных данных, обрабатываемых с помощью средств автоматизации. Произведено разграничение их со смежными составами преступлений и правонарушениями. Предлагаются свои решения по модернизации и толкованию рассматриваемых уголовно-правовых норм.

Ключевые слова: преступления в сфере компьютерной информации, уголовно-правовая охрана персональных данных, неприкосновенность частной жизни, персональные данные, компьютерная информация.

Как справедливо отмечает С.И. Никулин, развитие современного общества, основанного на использовании огромного количества информации, немыслимо без широкого внедрения в процессы его развития и функционирования компьютерных технологий. Такие технологии не только предназначены для хранения и обработки информации, но и являются одним из важнейших элементов в обеспечении внутренней и внешней безопасности государства, что обусловливается разработкой правовых норм, гарантирующих охрану и защиту информации, и использованием компьютерной техники [1, с. 638].

Сегодня зачастую высокие технологии становятся орудием в руках злоумышленников, посягающих на различные виды информации либо на другие социальные блага, вследствие чего возникает необходимость в надлежащей охране такой информации. По аналитическим данным, число утечек персональных данных в России в 2013 г. выросло в 2.2 раза, в результате чего скомпрометировано около 3.1 млн записей данных [2]. По данным статистики, представляемой различными аналитическими изданиями, ежегодно наблюдается тенденция роста противоправных деяний в области компьютерной информации, в частности в отношении персональных данных [3]. Однако статистика органов МВД РФ свидетельствует об обратном: с каждым годом уменьшается число случаев привлечения к ответственности за подобные посягательства [4]. Такие данные позволяют сделать вывод о высокой латентности преступлений в сфере компьютерной информации.

Должное правовое регулирование, касающееся обработки персональных данных, в России введено относительно недавно, хотя, как справедливо замечает Н.Е. Циулина [5, с. 48], впервые легальное определение персональных данных было установлено ещё в 1995 г. (24-ФЗ). 27 июня 2006 г. в целях обеспечения защиты прав и свобод человека и гражданина, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну, принят закон «О персональных данных» (152-ФЗ). При таких обстоятельствах представляется интересным выяснить, могут ли персональные данные быть предметом преступления и объектом уголовно-правовой охраны.

При определённых условиях неправомерные действия лиц, посягающих на персональные данные, квалифицируются по ст. 272 Уголовного кодекса (УК РФ). Диспозицией этой статьи предусматривается ответственность за неправомерный доступ к охраняемой законом компьютерной информации, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование компьютерной информации. *Непосредственным объектом* данного преступления являются отношения по поводу обеспечения целостности и сохранности компьютерной информации и безопасности функционирования электронных информационных систем.

Законом № 152-ФЗ регулируются отношения, связанные с обработкой особой категории информации (персональных данных), осуществляемой лицами с использованием средств автоматизации, в том числе в информационно-телекоммуникационных сетях. Средствами автоматизации могут признаваться любые средства вычислительной техники, в частности электронно-вычислительные машины и компьютеры. Сегодня затруднительно привести примеры автоматизированных средств, обрабатывающих информацию, в основе работы которых не лежат электронные схемы.

Однако ст. 1 закона № 152-ФЗ содержит оговорку, что регулированию подлежат также отношения без использования средств автоматизации, если обработка персональных данных без использования таких средств соответствует характеру действий (операций), совершаемых с персональными данными с использованием средств автоматизации, то есть позволяет осуществлять в соответствии с заданным алгоритмом поиск персональных данных, зафиксированных на материальном носителе и содержащихся в картотеках или иных систематизированных собраниях персональных данных, и (или) доступ к таким персональным данным.

Таким образом, вышеназванное положение позволяет сделать вывод, что не любые отношения попадают под охрану ст. 272 УК РФ, а только те, в которых непосредственно задействованы электронные средства обработки информации. В результате этого объектом уголовно-правовой охраны ст. 272 УК РФ персональные данные становятся в случае их обработки в автоматизированных вычислительных системах в виде электронной информации. Такое деяние, в сущности, является двухобъектным посягательством. При уголовно-правовой оценке действия лица будут образовывать разнообъектную идеальную совокупность преступлений, квалифицируемую соответственно по ст. 137 и 272 УК РФ. Субъект осуществляет посягательство, с одной стороны, на отношения по поводу обеспечения целостности и сохранности компьютерной информации, а с другой –

на конституционные права неприкосновенности частной жизни, личной и семейной тайны.

