20. Сугако, Л.А. Ход и итоги эвакуации населения БССР летом 1941 года: проблемные аспекты / Л. Сугако / Изв. Гомел. гос. ун-та имени Ф. Скорины. 2011. № 5 (68).

21. Сугака, Л.А. Эвакуацыя з БССР у гады Вялікай Айчыннай вайны: некаторыя асаблівасці сучаснай гістарыяграфіі праблемы / Л. Сугака // Великая Победа: героизм и подвиг народов : материалы Междунар. науч. конф. (Минск, 28–29 апр. 2005 г.) : в 2 т. Т. 1 / отв. ред. А.М. Литвин. Минск : Ин-т истории НАН Беларуси, 2006.

22. Эшелоны идут на Восток. Из истории перебазирования производительных сил СССР в 1941–1942 гг. : сб. ст. и воспоминаний / редкол.: Ю.А. Поляков (отв. ред.) [и др.]. М. : Наука, 1966.

Дата поступления в редакцию: 29.03.2012

УДК 004:34

***А.Н. Лепёхин**, кандидат юридических наук, доцент, начальник кафедры правовой информатики Академии МВД Республики Беларусь;*
***О.В. Кипченко**, старший инспектор по особым поручениям Департамента охраны МВД Республики Беларусь*

НЕКОТОРЫЕ ПРАВОВЫЕ АСПЕКТЫ ОБОРОТА ИНФОРМАЦИИ В СОЦИАЛЬНЫХ СЕТЯХ

Рассматриваются некоторые правовые аспекты обращения информации в виртуальном пространстве, а также в социальных сетях как наиболее используемых площадках для сетевого общения. Ставится ряд вопросов, требующих научной проработки: какая информация подлежит правовой защите, а также кто и с помощью каких мер должен защищать информацию в социальных сетях. С учетом анализа белорусского законодательства предпринимаются попытки разрешить эти вопросы и делается вывод о необходимости разработки нормативного правового акта, регламентирующего вопросы оборота персональных данных.

The article discusses some of the legal aspects of information on the virtual space, as well as in social networks, as the most used platforms for network communication. Raises a number of issues requiring scientific study - information to be legal protection, as well as who and with what measures should protect information in social networks. An analysis of the belarusian legislation attempts to resolve these issues and draw conclusions about the need for a legal act or regulations covering trafficking of personal data.

В современном мире развитие компьютерных технологий объективно приобретает все большую значимость. Качественные перестройки современного мира существенно расширили круг возможностей для общества в коммуникационной сфере, однако и породили вместе с собой проблемы, решение которых часто находится на начальных стадиях разработки. К одной из таких проблем относится и вопрос обеспечения информационной безопасности, особенно в социальных сетях, ведь круг лиц и пространство для преступлений, совершаемых в сфере высоких технологий, может быть почти бесконечным.

В силу этого важное значение имеет не только необходимость создания специализированного национального информационного права для безопасности и эффективности информационных технологий, отвечающего современной сфере прогрессирующих общественных отношений, но и баланса между ним и нормами международного информационного права.

С этой целью 9 ноября 2010 г. указом Президента Республики Беларусь № 575 была утверждена Концепция национальной безопасности Республики Беларусь [2], в которой как самостоятельное направление был выделен именно этот вид безопасности. Согласно этому документу под информационной безопасностью понимается состояние защищенности сбалансированных интересов личности, общества и государства от внешних и внутренних угроз в информационной сфере.

Рассматривая феномен социальных сетей в контексте обеспечения информационной безопасности, следует отметить, что на данный момент такие коммуникационные сети, по сути, являются огромной базой данных с самой разнообразной информацией о сотнях миллионов людей по всему миру, которая к тому же неплохо структурирована. В последнее время такие сети все больше открываются внешнему миру, а многие личные данные пользователей уже доступны для всех желающих. Чем больше человек общается в разнообразных социальных сетях, тем больше информации о нем можно собрать. Именно поэтому спорное утверждение о том, что «70 % информации спецслужбы собирают из открытых источников», в настоящее время приобретает вполне истинный характер.