Предметом неправомерного доступа к компьютерной информации некоторые авторы называют компьютерную информацию [6, с. 6], с чем нельзя в полной мере согласиться. Согласно ст. 2 и 5 закона № 149-ФЗ под информацией понимаются сведения (сообщения, данные) о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления (149-ФЗ). В соответствии со ст. 3 закона № 152-ФЗ персональными данными признаётся любая информация, относящаяся к прямо или косвенно определённому или определяемому физическому лицу (субъекту персональных данных).

Определяя в качестве предмета посягательства компьютерную информацию, в её понимании многие исследователи расходятся во мнениях [7, с. 613]. Такая бурная дискуссия была обусловлена тем, что законодателем компьютерная информация не определялась с момента принятия нового Уголовного кодекса Российской Федерации. И только закон № 420-ФЗ внёс изменения, определив в примечании 1 к ст. 272 УК РФ под компьютерной информацией сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи (420-ФЗ). Таким образом, законодатель соотнёс понятийный аппарат закона № 149-ФЗ и УК РФ.

В свою очередь, невольно расширились рамки обыденного понимания термина «компьютерная информация», так как к «компьютеру» тяжело отнести современные мобильные телефоны, «планшеты» и другие электронные устройства, обрабатывающие электронную информацию. Даже домашние телефоны, имеющие записные книжки, сейчас содержат в себе электронную информацию, относящуюся к определённым субъектам, однако такие сведения не всегда могут становиться предметом уголовно-правовой охраны.

Предметом преступления согласно диспозиции ст. 272 УК РФ может быть только охраняемая законом информация. Для признания сведений, охраняемых законом, подчёркивается необходимость наличия следующих условий: 1) законодательного основания для защиты информации от несанкционированного доступа и 2) принятия мер по её охране законным обладателем информации [8, с. 302–303]. Персональные данные подлежат охране и защите в силу целого ряда норм различных законов (Конвенция, Конституция РФ, 149-ФЗ, 152-ФЗ).

Своим предметом и целью Конвенция устанавливает защиту персональных данных – право для каждого физического лица на неприкосновенность частной жизни в отношении автоматизированной обработки касающихся его персональных данных. Примечательным фактом является то, что Россия приняла Конвенцию законом № 160-ФЗ с некоторыми заявлениями ещё в 2005 г. Процедура её ратификации закончилась 15 мая 2013 г., а вступила она в полную силу только 1 сентября 2013 г. [9].

Часть 1 ст. 24 Конституции РФ определяет, что сбор, хранение и распространение информации о частной жизни лица без его согласия не допускается. Эти положения имеют, в сущности, фундаментальный, системообразующий характер и определяют смысл и содержание значительного числа нормативно-правовых актов разного уровня, принятых в России для охраны и защиты персональных данных физических лиц.

Относительно второго обязательного условия отметим следующее. Лицо-оператор, производящее на законных основаниях обработку персональных данных, в силу закона обязано принимать необходимые организационные и технические меры или обеспечивать их принятие для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий.

Таким образом, предметом преступления, посягающего на персональные данные, обрабатываемые в автоматизированных системах, является охраняемая законом электронная информация, содержащая персональные данные физических лиц.

Объективная сторона преступления, предусмотренного ст. 272 УК РФ, выражается в форме действия – в неправомерном доступе к компьютерной информации. Законом № 149-ФЗ устанавливаются основные принципы, применяющиеся к порядку ограничения доступа к информации. Порядок ограничения доступа к персональным данным определён законом № 152-ФЗ. Статьёй 2 закона № 149-ФЗ доступ к информации определяется как возможность получения информации и её использования.

В.С. Карпов указывает, что доступ будет являться неправомерным, если: «1) лицо не имеет права на доступ к данной информации; 2) лицо имеет право на доступ к данной информации, однако осуществляет его помимо установленного порядка, с нарушением правил её защиты» [10, с. 87].

В.П. Ревин под неправомерным доступом понимает «действия лица, имеющего допуск к операциям соответствующего ранга, если доступ осуществлён с нарушением правил работы с данным компьютером, системой, сетью, обеспечивающими устройствами, например с отключением систем безопасности, с игнорированием физических условий, создавшихся в месте работы (например, высокой температуры), которые заведомо угрожают сохранности информации» [11, с. 295].

Имеется мнение, что «под использованием служебного положения, предусмотренного в диспозиции ч. 3 ст. 272 УК РФ, понимается использование возможности доступа к компьютерной информации, возникшей в результате выполняемой работы (по трудовому, гражданско-правовому договору) или влияния по службе на лиц, имеющих такой доступ (в данном случае субъектом преступления не обязательно является должностное лицо), то есть тех, кто на законных основаниях использует компьютерную информацию и средства её обращения (программисты, сотрудники, вводящие информацию в память компьютера, другие пользователи, а также администраторы баз данных, инженеры, ремонтники, специалисты по эксплуатации электронно-вычислительной техники и прочие» [12].