Современные социальные сети предлагают пользователям представить свои фото, видео, указать связи (в том числе и по типам); интересы; образование; информацию о работе; места, в

которых бывает человек; предпочитаемые продукты; личные мысли и т. д. Большинство информации доступно без регистрации, достаточно найти страницу пользователя в популярных социальных сетях, остальное можно увидеть после добавления пользователя в друзья (или без таких действий), а вся информация, включая личную переписку (как минимум), доступна администрации этой сети и никакие настройки приватности ее не скроют.

Важно понимать одну особенность: в интернете, как и в реальном мире, люди объединяются в определенные социальные группы (социальные маски), которые между собой не сильно пересекаются. Основное глобальное деление происходит по проектам, внутри которых целевая аудитория разбивается на неформальные группы по интересам, возрасту и другим признакам. Причем таких социальных масок может быть несколько: днем человеку нужно деловое общение, вечером общение с друзьями и семьей, по выходным общение, например, связанное с хобби, и т. д. У каждого набор масок будет свой, однако у каждой из них будут свои особенности, которые будут влиять на все поведение. Именно поэтому современный человек часто зарегистрирован в нескольких социальных сетях, в которых он удовлетворяет разные потребности и дает о себе разную информацию, а в последнее время многие заводят даже по несколько аккаунтов (учетных записей) в каждой социальной сети, чтобы иметь возможность «надевать» разные социальные маски. Кроме того, человек постепенно меняется: он стареет, у него меняются интересы, жизненные приоритеты и т. д. А это означает, что вчерашние школьники, которые общались «ВКонтакте», завтра могут уже общаться в LinkedIn совсем с другими жизненными приоритетами и захотят показывать совсем другую информацию о себе. Именно поэтому является важным самостоятельная фильтрация информации о себе в социальных сетях.

Следует отметить, что за последние три-четыре года тема информационной безопасности и приватности в социальных сетях привлекает достаточно много внимания. Это вполне объяснимо: сети все больше открываются внешнему миру, уже имелись случаи утечки личных данных, аккаунты пользователей достаточно легко взламываются, а у администрации сетей есть доступ к любой информации. Но все это только внешняя часть, которая лежит на поверхности и о которой пишет пресса, однако далеко не полная картина потенциальных угроз для личных данных.

Самым безобидным, на первый взгляд, вариантом использования личных данных без разрешения пользователя можно считать внутренние механизмы социальных сетей для показа таргетированной рекламы, подбора потенциальных знакомых или отбора потенциально интересного контента. Эти механизмы стали стандартом почти во всех социальных сетях, и никто не скрывает данный факт: все они собирают и анализируют личные данные, которых в любой сети очень много, а потом используют их в коммерческих целях. Более того, ряд социальных сетей передают личные данные во внешний мир и уже официально признали этот факт. Достаточно серьезные проблемы пользователям создает утечка личных данных по вине сети, что неоднократно случалось в разных коммуникационных проектах. Примером одной из самых больших по размерам можно считать утечку личных данных 77 млн пользователей игровой сети PlayStation Network в апреле 2011 г. Анализируя характер инцидента, следует отметить, что до конца не ясны последствия этого происшествия, поскольку, возможно, также имела место и утечка платежных данных пользователей, что может повлечь причинение им материального ущерба.

Еще более серьезные проблемы может вызвать взлом отдельных аккаунтов (учетных записей) и получение доступа ко всей личной информации отдельного пользователя, если цель злоумышленников – определенный человек. В настоящее время сделать это достаточно просто даже обычному пользователю, который знает человека и может использовать методы социальной инженерии, а также воспользоваться специальными услугами по взлому. Мотивация злоумышленников может быть самая разная, от взлома аккаунтов должностных лиц определенной компании в целях промышленного шпионажа до личных целей. Так, например, брачные юристы США уже сейчас фиксируют каждый пятый развод из-за социальных сетей: супруги получают доступ к профилю партнера, находят там переписку с любовником (любовницей) и в результате это приводит к разводу.