И.А. Клепницкий считает, что неправомерным доступом к компьютерной информации является приобретение и использование лицом возможности получать информацию, вводить её либо влиять на процесс обработки информации [13, с. 353]. С.В. Бородин подчёркивает, что «под неправомерным доступом к охраняемой законом информации следует понимать самовольное получение информации без разрешения собственника или владельца. При этом неправомерный доступ к компьютерной информации характеризуется ещё и нарушением

установленного порядка обращения к этой информации. Если нарушен установленный порядок доступа к охраняемой законом информации, согласие её собственника или владельца не исключает правомерности доступа к ней» [14, с. 701].

В.В. Воробьёв считает, что неправомерный доступ к компьютерной информации – это «несанкционированное собственником или иным законным владельцем компьютерной информации проникновение к ней, в том числе с возможностью ознакомления, которое позволяет распоряжаться этой информацией (уничтожать, блокировать, модифицировать, копировать) и создает опасность как для самой информации, так и для интересов собственника» [6, с. 7].

Таким образом, при определении понятия неправомерного доступа выделяется: а) его расширительное толкование как нарушения порядка обращения с информацией и использования возможности лицом получения информации; б) толкование в узком смысле, при котором необходимым признаком неправомерности является проникновение в информационную систему и преодоление её средств защиты, обеспечивающих охрану информации.

Соглашаясь с расширительным толкованием неправомерного доступа к персональным данным, мы определённо сталкиваемся с конкуренцией диспозиций норм, изложенных в ст. 13.11, 13.14 Кодекса об административных правонарушениях (КоАП РФ) и ст. 272 УК РФ.

Состав, предусмотренный ст. 13.14 КоАП РФ, устанавливает ответственность за разглашение информации, доступ к которой ограничен федеральным законом (за исключением случаев, когда разглашение такой информации влечёт уголовную ответственность), лицом, получившим доступ к такой информации в связи с исполнением служебных или профессиональных обязанностей, за исключением случаев, указанных в ч. 1 ст. 14.33 КоАП РФ. Статьёй 13.11 КоАП РФ предусматривается ответственность за нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных). Если в первом случае при квалификации действий лица мы можем преодолеть межотраслевую коллизию согласно диспозиции статьи, устанавливающей возможность привлечения к ответственности по УК РФ при охране таких отношений, то во втором случае преодоление такой конкуренции весьма затруднительно.

Под нарушением установленного законом порядка распространения информации могут пониматься действия лица по передаче персональных данных третьим лицам без согласия субъекта, которые образуют состав правонарушения, предусмотренный ст. 13.11 КоАП РФ. При широком толковании неправомерного доступа к компьютерной информации те же действия подпадают под признаки состава преступления.

Именно по объективной стороне деяния – правомерности доступа к персональным данным в узком смысле – представляется возможным разграничивать административные правонарушения в сфере надлежащего порядка обработки персональных данных и уголовные преступления, посягающие на персональные данные. В зависимости от того, был ли правомерным доступ у лица к такой информации, деяние подлежит квалификации по совокупности преступлений, предусмотренных ст. 137, 272 УК РФ либо ст. 137 УК РФ с привлечением к административной ответственности по ст. 13.11 КоАП РФ. Таким образом, сре-

ди преступлений в сфере компьютерной информации особняком стоят деяния, посягающие на персональные данные, обрабатываемые с применением автоматизированных средств, ввиду особого порядка их охраны.

В заключение отметим, что во избежание ошибок при квалификации при различном понимании правомерности доступа к компьютерной информации является целесообразным её толкование Пленумом Верховного Суда РФ. По причине наличия особых требований к охране персональных данных и в целях должной уголовно-правовой охраны общественных отношений, возникающих в связи с обработкой персональных данных, возможно введение квалифицированного состава преступления в главу 28 УК РФ. Диспозиция такого состава преступления может пониматься как неправомерный доступ к персональным данным, обрабатываемым в автоматизированных системах, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование персональных данных.

Summary

R.R. Gajfutdinov. Criminal Characteristics of Infringement on Personal Data Undergoing Automated Processing.

In this article, we consider topical issues related to the criminal characteristics of infringement on personal data of individuals, based on the analysis of criminal and administrative laws in effect and achievements in the modern theory of law. We reveal problem areas in the qualification of crimes against the protected processing procedures and integrity of personal data treated by automated facilities. We also make a distinction between these crimes and the related crimes and offenses. In addition, we propose our own solutions for modernization and interpretation of the criminal rules under study.