Помимо указанных выше угроз оборота личной информации в социальных сетях следует также указать на использование вирусных и вредоносных программ, распространяемых через социальные сети, и фишинговых сайтов, которые используются для неправомерного завладе-

ния логинами и паролями пользователя и последующего использования их для различных незаконных действий (например, автоматическая рассылка спама от лица пользователя, совершение клеветнических действий, хищение денежных средств и др.).

Вместе с тем наиболее серьезная угроза социальных сетей заключается в том, что доступ ко всей личной информации есть у довольно большой группы людей и они могут в любой момент ее просматривать, даже если человек удалил что-то из сети. Во-первых, это сотрудники самой социальной сети: у них есть доступ к базам данных, в которых содержится вся информация, а также специальные инструменты входа в аккаунты пользователей, как, например, специальный мастер-пароль в Facebook, который позволяет войти в любой аккаунт. Во-вторых, доступ к информации по запросу также имеют правоохранительные органы (вопрос заключается только в физическом расположении серверов социальной сети). Не так давно Дж. Ассандж, основатель Wikileaks, заявил, что Facebook имеет специальный интерфейс, который использует разведка США, а в России популярная сеть «ВКонтакте» уже успела публично признать факты сотрудничества с правоохранительными органами и передачи личных данных. Можно достаточно критично относится к таким заявлениям, вместе с тем следует понимать, что это вполне логично, поскольку сотрудники социальных сетей не могут не иметь доступ к личным данным, в этом заключается их работа, а сотрудники правоохранительных органов проводят специальные мероприятия в сетях, направленные на получение необходимой информации. Такое положение дел не избавляет пользователя от опасности передачи личных данных третьим лицам, причем часто такими данными могут быть целые психологические портреты или конфиденциальная информация.

Следует отметить, что в последнее время пользователи все меньше доверяют социальным сетям и все чаще начинают фильтровать информацию, которую готовы доверить сети, давать ложную информацию или вообще удаляются из сети, однако даже удаление не дает уверенности: часто информация сохраняется на серверах компании и может использоваться в дальнейшем, в частности, так делают Facebook, «ВКонтакте» и другие сети.

Подводя итог, следует выделить несколько вопросов, требующих научной проработки: 1) что является объектом правовой защиты в социальных сетях, 2) кто и какие меры по защите такой информации должен принимать? Отвечая на первый вопрос, необходимо отметить, что основной информацией, содержащейся на страничках в социальных сетях различного уровня и масштаба, являются персональные данные.

В настоящее время в большинстве стран мира под персональными данными принято понимать любую информацию, относящуюся к определяемому с ее помощью человеку (физическому лицу). К таким сведениям относятся фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, номера паспорта и карточки социального страхования и т. д. Кроме того, к персональным данным относятся сведения о семейном, социальном, имущественном положении, образовании, профессии, доходах. Персональные данные относятся к сведениям конфиденциального характера, и потому должны защищаться от иных лиц.

Рассматривая проблему защиты персональных данных, следует сказать, что она в некоторой степени урегулирована в белорусском законодательстве законом «Об информации, информатизации и защите информации» [1]. Этим законом предусмотрено, что к информации, распространение и (или) предоставление которой ограничено, отнесена информация о частной жизни физического лица и персональные данные. Кроме того, отдельно установлено, что никто не вправе требовать от физического лица предоставления информации о его частной жизни и персональных данных, включая сведения, составляющие личную и семейную тайну, тайну телефонных переговоров, почтовых и иных сообщений, касающихся состояния его здоровья, либо получать такую информацию иным образом помимо воли данного физического лица, кроме случаев, установленных законодательными актами Республики Беларусь. Сбор, обработка, хранение информации о частной жизни физического лица и персональных данных, а также пользование ими осуществляются с согласия данного физического лица, если иное не установлено законодательными актами Республики Беларусь.

Рассматривая механизм защиты такой информации, следует сказать, что в ст. 32 рассматриваемого закона указывается необходимость защиты персональных данных, согласно которой меры по защите персональных данных от разглашения должны быть приняты с момента, когда персональные данные были предоставлены физическим лицом, к которому они относят-

ся, другому лицу либо когда предоставление персональных данных осуществляется в соответствии с законодательными актами Республики Беларусь.