Keywords: crimes in the sphere of computer information, legal protection of personal data, privacy, personal data, computer information.

Источники

24-ФЗ – Федеральный закон от 20 февр. 1995 г. № 24-ФЗ «Об информации, информатизации и защите информации» (утратил силу) // Собрание законодательства Российской Федерации (СЗ РФ). – 1995. – № 8. – Ст. 609.

152-ФЗ – Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных». – URL: http://www.consultant.ru/popular/o-personalnyh-dannyh/, свободный.

УК РФ – Уголовный кодекс Российской Федерации от 13 июня 1996 г. № 63-ФЗ. – URL: http://www.consultant.ru/popular/ukrf/, свободный.

149-ФЗ – Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации». – URL: http://base.consultant.ru/cons/cgi/online.cgi?req=doc;base=LAW;n=165971, свободный.

420-ФЗ – Федеральный закон от 7 дек. 2011 г. № 420-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации». – URL: http://base.consultant.ru/cons/cgi/online.cgi?req=doc;base=LAW;n=156591, свободный.

Конвенция – Конвенция о защите физических лиц при автоматизированной обработке персональных данных. – URL: http://base.consultant.ru/cons/cgi/online.cgi?req=doc;base=LAW;n=121499, свободный.

Конституция РФ – Конституция Российской Федерации (принята всенародным голосованием 12 дек. 1993 г.). – URL: http://www.consultant.ru/popular/cons/, свободный.

160-ФЗ – Федеральный закон от 19 дек. 2005 г. № 160-ФЗ «О ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных» // СЗ РФ. – 2005. – № 52. – Ст. 5573.

КоАП РФ – Кодекс Российской Федерации об административных правонарушениях от 30 дек. 2001 г. № 195-ФЗ. – URL: http://www.consultant.ru/popular/koap/, свободный.

Литература

1. Уголовное право. Общая и Особенная части. – М.: Норма, 2014. – 784 с.
2. Число утечек персональных данных в РФ в 2013 г. выросло в 2.2 раза // Интерфакс. – URL: http://www.interfax.ru/russia/361357, свободный.
3. Рынок преступлений в области высоких технологий: состояние и тенденции 2013 года // Group-IB. – URL: http://www.group-ib.ru/index.php/o-kompanii/1008-analytics?view=article&id=1155, свободный.
4. Состояние преступности // Пресс-центр МВД. – 2014. – URL: http://mvd.ru/presscenter/statistics/reports, свободный.
5. *Циулина Н.Е.* Формирование и развитие правовой категории «персональные данные» // Вестн. УрФО. Безопасность в информационной сфере. – 2013. – № 1(7). – С. 47–52.
6. *Воробьёв В.В.* Преступления в сфере компьютерной информации: Юридическая характеристика составов и квалификация: Автореф. дис. … канд. юрид. наук. – Н. Новгород, 2000. – 28 с.
7. Уголовное право России. Особенная часть. – М.: Статут, 2012. – 943 с.
8. Российское уголовное право. Особенная часть. – М.: Инфра-М: Контракт, 2012. – 448 с.
9. О ратификации Россией Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных. – URL: http://www.coe.mid.ru/doc/avt_obr_PD.htm, свободный.
10. *Карпов В.С.* Уголовная ответственность за преступления в сфере компьютерной информации: Дис. … канд. юрид. наук. – Красноярск, 2002. – 202 с.
11. *Ревин В.П.* Преступления в сфере компьютерной информации // Уголовное право России. Особенная часть. – М.: Юстицинформ, 2009. – С. 289–301.
12. Методические рекомендации по осуществлению прокурорского надзора за исполнением законов при расследовании преступлений в сфере компьютерной информации // Генеральная прокуратура Российской Федерации. – URL: http://genproc.gov.ru/documents/nauka/document-104550/, свободный.
13. *Клепницкий И.А.* Преступления в сфере компьютерной информации // Уголовное право Российской Федерации. Особенная часть. – М.: Юристъ, 1996. – С. 347–358.
14. *Бородин С.В.* Преступления в сфере компьютерной информации // Комментарий к УК РФ. – М.: Юристъ, 2000. – С. 699–706.

Поступила в редакцию
10.04.14

Гайфутдинов Рамиль Рустамович – ассистент кафедры уголовного права, Казанский (Приволжский) федеральный университет, г. Казань, Россия.
E-mail: *gayfutdinov.r@yandex.ru*