Очевидно, возникает вопрос: о каких мерах идет речь? Законом определены правовые, организационные и технические меры по защите информации. К правовым мерам отнесены заключаемые обладателем информации с пользователем информации договоры, в которых устанавливаются условия пользования информацией, а также ответственность сторон по договору за нарушение указанных условий; к организационным мерам – обеспечение особого режима допуска на территории (в помещения), где может быть осуществлен доступ к информации (материальным носителям информации), а также разграничение доступа к информации по кругу лиц и характеру информации; к техническим – использование средств защиты информации, в том числе криптографических, а также систем контроля доступа и регистрации фактов доступа к информации.

Следует отметить, что в законодательстве Республики Беларусь нет отдельного нормативного правового акта, которым регламентировались бы вопросы защиты персональных данных. Вместе с тем в нормативных правовых актах Республики Беларусь регламентировано право на тайну личной жизни граждан и в некоторой степени определен порядок защиты такой информации.

Так, в соответствии с нормами ст. 28 Конституции Республики Беларусь каждый имеет право на защиту от незаконного вмешательства в его личную жизнь, в том числе от посягательства на тайну его корреспонденции, телефонных и иных сообщений, на его честь и достоинство.

Кроме того, отдельными нормативными правовыми актами регламентируется порядок доступа к информации о личной жизни граждан, порядок защиты информации, лицензирования деятельности по технической защите информации. Указанные вопросы в определенной степени урегулированы:

Инструкцией о порядке доступа к архивным документам, содержащим сведения, относящиеся к личной тайне граждан, и о признании утратившим силу приказа Комитета по архивам и делопроизводству Республики Беларусь от 3 июля 1996 г. № 21, утвержденной постановлением Министерства юстиции Республики Беларусь от 24 мая 2012 г. № 132;

Кодексом Республики Беларусь об административных правонарушениях, в котором содержатся несколько статей, направленных на защиту информации, в том числе персонального характера. Так, ст. 22.6 кодекса предусмотрена ответственность за несанкционированный доступ к информации, хранящейся в компьютерной системе, сети или на машинных носителях, сопровождающийся нарушением системы защиты. Статьей 22.7 Кодекса Республики Беларусь об административных правонарушениях предусмотрена ответственность за использование не прошедших подтверждение соответствия требованиям технических нормативных правовых актов в области технического нормирования и стандартизации информационных систем, баз и банков данных, а также средств защиты информации, если они в соответствии с законодательством подлежат обязательному подтверждению соответствия (за исключением средств защиты информации, составляющей государственную тайну). Статьей 22.13 Кодекса Республики Беларусь об административных правонарушениях предусмотрена ответственность за умышленное разглашение коммерческой или иной охраняемой законом тайны без согласия ее владельца лицом, которому такая коммерческая или иная тайна известна в связи с его профессиональной или служебной деятельностью, если это деяние не влечет уголовной ответственности;

Уголовным кодексом Республики Беларусь предусмотрены меры уголовной ответственности за незаконные собирание либо распространение сведений о частной жизни, составляющих личную или семейную тайну другого лица, без его согласия (ст. 179). Также за несанкционированный доступ к информации, хранящейся в компьютерной системе, сети или на машинных носителях, сопровождающийся нарушением системы защиты (несанкционированный доступ к компьютерной информации), повлекший по неосторожности изменение, уничтожение, блокирование информации или вывод из строя компьютерного оборудования либо причинение иного существенного вреда, предусмотрена ответственность в соответствии со ст. 349. За изменение информации, хранящейся в компьютерной системе, сети или на машинных носителях, либо внесение заведомо ложной информации, причинившие существенный вред, при отсутствии признаков преступления против собственности (модификация компьютерной информации) ответственность предусмотрена ст. 350. Кроме того, предусмотрена ответственность за умышленные уничтожение, блокирование, приведение в непригодное состояние компьютерной информации или программы, либо вывод из строя компьютерного оборудования, либо разрушение компьютерной системы, сети или машинного носителя (компьютерный саботаж) (ст. 351),

а также несанкционированное копирование либо иное неправомерное завладение информацией, хранящейся в компьютерной системе, сети или на машинных носителях, либо перехват информации, передаваемой с использованием средств компьютерной связи (ст. 352).

Таким образом, несмотря на некоторую фрагментарную урегулированность вопросов защиты информации в виртуальном пространстве, включая социальные сети, остаются актуальными проблемы разработки единого нормативного правого акта, регулирующего вопросы защиты персональных данных (личной информации) в информационных системах, так как нет единого подхода к пониманию этой категории (нормативном ее закреплении) и перечне мер, необходимых для ее защиты. Поскольку необходимость защиты персональных данных обусловлена высокой вероятностью негативных последствий, сопровождающих каждую утечку информации, в том числе и утечку персональных данных, которая в конечном итоге оборачивается моральными и материальными потерями для допустивших ее, что подтверждается многолетними аналитическим данными в сфере защиты информации.

Библиографические ссылки

1. Об информации, информатизации и защите информации : закон Респ. Беларусь, 10 нояб. 2008 г., № 455-З // КонсультантПлюс : Беларусь. Технология 3000 [Электронный ресурс] / ООО «ЮрСпектр». Минск, 2012.

2. Об утверждении Концепции национальной безопасности Республики Беларусь : указ Президента Респ. Беларусь, 9 нояб. 2010 г., № 575 : в ред. указа Президента Респ. Беларусь от 30.12.2011 // КонсультантПлюс : Беларусь. Технология 3000 [Электронный ресурс] / ООО «ЮрСпектр». Минск, 2012.

Дата поступления в редакцию: 25.09.2012

УДК 159.9:34

А.Н. Пастушеня, *доктор психологических наук, профессор, заведующий кафедрой психологии и педагогики Академии МВД Республики Беларусь*

ТЕОРЕТИКО-МЕТОДОЛОГИЧЕСКИЕ ОСНОВАНИЯ ИЗУЧЕНИЯ ПСИХОЛОГИЧЕСКОГО ГЕНЕЗИСА ПРЕСТУПЛЕНИЯ

Рассматривается один из основных аспектов психологического изучения преступного поведения – генетический, призванный раскрыть развивающийся во времени процесс его порождения. Указывается практическое значение такого изучения преступного деяния для уголовной юстиции. В качестве результирующего этапа психической деятельности субъекта, подготавливающей его преступное поведение во внутреннем плане, определяется оперативная готовность к совершению деяния. Отмечаются психологические феномены, присущие формированию такой готовности. Приводятся основные типы генезиса преступного поведения.

The article throws light on one of the main aspects of psychological research of criminal behavior - genetic, directed to disclose developing in time the process of its outcome. The practical importance of such research of criminal act for criminal justice is pointed out. As a resulting stage of psychological activity of a subject, preparing its criminal behavior in his inner plan, operative readiness to commit an act is defined. Psychological phenomena inherent in forming such readiness are pointed out.

Преступное деяние, как и любой поведенческий акт человека, детерминируется его внутренней психической деятельностью, которая интегрирует многообразие отражательно-регулятивных процессов. В числе этих процессов восприятие обстоятельств ситуации, осмысление и оценка их значения, переживание чувств, формирование побуждений (мотивообразование), обдумывание необходимых собственных действий (целеполагание), принятие решения действовать определенным преступным способом и по определенному плану, регуляция исполнения решения и т. п. Результатом психической деятельности является подготовка поведения во внутреннем плане – формирование состояния готовности к совершению деяния и, далее, исполнительная регуляция целенаправленных действий. Формирование готовности к конкретному преступному деянию представляет собой процесс, развивающийся во времени. Этот процесс может быть краткосрочным – проявляться как реакция на определенные обстоятельства, в том числе на действия другого человека, но может быть и весьма продолжительным. При относительно продолжительном формировании криминальной готовности у субъекта в каждый отдельный период времени могут доминировать отдельные процессы психической деятельности: в одно время он может сосредоточивать внимание на наблюдении за ситуацией или на восприятии информации другого человека и осмыслении ее